ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΥΠΟΛΟΓΙΣΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών στην
Επιστήμη & Τεχνολογία της Πληροφορικής και των Υπολογιστών
Ειδίκευση Δικτύων Επικοινωνιών και Κατανεμημένων Συστημάτων

Μεταπτυχιακή Διπλωματική Εργασία

Η χρήση των ασύρματων δικτύων αισθητήρων (WSNs) για την προστασία κρίσιμων υποδομών τηλεπικοινωνιών από κακόβουλες ενέργειες και φυσικές καταστροφές

Καπάτος Γρηγόριος
MCSE 19037
Παραμυθέλλης Βασίλειος
MCSE 19050

Εισηγητές: Δρ. Μπόγρης Αντώνιος, Καθηγητής
Δρ. Χοχλιούρος Ιωάννης, Καθηγητής

ΑΘΗΝΑ, 2021

UNIVERSITY OF WEST ATTICA
SCHOOL OF ENGINEERS
DEPARTMENT OF COMPUTER ENGINEERING

Master of Science in
Science and Technology of Informatics and Computers
Option: Communication Networks & Distributed Systems

Master Thesis

Integrating Wireless Sensors Networks (WSNs) to protect critical telecommunications infrastructures from malicious actions and natural disasters

Kapatos Grigoris
MCSE 19037
Paramythellis Vasileios
MCSE 19050

Supervisors: Dr. Bogris Antonios, Professor
Dr. Chochliouros Ioannis, Professor

ATHENS, 2021

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Η χρήση των ασύρματων δικτύων αισθητήρων (WSNs) για την προστασία κρίσιμων υποδομών τηλεπικοινωνιών από κακόβουλες ενέργειες και φυσικές καταστροφές

Γρηγόρης Καπάτος
A.M.: MCSE19037

Βασίλειος Παραμυθέλλης
A.M.: MCSE19050

Εισηγητές:

Δρ. Ιωάννης Χοχλιούρος, Καθηγητής
Δρ. Αντώνιος Μπόγρης, Καθηγητής

Εξεταστική Επιτροπή:

Δρ. Αντώνιος Μπόγρης, Καθηγητής
Δρ. Νικόλαος Μυριδάκης, Καθηγητής
Δρ. Ιωάννης Χοχλιούρος, Καθηγητής

Antonios Bogris Digitally signed by Antonios Bogris Date: 2021.12.14 17:52:02 +02'00'

Nikolaos Myridakis Digitally signed by Nikolaos Myridakis Date: 2021.12.14 20:45:44 +02'00'

Ημερομηνία εξέτασης: Παρασκευή 10/12/2021

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΩΝ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Οι κάτωθι υπογεγραμμένοι 1) ΓΡΗΓΟΡΙΟΣ ΚΑΠΑΤΟΣ του ΣΙΜΟΥ, με αριθμό μητρώου MCSE19037 και 2) ΒΑΣΙΛΕΙΟΣ ΠΑΡΑΜΥΘΕΛΛΗΣ του ΠΑΝΑΓΙΩΤΗ, με αριθμό μητρώου MCSE19050 φοιτητές του Προγράμματος Μεταπτυχιακών Σπουδών ΕΠΙΣΤΗΜΗ & ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ του Τμήματος ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΥΠΟΛΟΓΙΣΤΩΝ της Σχολής ΜΗΧΑΝΙΚΩΝ του Πανεπιστημίου Δυτικής Αττικής, δηλώνουμε ότι:
«Είμαστε συγγραφείς αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχαμε για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες κάναμε χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνουμε ότι αυτή η εργασία έχει συγγραφεί από εμάς αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μας, όσο και του Ιδρύματος.
Παράβαση της ανωτέρω ακαδημαϊκής μας ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μας».
Επιθυμούμε την απαγόρευση πρόσβασης στο πλήρες κείμενο της εργασίας μας μέχρι την απόκτηση του πτυχίου μας και έπειτα από αίτηση μας στη Βιβλιοθήκη και έγκριση των επιβλεπόντων καθηγητών.

The undersigned 1) GRIGORIS SIMOY KAPATOS with registry number MCSE19037 and 2) VASSILIOS PANAGIOTI PARAMYTHELLIS with register number MCSE19050 students of post graduate program SCIENCE & TECHNOLOGY OF COMPUTING AND COMPUTERS of COMPUTER ENGINEERING dpt. Of ENGINEERING Faculty of University West Attica, we declare that:
"We are the authors of this master's thesis and that all the help we had for its preparation is fully recognized and refers to the work. Also, any sources from which we used data, ideas or words, whether exact or paraphrased, are listed in their entirety, with full reference to the authors, the publisher or the magazine, including the sources that may have been used by the internet. We also certify that this work has been written exclusively by us and is a product of intellectual property of both us and the foundation.
Violation of our academic responsibility is an essential reason for the revocation of our degree".
We wish the denial of access to the full text of our work until our degree is obtained and upon our request to the library and approval of the supervising professors.

Ονοματεπώνυμο & Υπογραφή Υποψηφίων
(Surname and first name of the candidate):

ΚΑΠΑΤΟΣ ΓΡΗΓΟΡΙΟΣ
(KAPATOS GRIGORIOS)

ΠΑΡΑΜΥΘΕΛΛΗΣ ΒΑΣΙΛΕΙΟΣ
(PARAMYTHELLIS VASILEIOS)

ΕΥΧΑΡΙΣΤΗΡΙΟ ΣΗΜΕΙΩΜΑ

Θα θέλαμε να ευχαριστήσουμε θερμά τους επιβλέποντες καθηγητές κυρίους Μπόγρη Αντώνη και Χοχλιούρο Ιωάννη, τόσο για την ανάληψη της επίβλεψης της εργασίας, όσο και για την υποστήριξή τους στο έργο μας.

Επιπλέον, θα θέλαμε να ευχαριστήσουμε το σύνολο των καθηγητών καθώς και των συμφοιτητών μας, με τους οποίους αποκτήσαμε μια εποικοδομητική και ωφέλιμη συνεργασία στη διάρκεια του προγράμματος εκπαίδευσης αλλά και των εξεταστικών περιόδων.

Τέλος, θα θέλαμε να ευχαριστήσουμε θερμά τις οικογένειές μας για την υποστήριξή τους με τον καλύτερο δυνατό τρόπο, αλλά και για την υπομονή τους σε όλη τη διάρκεια των σπουδών μας.

ΠΕΡΙΛΗΨΗ

Στο σύγχρονο κόσμο, το Διαδίκτυο (Internet) ενσωματώνεται ολοένα και περισσότερο στη ζωή μας παρέχοντας μεγαλύτερες ταχύτητες σύνδεσης, δυνατότητα διακίνησης δεδομένων μεγάλου όγκου και αυξημένο επίπεδο ασφάλειας. Η ανάγκη σύνδεσης στο Διαδίκτυο των ηλεκτρονικών προϊόντων που εξυπηρετούν την καθημερινότητά μας, μέσα από αυτό που αποκαλούμε ως το «Διαδίκτυο των Πραγμάτων» ή αλλιώς “Internet of Things” (IoT), είναι αυτή που εμφανίζεται ως η πλέον σύγχρονη τεχνολογική τάση στην επιστήμη της πληροφορικής και των υπολογιστών. Η ολοένα αυξανόμενη κίνηση δεδομένων καθώς και η εκθετική αύξηση του αριθμού των συνδεδεμένων συσκευών/εξοπλισμών, εγείρουν νέες προκλήσεις για τα υφιστάμενα δίκτυα, τέτοιες ώστε τα νέα δίκτυα ασύρματων και κινητών επικοινωνιών πέμπτης γενιάς (5G) καλούνται να ικανοποιήσουν, διαμορφώνοντας ένα πολλά υποσχόμενο περιβάλλον ανάπτυξης.

Σε συνέχεια των εξελίξεων αυτών, οι τεχνολογίες των αισθητήρων καθώς και των υποκείμενων ασύρματων/κινητών δικτύων επικοινωνιών, οι οποίες με την σειρά τους συνθέτουν τη μεγαλύτερη εικόνα αυτού που ορίζεται ως το “IoT”, δύνανται να εφαρμοστούν τόσο για την ανίχνευση και την παρακολούθηση όσο και για την καταγραφή συμβάντων σε μια περιοχή, με στόχο την προστασία της περιοχής αυτής από κακόβουλες ενέργειες και/ή από φυσικές καταστροφές.

Οι μέθοδοι που χρησιμοποιούνται ώστε η χρήση των WSNs (Wireless Sensor Networks) να προστατέψει τομείς Κρίσιμων – ή μη – (Τηλεπικοινωνιακών) Υποδομών από φαινόμενα όπως μη εξουσιοδοτημένη πρόσβαση, κλοπή, δολιοφθορά, πυρκαγιά, πλημμύρα κ.α., προκύπτουν από τη σύνθετη αποτίμηση της επικινδυνότητας η οποία βασίζεται σε συγκεκριμένη μεθοδολογία, ανά περίπτωση.

Ωστόσο, η παρουσία περιοριστικών παραγόντων σε ένα ασύρματο δίκτυο αισθητήρων σε συνδυασμό με το ασύρματο μέσο μετάδοσης και την απομακρυσμένη και χωρίς ανθρώπινη επίβλεψη λειτουργία, ενίοτε καθιστούν το δίκτυο αυτό «ευαίσθητο» σε επιθέσεις ή άλλου είδους προσβολές. Οι επιθέσεις αυτές θέτουν υπό αμφισβήτηση τις απαιτήσεις ασφαλείας, στοχεύοντας στις λειτουργίες του ίδιου του δικτύου αλλά και στην κατάρρευση της αρχιτεκτονικής του. Για τον λόγο αυτό, οι μηχανισμοί και τα πρωτόκολλα προστασίας έναντι επιθέσεων τα οποία έχουν αναπτυχθεί και τυγχάνουν εφαρμογής στην ευρύτερη «αγορά» των τηλεπικοινωνιακών εφαρμογών και υποδομών, έχουν τόσο σημαντικό ρόλο όσο και η φυσική υπόσταση του ίδιου του δικτύου.

Λέξεις κλειδιά: Ασύρματα Δίκτυα Αισθητήρων, Διαδίκτυο των Πραγμάτων (IoT), Δίκτυα Επικοινωνιών Πέμπτης Γενιάς (5G), Κρίσιμες Υποδομές, Ανάλυση κινδύνου, Ραδιοσυχνοτική Αναγνώριση (RFID), Αισθητήρες, Προστασία WSN, Επιθέσεις Κατανεμημένης Άρνησης (Παροχής) Υπηρεσίας (DDoS), Νέφος, Ανάλυση Εικόνας, Μη Επανδρωμένα Οχήματα (UAVs), Πυρανίχνευση

ABSTRACT

In today's world, the Internet is increasingly integrating into our every-day lives, providing faster connection speeds, the ability to handle huge amounts of data and an increased level of security. The need to connect to the Internet, for the electronic products that serve our daily lives through what we call as the “Internet of Things” (IoT) is what appears to be among the most important modern technological trends in information science and computers. The increasing data traffic as well as the exponential increase in the number of connected devices/equipment, raise new challenges for the existing networks; in this global revolutionary framework the new fifth generation (5G) of mobile and wireless communications networks are called to “meet” related requirements, thus forming a challenging environment for further development and growth.

Following these state-of-the-art tools, sensor technologies as well as wireless sensor networks which in turn compose the larger picture of what is defined as the “IoT”, can be applied and/or implemented both to detect, monitor and record events in a dedicated area, with the aim of protecting that area from malicious acts and/or from natural disasters.
The methods applied to use WSNs so that to protect Critical – or other – (Telecommunication) Infrastructure areas from unauthorized access, theft, sabotage, fire, flood, etc., result from the complex risk assessment in these areas based on a specific methodology, per case.

However, the presence of limiting factors in a wireless sensor network, in combination with the wireless transmission medium and the remote - and occasionally unattended operation - make this network “susceptible” to potential attacks. These attacks “call into question” the considered security requirements such as the availability, confidentiality, authenticity and integrity of devices, thus targeting the proper functioning of the underlying network infrastructures and/or even the collapse of the network architecture. For this reason, the mechanisms and protocols for network protection against such sort of attacks as have been developed and are applied in the market sector, they have a major role to realize, being as important as the physical instance of the wireless network itself.

Keywords: Wireless Sensor Networks, Internet of Things (IoT), Fifth Generation Communication Networks, 5G, Critical Infrastructures (CIs), Risk Analysis, Radio Frequency Identification (RFID), Sensors, WSN Protection, Distributed Denial-of-Service (DDoS) Attacks, Cloud, Video Analytics (VA), Unmanned Vehicles, UAVs, Fire Detection

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

2D	Two-Dimensional
3D	Three-Dimensional
3G	The Third Generation of Mobile (and Wireless) Communications
3G-PLC	The Third Generation of Mobile (and Wireless) Communications – Power Line Communication
4G	The Fourth Generation of Mobile (and Wireless) Communications
4G-LTE	Fourth Generation Long-Term Evolution
5G	The Fifth Generation of Mobile (and Wireless) Communications
6LowPAN	Internet Protocol version 6 (IPv6) and Low-power Wireless Personal Area Networks (LoWPAN)
AC	Access Control
ADC	Analog to Digital Converter
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AOA	Angle of Arrival
AODV	Ad-Hoc On-demand Distance Vector
AR	Augmented Reality
B2B	Business-to-Business
BB	Base Band
BBU	Base Band Unit
BS	Base Station
BSD	Berkeley Software Distribution
BSI	British Standards International
C4ISRT	Command, Control, Communication, Computing, Intelligence, Surveillance, Reconnaissance and Targeting
C-RAN	Cloud-Radio Access Network
CAGR	Compound Annual Growth Rate
CAPEX	Capital Expenses
CCD	Charge Coupled Device
CCTV	Closed Circuit Television
CD	Digital Converter
CEN	Comité Européen de Normalization
CI	Critical Infrastructure
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CISA	Cybersecurity & Infrastructure Security Agency
CMOS	Complementary Metal Oxide Semicoductor
CNN	Convolutional Neural Network
CP	Control Plane
CTS	Clear to Send
CWP	Commission Work Program
DAC	Digital to Analog Converter
DAWWSEN	Defense Mechanism Against Wormhole attacks in Wireless Sensor Networks
DB	Data Base

DD	Directed Diffusion
DDoS	Direct Denial-of-Service
DEMA	Differential Electro Magnetic Analysis
DMZ	Demilitarized Zone
DoS	Denial of Service
DP	Data Plane
DPA	Differential Power Analysis
DRP	Disaster Recovery Plan
DSP	Digital Signal Processing
DSR	Dynamic Source Routing
DTN	Delay Tolerant Network
DVR	Digital Video Recorder
DWDM	Dense Wavelength Division Multiplexing
E2E	End-to-End
ECI	European Critical Infrastructure
EGAT	Electricity Generating Authority Thailand
EM	Electro-Magnetic
eMBB	enhanced Mobile Broadband
ENISA	European Union Agency for Cybersecurity
EPCIP	European Programme for Critical Infrastructure Protection
FDD	Frequency Division Duplex
FHSS	Frequency Hopping Spread Spectrum
FoV	Field of View
fps	frames per second
FW	Fire Wall
GAF	Geographic Adaptive Fidelity
Gbps	Gigabytes per second
GEAR	Geographic and Energy Aware Routing
GIS	Global Information System
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSD	Ground Sampling Distance
GSM	Global System for Mobile Communications
HCI	Human Computer Interface
HD	High Definition
HMI	Human Machine Interface
HOG	Histogram of Oriented Gradients
HSN	Home Seismometer
HSPD	Homeland Security Presidential Directive
HVAC	Heating, Ventilation, and Air Conditioning
HW	Hardware
IaaS	Infrastructure as a Service
IDS	Intrusion Detection System
IEC	International Electrotechnical Committee
IEEE	Institute of Electrical and Electronics Engineers
IHOP	Interleaved Hop-by-Hop Authentication
IMT	International Mobile Telecommunications

INGV	Intituto Nazionale di Geofisica e Vulcanologia
INSENS	Intrusion Tolerant Routing protocol for Wireless Sensor Networks
IoB	Internet of Bodies
IoT	Internet of Things
IP	Internet Protocol
IPv6	IP version 6
IT	Information Technology
ITU	International Telecommunication Union
ISM	Industrial, Scientific and Medical
ISMS	Information Security Management System
ISO	International Organization for Standardization
IWSN	Industrial Wireless Sensor Network
JMA	Japan Meteorological Agency
LAN	Local Area Network
LEACH	Low Energy Adaptive Clustering
LIDAR	Light Detection And Ranging
LoRaWAN	Long Range Wide Area Network
LowPAN	Low-power Personal Area Network
LTE	Long Term Evolution
M2M	Machine-to-Machine
MAC	Medium Access Control
MANET	Mobile ad-hoc Network
MEMS	Micro Electronic Mechanical Systems
mIoT	massive Internet of Things
ML	Machine Learning
mMTC	massive Machine Type Communications
MMSPEED	Multi path and Multi SPEED
MNS	Massive Notification System
MPR	Multiple Parent Routing
µTESLA	micro Timed, Efficient, Streaming, Loss – tolerant, Authentication Protocol
NB	Narrow Band
NB-IoT	Narrow Band IoT
NFV	Network Function Virtualization
NN	Neural Network
NR	New Radio
NVR	Network Video Recorder
OC	Object Catching
OM	Object Monitoring
OMT	Object Movement Tracing
ONVIF	Open Network Video Interface Forum
PaaS	Platform as a Service
PDCA	Plan-Do-Check-Act
PEGASIS	Power - Efficient Gathering in Sensor Information Systems
PIN	Personal Identification Number
PIR	Passive InfraRed
PLC	Power Line Communication
PLC	Programmable Logic Controller

POTS	Plain Old Telephone Service
PSIM	Physical Security Integration Management
PTZ	Pan-Tilt-Zoom
PV	Photo-Voltaic
QoS	Quality of Service
RAM	Random Access Memory
RAT	Radio Access Terminal
RF	Radio-Frequency
RFID	Radio-Frequency Identification
RPL	Real-time Programming Language
RRH	Remote Radio Head
RSS	Radio Signal Strength
RTLS	Real-Time Location System
RTS	Reliable Transport Solution
RTS	Request to Send
RTU	Remote Telemetry Unit
RW	Random Walk
Rx	Reception
SaaS	Software as s Service
SAR	Sequential Assignment Routing
SCADA	Supervisory Control and Data Acquisition
SDN	Software Defined Network
SDP	Software Defined Protocol
SDT	Software-Defined Topology
SEC	Securities and Exchange Commission
SEF	Statistical En-route Filtering
SEMA	Simple Electro Magnetic Analysis
SIMD	Single Instruction Multiple Data
SLA	Service Level Agreement
SMECN	Small Minimum Energy Communication Network
SNEP	Sensor Network Encryption Protocol
SNR	Signal to Noise Ratio
SONAC	Service Oriented Network Auto Creation
SOP	Self Organized Protocol
SPA	Simple Power Analysis
SPAN	Switch Port Analyzer
SPARK	Smart PARKing
SPEED	Stateless Protocol of Energy-Efficient Devices
SPIN	Sensor Protocols for Information via Negotiation
SPINS	Security Protocols for Sensor Networks
SQL	Structured Query Language
SW	Software
TC	Technical Committee
TCP	Transmission Control Protocol
TDD	Time Division Duplex
TDMA	Time Division Multiple Access
TEDS	Transducer Electronic Data Sheet

TEEN	Threshold - Sensitive Energy Efficient Protocol
TEG	Thermo-Electric Generator
TDOA	Time Difference of Arrival
TOA	Time of Arrival
TTDD	Two-Tier Data Dissemination
Tx	Transmission
UAV	Unmanned Aerial Vehicle
UC	Use Case
UGS	Unattended Ground Sensor
UHD	Ultra-High Definition
uIP	Micro-Internet Protocol
UP	User Plane
URLLC	Ultra-Reliable and Low Latency Communications
USB	Universal Serial Bus
UWSN	Underwater Wireless Sensor Network
VA	Video Analytics
VCA	Video Content Analysis
VGA	Virtual Grid Architecture
VM	Virtual Machine
VMD	Video Motion Detection
VMS	Video Management Software
VNI	Virtual Network Interface
VPN	Virtual Private Network
VR	Virtual Reality
WAN	Wide Area Network
WCDMA	Wideband Code Division Multiple Access
Wi-Fi, WiFi	Wireless Fidelity
WoT	World of Things
WSN	Wireless Sensor Network
WWW	World Wide Web

1

Εισαγωγή

Στη σημερινή κοινωνία, το πλήθος των συσκευών που είναι συνδεδεμένες στο Διαδίκτυο αυξάνεται καθημερινά με εκθετικό ρυθμό. Ζώντας ήδη στην εποχή του Διαδικτύου των Πραγμάτων (Internet of Things, IoT), την επόμενη δεκαετία ο αριθμός των διασυνδεδεμένων συσκευών υπολογίζεται να έχει ξεπεράσει πολλαπλάσια τον αριθμό των ανθρώπων που βρίσκονται στην γη [1]. Έτσι, καθημερινά παρατηρούμε καινούργιους τύπους συσκευών που συνδέονται στο Διαδίκτυο και μάλιστα καθόλη τη διάρκεια της ημερήσιας λειτουργίας τους, όπως τα έξυπνα κινητά τηλέφωνα, τα tablets (πινακίδια), οι έξυπνες τηλεοράσεις, τα έξυπνα ρολόγια κ.ο.κ. Επιπλέον, η κίνηση των δεδομένων που παράγονται από τις κινητές συσκευές οι οποίες απαρτίζουν το IoT εξυπηρετείται από τα υπάρχοντα δίκτυα επικοινωνιών, θέτοντας επιτακτικά πλέον την ανάγκη για υψηλές ταχύτητες και για επαυξημένη χωρητικότητα. Το ασύρματο δίκτυο 5ης γενιάς (5G) αναμένεται να ικανοποιήσει τις ανάγκες αυτές, ενσωματώνοντας το IoT μέσα σε ένα νέο αναδυόμενο τεχνολογικό περιβάλλον αναφοράς, αναδεικνύοντας ταυτόχρονα αρκετές καινοτόμες προκλήσεις.

Ως συνέπεια των ανωτέρω, η χρήση των ασύρματων αισθητήρων στα πλαίσια της οντότητας που ονομάζεται ως το IoT ήταν αναμενόμενο να βρει άμεση εφαρμογή και στον τομέα των συστημάτων ασφαλείας. Σταδιακά, με την ανάπτυξη των τεχνολογιών, οι ασύρματοι αισθητήρες εμφανίστηκαν σε συστήματα επιτήρησης και καταγραφής εικόνας, σε συστήματα ανίχνευσης κίνησης, ανίχνευσης δόνησης, ανίχνευσης καπνού κ.α., ώστε πλέον η ανάγκη χρήσης καλωδίων έπαψε να είναι απαραίτητη [2]. Επιπλέον, οι δικτυακοί κόμβοι αυτών των αισθητήρων μπορούν να επικοινωνήσουν είτε μεταξύ τους είτε με αυτό που ορίζεται ως «σταθμός βάσης» (Base Station - BS) προκειμένου να δρομολογηθούν τα σήματα που αφορούν στην παρατήρηση και στην καταγραφή των συνθηκών του περιβάλλοντος χώρου και για να αποκαλύψουν ιδιότητες και/ή γεγονότα τα οποία συμβαίνουν σε μια ορισμένη περιοχή.

Αυτή η συνθήκη λειτουργίας, σε συνδυασμό με τη μικρή κατανάλωση ενέργειας αλλά και τις χαμηλές ανάγκες συντήρησης, βρήκε ευρεία εφαρμογή στα πεδία που

συμπεριλαμβάνουν και φιλοξενούν τις αποκαλούμενες ως Κρίσιμες Υποδομές (Critical Infrastructures - CIs). Η παρούσα διατριβή επικεντρώνεται στην προστασία με συσκευές IoT, του τμήματος εκείνου των Κρίσιμων Υποδομών το οποίο αφορά στις Τηλεπικοινωνίες και στα Πληροφοριακά Συστήματα.

Ωστόσο, με την αύξηση των διασυνδεδεμένων συσκευών, όπως εύλογα προκύπτει ως λογικό επακόλουθο, αυξήθηκε και το εύρος των επιθέσεων που μπορούν να ασκηθούν από διαφορετικούς επίδοξους «εισβολείς». Άρα, εκτός από τη μελέτη προστασίας των Κρίσιμων Υποδομών χρησιμοποιώντας τα ασύρματα δίκτυα ως συστήματα ασφαλείας θα πρέπει να γίνεται αποτίμηση τόσο των κινδύνων όσο και των μεθόδων προστασίας που μπορούν να χρησιμοποιηθούν, προκειμένου να εξασφαλίζεται η απρόσκοπτη λειτουργία και η διαθεσιμότητα των δικτύων αυτών. Οι εισβολείς αναζητούν τρωτότητες που υπάρχουν στα προγράμματα (software) και/ή στο υλισμικό (hardware) και τούτο διότι τρωτότητες/προσβλητότητες διαφορετικών μορφών μπορούν να υπάρχουν σχεδόν σε όλες τις προγραμματιζόμενες μονάδες, ανεξάρτητα από το εάν πρόκειται για μία συγκεκριμένη συνάρτηση ενός προγράμματος ή ένα σύστημα ελέγχου σε ένα εργοστάσιο παραγωγής ηλεκτρικής ενέργειας. Όσο πολυπλοκότερη και μεγαλύτερη είναι μία εφαρμογή, τόσο δυσκολότερη γίνεται η διαδικασία ελέγχου της για λάθη στον αντίστοιχο κώδικα ορθής λειτουργίας της, τα οποία μπορούν να οδηγήσουν σε ενδεχόμενες τρωτότητες. Αντίστοιχα, όσο μεγαλύτερο καθίσταται ένα δίκτυο, τόσο δυσκολότερη γίνεται η διαχείρισή του και ακόμα πιο δύσκολη καθίσταται η πρόκληση για τους διαχειριστές ώστε να το διατηρούν ως επαρκώς ασφαλές.

Στις ενότητες που θα συναντήσουμε στα επόμενα κεφάλαια της παρούσας διατριβής, περιγράφονται:

- Η έννοια, τα χαρακτηριστικά, οι εφαρμογές, ο τρόπος λειτουργίας αλλά και οι προβληματισμοί που τίθενται γύρω από την λειτουργία των WSNs (Κεφ. 2 - Τα Ασύρματα Δίκτυα Αισθητήρων)
- Η χρήση των αισθητήρων υπό την ευρύτερη έννοια της οντότητας που ονομάζεται ως IoT, καθώς και συναφείς προκύπτουσες εφαρμογές (Κεφ. 3 - Το Διαδίκτυο των Πραγμάτων)
- Η αναγκαιότητα ανάπτυξης των δικτύων 5G, προκειμένου εντός των δικτύων αυτών να επιτυγχάνεται η ομαλή και αξιόπιστη λειτουργία των WSNs και του IoT (Κεφ. 4 - Τα Δίκτυα Επικοινωνιών 5^{ης} Γενιάς)
- Ο ορισμός, η σημαντικότητα, και τα ζητήματα ασφαλείας των Κρίσιμων Υποδομών (Κ.Υ.), καθώς αναλύονται και οι εξαρτήσεις αυτών με τις υποδομές τηλεπικοινωνιών (Κεφ. 5 - Κρίσιμες Υποδομές)
- Εφαρμογές φυσικής προστασίας Κ.Υ., χρησιμοποιώντας τις τεχνολογίες Ασύρματων Δικτύων Αισθητήρων (Κεφ. 6 - Εφαρμογές Ασφαλείας με WSNs)
- Ζητήματα φυσικής και ψηφιακής ασφάλειας και τρόποι προστασίας των Ασύρματων Δικτύων Αισθητήρων (Κεφ. 7 - Η Ασφάλεια στα WSNs)
- Η τεκμηρίωση μέσα από πραγματικές περιπτώσεις χρήσης των προαναφερθέντων στοιχείων (Κεφ. 8 – Περιπτώσεις Χρήσης)

Τέλος, θα παρουσιαστούν συμπεράσματα και προβληματισμοί σχετικά με την χρήση των Ασυρμάτων Δικτύων Αισθητήρων στη φυσική ασφάλεια υποδομών.

2

Ασύρματα Δίκτυα Αισθητήρων

Ένα ασύρματο δίκτυο αισθητήρων (Wireless Sensor Network - WSN) αποτελείται από διασκορπισμένους αυτόνομους αισθητήρες στον περιβάλλοντα χώρο, ικανούς ώστε να λαμβάνουν και να παρέχουν πληροφορίες για τον έλεγχο μεταβλητών φυσικών μεγεθών, όπως είναι π.χ. η θερμοκρασία, ο ήχος, η ατμοσφαιρική πίεση, ο φωτισμός, η κίνηση κτλ.[1]. Μέσω της συνεργασίας των αισθητήρων, ένα WSN μεταφέρει όλα τα δεδομένα προς επεξεργασία σε μία συγκεκριμένη τοποθεσία.

Το κίνητρο για την ανάπτυξη ασύρματων δικτύων με αισθητήρες ήταν πρωτίστως οι στρατιωτικές εφαρμογές, όπως η παρακολούθηση των πεδίων μάχης [3]. Εντούτοις, σήμερα τέτοια δίκτυα χρησιμοποιούνται σε πολλές καταναλωτικές και βιομηχανικές εφαρμογές, αποσκοπώντας στην παρακολούθηση και στον έλεγχο της βιομηχανικής παραγωγής, στην παρακολούθηση κρίσιμων υποδομών αλλά και σε πολλές άλλες εφαρμογές [4].

Το ασύρματο δίκτυο αισθητήρων αποτελείται από κόμβους (nodes), με κάθε κόμβο να συνδέεται σε έναν ή περισσότερους αισθητήρες. Ο κόμβος αποτελείται από έναν ασύρματο πομπό και δέκτη, μία κεραία, έναν μικροελεγκτή, ένα ηλεκτρονικό κύκλωμα για τη διασύνδεση με τους αισθητήρες και μία πηγή ενέργειας (δηλαδή μία μπαταρία ή μία εναλλακτική μορφή συγκομιδής ενέργειας, όπως π.χ. φωτοβολταϊκός συλλέκτης).
Το κόστος των αισθητήριων κόμβων ποικίλει, ξεκινώντας από μερικά και φτάνοντας σε αρκετές εκατοντάδες δολάρια, ανάλογα με την πολυπλοκότητα των επιμέρους μεμονωμένων αισθητήριων κόμβων. Οι περιορισμοί σε μέγεθος και κόστος έχουν ως αποτέλεσμα αντίστοιχους περιορισμούς σε πόρους, όπως σχετικά με την ενέργεια, τη μνήμη, την υπολογιστική ταχύτητα και το εύρος ζώνης των επικοινωνιών [5].

[1] Dargie, W., and Poellabauer, C., "Fundamentals of wireless sensor networks: theory and practice", John Wiley and Sons, 2010, pp.168–183, 191–192.

2.1 Εφαρμογές Ασύρματων Δικτύων Αισθητήρων

Τα ασύρματα δίκτυα αισθητήρων σχεδιάστηκαν για τη χρήση συλλογής, επεξεργασίας και μεταφοράς δεδομένων σε πολύπλοκα περιβάλλοντα και σε πραγματικό χρόνο. Για τον λόγο αυτό, τα WSNs έχουν βρει εφαρμογή σε ένα πλήθος περιπτώσεων (βλ. Εικόνα 2-1) όπου ο έλεγχος και η επίβλεψη διαφόρων αναλογικών μεγεθών είναι ζωτικής σημασίας για τη διατήρηση της διαθεσιμότητας του δικτύου και για τη διασφάλιση της ποιότητας της προσφερόμενης εφαρμογής-υπηρεσίας.

Οι δημοφιλείς εφαρμογές, *μεταξύ άλλων*, περιλαμβάνουν την παρακολούθηση φυσικών μεγεθών και του περιβάλλοντος, την ενημέρωση για συμβάντα πυρκαγιάς, στρατιωτικές εφαρμογές, εφαρμογές ρομποτικής, τον βιομηχανικό ποιοτικό έλεγχο, την προστασία κρίσιμων υποδομών, τις τεχνολογίες έξυπνων σπιτιών, τις ευφυείς επικοινωνίες, τον έλεγχο κυκλοφορίας, κτλ.

Ωστόσο, ορισμένες ακόμα περισσότερο τεχνολογικά προχωρημένες και ίσως «εξεζητημένες» εφαρμογές περιλαμβάνουν, μεταξύ άλλων:

- Ανίχνευση βιολογικών παραμέτρων μέσω αισθητήρων νανοτεχνολογίας και χρήση της τεχνολογίας MEMS (Micro Electronic Mechanical Systems) [6].
- Απομακρυσμένη διάγνωση και σύσταση θεραπείας ασθενών στα πλαίσια τηλεϊατρικής, για απομακρυσμένες περιοχές πρόσβασης [7].
- Έλεγχο στάθμευσης ή απομακρυσμένη κράτηση θέσης στάθμευσης για περιοχές όπου εφαρμόζεται η τεχνολογία Smart PARKing (SPARK) [8].
- Αυτόνομο όχημα (autonomous automobile) και τηλεματική κατεύθυνση οχήματος [9].
- Διάγνωση προβλημάτων βιομηχανικών μονάδων και συντήρηση σε πραγματικό χρόνο [10].
- Στρατιωτικές εφαρμογές σε πραγματικό χρόνο στο πεδίο μάχης, στο πλαίσιο των συστημάτων που καλούνται ως C4ISRT (Command, Control, Communication, Computing, Intelligence, Surveillance, Reconnaissance and Targeting) [11].
- Παρακολούθηση ρύπανσης του αέρα, του νερού του εδάφους ή ακόμα και ακουστικής ρύπανσης [12].
- Παρακολούθηση κατανάλωσης στα πλαίσια του σχεδιασμού έξυπνων κτηρίων με χαρακτηριστικά την ευέλικτη διαχείριση συστημάτων θέρμανσης/ψύξης, τον αυτόματο κεντρικοποιημένο έλεγχο των ηλεκτρικών συσκευών, τη δυνατότητα κεντρικού ελέγχου λειτουργιών, την κατανάλωση ηλεκτρικής ισχύος, νερού, φυσικού αερίου κλπ. και εν τέλει τη βελτιστοποίηση της διαχείρισης των φυσικών πόρων, προς όφελος του περιβάλλοντος και της αειφόρου ανάπτυξης [13].

Προφανώς, τα παραπάνω σημεία συνιστούν ορισμένες μόνο από τις δυνητικά παρεχόμενες εφαρμογές, ενώ στην πραγματικότητα το πλήθος των εφαρμογών που μπορούν να υλοποιηθούν με την χρήση WSNs είναι πολύ μεγαλύτερο.

Στην παρούσα διατριβή θα μας απασχολήσουν οι εφαρμογές οι οποίες συμπεριλαμβάνουν την χρήση των WSNs για την προστασία των κρίσιμων υποδομών τηλεπικοινωνίας, όπου οι

ανθρώπινη παρέμβαση αλλά και οι περιβαλλοντικές απειλές είναι ζωτικής σημασίας, ώστε η διαθεσιμότητα του δικτύου να μην απειλείται.

Εικόνα 2-1: Εφαρμογές ασύρματων δικτύων αισθητήρων [14]

2.2 Περιγραφή Κόμβου Αισθητήρα

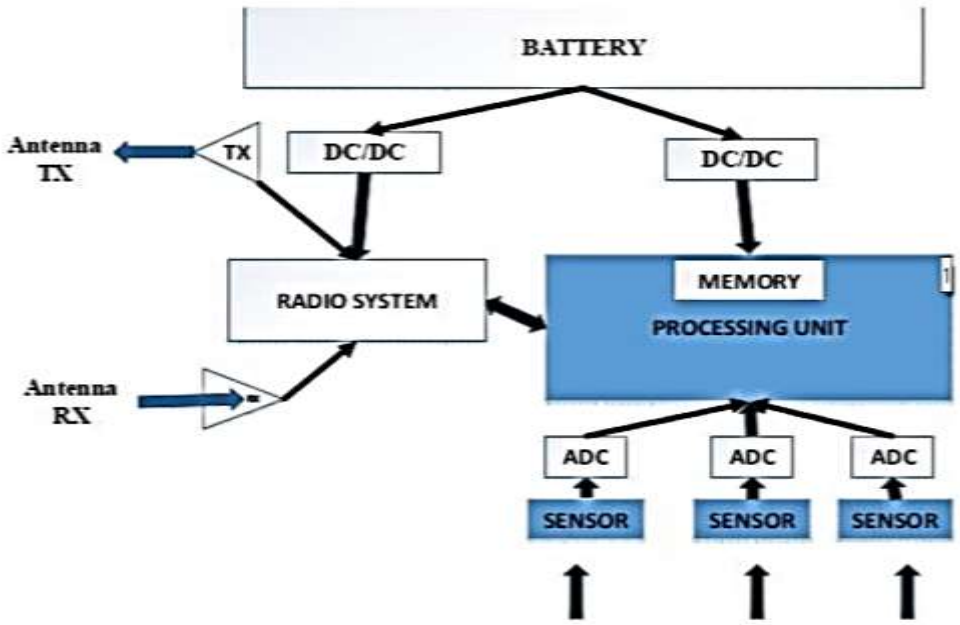
Λόγω της ραγδαίας αύξησης των εφαρμογών που χρησιμοποιούν ασύρματα δίκτυα αισθητήρων έγινε προσπάθεια μείωσης του όγκου των συσκευών αυτών, καθώς επίσης και μείωσης του κόστους παραγωγής τους ώστε να είναι πραγματικά κα ουσιαστικά συμφέρουσα η χρήση και η υλοποίησή τους σε ευρεία κλίμακα, υπό τα μεγέθη των πραγματικών αγορών.

Σε αυτά τα δίκτυα αισθητήρων ενίοτε συναντάμε διαφορετικές τοπολογίες, αρχιτεκτονικές και πρωτόκολλα δρομολόγησης σε σχέση με αυτά που είναι γνωστά στα παραδοσιακά ασύρματα δίκτυα. Ένας σοβαρός λόγος που συμβαίνει αυτό έχει να κάνει και με τα χαρακτηριστικά που διαθέτει ο κόμβος αισθητήρα. Το μικρό του μέγεθος, που όπως είπαμε είναι κρίσιμο χαρακτηριστικό του, δεν προσφέρει περιθώρια στον σχεδιαστή για να χρησιμοποιήσει ισχυρές πηγές ενέργειας ιδίως λόγω του περιορισμένου χώρου, έχοντας ως αποτέλεσμα το να είναι εφικτή μόνο η χρήση μικρών μπαταριών. Αυτό, οδηγεί νομοτελειακά σε μικρή επεξεργαστική ισχύ και χρόνο ζωής του κόμβου. Γι’ αυτούς τους λόγους υπάρχει αυτού του είδους η διαφοροποίηση όσον αφορά στη λειτουργία των δικτύων, με κοινό παρονομαστή την εξοικονόμηση ενέργειας και, *ως εκ τούτου*, την επικείμενη μεγιστοποίηση του χρόνου ζωής τους.

Αναλυτικότερα, ένας κόμβος αισθητήρα αποτελείται από τα εξής βασικά μέρη (βλ. Εικ. 2-2):

- **Πομπός/Δέκτης:** Το σύστημα πομποδέκτη ενός ασύρματου δικτύου αισθητήρων επιτρέπει την άμεση επικοινωνία μεταξύ του κόμβου αισθητήρα με το εξωτερικό περιβάλλον.
- **Μικροελεγκτής**: Ο Μικροελεγκτής (μονάδα επεξεργασίας) σε ένα σύστημα ασύρματων αισθητήρων που αξιολογεί τους κόμβους, εξάγει σημαντικές πληροφορίες και φροντίζει για την εφαρμογή των πρωτοκόλλων που χρησιμοποιεί ο κόμβος.
- **Πηγή Ενέργειας:** Το στοιχείο που είναι απαραίτητο για τη λειτουργία ενός κόμβου, παρέχοντας ενεργειακή τροφοδοσία.
- **Αισθητήρες**: Είναι οι συσκευές που μετατρέπουν αναλογικά σήματα του περιβάλλοντος σε ηλεκτρικά σήματα προς επεξεργασία.

Επιπρόσθετα, σε έναν κόμβο θα συναντήσουμε βοηθητικές βαθμίδες και υποσυστήματα όπως είναι το Σύστημα Εύρεσης Θέσης, το Σύστημα Κινητοποίησης, ο Μετατροπέας Αναλογικού Σήματος σε Ψηφιακό Σήμα (ADC) και η Μνήμη.



Εικόνα 2-2: Κύκλωμα ασύρματου κόμβου αισθητήρα

2.3 Χαρακτηριστικά Κόμβου Αισθητήρα

Ορισμένα από τα βασικά χαρακτηριστικά που διαθέτουν οι κόμβοι ενός δικτύου ασύρματων αισθητήρων είναι τα παρακάτω [15, 16]:

- **Συμπαγές και μικρό μέγεθος:** Οι κόμβοι αισθητήρων είναι μικροί σε μέγεθος και περιορισμένης εμβέλειας. Λόγω του μεγέθους τους, η ενέργειά τους είναι περιορισμένη και έτσι οι δυνατότητες επικοινωνίας είναι συνήθως χαμηλές.

- **Χαμηλό κόστος:** Μία υλοποίηση δικτύου ασύρματων αισθητήρων συνήθως αποτελείται από εκατοντάδες ή και χιλιάδες κόμβους. Για να μειώσουμε το συνολικό κόστος του δικτύου, θα πρέπει να διατηρήσουμε το κόστος κάθε κόμβου όσο χαμηλά γίνεται.

- **Μικρή κατανάλωση ισχύος:** Η ενέργεια σε ένα δίκτυο ασύρματων αισθητήρων χρησιμοποιείται για διαφορετικούς σκοπούς, όπως για την υπολογιστική μονάδα, την ασύρματη επικοινωνία και την αποθήκευση δεδομένων. Το τμήμα του ασύρματου αισθητήρα που καταναλώνει τη μεγαλύτερη ενέργεια είναι αυτό που εκτελεί την ασύρματη επικοινωνία. Καθώς οι περισσότεροι κόμβοι ενός ασύρματου δικτύου τροφοδοτούνται από μπαταρίες, η αυτονομία τους είναι συνήθως περιορισμένη. Για το λόγο αυτό, θα πρέπει να λαμβάνεται υπόψη η κατανάλωση ισχύος βάσει των αλγορίθμων και των πρωτοκόλλων, στη φάση της σχεδίασης.

- **Δυνατότητες επικοινωνίας:** Τα δίκτυα ασύρματων αισθητήρων τυπικά επικοινωνούν χρησιμοποιώντας ραδιοκύματα σε ένα ασύρματο κανάλι. Το ασύρματο κανάλι έχει τη δυνατότητα να επικοινωνεί σε περιορισμένες αποστάσεις, με αμφίδρομο ή μονόδρομο τύπο επικοινωνίας. Συνήθως το περιβάλλον επικοινωνίας δεν είναι ιδανικό (ύπαρξη εμποδίων, καιρικά φαινόμενα), με αποτέλεσμα το δίκτυο να μην λειτουργεί ομαλά. Έτσι, το υλισμικό και το λογισμικό του δικτύου θα πρέπει να είναι κατάλληλα ανεπτυγμένα με σκοπό την ασφάλεια, την επανατακτικότητα, την αξιοπιστία και την ευελιξία.

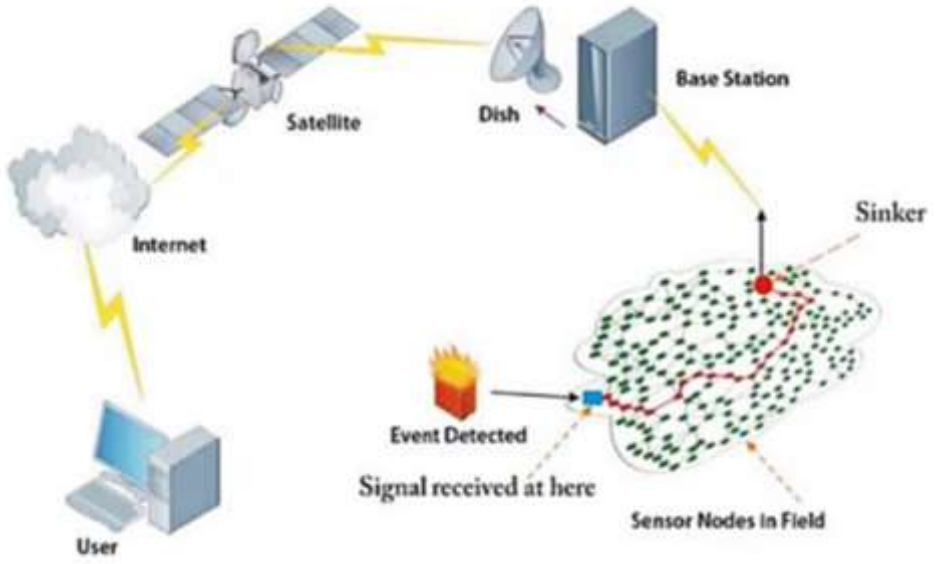
- **Ασφάλεια και Ιδιωτικότητα:** Κάθε κόμβος θα πρέπει να έχει αποδοτικούς μηχανισμούς ασφαλείας ώστε να αποτρέπει ενδεχόμενη μη εξουσιοδοτημένη πρόσβαση, επιθέσεις και αλλοίωση ή καταστροφή της πληροφορίας που βρίσκεται στον κόμβο.

- **Κατανεμημένη ανίχνευση και επεξεργασία:** Ο μεγάλος αριθμός των κόμβων-αισθητήρων είναι κατανεμημένος ομοιόμορφα ή με τυχαίο τρόπο. Ο κάθε κόμβος είναι ικανός ώστε να συλλέγει, να ταξινομεί, να επεξεργάζεται και να στέλνει τα δεδομένα στην αντίστοιχη βάση δεδομένων (DB). Ως αποτέλεσμα, η κατανεμημένη ανίχνευση προσφέρει την προοπτική ευελιξίας του συστήματος.

- **Δυναμική τοπολογία**: Γενικά, το δίκτυο ασύρματων αισθητήρων είναι ένα δίκτυο το οποίο μπορεί να υπόκειται σε συχνές αλλαγές. Ένας κόμβος του δικτύου μπορεί να αποτύχει να ανταποκριθεί λόγω έλλειψης ενέργειας ή άλλων παραγόντων, ενώ το κανάλι επικοινωνίας μπορεί να διαταραχθεί ή ένας άλλος κόμβος να προστεθεί.

Όλοι οι παραπάνω παράγοντες είναι ικανοί ώστε να μεταβάλλουν την τοπολογία του δικτύου. Για το λόγο αυτό, ο κάθε κόμβος πρέπει να είναι εφοδιασμένος με κατάλληλες λειτουργίες αναδιαμόρφωσης και αυτό-προσαρμογής, όταν μία αλλαγή κριθεί απαραίτητη.

- **Έξυπνη επικοινωνία:** Εάν ένας κόμβος χρειάζεται να επικοινωνήσει με τον σταθμό βάσης ή με έναν άλλο κόμβο ο οποίος είναι πέρα από την εμβέλεια του, πρέπει να αξιοποιήσει την επικοινωνία πολλαπλών αλμάτων (multi-hop communication) μέσω των ενδιάμεσων κόμβων. Επίσης, οι κόμβοι πρέπει να συνεργάζονται ώστε να προσαρμόζονται στον κατανεμημένο εφαρμοστέο αλγόριθμο για να διαμορφώνουν το δίκτυο με αυτόματο τρόπο.



Εικόνα 2-3: Ένα τυπικό δίκτυο ασύρματων αισθητήρων, υπό μια ευρύτερη δικτυακή θεώρηση [17]

2.4 Πρωτόκολλα Δρομολόγησης

Το πρωτόκολλο δρομολόγησης (routing protocol) ή αλλιώς πρωτόκολλο επικοινωνίας (communication protocol), είναι η διαδικασία εκείνη κατά την οποία γίνεται η επιλογή της κατάλληλης διαδρομής για τα δεδομένα που ταξιδεύουν από την πηγή προς τον προορισμό. Κατά την επιλογή της διαδρομής αυτής συνήθως συναντώνται διάφορες δυσκολίες οι οποίες σχετίζονται με τον συντομότερο δρόμο, την ασφάλεια των δεδομένων, τον τύπο του δικτύου, τα χαρακτηριστικά του καναλιού μετάδοσης και λήψης και τελικά τις μετρήσεις απόδοσης.

Τα δεδομένα που ανιχνεύονται από τους κόμβους αισθητήρων σε ένα ασύρματο δίκτυο αισθητήρων προωθούνται συνήθως στον σταθμό βάσης ο οποίος με την σειρά του συνδέει το δίκτυο αισθητήρων με τα άλλα δίκτυα επικοινωνίας, όπως για παράδειγμα το τοπικό

δίκτυο (LAN) ή το δίκτυο ευρείας περιοχής (WAN). Εκεί τα δεδομένα συλλέγονται, υπόκεινται σε ανάλυση και τελικά αποφασίζεται η ανάληψη κάποιας δράσης.

Κατά τον σχεδιασμό ενός πρωτοκόλλου δρομολόγησης, θα πρέπει σε κάθε περίπτωση να λαμβάνονται υπόψη τα παρακάτω ιδιαίτερα χαρακτηριστικά:

- **Ενεργειακή απόδοση:** Τα ασύρματα δίκτυα αισθητήρων τροφοδοτούνται κυρίως από μπαταρία, οπότε η κατανάλωση φορτίου και η ενεργειακή ανεπάρκεια είναι ένα σημαντικό ζήτημα. Η απόδοση των κόμβων αισθητήρα επηρεάζεται αρνητικά, όταν η μπαταρία «πέσει» κάτω από ένα προκαθορισμένο κατώτατο όριο. Λαμβάνοντας υπόψη ότι σε ένα ασύρματο δίκτυο αισθητήρων ενδέχεται να υπάρχουν χιλιάδες κόμβοι, όπου ο καθένας εκ των οποίων έχει περιορισμένους πόρους ενέργειας στην διάθεσή του, το πρωτόκολλο δρομολόγησης θα πρέπει να σχεδιάζεται με πρωταρχικό σκοπό την ενεργειακή απόδοση [18].

- **Πολυπλοκότητα**: Η πολυπλοκότητα ενός πρωτοκόλλου δρομολόγησης μπορεί να επηρεάσει την απόδοση ολόκληρου του ασύρματου δικτύου. Η αιτία για αυτή τη συνθήκη είναι οι ανεπαρκείς ικανότητες υλισμικού και οι ακραίοι περιορισμοί ενέργειας [19].

- **Επεκτασιμότητα**: Καθώς οι αισθητήρες εξελίσσονται συνεχώς οδεύοντας προς φθηνότερα αλλά και συχνά αρτιότερα τεχνολογικά προϊόντα, το πρωτόκολλο δρομολόγησης θα πρέπει να υποστηρίζει τη δυνατότητα επέκτασης του δικτύου οποιαδήποτε στιγμή, χωρίς να προκύψει το ενδεχόμενο διακοπής ή παύσης των υπολοίπων σημάτων μετάδοσης [20].

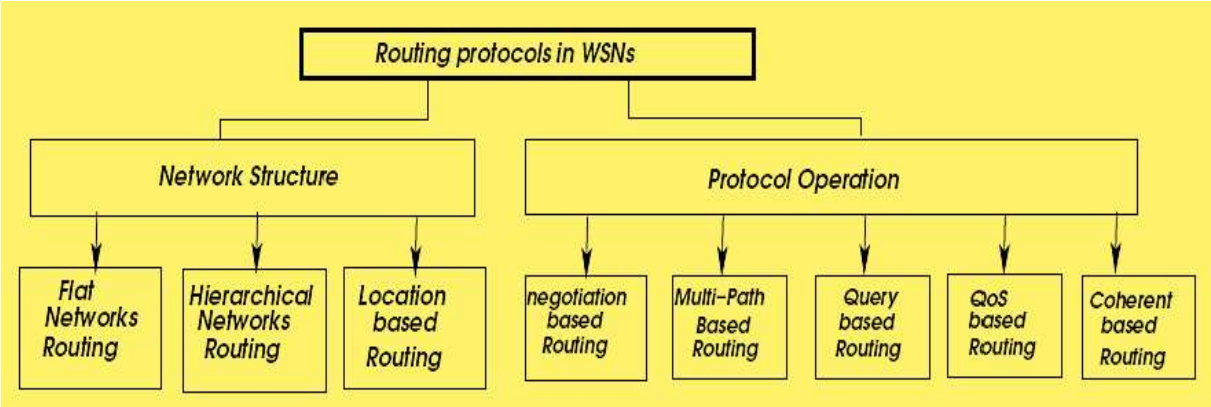
- **Καθυστέρηση:** Ορισμένες εφαρμογές απαιτούν άμεση αντίδραση ή τουλάχιστον απόκριση χωρίς σημαντική καθυστέρηση, όπως π.χ. η παρακολούθηση της αύξησης της θερμοκρασίας, η παρακολούθηση ενός συναγερμού, κτλ. Υπό αυτή τη θεώρηση, το πρωτόκολλο δρομολόγησης θα πρέπει να προσφέρει την ελάχιστη δυνατή καθυστέρηση (low latency) [21].

- **Επανατακτικότητα:** Λαμβάνοντας υπόψη το γεγονός ότι τα ασύρματα δίκτυα πολλές φορές αναπτύσσονται σε εξαιρετικά επικίνδυνα ή «ευάλωτα» περιβάλλοντα, περιστασιακά ένας κόμβος μπορεί να υπολειτουργήσει ή/και να τεθεί εκτός λειτουργίας (ακόμα και να καταστραφεί για κάποιο λόγο) και συνεπώς να «χαθεί» από το υπόλοιπο δίκτυο. Το πρωτόκολλο δρομολόγησης θα πρέπει να έχει την εύλογη ικανότητα αναπροσαρμογής [22].

- **Ασφάλεια**: Τα WSNs συχνά αναπτύσσονται υπό δυσμενείς και μη ασφαλείς συνθήκες, όπου ένας εισβολέας μπορεί να δημιουργήσει διαφορετικούς τύπους απειλών προκειμένου να προβάλει και να «φθείρει» ένα δίκτυο. Επίσης, εκτός από τις παραδοσιακές απειλές προσβολών, υπάρχουν και προηγμένες απειλές, οι οποίες βασίζονται σε αγνώστου τύπου επιθέσεις για τις οποίες τα παραδοσιακά στοιχεία ασφαλείας είναι συχνά ανεπαρκή. Ως εκ τούτου, η προστασία από απειλές με δυναμική αλλαγή χαρακτηριστικών είναι σημαντική [23].

2.4.1 Κατηγορίες Πρωτοκόλλων Επικοινωνίας

Η δρομολόγηση στα WSNs μπορεί να διαχωριστεί σε δύο βασικές κατηγορίες, ήτοι: α) στα πρωτόκολλα δρομολόγησης που στηρίζονται στην **δομή του δικτύου** και β) στις τεχνικές δρομολόγησης που βασίζονται στην **λειτουργία του πρωτοκόλλου** (βλ. Εικόνα 2-4). Η κατηγοριοποίηση αυτή είναι αρκετά ευρεία και κάτω από κάθε κατηγορία υπάρχουν συγκεκριμένες υποκατηγορίες [26].



Εικόνα 2-4: Ταξινόμηση πρωτοκόλλων δρομολόγησης για WSNs [26]

Επίσης, τα πρωτόκολλα δρομολόγησης μπορούν να κατηγοριοποιηθούν σύμφωνα με τον τρόπο τον οποίο επιλέγει η πηγή μετάδοσης του μηνύματος προς τον αντίστοιχο προορισμό.

Διακρίνονται οι ακόλουθες περιπτώσεις [28]:

- **Προδραστικά πρωτόκολλα (proactive protocols)**: Στην περίπτωση αυτή οι διαδρομές έχουν ήδη υπολογιστεί πριν ζητηθούν. Όταν οι κόμβοι είναι στατικοί, προτιμώνται πρωτόκολλα αυτής της κατηγορίας. Σε αυτόν τον τύπο προδραστικού πρωτοκόλλου, κάθε κόμβος σε ένα δίκτυο διατηρεί έναν ή περισσότερους πίνακες δρομολόγησης που ενημερώνονται τακτικά. Κάθε κόμβος στέλνει ένα μήνυμα μετάδοσης σε ολόκληρο το δίκτυο εάν υπάρχει αλλαγή στην τοπολογία του δικτύου. Ωστόσο, αυτό συνεπάγεται πρόσθετο γενικό κόστος λόγω της διατήρησης ενημερωμένων πληροφοριών και, ως εκ τούτου, μπορεί να επηρεαστεί η απόδοση του δικτύου. Σε κάθε περίπτωση, παρέχονται πραγματικές πληροφορίες για τη διαθεσιμότητα του δικτύου.

- **Αντιδραστικά πρωτόκολλα (reactive protocols)**: Στην περίπτωση αυτή οι διαδρομές υπολογίζονται μετά από ζήτηση, με σκοπό την «ανακάλυψη» και «σχεδίαση» του καλύτερου μονοπατιού-διαδρομής (path) ώστε να δημιουργείται η ελάχιστη κατανάλωση ενέργειας. Αυτός ο τύπος πρωτοκόλλων διατηρεί νέες λίστες προορισμών και τις διαδρομές τους, διανέμοντας περιοδικά πίνακες δρομολόγησης σε όλο το δίκτυο. Τα κύρια μειονεκτήματα τέτοιων αλγορίθμων είναι: 1) Αντίστοιχη ποσότητα δεδομένων για συντήρηση και 2) αργή αντίδραση στην αναδιάρθρωση (όποτε χρειαστεί) όπως και ενδεχόμενες αστοχίες.

- **Υβριδικά πρωτόκολλα (hybrid protocols)**: Αυτά συνιστούν συνδυασμό των δύο παραπάνω κατηγοριών, συνδυάζοντας τα πλεονεκτήματα της προδραστικής και της αντιδραστικής δρομολόγησης. Η δρομολόγηση καθορίζεται αρχικά με κάποιες προοπτικές διαδρομές και στη συνέχεια η ζήτηση εξυπηρετείται από επιπλέον ενεργοποιημένους κόμβους. Η επιλογή της μίας ή της άλλης μεθόδου απαιτεί δράσεις εκ των προτέρων καθορισμού, ιδίως για τυπικές περιπτώσεις [30]. Τα κύρια μειονεκτήματα τέτοιων πρωτοκόλλων συνίστανται στα εξής: 1) Το «όποιο» ενδεχόμενο πλεονέκτημα εξαρτάται από τον αριθμό των άλλων εμπλεκόμενων κόμβων που ενεργοποιούνται στο ευρύτερο σύστημα και 2) η αντίδραση στη ζήτηση κίνησης εξαρτάται από τη διαβάθμιση του όγκου κίνησης.

2.4.2 Πρωτόκολλα βασιζόμενα στη Δομή του Δικτύου

Σε αυτή την τάξη πρωτοκόλλων ανήκουν οι οικογένειες των «οριζοντίων δρομολογήσεων» (flat routing), των «ιεραρχικών δρομολογήσεων» (hierarchical routing) ή cluster-based routing (δρομολογήσεις που βασίζονται σε συστάδες) και των «δρομολογήσεων που βασίζονται σε εντοπισμό θέσης» (location based routing).

2.4.2.1 Flat routing

Στα δίκτυα οριζόντιας δρομολόγησης κάθε κόμβος έχει τον ίδιο ρόλο με τους υπόλοιπους κόμβους και όλοι οι κόμβοι συνεργάζονται για να φέρουν εις πέρας μία κοινή αποστολή, η οποία συνίσταται στη μετάδοση του αρχικού μηνύματος. Τα δίκτυα οριζόντιας δρομολόγησης είναι κυρίως εκείνα που δεν λειτουργούν με προκαθορισμένη διάταξη και περίμετρο δικτύου. Επιτρέπουν την παράδοση πακέτων μεταξύ δρομολογητών μέσω οποιασδήποτε διαθέσιμης διαδρομής χωρίς να λαμβάνεται υπόψη η ιεραρχία, η διανομή και η σύνθεση του δικτύου. Το πρωτόκολλο δικτύων οριζόντιας δρομολόγησης εφαρμόζεται σε δίκτυα οριζόντιας δρομολόγησης όπου κάθε κόμβος δρομολογητή συλλέγει και διανέμει τις πληροφορίες δρομολόγησης με τους γειτονικούς του δρομολογητές. Ολόκληρος ο συμμετέχων κόμβος που αντιμετωπίζεται από το πρωτόκολλο οριζόντιας δρομολόγησης εκτελεί τον ίδιο ρόλο στον συνολικό μηχανισμό δρομολόγησης [31].

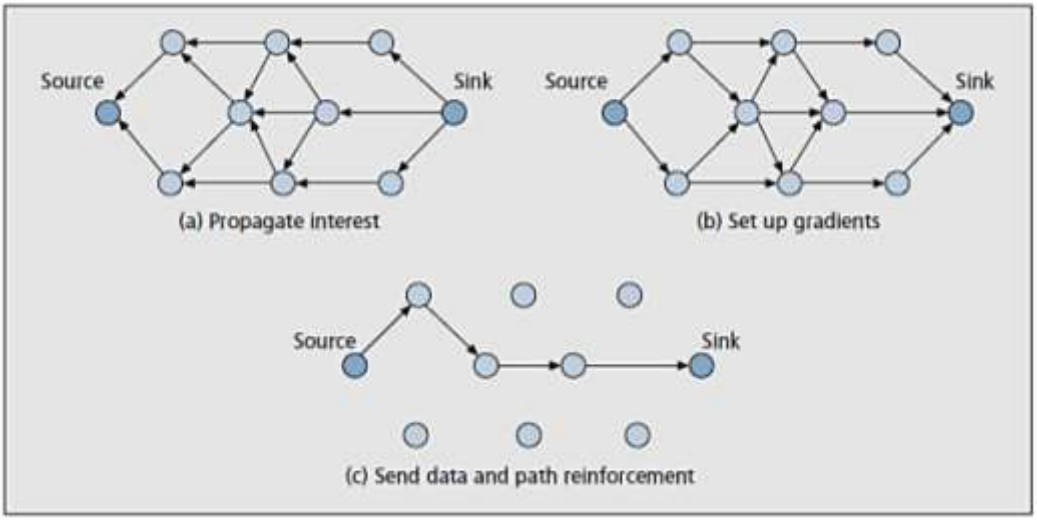
Το πρωτόκολλο δρομολόγησης πληροφοριών, το πρωτόκολλο δρομολόγησης εσωτερικής πύλης και το βελτιωμένο πρωτόκολλο δρομολόγησης εσωτερικής πύλης είναι δημοφιλή παραδείγματα πρωτοκόλλων οριζόντιας δρομολόγησης.

Σε αυτού του είδους τα πρωτόκολλα, η πληροφορία μεταδίδεται σε κάθε κόμβο, θεωρώντας πως όλοι οι κόμβοι είναι δυνητικοί σταθμοί βάσης. Έτσι, δίνεται η δυνατότητα στον χρήστη να αιτηθεί την πληροφορία από οποιονδήποτε κόμβο και να λάβει απάντηση άμεσα. Οι αρχικές προσεγγίσεις (π.χ. τα πρωτόκολλα SPIN (Sensor Protocols for Information via Negotiation) και Directed Diffusion) έδειξαν ότι η εξοικονόμηση ενέργειας μέσω της διαπραγμάτευσης των δεδομένων είναι εφικτή, εφόσον οι πλεονάζουσες πληροφορίες διαγράφονται κατόπιν της εκτέλεσης της εντολής από τον χρήστη [32].

Συνοπτικά περιγράφονται παρακάτω τα πιο σημαντικά πρωτόκολλα της κατηγορίας αυτής:

3. **SPIN (Sensor Protocols for Information via Negotiation - Πρωτόκολλα Αισθητήρων για Πληροφορίες μέσω Διαπραγμάτευσης)**: Οι κόμβοι που χρησιμοποιούν το πρωτόκολλο αυτό αναθέτουν ένα όνομα υψηλού επιπέδου στα μεταδεδομένα (meta-data) που συλλέγουν και διεξάγουν διαπραγματεύσεις, πριν αποσταλεί κάποια πληροφορία. Αυτό εξασφαλίζει ότι δεν θα υπάρχει πλεονάζουσα πληροφορία στο δίκτυο. Επιπλέον, το πρωτόκολλο έχει τη δυνατότητα πρόσβασης στις πληροφορίες του επιπέδου ενέργειας του κόμβου και με αυτό τον τρόπο είναι σε θέση ώστε να προσαρμόζει τη λειτουργία του, ανάλογα με την τιμή του αποθέματος. Η διαπραγμάτευση των μεταδεδομένων από το SPIN επιλύει κλασικά προβλήματα όπως είναι η παροχή περιττών πληροφοριών, η επικάλυψη περιοχών ανίχνευσης και η διαθεσιμότητα πόρων, επιτυγχάνοντας έτσι σημαντική ενεργειακή απόδοση.

4. **Κατευθυνόμενη διάχυση (directed diffusion)**: Η βασική ιδέα στην περίπτωση αυτή είναι ο συνδυασμός των δεδομένων που προέρχονται από διαφορετικές πηγές μέσα στη διαδρομή ή δια «ενδοδικτυακής συνάθροισης» (in-network aggregation) εξαλείφοντας έτσι την πλεονάζουσα πληροφορία και μειώνοντας το πλήθος των εκπομπών. Κατά αυτόν τον τρόπο μειώνονται οι απαιτήσεις κατανάλωσης ενέργειας και επιτυγχάνεται διεύρυνση του χρόνου ζωής του δικτύου [33].



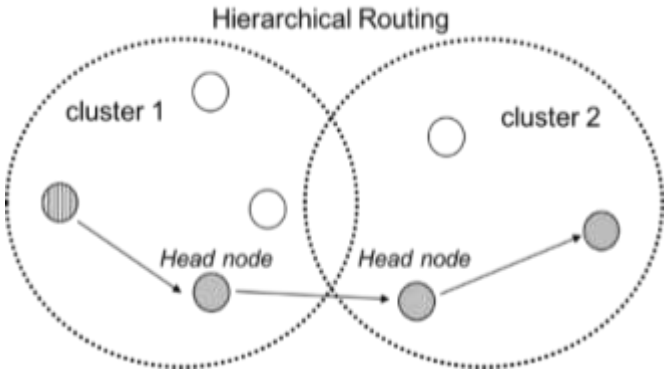
Εικόνα 2-5: Σχηματική παράσταση πρωτοκόλλου directed diffusion [35][2]

[2] Όπως φαίνεται στην Εικ.2-5, ο σταθμός βάσης αρχικά στέλνει το αίτημα για δεδομένα με ευρυεκπομπή (broadcast) που διαδίδεται με διαδικασία διαδοχικών αλμάτων (hop-by-hop). Κάθε κόμβος σημειώνει από ποιόν συγκεκριμένο κόμβο έλαβε το αίτημα, ώστε να επιστρέψει σε αυτόν τα δεδομένα όταν τα λάβει από κάποιον άλλο κόμβο (set up gradients). Έτσι δημιουργούνται «μονοπάτια» από τον προορισμό πίσω προς την πηγή του αιτήματος και επιλέγεται το καλύτερο εξ αυτών για να αποφευχθεί η πλημμύρα/υπερχείλιση πληροφοριών (flooding).

5. **Energy-Aware routing (δρομολόγηση με γνώση της ενέργειας)**: Στο πρωτόκολλο δρομολόγησης με γνώση της ενέργειας, ένας κόμβος με υψηλό λόγο της παραμένουσας ενέργειας (residual energy) προς τη μέση παραμένουσα ενέργεια όλων των γειτονικών κόμβων στο εύρος των συστάδων του, έχει μεγάλη πιθανότητα ώστε να καταστεί η «κεφαλή» της συστάδας (cluster head). Αυτό μπορεί να επιτρέψει καλύτερο χειρισμό στις ετερογενείς ενεργειακές περιστάσεις σε σχέση με τους υπάρχοντες αλγόριθμους συσταδοποίησης (clustering algorithms), οι οποίοι εκλέγουν την κεφαλή συστάδας μόνο με βάση την παραμένουσα ενέργεια ενός κόμβου. Μετά τη φάση σχηματισμού συστάδας, το πρωτόκολλο δρομολόγησης με γνώση της ενέργειας κατασκευάζει ένα ανοιγόμενο δέντρο (spanning tree) πάνω από το σύνολο των κεφαλών συστάδων. Μόνο ο ριζικός κόμβος (root node) αυτού του δέντρου μπορεί να επικοινωνήσει με τον κόμβο συγκέντρωσης δεδομένων (sink node) με επικοινωνία απλού άλματος (single-hop). Επειδή η ενέργεια που καταναλώνεται για όλες τις επικοινωνίες στο δίκτυο μπορεί να υπολογιστεί από το μοντέλο ελεύθερου χώρου (free space model), η ενέργεια θα εξοικονομηθεί σε μεγάλο επίπεδο, και αυτό οδηγεί σε μακροζωία του δικτύου των αισθητήρων [36].

2.4.2.2 Hierarchical network routing

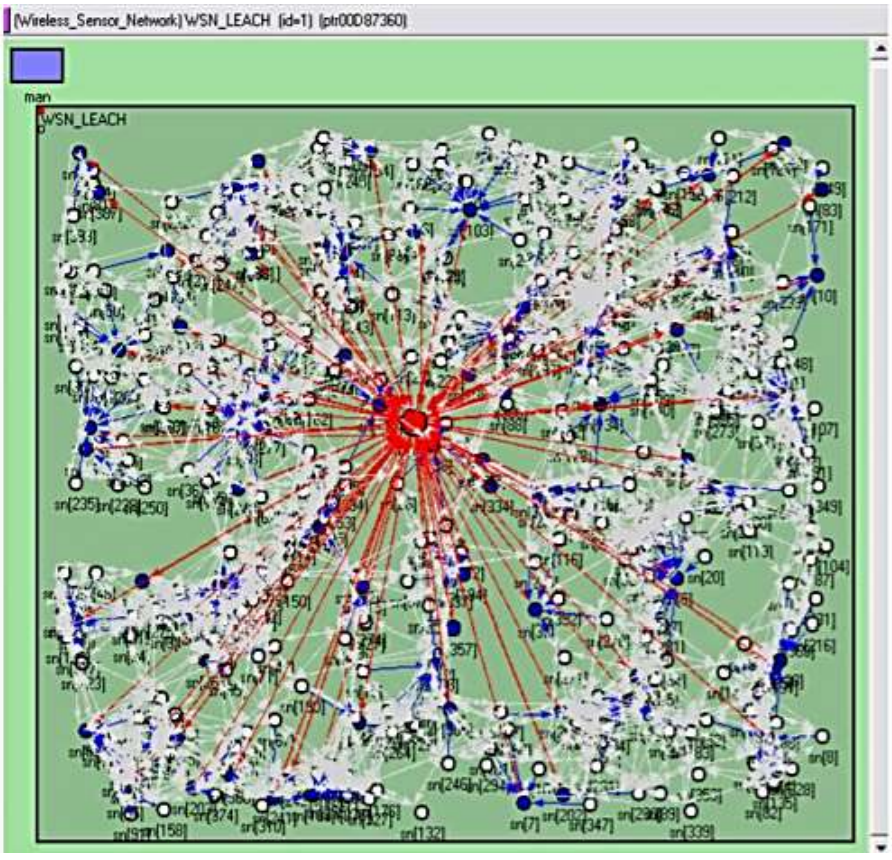
Οι τεχνικές ιεραρχικής δρομολόγησης δικτύου προτάθηκαν αρχικά για ενσύρματα δίκτυα και είναι γνωστές ως “cluster based” («βασιζόμενες σε συστάδες»), παρέχοντας σημαντικά πλεονεκτήματα σχετικά με την κλιμακοθετησιμότητα των δικτύων και τη συνεχή επικοινωνία [37]. Οι κόμβοι με υψηλά ενεργειακά αποθέματα διαχωρίζονται και χρησιμοποιούνται για να επεξεργαστούν και να στείλουν πληροφορίες, ενώ οι κόμβοι με χαμηλά ενεργειακά αποθέματα χρησιμοποιούνται μόνο για να λαμβάνουν πληροφορίες και για να τις μεταδίδουν στον σταθμό βάσης χρησιμοποιώντας την ελάχιστη δυνατή διαδρομή. Οι ομάδες των clusters (συστάδων) και ο ορισμός συγκεκριμένων διεργασιών στους επικεφαλής κόμβους έχει σημαντική συμβολή στο πώς κλιμακώνεται συνολικά το σύστημα, ο χρόνος ζωής και η χρήση της ενέργειας. Σε αυτό το σημείο, μέσω της ιεραρχικής δρομολόγησης μπορεί να γίνει μείωση της κατανάλωσης ενέργειας εντός της συστάδας, συγκεντρώνοντας και συγχωνεύοντας τα δεδομένα προκειμένου να μειωθούν τα μεταδιδόμενα πακέτα [39].



Εικόνα 2-6: Σχηματική παράσταση Hierarchical network routing [40]

Τα σημαντικότερα πρωτόκολλα τα οποία ανήκουν σε αυτή τη λειτουργική κατηγορία, συνοπτικά παρουσιάζονται παρακάτω:

1. **LEACH (Low Energy Adaptive Clustering – Προσαρμοστική Συσταδοποίηση Χαμηλής Ενέργειας)**: Το πρωτόκολλο LEACH χρησιμοποιεί τη λογική της διαχείρισης κατανεμημένων πληροφοριών στη συστάδα, επιλέγοντας αρχικά τυχαία ορισμένους κόμβους ως «επικεφαλής» και παρέχοντας εναλλάξ αυτόν τον ρόλο σε όλους τους κόμβους, ώστε να επιτευχθεί ομοιόμορφη κατανάλωση ενέργειας ανάμεσά τους. Το LEACH πραγματοποιεί περιοδική συλλογή δεδομένων από τους κόμβους, ενώ ελέγχονται κεντρικά οι συγκρούσεις μέσα σε μία συστάδα αλλά και μεταξύ των συστάδων.
   Συνεπώς, το πρωτόκολλο αυτό είναι κατάλληλο για εφαρμογές όπου απαιτείται συνεχής παρακολούθηση από το ασύρματο δίκτυο αλλά ο χρήστης δεν χρειάζεται άμεσα όλα τα πακέτα. Οι συχνές περιοδικές αποστολές ανούσιων πακέτων θα εξαντλούσαν τους ενεργειακούς πόρους, επομένως αυτό το πρωτόκολλο καθορίζει τον χρόνο μεταξύ δύο αποστολών και εναλλάσσει όλες τις κεφαλές των συστάδων.



Εικόνα 2-7: Λειτουργία πρωτοκόλλου LEACH σε ιεραρχική δρομολόγηση δικτύου [35]

2. **TEEN (Threshold – Sensitive Energy Efficient Protocol (Πρωτόκολλο ενεργειακής αποδοτικότητας με ευαισθησία ως προς το κατώφλι)):** Το πρωτόκολλο αυτό χρησιμοποιείται για εφαρμογές πραγματικού χρόνου (real-time applications) και εφαρμόζεται σε αντιδραστικά δίκτυα (reactive networks)[3]. Ο επικεφαλής κόμβος μίας συστάδας (cluster head) αποστέλλει στα μέλη της συστάδας ένα μήνυμα "hello" («χαιρετισμός») το οποίο συμπεριλαμβάνει ένα αυστηρό κατώφλι (hard threshold) και ένα ελαστικό κατώφλι (soft threshold). Όταν οι τιμές που λαμβάνουν οι κόμβοι βρίσκονται κοντά στην τιμή του αυστηρού κατωφλίου, τότε αυτοί ξεκινούν να αποστέλλουν πακέτα, μειώνοντας έτσι τις άσκοπες εκπομπές μεταξύ τους και του χρήστη. Με αυτό τον τρόπο, το TEEN χρησιμοποιεί το soft και hard threshold, που οδηγεί στη συνεχή παρακολούθηση ενός γεγονότος και επιπρόσθετα στη διατήρηση της ενέργειας και τη μείωση των εκπομπών [41].

3. **PEGASIS (Power – Efficient Gathering in Sensor Information Systems (Συλλογή με αποτελεσματικότητα ως προς την ισχύ, σε πληροφορικά συστήματα αισθητήρων)):** Το πρωτόκολλο αυτό αποτελεί εξέλιξη του LEACH ενώ η βασική ιδέα είναι ότι ένας κόμβος επιλέγεται ως επικεφαλής κόμβος ο οποίος στέλνει συγχωνευμένα δεδομένα στον σταθμό βάσης ανά γύρο επικοινωνίας. Ο επικεφαλής κόμβος επιλέγεται αναλόγως με την απόσταση από τον σταθμό βάσης, ενώ οι γειτονικοί κόμβοι αποστέλλουν δεδομένα μόνο σε αυτόν δημιουργώντας μία αλυσίδα επικοινωνίας. Επειδή απασχολούνται μόνο κοντινοί κόμβοι, μειώνεται εξαιρετικά το εύρος ζώνης και επίσης παρατείνεται σημαντικά η συνολική διάρκεια ζωής του δικτύου. Αν ένας κόμβος αποτύχει (π.χ. καταστραφεί), τότε το δίκτυο αναπροσαρμόζεται δημιουργώντας διαφορετική αλυσίδα επικοινωνίας. Το βασικό πλεονέκτημα του PEGASIS είναι η διπλάσια απόδοσή του σε πληθώρα μεγεθών δικτύου και τοπολογιών, αν και επιφέρεται καθυστέρηση στους απομακρυσμένους κόμβους στην αλυσίδα. Πρέπει να σημειωθεί, *επίσης*, ότι το σύνολο της κίνησης του δικτύου συνωστίζεται στον επικεφαλής κόμβο, το οποίο επίσης μπορεί να προκαλέσει την καθυστέρηση της μετάδοσης των δεδομένων [42].

	SPIN	LEACH	Directed Diffusion
Εύρεση βέλτιστης διαδρομής	Όχι	Όχι	Όχι
Διάρκεια ζωής δικτύου	Καλή	Πολύ καλή	Καλή
Διαχείριση πόρων	ΝΑΙ	ΝΑΙ	ΝΑΙ
Χρήση meta-data	ΝΑΙ	ΝΑΙ	ΝΑΙ

Πίνακας 2-1: Σύγκριση πρωτοκόλλων SPIN, LEACH & Directed Diffusion [43]

[3] Στη διαμόρφωση αντιδραστικού δικτύου, το σύστημα προσαρμόζεται αυτόματα σε οποιαδήποτε αλλαγή στην κατάσταση του δικτύου χωρίς να απαιτείται χειροκίνητη αναδιαμόρφωση. Για παράδειγμα, εάν η ενσύρματη διασύνδεση δικτύου αποσυνδεθεί ή εάν διατίθεται νέο ασύρματο δίκτυο, το σύστημα προσαρμόζεται με ανάλογο τρόπο.

Στην κατηγορία της ιεραρχικής δρομολόγησης, θα συναντήσουμε περισσότερα πρωτόκολλα λειτουργίας. Με κύριο άξονα την εξοικονόμηση ενέργειας, οι τεχνικές που χρησιμοποιούνται, παραλλάσσονται. Επιγραμματικά θα συναντήσουμε τα εξής [44]:

- **SMECN** (Small minimum energy communication network – μικρό, ελάχιστης ενέργειας, δίκτυο επικοινωνίας) - το SMECN λειτουργεί υπό την υπόθεση πως οι κόμβοι μπορεί να έχουν εμπόδια μεταξύ τους ενώ το δίκτυο διατηρεί τη σύνδεσή του.

- **SOP** (Self-organizing protocol – πρωτόκολλο υποκείμενο σε αυτο-οργάνωση), όπου διατίθενται κινητοί ή στάσιμοι ανομοιογενείς αισθητήρες. Ορισμένοι κόμβοι θα εξετάσουν το περιβάλλον και θα προωθήσουν τα δεδομένα στους δρομολογητές, οι οποίοι είναι στάσιμοι κόμβοι που λειτουργούν ως το backbone network (δίκτυο κορμού) της επικοινωνίας και οι οποίοι παρέχουν τα δεδομένα σε sink nodes (αποδέκτες κόμβους).

- **TTDD** (Two-tier data dissemination – διάχυση δεδομένων δύο σειρών-επιπέδων). Κατά την ανίχνευση ενός ερεθίσματος (διέγερσης - stimulus), αντί να περιμένει παθητικά τα ερωτήματα (queries) από τους αποδέκτες, η πηγή δεδομένων χτίζει προληπτικά μία δομή πλέγματος σε όλο το πεδίο και ρυθμίζει τις πληροφορίες προώθησης στους αισθητήρες που βρίσκονται πιο κοντά στα σημεία του πλέγματος [46].

Τα πρωτόκολλα της οριζόντιας δρομολόγησης σε σχέση με τα ιεραρχικά πρωτόκολλα διαφέρουν σε σημεία τα οποία αναγράφονται στον παρακάτω πίνακα:

Flat Routing	Hierarchical Routing
Παρουσία συγκρούσεων επίβαρου (overhead)	Αποφυγή συγκρούσεων
Ο κόμβος συναθροίζει τα εισερχόμενα δεδομένα από τους γείτονες	Συνάθροιση δεδομένων από τους επικεφαλής των συστάδων
Βέλτιστη δρομολόγηση με επιπρόσθετη πολυπλοκότητα	Απλή αλλά όχι βέλτιστη δρομολόγηση
Επί τόπου συνδέσεις χωρίς συγχρονισμό	Απαιτείται καθολικός συγχρονισμός
Κατανάλωση ενέργειας εξαρτώμενη από τον τύπο κίνησης	Ομοιόμορφη κατανάλωση ενέργειας
Κατανάλωση ενέργειας προσαρμοζόμενη στον τύπο κίνησης	Μη ελεγχόμενη κατανάλωση ενέργειας
Μη συμμετρική κατανομή καναλιών	Δίκαιη και συμμετρική κατανομή καναλιών

Πίνακας 2-2: Σύγκριση hierarchical και flat routing [47]

2.4.2.3 Δρομολόγηση που βασίζεται σε Εντοπισμό Θέσης

Σε αυτή την κατηγορία πρωτοκόλλων δρομολόγησης, η σχέση επικοινωνίας μεταξύ των κόμβων και του χρήστη καθορίζεται από την τοποθεσία. Η απόσταση μεταξύ των γειτονικών κόμβων εκτιμάται σύμφωνα με την ισχύ των εισερχόμενων σημάτων, ενώ σχετικές συντεταγμένες αποκτώνται με ανταλλαγή πληροφοριών μεταξύ των γειτόνων. Εναλλακτικά, η θέση των κόμβων μπορεί να είναι απευθείας διαθέσιμη μέσω επικοινωνίας με δορυφόρο την οποία προσδίδει η ενσωματωμένη μονάδα GPS (Παγκόσμιο Σύστημα Εντοπισμού Θέσης).

Στην περίπτωση της απευθείας δήλωσης συντεταγμένων από τους κόμβους, για την εξοικονόμηση ενέργειας χρησιμοποιείται σε αρκετά σχήματα η περιοδική λειτουργία “sleep” («ύπνος») η οποία καθιστά τον κόμβο σε κατάσταση μειωμένης κατανάλωσης όταν αυτός δεν καλείται να επικοινωνήσει. Συνοπτικά παρουσιάζονται τα παρακάτω ([49], [50]):

1. **GAF (Geographic Adaptive Fidelity – Γεωγραφική Προσαρμοσμένη Πιστότητα)**: Βασισμένο στη θέση των κόμβων, το πρωτόκολλο σχεδιάστηκε αρχικά για δίκτυα κινητής τηλεφωνίας και έπειτα εφαρμόστηκε σε WSNs. Η δικτυωμένη περιοχή χωρίζεται σε καθορισμένες ζώνες οι οποίες διαμορφώνουν ένα εικονικό πλέγμα, όπου μέσα σε αυτό ο κάθε κόμβος καλείται να επιτελέσει έναν συγκεκριμένο ρόλο [48]. Κάθε κόμβος χαρακτηρίζεται από τη θέση του στο GPS σύμφωνα με τις μοναδικές του συντεταγμένες. Οι κοντινοί του κόμβοι οι οποίοι βρίσκονται μέσα στην ίδια προκαθορισμένη ζώνη, τίθενται σε λειτουργία “sleep”. Έτσι εξοικονομείται σημαντική ενέργεια, ενώ ταυτόχρονα το πρωτόκολλο δίνει τη δυνατότητα υλοποίησης τόσο σε σταθερούς όσο και σε κινούμενους κόμβους.

2. **GEAR (Geographic and Energy Aware Routing – Γεωγραφική και με Γνώση της Ενέργειας Δρομολόγηση):** Βασική ιδέα του πρωτοκόλλου είναι η χρήση γεωγραφικών πληροφοριών κατά τη διασπορά αιτημάτων σε μεγάλες γεωγραφικές περιοχές. Το πρωτόκολλο μπορεί να μειώσει το πλήθος των εκπομπών DD (Directed Diffusion) προσπαθώντας να περιορίσει τις εκπομπές σε μία συγκεκριμένη γεωγραφική περιοχή και όχι σε ολόκληρο το δίκτυο. Η απόδοση του GEAR είναι πολύ καλή σε σύγκριση με παρόμοια πρωτόκολλα τα οποία δεν λαμβάνουν υπόψη τους τα διάφορα ενεργειακά θέματα που προκύπτουν.

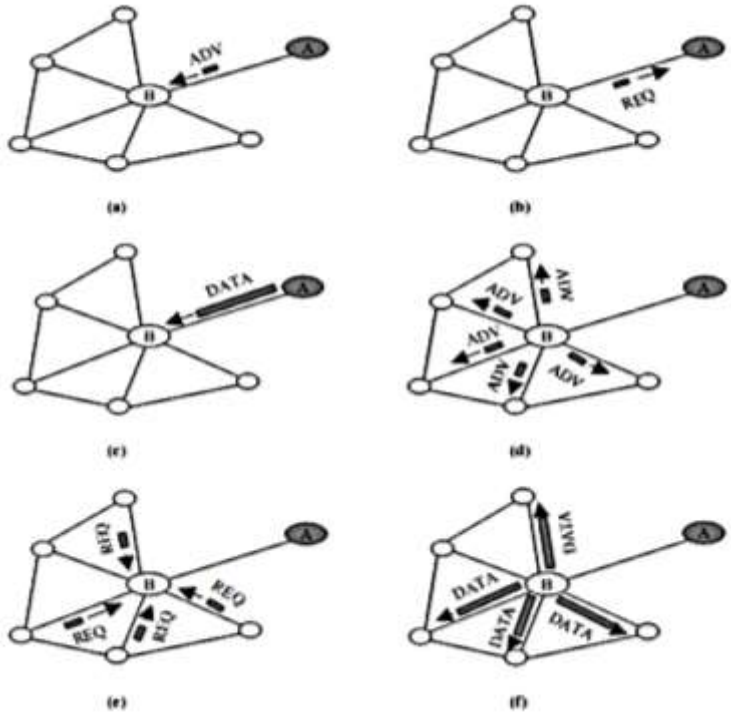
3. **SPAN** (Switch Port Analyzer – Αναλύτης Θύρας Μεταγωγέα)**:** Το πρωτόκολλο αυτό βασίζεται στη γεωγραφική θέση των κόμβων, ενώ επιλέγει κάποιους ως συντονιστές, με βάση τη θέση αυτή. Οι συντονιστές κόμβοι αποτελούν τον «κορμό» της επικοινωνίας καθώς προωθούν τα μηνύματα στο υπόλοιπο δίκτυο, εάν δύο γείτονες δεν μπορούν να επικοινωνήσουν μεταξύ τους ή μέσω άλλων. Ωστόσο, το γεγονός αυτό καθιστά τη σχεδίαση λιγότερο αποδοτική ως προς την κατανάλωση ενέργειας, εξαιτίας της ανάγκης για να διατηρούνται οι θέσεις των συντονιστών [51].

2.4.2.4 Πρωτόκολλα Προσανατολισμένα στις Λειτουργίες

Τα πρωτόκολλα αυτής της κατηγορίας χρησιμοποιούν πολλαπλά μονοπάτια αντί για μία συγκεκριμένη διαδρομή, με στόχο την αύξηση της αξιοπιστίας του δικτύου. Η ανοχή ενός πρωτοκόλλου στα σφάλματα μετράται σύμφωνα με την πιθανότητα να υπάρχει εναλλακτικό μονοπάτι μεταξύ πηγής και προορισμού, σε περίπτωση που το βασικό μονοπάτι τυχόν καταρρεύσει. Σε αυτού του είδους τα πρωτόκολλα, τα πολλαπλά μονοπάτια μένουν ενεργά μέσω της αποστολής συνεχών μνημάτων “hello”.

2.4.2.4.1 Πρωτόκολλα Δρομολόγησης που βασίζονται σε Διαπραγματεύσεις

Αυτά τα πρωτόκολλα χρησιμοποιούν υψηλού επιπέδου αναλυτές δεδομένων, ώστε να εξαλείψουν τις περιττές μεταδόσεις. Οι σχέσεις επικοινωνίας καθορίζονται σύμφωνα με τους διαθέσιμους πόρους. Το πιο γνωστό πρωτόκολλο αυτής της κατηγορίας είναι το πρωτόκολλο SPIN (Sensor Protocol for Information via Negotiation), το οποίο είναι σχεδιασμένο έτσι ώστε να διασπείρει τα δεδομένα από τον ένα κόμβο στον άλλο, θεωρώντας ότι κάθε κόμβος είναι ουσιαστικά ένας σταθμός βάσης. Συνεπώς, το αποτέλεσμα έγκειται στη μείωση της διπλότυπης πληροφορίας, διεξάγοντας μία σειρά από μηνύματα διαπραγμάτευσης πριν τα πραγματικά δεδομένα αποσταλούν [52].



Εικόνα 2-8: Συνοπτική λειτουργία πρωτοκόλλου SPIN-PP[4]

[4] Ο κόμβος A ξεκινά αποστέλλοντας τα δεδομένα του στον κόμβο B (a). Ο κόμβος B αποκρίνεται αποστέλλοντας ένα αίτημα στον κόμβο A (b). Αφού λάβει τα ζητούμενα δεδομένα (c), ο κόμβος B στέλνει στη συνέχεια αιτήσεις στους γείτονές του (d), οι οποίοι με τη σειρά τους στέλνουν αιτήματα πίσω στο B (e, f) [53].

2.4.2.4.2 Πρωτόκολλα Δρομολόγησης Πολλαπλών Διαδρομών

Τα πρωτόκολλα δρομολόγησης πολλαπλών διαδρομών παρέχουν διαφορετικές (πολλαπλές) διαδρομές για να φτάσουν τα δεδομένα στον προορισμό τους, παρέχοντας ως αποτέλεσμα την εξισορρόπηση φόρτου, τη χαμηλή καθυστέρηση και τη βελτιωμένη απόδοση δικτύου. Το πρωτόκολλο πολλαπλής δρομολόγησης παρέχει επίσης εναλλακτικές διαδρομές σε περίπτωση αποτυχίας οποιασδήποτε διαδρομής. Τα πυκνά δίκτυα ασύρματων αισθητήρων βασίζονται συνήθως σε πρωτόκολλα πολλαπλών διαδρομών. Για να διατηρηθούν τα μονοπάτια ενεργά, ένα είδος περιοδικών μηνυμάτων πρέπει να αποστέλλεται σε συγκεκριμένα χρονικά διαστήματα, επομένως η δρομολόγηση πολλαπλών διαδρομών δεν είναι ενεργειακά αποδοτικότερη. Τα πρωτόκολλα δρομολόγησης πολλαπλών διαδρομών είναι: 1) Multi path and Multi SPEED (MMSPEED) και 2) Sensor protocols for information via negotiation (SPIN) [54].

2.4.2.4.3 Πρωτόκολλα Δρομολόγησης που βασίζονται σε Ερωτήματα

Σε αυτό το είδος δρομολόγησης, οι κόμβοι προορισμού διαδίδουν μέσω του δικτύου ένα αίτημα δεδομένων. Ο κόμβος που μπορεί να ανταποκριθεί στο αίτημα, σύμφωνα με κριτήρια κατανάλωσης ενέργειας και αξιοπιστίας, απαντά προσφέροντας τα ζητούμενα δεδομένα. Κάθε γείτονας κόμβος διατηρεί μία λίστα με τους δικούς του γείτονες κόμβους και έναν πίνακα γεγονότων ο οποίος ανανεώνεται κάθε φορά που συμβαίνει ένα γεγονός. Με αυτόν τον τρόπο, το δίκτυο «μαθαίνει» ώστε να διαχειρίζεται τις ανάγκες ανταλλαγής πληροφοριών σύμφωνα με τις συντομότερες διαδρομές στο χρόνο. Εάν για κάποιο γεγονός δεν έχει δημιουργηθεί προηγούμενο μονοπάτι, τότε ο κόμβος μεταδίδει το αίτημα τυχαία προς όλες τις κατευθύνσεις και, εάν δεν πληροφορηθεί ότι το πακέτο έφτασε σε προκαθορισμένο χρόνο, τότε συμβαίνει κατάσταση υπερχείλισης-πλημμύρας (flooding) του δικτύου.

2.4.2.4.4 Πρωτόκολλα Δρομολόγησης που βασίζονται σε QoS

Στην κατηγορία αυτή, το δίκτυο πρέπει να «ισορροπήσει» μεταξύ της κατανάλωσης ενέργειας και της ποιότητας των υπηρεσιών (Quality of Service - QoS) που προσφέρονται στον χρήστη. Πιο συγκεκριμένα, το δίκτυο πρέπει να ικανοποιήσει παραμέτρους που έχουν τεθεί από τη μεριά του πελάτη και οι οποίες μπορεί να σχετίζονται με την καθυστέρηση, την κατανάλωση ενέργειας και την συντήρηση, το εύρος ζώνης κτλ.

Το πρωτόκολλο **SAR (Sequential Assignment Routing – Δρομολόγηση Ακολουθιακής Εκχώρησης)** είναι από τα πρώτα πρωτόκολλα δρομολόγησης για τα WSNs που εισάγουν την έννοια του QoS στις αποφάσεις δρομολόγησης. Σε αυτή την περίπτωση, μία διαδρομή εξαρτάται από τρεις παράγοντες, ήτοι: τους ενεργειακούς πόρους, την QoS και την προτεραιότητα του πακέτου. Χρησιμοποιείται προσέγγιση πολλαπλής διαδρομής για να αποφευχθεί η αποτυχία μίας μόνο διαδρομής, βάσει της οποίας δομείται κατόπιν των αποφάσεων του δικτύου μία δενδροειδής διαδρομή από τον αρχικό κόμβο έως τον σταθμό βάσης. Τα μονοπάτια του δέντρου δημιουργούνται έτσι ώστε να αποφεύγουν κόμβους με χαμηλή ενέργεια ή με χαμηλή εγγύηση QoS. Έτσι το SAR καθίσταται εν τέλει ένα πρωτόκολλο που στοχεύει στην αποδοτική λειτουργία ως προς την ενέργεια και στην ανοχή σε σφάλματα [55].

Άλλα ανάλογα πρωτόκολλα της κατηγορίας αυτής είναι τα **DSR**, **AODV** και **SPEED**.

Το **Dynamic Source Routing (DSR)** (Δυναμική Δρομολόγηση Πηγής) είναι ένα πρωτόκολλο δρομολόγησης για ασύρματα δίκτυα πλέγματος που σχηματίζει μία διαδρομή κατ' απαίτηση, όταν ένας κόμβος μετάδοσης ζητά μία τέτοια διαδρομή. Ωστόσο, χρησιμοποιεί τη δρομολόγηση πηγής αντί να βασίζεται στον πίνακα δρομολόγησης σε κάθε ενδιάμεση συσκευή [56].

Το **Ad hoc On-Demand Distance Vector (AODV) Routing** (Ειδικού Σκοπού Δρομολόγηση Διανυσματικής Απόστασης Κατ' Απαίτηση) είναι ένα πρωτόκολλο δρομολόγησης για κινητά ad hoc δίκτυα ("Mobile ad-hoc Networks" - MANETs) και άλλα ασύρματα ad hoc δίκτυα. Μπορεί να είναι αντιδραστικό ή προδραστικό. Επιτρέπει τη συντήρηση ενεργών διαδρομών και παρέχει επικοινωνία unicast (μονοεκπομπής) και multicast (πολυεκπομπής) [57].

Το **SPEED** είναι ένα πολύ αποτελεσματικό και επεκτάσιμο πρωτόκολλο για δίκτυα αισθητήρων όπου οι πόροι κάθε κόμβου είναι λιγοστοί. Είναι ειδικά προσαρμοσμένο να είναι ένας άπατρις, τοπικός αλγόριθμος με ελάχιστο γενικό έλεγχο [58].
Συνοψίζοντας, στους παρακάτω πίνακες μπορούμε να παρατηρήσουμε συγκεντρωτικά τα σημαντικότερα πρωτόκολλα σύμφωνα με την [59].

Πρωτόκολλο (Protocol)	**Ταξινόμηση (Classification)**	**Χρήση ενέργειας**	**Συνάθροιση δεδομένων (Data Aggregation)**	**Κλιμακοθετησιμότητα (Scalability)**	**Ποιότητα υπηρεσιών (QoS)**
SPIN	Οριζόντια / Πραγματοποιήθηκε από πηγή / Κεντρικά δεδομένα	Περιορισμένη	Ναι	Περιορισμένη	Όχι
DD	Οριζόντια / Πραγματοποιήθηκε από πηγή / Κεντρικά δεδομένα	Περιορισμένη	Ναι	Περιορισμένη	Όχι
LEACH	Ιεραρχική / Κεντρικός κόμβος	Υψηλή	Ναι	Καλή	Όχι
TEEN	Ιεραρχική	Υψηλή	Ναι	Καλή	Όχι
PEGASIS	Ιεραρχική	Μέγιστη	Όχι	Καλή	Όχι
VGA	Ιεραρχική	Χαμηλή	Ναι	Καλή	Όχι
SOP	Ιεραρχική	Χαμηλή	Όχι	Καλή	Όχι
GAF	Ιεραρχική / Με βάση τη θέση	Περιορισμένη	Όχι	Καλή	Όχι
SPAN	Ιεραρχική / Με βάση τη θέση	Περιορισμένη	Ναι	Περιορισμένη	Όχι
GEAR	Με βάση τη θέση	Περιορισμένη	Όχι	Περιορισμένη	Όχι
SAR	Επικεντρωμένη στα δεδομένα	Υψηλή	Ναι	Περιορισμένη	Ναι
SPEED	Επικεντρωμένη στα δεδομένα και την θέση	Χαμηλή	Όχι	Περιορισμένη	Ναι

Πίνακας 2-3: Κατηγορίες και ταξινόμηση δημοφιλέστερων πρωτοκόλλων WSN [59]

Τύπος εφαρμογής	Τοπολογία	Μέγεθος συστάδας (κόμβοι)	Πρωτόκολλο δρομολόγησης
Παρακολούθηση βιοτόπων	Κεφαλή συστάδας	10-100	SPAN, GAF
Περιβαλλοντική παρακολούθηση	Πολλαπλών αλμάτων / πολλαπλών διαδρομών	30-50	DD
Υγείας	Κεφαλή συστάδας	100	LEACH
	Star (αστέρας)	10-20	SAR, SPEED
Στρατιωτική	Πολλαπλών αλμάτων	200	GAF
Οικιακή/Γραφείου	Τριών Βαθμίδων	20-100	TEEN, GEAR
Παραγωγής/Εμπορική	Τριών Βαθμίδων	55	SAR

Πίνακας 2-4: Επιλογή πρωτοκόλλου σύμφωνα με την εφαρμογή [59]

2.4.3 Ποιότητα Υπηρεσίας και Παράμετροι Βελτίωσης

Η Διεθνής Ένωση Τηλεπικοινωνιών (International Telecommunication Union - ITU) ορίζει την ποιότητα υπηρεσίας (Quality of Service) ως το «σύνολο μίας τηλεπικοινωνιακής υπηρεσίας που φέρει την ικανότητά να ικανοποιεί τις απαιτούμενες ανάγκες του χρήστη» [60] και την ταξινομεί σε δύο βασικές κατηγορίες, ήτοι:
α) Την προσανατολισμένη στις ανάγκες της εκάστοτε εφαρμογής, και
β) την προσανατολισμένη στις ανάγκες του δικτύου.

Οι προκλήσεις που εμπλέκονται στην επίτευξη ποιότητας υπηρεσίας στα δίκτυα ασυρμάτων αισθητήρων εστιάζονται σε παραμέτρους όπως η ελαχιστοποίηση της κατανάλωσης ενέργειας, η ελαχιστοποίηση των συγκρούσεων στα πρωτόκολλα που βασίζονται στην διαπραγμάτευση και στην προσαρμογή των χρονικών θυρίδων σε πρωτόκολλα βασισμένα στον προγραμματισμό και η ελαχιστοποίηση των παρεμβολών. Ο μηχανισμός ποιότητας υπηρεσίας στα WSNs περιλαμβάνει την προσαρμογή του δικτύου, τον έλεγχο ισχύος, τον έλεγχο σφαλμάτων και την παρεχόμενη υπηρεσία. Το δίκτυο θα πρέπει να είναι σε θέση να παρέχει την απαιτούμενη ποιότητα υπηρεσίας η οποία εξαρτάται από τις απαιτήσεις των εφαρμογών. Λαμβάνοντας υπόψη αυτή τη συνθήκη, θα πρέπει να σημειωθεί ότι τα δίκτυα αισθητήρων καλύπτουν υπηρεσίες και δεδομένα διαφορετικής σημασίας που πρέπει, *αναλόγως της κρισιμότητας*, να ικανοποιούνται στο ακέραιο από το υποκείμενο δίκτυο.

Οι παράμετροι που θα πρέπει να λαμβάνονται υπόψη για την επίτευξη της ποιότητας υπηρεσίας, συνοπτικά θα πρέπει να είναι οι εξής [61]:

1. **Ελαχιστοποίηση της κατανάλωσης ενέργειας**: Η ελαχιστοποίηση της κατανάλωσης ενέργειας είναι σημαντική, λόγω της περιορισμένης ενεργειακής αυτονομίας των κόμβων αισθητήρων. Η κατανάλωση ενέργειας μπορεί να ελαχιστοποιηθεί αποφεύγοντας τις συγκρούσεις των δεδομένων και την ανάγκη αναμετάδοσης.

2. **Ελαχιστοποίηση της καθυστέρησης:** Η μείωση της καθυστέρησης από άκρο-σε-άκρο (end-to-end - E2E) μεταξύ κόμβου αισθητήρα και επικεφαλής κόμβου είναι σημαντική. Η μέση καθυστέρηση πρόσβασης μπορεί να ελαχιστοποιηθεί, βελτιστοποιώντας το μονοπάτι μετάδοσης της πληροφορίας από άκρο σε άκρο.

3. **Ελαχιστοποίηση παρεμβολών:** Δεδομένου ότι το ασύρματο μέσο είναι ένα κοινόχρηστο μέσο, υπάρχει πιθανότητα οι ανεπιθύμητες μεταδόσεις να προκαλέσουν παρεμβολές στην προβλεπόμενη μετάδοση. Οι παρεμβολές προκαλούν απώλειες πακέτων και επηρεάζουν στοιχεία όπως η απόδοση, η καθυστέρηση και η κατανάλωση ενέργειας. Οι παρεμβολές μπορούν να ελαχιστοποιηθούν μέσω της προσαρμογής του πλαισίου όπου ένας κόμβος μπορεί να επιχειρήσει πρόσβαση στο κοινόχρηστο μέσο, της βελτιστοποίησης του χρονισμού και της ρύθμισης της ισχύος εκπομπής.

4. **Κλιμακοθετησιμότητα (scalability):** Σε ένα δίκτυο αισθητήρων είναι γνωστό ότι οι κόμβοι ενδέχεται αδρανοποιηθούν και να τεθούν εκτός δικτύου, λόγω της πεπερασμένης τους ενεργειακής ικανότητας. Επομένως, πρέπει να λαμβάνεται σοβαρά υπόψη η ανάγκη προσαρμοστικών ενεργειών που επαφίενται στη δυναμική του δικτύου σε δεδομένη χρονική στιγμή.

2.5 Έλεγχος και Διαχείριση WSNs

Η βέλτιστη διαχείριση των πόρων και της λειτουργίας ενός WSN συναντάται στην βιβλιογραφία υπό τον όρο «υπηρεσίες δικτύου» (network services). Πρόκειται για υπηρεσίες που συντονίζουν και ελέγχουν τη λειτουργία των κόμβων, αντιμετωπίζοντας και επιλύοντας ζητήματα κρίσιμης σημασίας για τη λειτουργία των δικτύων WSN, όπως:

Προσδιορισμός θέσης των κόμβων (Localization): Στα δίκτυα WSN, οι κόμβοι που αναπτύσσονται στο πεδίο με ειδικό σκοπό (ad hoc) δεν έχουν εκ των προτέρων γνώση της θέσης τους. Οι υπάρχουσες μέθοδοι προσδιορισμού της θέσης περιλαμβάνουν χρήση GPS, χρήση κόμβων «φάρων» (“beacons”) ή «αγκυρών» (“anchors”) και εντοπισμό θέσης με βάση την εγγύτητα ως προς άλλους κόμβους γνωστής θέσης, ενώ σε επίπεδο λογισμικού αξιοποιούνται αλγόριθμοι για τον εντοπισμό της θέσης των κόμβων.

Συγχρονισμός των κόμβων του δικτύου (Synchronization): Ο συγχρονισμός σε ένα δίκτυο WSN είναι σημαντικός για την επιτυχή δικτύωση και για την εξοικονόμηση ενέργειας. Ο συγχρονισμός επιτρέπει στους κόμβους να συνεργάζονται αλλά και να μεταδίδουν δεδομένα σύμφωνα με ένα χρονικό προγραμματισμό γεγονότων και πληροφοριών.

Κάλυψη της περιοχής ενδιαφέροντος (Coverage): Η ανάπτυξη των αισθητήρων και η παρεχόμενη κάλυψη εξαρτώνται από τις απαιτήσεις της εφαρμογής. Συγκεκριμένα, η εξάρτηση αυτή αφορά στο κατά πόσο το υπό ανάπτυξη δίκτυο είναι στατικό (σταθεροί, μόνιμα τοποθετημένοι κόμβοι) ή κινητό (δυνατότητα κίνησης των κόμβων σε ένα δυναμικό περιβάλλον από πλευράς κάλυψης). Η πολυπλοκότητα που εισάγει σε ένα δίκτυο WSN η κινητικότητα των κόμβων είναι μεγάλη, τόσο σε φυσικό επίπεδο (δυνατότητες κίνησης - εποχούμενοι κόμβοι) όσο και σε επίπεδο αλγορίθμων. Η ρευστή τοπολογία του δικτύου επηρεάζει την κάλυψη, τη συνδεσιμότητα, τη διανομή και την προώθηση των δεδομένων.

Ασφάλεια δεδομένων και επικοινωνιών του δικτύου (Security): Η ασφάλεια αποτελεί κρίσιμο αντικείμενο στη σχεδίαση ενός δικτύου WSN, καθώς σε πολλές εφαρμογές θεωρείται σημαντική η αντιμετώπιση καταστάσεων όπως π.χ. η διακινδύνευση ακεραιότητας δεδομένων, οι υποκλοπές και παρεμβολές μεταδιδόμενης πληροφορίας, η είσοδος στο σύστημα μετάδοσης ψεύτικων μηνυμάτων πληροφορίας και η απώλεια πόρων του δικτύου.

Συνάθροιση των δεδομένων (Data Aggregation): Οι τεχνικές συνάθροισης και συμπίεσης δεδομένων αποσκοπούν στη μείωση του κόστους επικοινωνίας, στη βελτίωση της αξιοπιστίας της παρεχόμενης υπηρεσίας και στην εξοικονόμηση ενέργειας στο δίκτυο. Με τον όρο «συνάθροιση δεδομένων» εννοούμε τον συνδυασμό δεδομένων, προερχόμενων από πολλαπλούς αισθητήριους κόμβους, σε ένα κόμβο του δικτύου WSN ή στον επικεφαλής κόμβο μίας συστάδας. Η τεχνική συμπίεσης δεδομένων, περιλαμβάνει τη διαδικασία συμπίεσης του μεγέθους των δεδομένων στον αισθητήριο κόμβο και εν συνεχεία αποσυμπίεση, η οποία λαμβάνει χώρα στον σταθμό βάσης.

Ανοχή σε σφάλματα (fault tolerance): Σε ένα δίκτυο WSN με μεγάλο αριθμό κόμβων, είναι πιθανό κάποιοι κόμβοι να οδηγηθούν σε σφάλματα (απώλεια ή αλλοίωση πακέτων δεδομένων). Παράγοντες που οδηγούν σε σφάλματα είναι μεταξύ άλλων η έλλειψη ενέργειας, η φυσική καταστροφή κόμβων, παρεμβολές από γειτονικούς κόμβους και δυσμενείς συνθήκες περιβάλλοντος. Η αξιοπιστία του δικτύου πρέπει να διασφαλίζεται με την ανοχή τέτοιου είδους σφαλμάτων, δηλαδή η λειτουργία του δικτύου θα πρέπει να παραμένει ανεπηρέαστη από σφάλματα. Εάν αυτά εμφανιστούν σε κάποιο κρίσιμο αριθμό κόμβων, τότε είναι αναγκαία η μέριμνα των πρωτοκόλλων δρομολόγησης ώστε να καθορίσουν νέες διαδρομές δρομολόγησης για τη μετάδοση και προώθηση των δεδομένων προς τον σταθμό βάσης.

Δυνατότητα κλιμακοθετησιμότητας - Επεκτασιμότητα (Scalability): Χαρακτηριστικό των δικτύων WSN είναι το μεγάλο πλήθος κόμβων οι οποίοι μπορεί να είναι εκατοντάδες, χιλιάδες ή και περισσότεροι. Τα εφαρμοζόμενα πρωτόκολλα, σε κάθε εφαρμογή, οφείλουν να είναι σε θέση ώστε να διαχειρίζονται τόσο το μεγάλο πλήθος κόμβων όσο και τη μεγάλη χωρική πυκνότητα που ενδεχομένως μπορεί να εμφανίζεται. Επίσης, το δίκτυο θα πρέπει να προσφέρει τη δυνατότητα ανάπτυξης και επέκτασης, εάν σε αυτό πρέπει να προστεθούν περισσότεροι κόμβοι, χωρίς να αλλοιωθούν τα δομικά χαρακτηριστικά του.

Ποιότητα της Υπηρεσίας (Quality of Service – QoS): Τα δομικά στοιχεία ενός δικτύου οφείλουν να καλύπτουν τις απαιτήσεις ποιότητας του τελικού χρήστη, κάτι που αποτελεί βασική μέριμνα του σχεδιαστή του δικτύου. Ειδικότερα σε δίκτυα WSN, οι απαιτήσεις ποιότητας μπορούν να επικεντρώνονται σε θέματα ακρίβειας δεδομένων, καθυστέρησης μετάδοσης, συνάθροισης δεδομένων, ανοχής σφαλμάτων και κατανάλωσης ενέργειας.

Η διαχείριση πολλαπλών σταθμών βάσης είναι πρόκληση σε θέματα διασφάλισης ποιότητας της υπηρεσίας και το δίκτυο πρέπει να είναι σε θέση να υποστηρίζει διαφοροποιημένα επίπεδα QoS, ιδίως σε περίπτωση δικτύων με πολλά τερματικά.

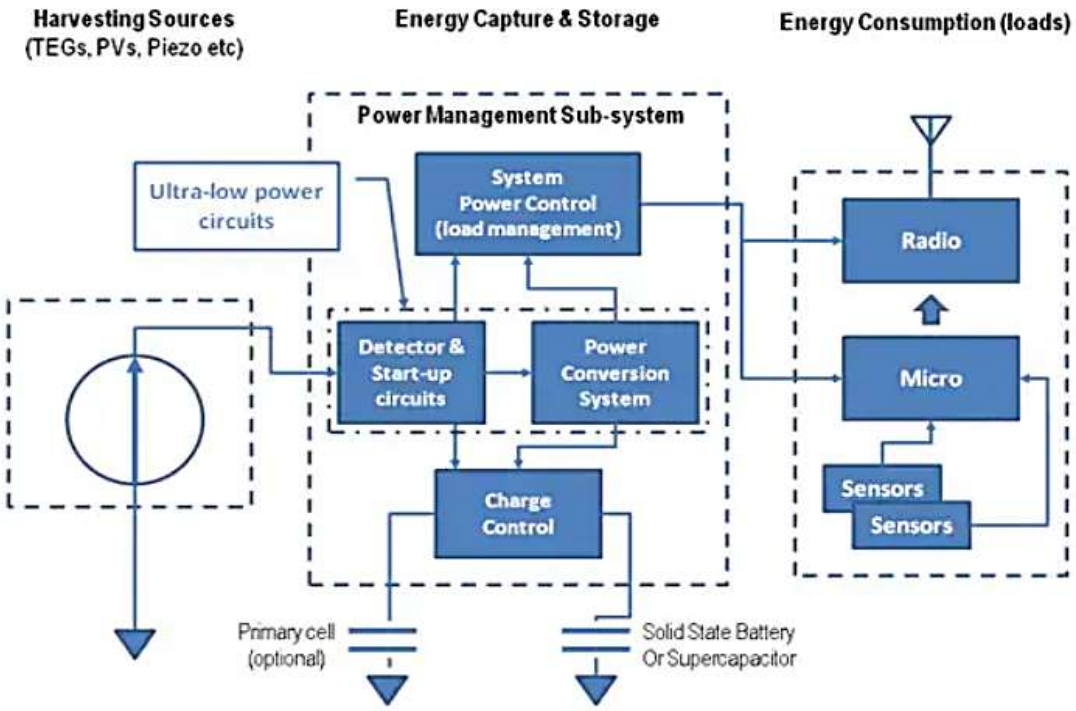
2.6 Διαχείριση Ενέργειας σε WSNs

Η διάρκεια ζωής των κόμβων εξαρτάται από την πηγή ενέργειας που διαθέτουν. Εκτός από αυτό, σε ορισμένες περιπτώσεις το σημείο που βρίσκεται ένας κόμβος στο δίκτυο επιβαρύνει περαιτέρω την κατανάλωση ενέργειας και, *ως εκ τούτου*, και τον κύκλο ζωής του δικτύου. Για παράδειγμα, ένας κόμβος που βρίσκεται κοντά στον επικεφαλής κόμβο χάνει πολύ γρήγορα την ενέργειά του λόγω της υπερφόρτωσης που υφίσταται, με συνέπεια όταν αυτός τεθεί εκτός λειτουργίας να δημιουργήσει δυνητικό πρόβλημα στη λειτουργία όλου του δικτύου. Σε τέτοιες περιπτώσεις χρειάζεται να εφαρμόζονται τεχνολογίες διαχείρισης ενέργειας ώστε η ενέργεια αυτών των σημαντικών κόμβων να χρησιμοποιείται με τον βέλτιστο δυνατό τρόπο. Όλες οι τεχνικές και αλγόριθμοι στα ασύρματα δίκτυα αισθητήρων θεωρούν το θέμα της ενέργειας ως «κρίσιμο περιορισμό» και στοχεύουν στην έξυπνη διαχείρισή της, ώστε να αυξάνεται η διάρκεια ζωής του δικτύου.

Όπως αναφέρθηκε ήδη, ένα WSN αποτελείται από έναν μεγάλο αριθμό κόμβων αισθητήρων που αναπτύσσονται σε έναν γεωγραφικό τομέα. Οι κόμβοι είναι συσκευές μικρής ισχύος που ενσωματώνουν την επεξεργασία, την ασύρματη επικοινωνία και την ανίχνευση. Οι κόμβοι οργανώνονται σε ομάδες/συστάδες και συνεργάζονται για να εκτελέσουν μία εφαρμογή που συνήθως έχει να κάνει με ανίχνευση και παρακολούθηση κάποιων φαινομένων. Τα ασύρματα δίκτυα αισθητήρων μπορούν λοιπόν να ανιχνεύσουν φυσικές περιβαλλοντικές πληροφορίες (π.χ. θερμοκρασία, υγρασία, δόνηση, επιτάχυνση) και να στείλουν τα δεδομένα τους μέσω πρωτοκόλλων δρομολόγησης στους σταθμούς βάσης. Από εκεί, μέσω κατάλληλης εφαρμογής, μπορεί να έχει δυνατότητα πρόσβασης σε αυτά ο εκάστοτε ενδιαφερόμενος χρήστης του δικτύου.
Ωστόσο, η κατανάλωση ενέργειας παραμένει ένα από τα κύρια εμπόδια στη διάδοση και ανάπτυξη αυτής της τεχνολογίας, ιδιαίτερα σε εφαρμογές που απαιτούν υψηλή ποιότητα υπηρεσίας. Οι κόμβοι συνήθως τροφοδοτούνται από απλές μπαταρίες που έχουν μικρή ικανότητα προσφοράς ενέργειας και συνήθως δεν μπορούν να επαναφορτιστούν ή/και να αντικατασταθούν εύκολα, λόγω περιβαλλοντικών περιορισμών. Παρόλα αυτά, τεχνικές όπως η χρήση αιολικής ή ηλιακής ενέργειας επιτρέπουν τη συχνή επαναφόρτιση των μπαταριών, ενώ εναλλακτικές πηγές τροφοδοσίας όπως είναι οι συστοιχίες υπερπυκνωτών μπορούν να αυξήσουν κατακόρυφα τη διάρκεια ζωής ενός κόμβου. Ο τομέας της επιστημονικής έρευνας προσανατολίζεται στην αποτελεσματική διαχείριση ενέργειας αρχικά στους ίδιους τους κόμβους αισθητήρων και έπειτα στις τεχνικές δρομολόγησης μέσω των ενεργειακά αποδοτικά πρωτόκολλων δρομολόγησης [52].

Η υπέρβαση της διάρκειας ζωής του δικτύου, η οποία θεωρείται ως ο χρόνος όπου όλοι οι κόμβοι του δικτύου έχουν μείνει χωρίς ενέργεια, είναι ένα κρίσιμο θέμα το οποίο ερευνάται και αναπτύσσεται συνεχώς. Στη σχεδίαση οποιουδήποτε έργου, οι προτεινόμενες ενέργειες και τεχνικές θα πρέπει να επεκτείνουν τη διάρκεια ζωής του δικτύου χωρίς να «θυσιάζουν» την αξιοπιστία του [63].

Στην παρακάτω εικόνα παρατηρούμε σχηματικά τον τρόπο με τον οποίο εναλλακτικές πηγές ενέργειας θα μπορούσαν να συμβάλλουν αθροιστικά στη βελτίωση του χρόνου ζωής ενός κόμβου. Στην αριστερή βαθμίδα βρίσκεται η πηγή ενέργειας, στην μεσαία βαθμίδα τα κυκλώματα χαμηλής κατανάλωσης τα οποία αποθηκεύουν, διαχειρίζονται και διαθέτουν την ενέργεια στον κόμβο, ο οποίος απεικονίζεται στη δεξιά βαθμίδα.



Εικόνα 2-9: Υψηλή αρχιτεκτονική διαχείρισης ενέργειας σε ένα WSN (digikey, 2021)[5]

2.6.1 Αιτίες Ενεργειακής Σπατάλης

Σε ορισμένες περιπτώσεις δικτύων WSNs εντοπίζεται σπατάλη στο ενεργειακό απόθεμα, παρόλο που η αρχική σχεδίαση δεν προβλέπει κάτι τέτοιο. Οι αιτίες που μπορεί να οδηγήσουν ένα δίκτυο σε σπατάλη ενέργειας μπορεί να είναι οι εξής:

- **Συγκρούσεις πακέτων δεδομένων (collisions):** Όταν ένας κόμβος λαμβάνει περισσότερα από ένα πακέτα συγχρόνως, αυτά τα πακέτα συγκρούονται. Όλα τα πακέτα που προκαλούν την σύγκρουση απορρίπτονται και αναμεταδίδονται.

- **Υπερμετάδοση (overhearing):** Όταν ένας αποστολέας μεταδώσει ένα πακέτο, όλοι οι κόμβοι στην εμβέλεια εκπομπής του θα λάβουν αυτό το πακέτο, ακόμα και εάν το εν λόγω πακέτο δεν αφορά σε αυτούς τους κόμβους. Έτσι έχουμε σπατάλη ενέργειας όταν ένας κόμβος λαμβάνει πακέτα που δεν προορίζονται για αυτόν.

[5] Βλέπε σχετικά: https://www.digikey.com/en/articles/addressing-the-challenges-of-power-management-in-wireless-sensor-networks-wsns

- **Αδρανή κανάλια:** Η περίπτωση αυτή συμβαίνει όταν ένας κόμβος αναμένει από ένα αδρανές κανάλι για να λάβει τυχόν δεδομένα.

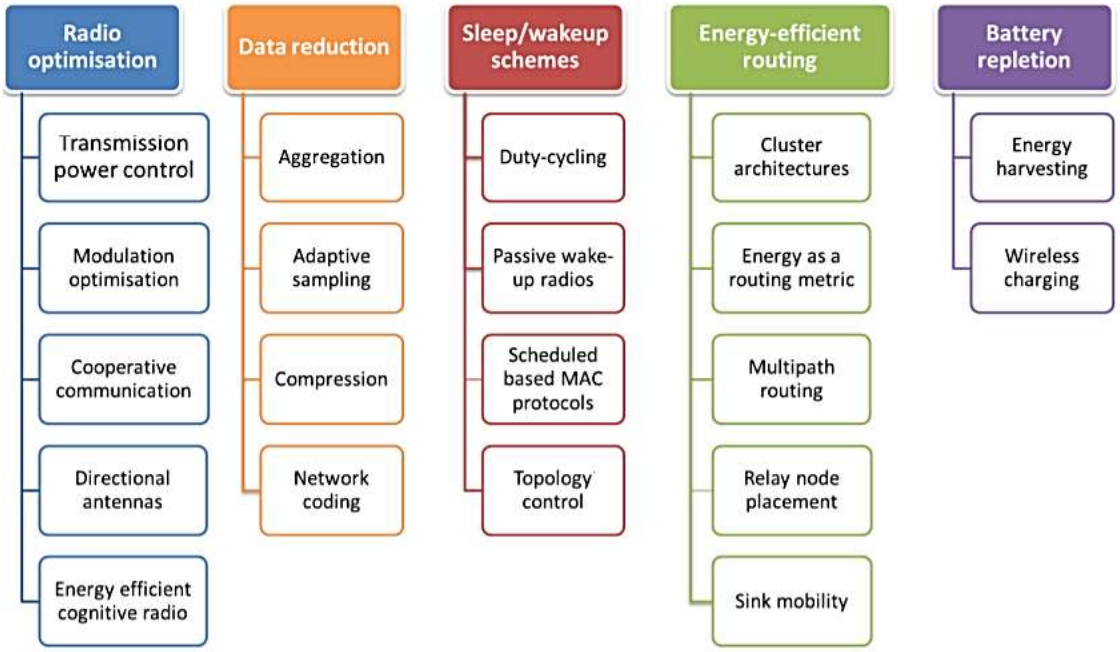
- **Παρεμβολές:** Κάθε κόμβος που βρίσκεται ανάμεσα στο φάσμα εκπομπής και στο φάσμα παρεμβολών λαμβάνει πακέτα που δεν είναι σε θέση να αποκωδικοποιήσει σωστά.

- **Αποτυχία επικοινωνίας:** Όταν υφίσταται αποτυχία επικοινωνίας μεταξύ γειτονικών κόμβων, τότε τα πακέτα έχουν αποσταλεί άσκοπα.

- **Αποτυχία λειτουργίας ύπνου:** Στην περίπτωση αυτή, ενώ ένας κόμβος πρέπει να μπει σε κατάσταση «ύπνου» (sleep mode) για να εξοικονομήσει ενέργεια, η λειτουργία αυτή αποτυγχάνει.

2.6.2 Μηχανισμοί Εξοικονόμησης Ενέργειας σε WSNs

Οι διάφοροι μηχανισμοί για την εξοικονόμηση ενέργειας σε WSNs ενδεικτικά και όχι περιοριστικά παρατίθενται στην Εικόνα 2-10.



Εικόνα 2-10: Ταξινόμηση των τεχνικών εξοικονόμησης ενέργειας [64]

Διακρίνονται οι ακόλουθες περιπτώσεις:

Τεχνικές συνάθροισης δεδομένων: Στόχος αυτών των τεχνικών είναι η μείωση του όγκου δεδομένων που πρέπει να μεταδίδονται μεταξύ των κόμβων, λόγω του υψηλού κόστους μετάδοσης. Παρά το γεγονός ότι καταναλώνεται μεγαλύτερη επεξεργαστική ισχύς, άρα και ενέργεια, αυτή είναι μικρότερη από εάν τα δεδομένα αποστέλλονταν χωρίς να έχουν υποστεί συνάθροιση. Το πρωτόκολλο LEACH είναι ένα πρωτόκολλο του οποίου η φιλοσοφία συνίσταται σε δράσεις συνάθροισης των δεδομένων που υπάρχουν σε έναν κόμβο, και τα οποία πρέπει να αποσταλούν στον σταθμό βάσης. Η διάρκεια ζωής των επιμέρους αισθητήρων αυξάνεται επίσης, επειδή η ενέργεια διαχέεται ομοιόμορφα στο δίκτυο.

Sleep/Active Scheduling (Χρονοπρογραμματισμός κατάστασης ύπνου/ενεργούς κατάστασης): Οι κόμβοι μπορούν να εναλλάσσονται μεταξύ δύο καταστάσεων “active” (“on” – «σε λειτουργία») και “sleep” (“off” – «εκτός λειτουργίας»). Όταν ένας κόμβος ανιχνεύσει ένα γεγονός παραμένει ενεργός και στέλνει τα δεδομένα σε όλους τους αμέσως επόμενους γειτονικούς του κόμβους. Ο κόμβος μεταδίδει τα δεδομένα μέχρι όλοι οι γείτονές του να τα λάβουν. Όταν όλοι οι γείτονες λάβουν επιτυχώς τα δεδομένα, τότε ο κόμβος μπορεί να επιστρέψει στην κατάσταση που είχε προγραμματιστεί να είναι. Οι γειτονικοί κόμβοι συνεχίζουν τη μετάδοση στους αμέσως επόμενους δικούς τους γείτονες, μέχρι να φτάσουν τα δεδομένα στον σταθμό βάσης. Έτσι το δίκτυο κάθε στιγμή έχει ενεργούς μόνο τους κόμβους που χρειάζονται για συγκεκριμένη αναμετάδοση κάποιων δεδομένων, επιτυγχάνοντας εξοικονόμηση ενέργειας.

Ένα προφανές πρόβλημα το οποίο εμφανίζεται σε αυτή την περίπτωση είναι η καθυστέρηση που παρατηρείται όταν ένα πακέτο προσπαθήσει να δρομολογηθεί μέσω ενός κόμβου που είναι εκείνη τη στιγμή σε κατάσταση sleep (off). Η καθυστέρηση στο δίκτυο επηρεάζεται από την τυχαία τοποθέτηση των κόμβων, από την τυχαία εμβέλεια και από τις τυχαίες active (on) και sleep (off) καταστάσεις τους.

Μείωση της ενέργειας που καταναλώνεται κατά την ανίχνευση: Όσο μικρότερο είναι το εμβαδόν που καλύπτει ένας αισθητήρας τόσο χαμηλότερη είναι η ποσότητα ενέργειας που καταναλώνει. Η εκάστοτε εφαρμογή καθορίζει τη συχνότητα της δραστηριότητας της εκπομπής, αλλά μπορεί εξοικονομηθεί ενέργεια με τη μείωση της περιοχής κάλυψης ενός αισθητήρα. Ως αποτέλεσμα, προκειμένου να καλυφθεί η περιοχή εντελώς, πρέπει να αυξηθούν αριθμητικά οι αισθητήρες του δικτύου. Αυτή η μέθοδος μπορεί να αυξήσει σημαντικά το προσδόκιμο ζωής ενός κόμβου αισθητήρα στο δίκτυο.

Βελτιστοποίηση διαμόρφωσης (modulation optimization): Η βελτιστοποίηση της διαμόρφωσης στοχεύει στο να βρει τις βέλτιστες παραμέτρους διαμόρφωσης που οδηγούν στην ελάχιστη κατανάλωση ενέργειας του ραδιοπομπού. Πολλές φορές η εξάντληση των πόρων προκαλείται από την κατανάλωση ισχύος του κυκλώματος και την κατανάλωση ισχύος του μεταδιδόμενου σήματος. Διαμορφώνοντας την ισχύ εκπομπής, μπορούμε να μειώσουμε ανάλογα την κατανάλωση ενέργειας. Εντούτοις, και σε αυτή την περίπτωση ενέχει ο κίνδυνος δημιουργίας θορύβου στο σήμα.

Βελτιστοποίηση ασυρμάτου: Η μονάδα ασυρμάτου είναι το κύριο συστατικό που προκαλεί εξάντληση της μπαταρίας των κόμβων αισθητήρα. Για να μειωθεί η απαγωγή ενέργειας λόγω ασύρματων επικοινωνιών, οι ερευνητές προσπάθησαν να βελτιστοποιήσουν τις παραμέτρους του ραδιοπομπού και του ραδιοδέκτη, όπως με σχήματα κωδικοποίησης και διαμόρφωσης, μετάδοση ισχύος και με κατεύθυνση της κεραίας [65, 66].

Μείωση δεδομένων: Μία άλλη κατηγορία λύσεων στοχεύει στη μείωση του όγκου των δεδομένων που θα παραδοθούν. Δύο μέθοδοι μπορούν να υιοθετηθούν από κοινού, ήτοι: ο περιορισμός των περιττών πακέτων δεδομένων αλλά και ο περιορισμός των εργασιών ανίχνευσης εναλλακτικών μονοπατιών, που αμφότεροι ωφελούν στην εξοικονόμηση ενέργειας [67].

Σχέδιο ύπνου/αφύπνισης: Οι καταστάσεις αδράνειας είναι σημαντικές πηγές κατανάλωσης ενέργειας στο ραδιόφωνο. Τα σχήματα ύπνου / αφύπνισης στοχεύουν στην προσαρμογή της δραστηριότητας κόμβων για εξοικονόμηση ενέργειας θέτοντας τη συσκευή σε κατάσταση αναστολής λειτουργίας [68].

3

Διαδίκτυο των Πραγμάτων (IoT)

Το Διαδίκτυο των Πραγμάτων ή Ίντερνετ των Πραγμάτων (αγγλικά: Internet of Things, IoT) αποτελεί το δίκτυο επικοινωνίας πληθώρας συσκευών, οικιακών συσκευών, αυτοκινήτων καθώς και κάθε αντικειμένου που ενσωματώνει ηλεκτρονικά μέσα, λογισμικό, αισθητήρες και συνδεσιμότητα σε δίκτυο ώστε να επιτρέπεται η σύνδεση και η ανταλλαγή δεδομένων. Απλούστερα, η φιλοσοφία του IoT είναι η σύνδεση όλων των ηλεκτρονικών συσκευών μεταξύ τους ή στο Διαδίκτυο (world wide web (www) - παγκόσμιος ιστός) [71].

Το Διαδίκτυο των Πραγμάτων μπορεί να εκληφθεί ως ένα εκτεταμένο όραμα με τεχνολογικές και κοινωνικές επεκτάσεις, ενώ ο όρος Internet of Things αποδόθηκε την δεκαετία του 1990 από τον Kevin Ashton[6]. Μέσω της αξιοποίησης των δυνατοτήτων αναγνώρισης, καταγραφής δεδομένων, επεξεργασίας και επικοινωνίας, το IoT χρησιμοποιεί πλήρως τα «αντικείμενα-πράγματα» για να προσφέρει υπηρεσίες σε κάθε είδους εφαρμογές, εξασφαλίζοντας ταυτόχρονα ότι πληρούνται οι απαιτήσεις ασφάλειας και προστασίας της ιδιωτικής ζωής.

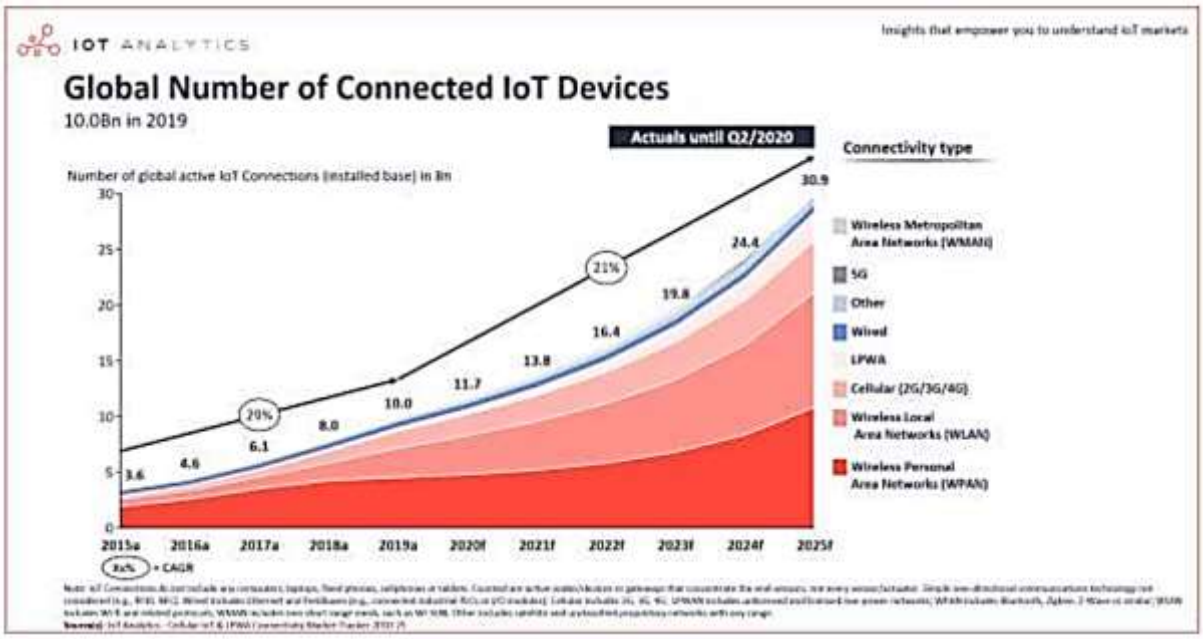
3.1 Το Διαδίκτυο των Αντικειμένων

Η τεχνολογία IoT συστήνει ένα πολύπλοκο δίκτυο το οποίο διασυνδέει τα «αντικείμενα-πράγματα» με το Διαδίκτυο μέσω της χρήσης τυποποιημένων πρωτοκόλλων επικοινωνίας. Τα διασυνδεδεμένα «πράγματα» έχουν φυσική ή εικονική αναπαράσταση στον ψηφιακό κόσμο, δυνατότητα ανίχνευσης και ενεργοποίησης, δυνατότητα προγραμματισμού, είναι μοναδικώς αναγνωρίσιμα και προσφέρουν υπηρεσίες μέσω της αξιοποίησης των παραπάνω χαρακτηριστικών [73].

[6] Ο όρος αποδίδεται σύμφωνα με τους Zhang και συνεργάτες, στο άρθρο: Zhang, W.E., et al. (2020): "The 10 Research Topics on the Internet of Things". In Proceedings of the 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC), 2020, pp.34-43.

Οι πρόοδοι που έχουν σημειωθεί στις τεχνολογίες επικοινωνίας και πληροφοριών δεδομένου και του IoT, εισάγουν το Διαδίκτυο των Πραγμάτων και στις υπηρεσίες ασφάλειας των κρίσιμων υποδομών. Οι ευπάθειες, *ωστόσο*, των συστημάτων αυτών περιλαμβάνουν τη γρήγορη εξάντληση των πόρων ενέργειας και την πιθανότητα της δολιοφθοράς μέσω λογισμικών υποκλοπών ή κακόβουλων ιών. Ως εκ τούτου, η φύση των ασύρματων αισθητήρων και του IoT επιτρέπει τη διεξαγωγή του ρόλου αυτής της οντότητας για το σκοπό της προστασίας των υποδομών· από την άλλη όμως επιβάλλει την προστασία του ίδιου συστήματος από κακόβουλες επιθέσεις και δολιοφθορά [74].

Παρά τη συνεχιζόμενη πανδημία Covid-19, η αγορά του Διαδικτύου των Πραγμάτων συνεχίζει να αναπτύσσεται. Το 2020, για πρώτη φορά, υπήρχαν περισσότερες συνδέσεις IoT από ό,τι οι συνδέσεις εκτός IoT (smartphone, φορητοί υπολογιστές και υπολογιστές). Από τα 21,7 δισεκατομμύρια ενεργές συνδεδεμένες συσκευές παγκοσμίως, τα 11,7 δισεκατομμύρια (ή 54%) εκτιμήθηκαν ως συνδέσεις συσκευών IoT περί το τέλος του 2020. Μέχρι το 2025, αναμένεται ότι θα υπάρξουν περισσότερες από 30 δισεκατομμύρια συνδέσεις IoT, σχεδόν 4 συσκευές IoT ανά άτομο κατά μέσο όρο [75] (βλ. Εικόνα 3-1).



Εικόνα 3-1: Ρυθμός αύξησης διασυνδεδεμένων συσκευών IoT παγκοσμίως [75]

3.2 Είδη Αισθητήρων στο IoT

Προκειμένου οι ασύρματοι αισθητήρες που αποτελούν στο δίκτυο IoT να συμπεριφέρονται έξυπνα, το πρότυπο IEEE 1451[7] θέσπισε την προσθήκη μίας συσκευής μνήμης στον σχεδιασμό τους. Η συσκευή μνήμης αποθηκεύει ένα ηλεκτρονικό φύλλο δεδομένων του μορφοτροπέα (TEDS - Transducer Electronic Data Sheet) το οποίο περιέχει την ταυτοποίηση

[7] Για περισσότερες πληροφορίες βλέπε, *μεταξύ άλλων*: https://en.wikipedia.org/wiki/IEEE_1451

του αισθητήρα, τη βαθμονόμησή του, δεδομένα διόρθωσης και πληροφορίες σχετικές με τον κατασκευαστή. Ο στόχος που εξυπηρέτησε το πρωτόκολλο IEEE 1451[8] ήταν η δυνατότητα πρόσβασης στα στοιχεία του αισθητήρα από τα δίκτυα υπολογιστών με ενσύρματο ή ασύρματο τρόπο. Η εμφάνιση της τεχνολογίας του IoT και η σταδιακή αύξηση στην υπολογιστική ισχύ του μικροεπεξεργαστή επέτρεψαν στη βιομηχανία να κατασκευάσει έξυπνους αισθητήρες με βελτιωμένες λειτουργίες ανίχνευσης και επεξεργασίας σημάτων. Η δυνατότητα, εκτός των άλλων, και της τοπικής επεξεργασίας σημάτων επέτρεψε την επεξεργασία δεδομένων, την ερμηνεία και τη λήψη αποφάσεων [76].

Τα κυριότερα είδη αισθητήρων τους οποίους θα συναντήσουμε στο IoT, παρουσιάζονται παρακάτω ([77], [78]):

1. **Αισθητήρας θερμοκρασίας**
   Οι αισθητήρες θερμοκρασίας μετρούν την ποσότητα θερμικής ενέργειας σε μία πηγή, επιτρέποντάς τους να ανιχνεύουν αλλαγές θερμοκρασίας και να μετατρέπουν αυτές τις αλλαγές σε δεδομένα. Ορισμένες εφαρμογές, απαιτούν συχνά οι θερμοκρασίες περιβάλλοντος να βρίσκονται σε συγκεκριμένα επίπεδα ή να μην ξεπερνούν ένα συγκεκριμένο κατώφλι.

2. **Αισθητήρας υγρασίας ή διαρροής**
   Αυτοί οι τύποι αισθητήρων μετρούν την ποσότητα υδρατμών του αέρα ή άλλων αερίων στην ατμόσφαιρα. Οι αισθητήρες υγρασίας βρίσκονται συνήθως σε συστήματα θέρμανσης, εξαερισμού και κλιματισμού.

3. **Αισθητήρας πίεσης**
   Ανιχνεύει αλλαγές σε αέρια και υγρά μέσα. Όταν αλλάζει η πίεση, ο αισθητήρας ανιχνεύει αυτές τις αλλαγές και τις επικοινωνεί σε συνδεδεμένα συστήματα.

4. **Αισθητήρας εγγύτητας (proximity sensor)**
   Ο αισθητήρας εγγύτητας μπορεί να ανιχνεύσει μία σειρά αντικειμένων με τη βοήθεια εκπομπής ηλεκτρομαγνητικού πεδίου ή δέσμης ηλεκτρομαγνητικών ακτινοβολιών χωρίς να προηγηθεί φυσική επαφή.

5. **Επιταχυνσιόμετρο**
   Τα επιταχυνσιόμετρα εντοπίζουν την επιτάχυνση ενός αντικειμένου, δηλαδή τον ρυθμό αλλαγής της ταχύτητας του αντικειμένου, σε σχέση με το χρόνο. Τα επιταχυνσιόμετρα μπορούν επίσης να ανιχνεύσουν αλλαγές στη βαρύτητα. Οι περιπτώσεις χρήσης για επιταχυνσιόμετρα περιλαμβάνουν έξυπνα βηματόμετρα και παρακολούθηση στόλων οδήγησης, αντικλεπτικές εφαρμογές κλπ. Αυτός ο αισθητήρας αποτελεί την πλειονότητα των έξυπνων συσκευών.

[8] Η οικογένεια των προτύπων διασύνδεσης έξυπνων αισθητήρων, με την ονομασία IEEE 1451, δημιουργήθηκε από την Επιτροπή Τεχνολογίας Αισθητήρων της IEEE (IEEE Instrumentation and Measurement Society TC-9) Πηγή: NIST IEEE-P1451 Draft Standard Home Page. http://ieee1451.nist.gov/

6. **Γυροσκόπιο**
   Οι αισθητήρες γυροσκοπίου μετρούν τον γωνιακό ρυθμό ή την ταχύτητα, που συχνά ορίζεται ως η ταχύτητα περιστροφής γύρω από έναν άξονα. Οι περιπτώσεις χρήσης περιλαμβάνουν αυτοκίνητα, συστήματα ελέγχου ευστάθειας, ανίχνευση κίνησης για βιντεοπαιχνίδια, προστασία ανθρώπου ή αντικειμένου από πτώση (man-down), συστήματα ανίχνευσης μετατόπισης κάμερας ή κινητών τηλεφώνων, tablets, κλπ.

7. **Αισθητήρας αερίου**
   Αυτοί οι τύποι αισθητήρων παρακολουθούν και ανιχνεύουν αλλαγές στην ποιότητα του αέρα, συμπεριλαμβανομένης της παρουσίας τοξικών, εύφλεκτων ή επικίνδυνων αερίων. Οι βιομηχανίες που χρησιμοποιούν αισθητήρες αερίου περιλαμβάνουν εξόρυξη, πετρέλαιο και φυσικό αέριο, χημική έρευνα και κατασκευή. Μία κοινή περίπτωση χρήσης είναι οι ανιχνευτές μονοξειδίου του άνθρακα που χρησιμοποιούνται σε πολλά σπίτια.

8. **Αισθητήρας κίνησης παθητικού υπέρυθρου (Passive Infrared – PIR)**
   Αυτοί οι τύποι αισθητήρων παρακολουθούν το περιβάλλον τους, είτε εκπέμποντας είτε ανιχνεύοντας υπέρυθρη ακτινοβολία. Οι υπέρυθροι αισθητήρες χρησιμοποιούνται ευρέως στον τομέα της ασφάλειας για την ανίχνευση μη εξουσιοδοτημένης κίνησης εντός περιοχής. Σε άλλες περιπτώσεις θα τους συναντήσουμε σε μία ποικιλία διαφορετικών έργων IoT, συμπεριλαμβανομένης της υγειονομικής περίθαλψης.

9. **Οπτικοί αισθητήρες**
   Οι οπτικοί αισθητήρες μετατρέπουν τις ακτίνες φωτός σε ηλεκτρικά σήματα. Οι οπτικοί αισθητήρες κατά κύριο λόγω χρησιμοποιούνται στις κάμερες ασφαλείας και σε άλλων ειδών κάμερες, οι οποίες χρησιμοποιούνται σε πάρα πολλές εφαρμογές.

10. **Αισθητήρας στάθμης**
    Οι αισθητήρες στάθμης χρησιμοποιούνται για την ανίχνευση του επιπέδου των ουσιών που περιλαμβάνουν υγρά, σκόνες και κοκκώδη υλικά.

Εικόνα 3-2: Η μικρότερη κάμερα παγκοσμίως, διαστάσεων 1,16x0,58x0,58 mm

3.3 Αρχιτεκτονική του IoT

Μία γενική αρχιτεκτονική IoT αποτελείται από τρία επίπεδα, δηλαδή την εφαρμογή, τη μεταφορά και την ανίχνευση. Το επίπεδο εφαρμογών χρησιμοποιεί έξυπνες τεχνολογίες υπολογιστών (π.χ. εξόρυξη δεδομένων, υπολογιστική νέφους) για την εξαγωγή πολύτιμων πληροφοριών από την επεξεργασία ογκωδών δεδομένων και παρέχει μία διεπαφή μεταξύ χρηστών και IoT. Το επίπεδο μεταφοράς είναι υπεύθυνο για τις λειτουργίες δικτύου, ενώ το επίπεδο ανίχνευσης συλλέγει δεδομένα. Το επίπεδο ανίχνευσης είναι υπεύθυνο για τη συλλογή των πληροφοριών και του θέματος των αναγνωρίσεων. Παρά τα πλεονεκτήματα όπως η ευκολότερη αναγνώριση και διαχείριση προβλημάτων, η ευελιξία και η έλλειψη ασφάλειας του επιπέδου εφαρμογής είναι πρωταρχικός περιορισμός.

Μία κλιμακούμενη και αυτορρυθμιζόμενη αρχιτεκτονική διομότιμης δικτύωσης (“peer-to-peer”) για το δίκτυο IoT μεγάλης κλίμακας υπάρχει από το 2014 [90]. Ο στόχος ήταν η παροχή αυτοματοποιημένων υπηρεσιών και μηχανισμών ανακάλυψης πόρων, οι οποίοι δεν απαιτούν ανθρώπινη παρέμβαση για τη διαμόρφωσή τους. Η λύση βασίζεται στην τοπική και παγκόσμια ανακάλυψη υπηρεσιών που επιτρέπει την επιτυχή αλληλεπίδραση και τη διατήρηση της αμοιβαίας ανεξαρτησίας. Η κύρια σημασία αυτής της λύσης είναι ότι τα πειράματά της διεξάγονται σε συσκευές πραγματικού κόσμου που καθιστούν το αποτέλεσμα πιο αξιόπιστο. Ωστόσο, η πιθανότητα εμφάνισης σφάλματος είναι ο κύριος παράγοντας της ύπαρξης υψηλότερης αξιόπιστης λύσης, από την άποψη της αρχιτεκτονικής του IoT.

Η αρχιτεκτονική που βασίζεται σε δίκτυο (“Software-defined network” - SDN) με βάση το λογισμικό για το IoT, έχει ως στόχο την παροχή υπηρεσιών υψηλού επιπέδου στις διάφορες εργασίες IoT σε ετερογενή περιβάλλοντα ασύρματου δικτύου [91]. Η προτεινόμενη αρχιτεκτονική παρέχει πολλά οφέλη, δηλαδή ευελιξία, αποτελεσματικότητα και βελτιωμένη διαχείριση όσον αφορά στη ροή και στους πόρους εργασιών. Αρκετές υπάρχουσες μελέτες αποκαλύπτουν ότι η ασύρματη αρχιτεκτονική που βασίζεται σε SDN μπορεί να συμβάλει στην επίτευξη των στόχων του IoT όσον αφορά στην καλύτερη ποιότητα υπηρεσιών, στην επεκτασιμότητα, στη γρήγορη και εύκολη ανάπτυξη των πόρων και στην ανάκτηση σημασιολογικών πληροφοριών χωρίς πλαίσιο ([92], [93]).

Μία αρχιτεκτονική του IoT που ονομάζεται 3G-PLC έχει προταθεί από τους Hsieh & Lai το 2011 [94]. Η αρχιτεκτονική συνδυάζει δύο εξελιγμένα δίκτυα επικοινωνίας, ήτοι: επικοινωνία γραμμών ισχύος (“Power Line Communication” - PLC) και το δίκτυο 3G. Το κίνητρο πίσω από τη χρήση αυτών των δύο δικτύων ήταν ο παράγοντας κλιμάκωσης [94]. Ο στόχος αυτής της προσέγγισης ήταν να ενσωματώσει τα επίπεδα πλαισίου IoT όπως το επίπεδο αντίληψης, το στρώμα συγκέντρωσης, το επίπεδο δικτύου και το επίπεδο εφαρμογής. Η συναφής προτεινόμενη αρχιτεκτονική προσφέρει αξιοσημείωτα πλεονεκτήματα, όπως είναι το μειωμένο κόστος κατασκευής δικτύου και οι βελτιωμένες υπηρεσίες σε σύγκριση με τους ανταγωνιστές δικτύου οπισθόζευξης (backhaul). Ωστόσο, η έλλειψη ενσωμάτωσης παραμέτρων ετερογένειας δικτύου είναι ένας από τους πρωταρχικούς περιορισμούς της.

Έχει αποδειχθεί ότι η χρήση μελλοντικής αρχιτεκτονικής στο Διαδίκτυο που ονομάζεται “Mobility First” («Πρώτα η Κινητότητα») μπορεί να βοηθήσει στην αντιμετώπιση πολλών

προκλήσεων που σχετίζονται με τα κινητά τηλέφωνα όταν ενεργούν ως πηγαίες πύλες WSN σε συστήματα IoT [95]. Η χωρητικότητα του συστήματος αναλύεται και συγκρίνεται με το ρυθμό δεδομένων του αισθητήρα σε ένα συγκεκριμένο σημείο πρόσβασης. Αν και η προτεινόμενη εργασία μπορεί να προσφέρει πολλά οφέλη, όπως υψηλή ασφάλεια και ad hoc υπηρεσίες, ωστόσο, η έλλειψη μηχανισμών κινήτρων για τους κινητούς συνεισφέροντες στο σύστημα είναι ένα από τα μειονεκτήματα.

3.4 Υποστηριζόμενες Τεχνολογίες και Εφαρμογές

Ορισμένες από τις σημαντικές εφαρμογές IoT ονομάζονται έξυπνες μεταφορές, έξυπνο σπίτι, έξυπνη υγειονομική περίθαλψη, έξυπνο δίκτυο, έξυπνος φωτισμός και έξυπνο κτίριο, για να αναφέρουμε μερικές. Αυτές οι εφαρμογές διευκολύνουν τους ανθρώπους σε διαφορετικές πτυχές της καθημερινής ζωής. Π.χ., το έξυπνο σύστημα μεταφοράς βοηθά στη μείωση της κυκλοφοριακής συμφόρησης παρέχοντας κατάλληλη εναλλακτική διαδρομή. Επιπλέον, η προγνωστική ανάλυση έξυπνων δεδομένων μεταφοράς βοηθά στην ελαχιστοποίηση των ατυχημάτων. Τα έξυπνα σπίτια επιτρέπουν στους κατοίκους να ελέγχουν εξ αποστάσεως πολλές από τις οικιακές συσκευές. Μέσω έξυπνων εφαρμογών υγειονομικής περίθαλψης, οι ασθένειες μπορούν να διαγνωστούν νωρίτερα, με προφανή οφέλη στην υγεία των εκάστοτε εμπλεκομένων. Σε ένα έξυπνο περιβάλλον δικτύου, οι έξυπνοι μετρητές ενέργειας χρησιμοποιούνται για τη μέτρηση της κατανάλωσης και οι μετρήσεις αποστέλλονται αυτόματα στο δίκτυο. Μέσω της εφαρμογής έξυπνου φωτισμού, οι αισθητήρες χαμηλού κόστους και η ασύρματη συνδεσιμότητα μπορούν να ενσωματωθούν σε λαμπτήρες και φωτιστικά. Το έξυπνο κτίριο είναι μια άλλη σημαντική εφαρμογή IoT, όπου το κτήριο ως «οντότητα» χρησιμοποιεί πλήρως τις τεχνολογίες πληροφοριών και επικοινωνίας. Με λίγα λόγια, οι εφαρμογές IoT διευκολύνουν τους ανθρώπους στην καθημερινή τους ζωή [80].

Οι συσκευές IoT δεν μπορούν να λειτουργήσουν χωρίς τη σύνδεση δικτύου. Για να ενεργοποιηθεί η συνδεσιμότητα μεταξύ ετερογενών έξυπνων συσκευών, χρησιμοποιούνται διάφορες τεχνολογίες δικτύωσης και επικοινωνίας, όπως Sigfox[9], Neul[10], 6LowPAN[11], LoRaWAN[12], κυψελοειδή και καθορισμένα από λογισμικό δίκτυα. Το Sigfox είναι μια ευρεία γκάμα τεχνολογίας, καθώς η κάλυψή του είναι μεταξύ Wi-Fi και κινητής τηλεφωνίας. Ο στόχος του Sigfox είναι να υποστηρίξει τις περιορισμένες συσκευές τροφοδοσίας όσον αφορά στη μεταφορά δεδομένων.

Η **Neul** είναι μία νέα τεχνολογία ασύρματου δικτύου ευρείας εμβέλειας, που έχει σχεδιαστεί για να υποστηρίζει το IoT.

---

[9] Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2018, March): "Overview of cellular LPWAN technologies for IoT deployment: Sigfox, LoRaWAN, and NB-IoT". In Proceedings of the 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), pp.197-202. IEEE.

[10] https://plc247.com/iot-protocols-part10-neul/

[11] Pongle, P., & Chavan, G. (2015, January): "A survey: Attacks on RPL and 6LoWPAN in IoT". In Proceedings of the 2015 International Conference on Pervasive Computing (ICPC), pp.1-6. IEEE.

[12] Triantafyllou, A., Sarigiannidis, P., & Lagkas, T. D. (2018): "Network protocols, schemes, and mechanisms for internet of things (IoT): Features, open challenges, and trends". Wireless Communications and Mobile Computing, Hindawi, 2018. https://www.hindawi.com/journals/wcmc/2018/5349894/

Το **6LowPAN** (Low-power Personal Area Network) είναι πρωτόκολλο δικτύου με βάση το IP, το οποίο καθορίζει τους νέους μηχανισμούς συμπίεσης και συμπίεσης κεφαλίδας. Μπορεί να χρησιμοποιηθεί σε πολλαπλές πλατφόρμες επικοινωνίας οι οποίες βασίζονται στο πρότυπο λειτουργίας ασύρματων δικτύων IEEE 802.15.4[13].

Το **LoRaWAN** (δίκτυο ασύρματης περιοχής χαμηλής εμβέλειας) έχει επίσης σχεδιαστεί για να στοχεύει δίκτυο ευρείας περιοχής. Επιπλέον, υποστηρίζει χαμηλού κόστους κινητή αμφίδρομη επικοινωνία στο IoT ενισχύοντας την ασφάλεια. Για την υποστήριξη λειτουργιών υπεραστικών εφαρμογών IoT, χρησιμοποιούνται δυνατότητες επικοινωνίας Cellular (GSM / 3G / 4G). Θεωρείται ως το πιο ιδανικό για έργα χαμηλού εύρους ζώνης δεδομένων που βασίζονται σε αισθητήρες. Η δικτύωση που καθορίζεται από το λογισμικό είναι μία αναδυόμενη τεχνολογία που μπορεί να βοηθήσει στην έξυπνη δρομολόγηση της κίνησης, στην εξάλειψη των σημείων συμφόρησης και στη βελτίωση της αποτελεσματικότητας για την επεξεργασία των δεδομένων που παράγονται από το IoT χωρίς να δημιουργηθεί μεγαλύτερη πίεση στο δίκτυο [80].

Το IoT μπορεί να προσφέρει πολλά οφέλη στις επιχειρήσεις. Οι επιχειρηματικοί στόχοι του IoT εστιάζονται, *ιδίως*, στα κάτωθι: αυτοματοποίηση μάρκετινγκ (εμπορική προώθηση), μειωμένο κόστος, πρόσβαση δεδομένων πώλησης, στοχευμένες υπηρεσίες πελατών και βελτιωμένες διαδικασίες αλυσίδας εφοδιασμού. Οι έξυπνες εφαρμογές με δυνατότητα IoT δημιουργούν γνώση σχετικά με τους πελάτες όσον αφορά στο ιστορικό του πελάτη (π.χ. πρότυπα αγορών και προτιμήσεις). Αυτό μπορεί να επιτρέψει στις επιχειρήσεις να ανακαλύψουν σε πραγματικό χρόνο το ποιες θα είναι οι ανάγκες των πελατών τους και στο μέλλον να προβλέψουν το ποια προϊόντα θα έχουν ζήτηση. Με αυτόν τον τρόπο μπορεί να ενεργοποιηθεί η αυτοματοποίηση του μάρκετινγκ.
Μέσω της διαδικτυακής συνδεσιμότητας, δίνεται η δυνατότητα παραγγελίας αγαθών μέσω Διαδικτύου, η οποία μπορεί να εξυπηρετήσει στην εξοικονόμηση χρημάτων μειώνοντας το κόστος μετάβασης στο φυσικό κατάστημα. Καθώς οι συσκευές IoT παράγουν τεράστιο όγκο δεδομένων, αναλύοντας αυτά τα δεδομένα, ο επιχειρηματίας μπορεί εύκολα να ξέρει πώς, γιατί και πού τα προϊόντα χρησιμοποιούνται και αγοράζονται, γεγονός που μπορεί να οδηγήσει στη δημιουργία αποτελεσματικότερων στρατηγικών σχεδίων για τις εταιρείες. Επιπλέον, οι υπηρεσίες των πελατών και οι διαδικασίες αλυσίδας εφοδιασμού (logistics) μπορούν επίσης να βελτιωθούν μέσω της ανάλυσης των δεδομένων που δημιουργούνται από τις συσκευές IoT κάθε ατόμου. Εν ολίγοις, το IoT μπορεί να βοηθήσει στην επίτευξη πολλών επιχειρηματικών στόχων [81].

[13] Το πρότυπο IEEE 802.15.4 καθορίστηκε το 2003 από την Επιτροπή IEEE 802.15 και καθορίζει το φυσικό επίπεδο ελέγχου και ελέγχου πρόσβασης πολυμέσων για LR-WPAN. IEEE 802.15 WPAN™ Task Group 4, http://www.ieee802.org/15/pub/TG4.html

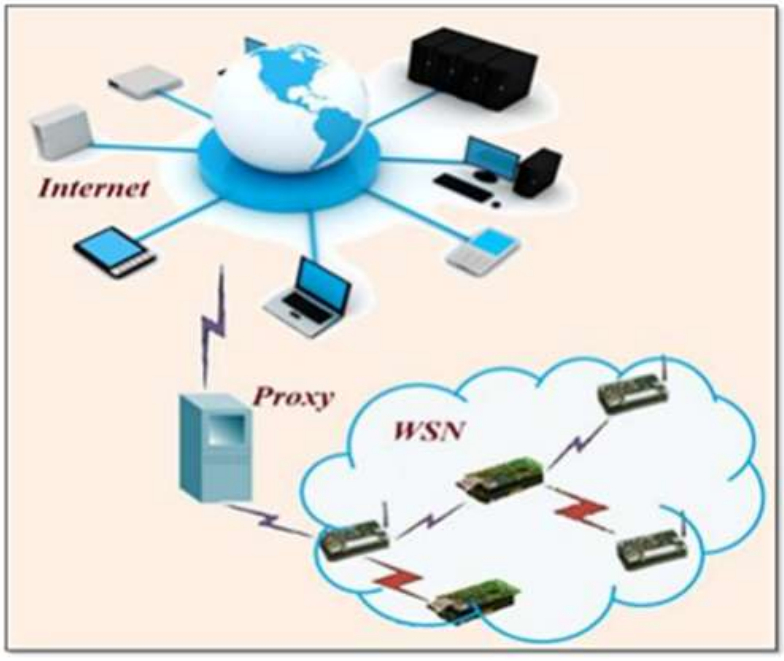
3.5 Ενσωμάτωση WSNs στο IoT

Τα WSNs μπορούν να συνδεθούν σε ένα δίκτυο IP χρησιμοποιώντας τρεις τύπους λύσεων που περιλαμβάνουν αρχιτεκτονική μεσολάβησης, δίκτυα ανεκτικής καθυστέρησης και μικροσκοπική υλοποίηση TCP / IP.

3.5.1 Proxy Architecture

Η αρχιτεκτονική πληρεξουσίου (ή μεσολάβησης) (Proxy Architecture) είναι η πιο κοινή μέθοδος σύνδεσης WSNs σε δίκτυο IP. Σε αυτή τη μέθοδο, ένας ειδικός διακομιστής μεσολάβησης αναπτύχθηκε μεταξύ του WSN και του δικτύου IP. Ο διακομιστής μεσολάβησης είναι ένα συμβατικό πρόγραμμα που εκτελείται στον υπολογιστή πύλης.

Ο διακομιστής μεσολάβησης μπορεί να εκτελεστεί με δύο τρόπους: ως μεταγωγέας (ρελέ) ή ως front-end (πρόσθιο άκρο). Στην πρώτη περίπτωση, ο διακομιστής μεσολάβησης μεταφέρει τα δεδομένα IP που προέρχονται από WSN σε συγκεκριμένο πελάτη στο Διαδίκτυο. Ο πελάτης πρέπει να δηλώσει ένα συγκεκριμένο ενδιαφέρον για τα δεδομένα με έναν διαθέσιμο διακομιστή μεσολάβησης και, στη συνέχεια, ο διακομιστής μεσολάβησης θα μεταδώσει αυτά τα δεδομένα στον προορισμό. Στη δεύτερη περίπτωση, ο διακομιστής μεσολάβησης συλλέγει όλα τα δεδομένα που προέρχονται από WSN στη βάση δεδομένων και εν συνεχεία ενεργεί ως διακομιστής βάσης δεδομένων σε ένα δίκτυο IP. Οι πελάτες στο Διαδίκτυο μπορούν να υποβάλουν ερώτημα στον διακομιστή μεσολάβησης για δεδομένα αισθητήρα με διάφορους τρόπους, όπως μέσω ερωτημάτων SQL (Structured Query Language) ή διεπαφών που βασίζονται στον Ιστό.

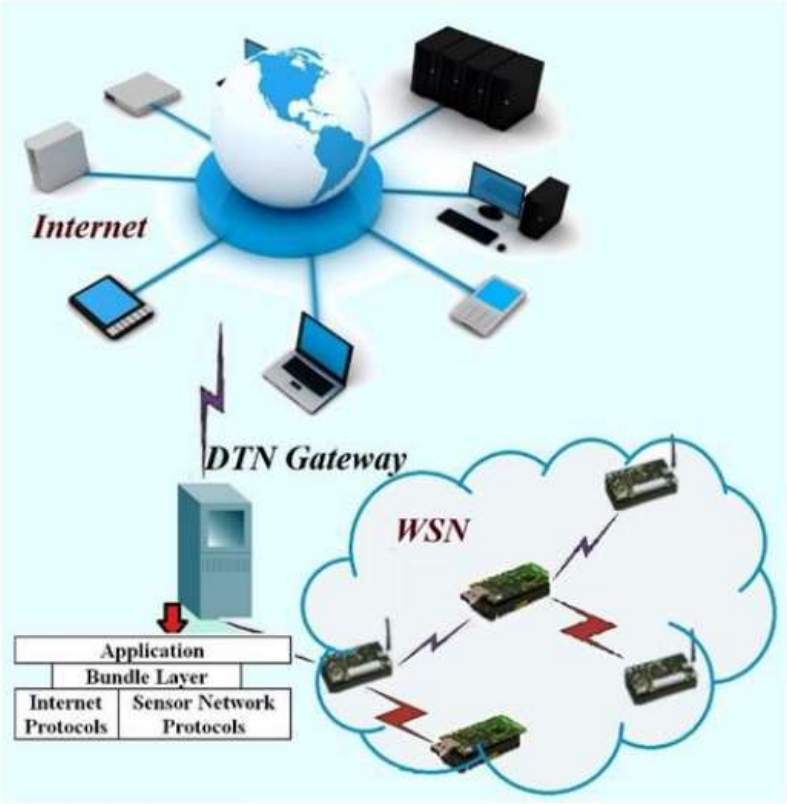


Εικόνα 3-3: Αρχιτεκτονική Proxy [82]

3.5.2 Delay Tolerant Networks

Τα DTNs (Δίκτυα με Ανοχή ως προς την Καθυστέρηση) έχουν αναπτυχθεί για περιβάλλοντα που θέτουν συγκεκριμένες προκλήσεις όπως π.χ. μεγάλη και μεταβλητή καθυστέρηση, συχνός μερισμός δικτύου, δυνητικά υψηλά ποσοστά δυφιακών σφαλμάτων (bit errors) και ασύμμετροι ρυθμοί δεδομένων. Το DTN χρησιμοποιεί μία υπερκείμενη αρχιτεκτονική που βασίζεται σε μεταγωγή μηνυμάτων αποθήκευσης και προώθησης που ονομάζονται δέσμες (bundles). Το στρώμα δέσμης εφαρμόζεται ως το κορυφαίο στρώμα (top layer). Στην πραγματικότητα, αυτό υλοποιείται στο στρώμα εφαρμογής του πρωτοκόλλου TCP/IP.

Το DTN αποτελείται από ένα σύνολο περιοχών που μοιράζονται ένα κοινό στρώμα το οποίο καλείται ως στρώμα δέσμης (bundle layer). Το στρώμα δέσμης είναι υπεύθυνο για την αποθήκευση μηνυμάτων εάν δεν υπάρχει καμία διαθέσιμη ζεύξη προς τον προορισμό, μήνυμα τεμαχίου και αξιοπιστία από άκρο σε άκρο. Κάθε περιοχή έχει μία ή περισσότερες πύλες DTN που θα προωθούν μηνύματα δέσμης μεταξύ των περιοχών για να φτάσουν στην τελευταία πύλη DTN που θα παραδώσει το μήνυμα σε κεντρικούς (ξένιους) υπολογιστές (host computers) στην περιοχή της.



Εικόνα 3-4: Αρχιτεκτονική DTN [82]

3.5.3 Tiny TCP/IP Implementations

Υπήρχαν πολλά πλεονεκτήματα για την εφαρμογή TCP / IP, για να βρεθεί τρόπος ώστε να ταιριάζει στον περιορισμό ενός μικρού ενσωματωμένου (embedded) συστήματος. Το μικροσκοπικό (tiny) TCP/IP ή αλλιώς "μIP" είναι μία υλοποίηση ανοικτού κώδικα της στοίβας πρωτοκόλλου που προορίζεται για χρήση με μικροελεγκτές 8 και 16 διφυών (bits). Το πρωτόκολλο αρχικά αναπτύχθηκε από τον Adam Dunkels του ομίλου "Networked Embedded Systems" στο Σουηδικό Ινστιτούτο Πληροφορικής, με άδεια χρήσης BSD[14], ενώ η ανάπτυξη συνεχίστηκε περαιτέρω από μια ευρεία ομάδα προγραμματιστών [105].

Το μIP μπορεί να είναι πολύ χρήσιμο σε ενσωματωμένα συστήματα επειδή απαιτεί πολύ μικρές ποσότητες κώδικα και RAM. Έχει μεταφερθεί σε διάφορες πλατφόρμες συμπεριλαμβανομένων των πλατφορμών[15] DSP[16]. Η αρχιτεκτονική του διακομιστή μεσολάβησης είναι περίπλοκη, απαιτεί συγκεκριμένα στοιχεία και χρησιμοποιείται συνήθως για έναν συγκεκριμένο τύπο εφαρμογής. Τα δίκτυα που είναι ανεκτικά σε σχέση με τη λανθάνουσα καθυστέρηση (tolerant latency networks) μπορούν συχνά να κοινοποιούνται όταν οι κόμβοι είναι αδρανείς ή όταν οι κόμβοι αποτυγχάνουν λόγω ενεργειακού προβλήματος. Και στις δύο περιπτώσεις, η διαδρομή από άκρο σε άκρο μπορεί να διαταραχθεί και τα ποσοστά εγκατάλειψης πακέτων στο WSN μπορεί να είναι αρκετά υψηλά.

3.6 Έξυπνη Πόλη

Σε ένα γενικότερο πλαίσιο ερμηνείας, μία «έξυπνη πόλη» είναι ένας τόπος όπου τα παραδοσιακά δίκτυα και υπηρεσίες γίνονται πιο ευέλικτα, αποτελεσματικότερα και βιώσιμα με τη χρήση τεχνολογιών πληροφοριών και τηλεπικοινωνίας, για τη βελτίωση της λειτουργίας της προς το όφελος των κατοίκων της. Με άλλα λόγια, σε μία έξυπνη πόλη, οι ψηφιακές τεχνολογίες «μεταφράζονται» σε καλύτερες δημόσιες υπηρεσίες/ευκολίες για τους κατοίκους και σε καλύτερη χρήση των διαθέσιμων πόρων, ενώ επηρεάζεται λιγότερο το περιβάλλον.

Ένας από τους επίσημους ορισμούς της «έξυπνης πόλης» είναι ο ακόλουθος [106]: Μια πόλη «*που συνδέει τη φυσική υποδομή, την υποδομή τεχνολογίας πληροφοριών, την κοινωνική υποδομή και την επιχειρηματική υποδομή για να αξιοποιήσει τη συλλογική νοημοσύνη της πόλης*». Οποιοσδήποτε συνδυασμός διαφόρων έξυπνων στοιχείων/συσκευών/εξοπλισμών/εφαρμογών μπορεί να καταστήσει τις πόλεις ως έξυπνες. Εντούτοις, μία πόλη δεν χρειάζεται να έχει όλα αυτά τα στοιχεία για να χαρακτηριστεί ως «έξυπνη». Ο αριθμός των έξυπνων εξαρτημάτων εξαρτάται από το κόστος και τη διαθέσιμη τεχνολογία [83].

---

[14] Για περισσότερες πληροφορίες βλέπε, *μεταξύ άλλων*: https://en.wikipedia.org/wiki/BSD_licenses

[15] Metzinger, Z. (March 25, 2008): "Application Note 4205 - Using the uIP Stack to Network a MAXQ Microcontroller". Maxim Integrated Products, Inc.

[16] Barnett, D., and Massa, A.J. (February 1, 2005): "Inside the uIP Stack". Dr Dobbs Journal.

Τα στοιχεία των έξυπνων πόλεων περιλαμβάνουν έξυπνες υποδομές, έξυπνα κτίρια, έξυπνες μεταφορές, έξυπνη ενέργεια, έξυπνη υγειονομική περίθαλψη, έξυπνη τεχνολογία, έξυπνη διακυβέρνηση, έξυπνη εκπαίδευση και έξυπνους πολίτες. Διαφορετικές έξυπνες πόλεις έχουν διαφορετικά επίπεδα αυτών των έξυπνων στοιχείων, ανάλογα με το τον τομέα στον οποίο εκάστοτε εστιάζουν [84].

Τα διάφορα χαρακτηριστικά των έξυπνων πόλεων περιλαμβάνουν τη βιωσιμότητα, την ποιότητα ζωής, την αστικοποίηση και την ευφυΐα. Η βιωσιμότητα μίας έξυπνης πόλης σχετίζεται με τις υποδομές και τη διακυβέρνηση της πόλης, με την ενέργεια και την κλιματική αλλαγή, με τη ρύπανση και τα απόβλητα, αλλά και με κοινωνικά ζητήματα, τα οικονομικά και την υγεία. Η ποιότητα ζωής μπορεί να «μετρηθεί»-αποτιμηθεί με βάση τη συναισθηματική και οικονομική ευημερία των πολιτών [86].

4

Δίκτυα 5ης Γενιάς (5G)

Ο όρος "5G" αναφέρεται στην πέμπτη γενιά ασύρματης τηλεπικοινωνιακής τεχνολογίας που θα έχει τεράστιο αντίκτυπο σε πολλές πτυχές της καθημερινής μας ζωής. Η κίνηση των δικτύων κινητής τηλεφωνίας συνεχίζει να αυξάνεται με πολύ γρήγορο τρόπο, λόγω των νέων προσφερόμενων τεχνολογιών και συναφών εφαρμογών, όπως π.χ. οι εφαρμογές εικονικής πραγματικότητας, η ροή βίντεο υψηλής ανάλυσης και τα online (επιγραμμικά) παιχνίδια σε περιβάλλον cloud (νέφους). Σε λίγα χρόνια, οι υφιστάμενες υπηρεσίες 4G δεν θα ήταν σε θέση ώστε να ικανοποιήσουν την ταχύτητα της αύξησης της κίνησης αλλά και τις αναμενόμενες απαιτήσεις των νέων επιστημονικών τεχνολογιών, όπως τα μη επανδρωμένα αεροσκάφη (Unmanned Aerial Vehicles - UAVs), η εικονική πραγματικότητα (Virtual Reality - VR) και τα αυτόνομα οχήματα (autonomous vehicles).

Ως εκ τούτου, ακαδημαϊκοί και βιομηχανικοί ερευνητές έχουν καταβάλει πολλές προσπάθειες για να καταστήσουν τα συστήματα 5G ως πραγματικότητα. Για το σκοπό αυτό έχουν αμφότεροι καταλήξει σε συναίνεση ότι τα συστήματα 5G θα χρησιμοποιούν αυξανόμενες εξέχουσες τεχνολογίες όπως η εικονικοποίηση λειτουργιών δικτύου (Network Function Virtualization - NFV) και η δικτύωση που καθορίζεται από λογισμικό (Software-defined Networking - SDN) για την επίτευξη των στόχων τους. Χρησιμοποιώντας τις νέες τεχνολογίες, το 5G θα είναι πολύ ανώτερο από το τρέχον δίκτυο όσον αφορά στην ταχύτητα μετάδοσης [109].

Το 5G θα παρέχει ρυθμούς μετάδοσης δεδομένων έως και 10 Gbps, που είναι 10 έως 100 φορές υψηλότεροι από αυτούς που σήμερα προσφέρουν οι τεχνολογίες 4G και 4G-LTE. Το 5G αναμένεται να ξεπεράσει τα δίκτυα υπεραποδόμησης και να συνδυάσει υπάρχουσες τεχνολογίες όπως το Διαδίκτυο των πραγμάτων (Internet of Things - IoT), το νέφος (cloud), τα μεγάλα δεδομένα (big data), την τεχνητή νοημοσύνη (AI) για να υποστηρίξει τη δημιουργία καινοτόμων υπηρεσιών.

Εκτός από τη βελτίωση της ταχύτητας, ένα άλλο σημαντικό χαρακτηριστικό του 5G είναι η χαμηλότερη λανθάνουσα καθυστέρηση (latency). Στην πραγματικότητα, στην εποχή των επερχόμενων δικτύων 5G, ο χρόνος καθυστέρησης είναι μικρότερος από ένα χιλιοστό του

δευτερολέπτου (ms), ο οποίος είναι σχεδόν ίσος με τον χρόνο μηδενικής απόκρισης δεδομένων στον πραγματικό κόσμο. Όχι μόνο αυτό, αλλά βάσει του εξαιρετικά εκτενούς εύρους ζώνης του 5G ανά μονάδα περιοχής, της συνδεσιμότητας ανά μονάδα, της κάλυψης (σχεδόν 100%) και της δυνατότητας σύνδεσης συσκευών, μπορεί να δημιουργηθεί ένα οικοσύστημα, όπου «έξυπνα δίκτυα» μπορούν να χρησιμοποιηθούν για μεγάλες ιατρικές συσκευές και για να παρέχουν διαδραστικότητα σε πραγματικό χρόνο [110].

Το 5G είναι ένα δίκτυο που αναμένεται να λύσει ή τουλάχιστον να κάνει πιο εύκολη την επίλυση των πιο κρίσιμων τρεχόντων κοινωνικών προβλημάτων όπως η αλλαγή του κλίματος, η ασφάλεια από καταστροφές και η κυκλοφοριακή συμφόρηση. Πλέον, εταιρείες από όλον τον κόσμο έχουν αναλάβει τον αγώνα στην έρευνα και ανάπτυξη για την εξαγωγή της επερχόμενης τεχνολογίας 5ης γενιάς (5G) στις αγορές, η οποία θεωρείται ότι είναι η πιο σημαντική πηγή εσόδων στο μέλλον, ενώ αναμένεται ότι οι μελλοντικές τεχνολογίες στο πλαίσιο του 5G θα επιφέρουν τεράστιες αλλαγές και στη βιομηχανία παραγωγής και διαχείρισης ενέργειας [112].

Στον παρακάτω πίνακα αποτυπώνονται ενδεικτικά ορισμένες βασικές υπηρεσίες οι οποίες δύνανται να αναδυθούν μέσα από την τεχνολογία 5G:

Είδος υπηρεσίας	Περιγραφή
Μετάδοση εικόνας & ήχου	• Επαυξημένη πραγματικότητα (AR) • Εικονική πραγματικότητα (VR) • Τηλεδιάσκεψη υψηλής ανάλυσης
Τεχνητή νοημοσύνη	• Εξατομικευμένη τεχνητή νοημοσύνη για βοήθεια στην καθημερινότητα • Ανάπτυξη διαστημικών υπηρεσιών με χρήση τεχνητής νοημοσύνης
Υποδομές	• Έξυπνο σπίτι, έξυπνη πόλη • Διαχείριση ενέργειας • Προστασία κρίσιμων υποδομών
Αυτονομία	• Μη επανδρωμένα οχήματα (UAVs) • Αυτόνομο αυτοκίνητο • Υπηρεσίες αυτόνομων αεροσκαφών (drones)
Ασφάλεια	• Νευρωνικά δίκτυα παρακολούθησης εικόνας • Ταυτοποίηση και αναγνώριση οχημάτων & ανθρώπων • Εξατομικευμένες υπηρεσίες δημόσιας και ιδιωτικής ασφάλειας
Δημόσιες υπηρεσίες	• Τηλεϊατρική • Υπηρεσίες διάσωσης και παροχής βοήθειας • Υπηρεσίες πολιτικής προστασίας

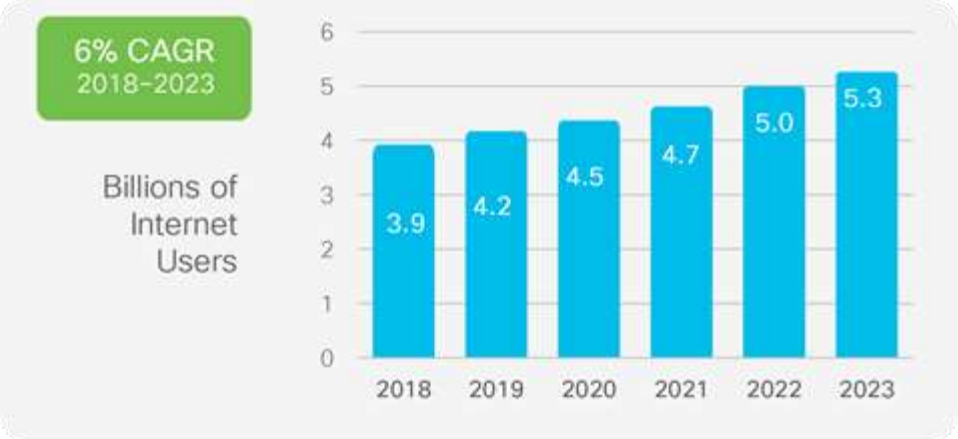
Πίνακας 4-1: Αναδυόμενες υπηρεσίες με την τεχνολογία 5G[17]

[17] Kim Bumsu (2019): ICT-Based Business Communication with Customers in the 4th Industrial Revolution Era. Business Communications Research and Practice 2(2), 55-61. https://doi.org/10.22682/bcrp.2019.2.2.55

4.1 Αναγκαιότητα και Λόγοι Ανάπτυξης Δικτύων 5G

Το 5G αναμένεται να αποφέρει σημαντικά οικονομικά οφέλη στις παγκόσμιες αγορές. Οι αναλυτές εκτιμούν ότι στις Ηνωμένες Πολιτείες, το 5G θα μπορούσε να δημιουργήσει έως και 3 εκατομμύρια νέες θέσεις εργασίας και να προσθέσει 500 δισεκατομμύρια δολάρια στο ακαθάριστο εγχώριο προϊόν (ΑΕΠ) της χώρας. Σε παγκόσμιο επίπεδο, οι αναλυτές εκτιμούν ότι οι τεχνολογίες 5G θα μπορούσαν να δημιουργήσουν 12,3 τρισεκατομμύρια δολάρια σε δραστηριότητες πωλήσεων σε πολλές βιομηχανίες και να υποστηρίξουν 22 εκατομμύρια θέσεις εργασίας έως το 2035. Ως εκ τούτου, εταιρείες τεχνολογίας σε όλο τον κόσμο αγωνίζονται για να αναπτύξουν προϊόντα 5G και ορισμένες χώρες (δηλαδή, κεντρικές κυβερνήσεις) ενεργούν στρατηγικά για την υποστήριξη της ανάπτυξης 5G. Αυτός ο αγώνας για την ανάπτυξη προϊόντων 5G και τη σύλληψη της παγκόσμιας αγοράς 5G ονομάζεται συχνά «αγώνας προς το 5G» [114].

Η κίνηση των δεδομένων που παράγονται από τις κινητές τηλεφωνικές συσκευές, αλλά και από τις διάφορες συσκευές που απαρτίζουν το Διαδίκτυο των Αντικειμένων (Internet of Things - IoT), σήμερα εξυπηρετούνται από τα υπάρχοντα δίκτυα επικοινωνιών τέταρτης γενιάς (4G, 4G+). Τα δίκτυα αυτά έχουν συγκεκριμένες απαιτήσεις, καθώς καθιστούν δυνατή την επικοινωνία μεταξύ στοιχείων του Διαδικτύου των Αντικειμένων, και επίσης εξυπηρετούν τις ευρυζωνικές υπηρεσίες. Όμως, ο ολοένα αυξανόμενος όγκος των δεδομένων που διαχειρίζονται τα δίκτυα, εκτιμάται ότι έως το 2025 θα φθάσει τα 35 Exabytes. Επίσης, ο αριθμός των συσκευών του IoT και των δεδομένων που απορρέουν από αυτές αναμένεται να αυξηθεί εκθετικά, καθώς ο αριθμός των μηχανών θα ξεπεράσει τα κινητά τηλέφωνα. Έτσι, εμφανίζεται επιτακτική η ανάγκη ανάπτυξης ενός νέου δικτύου επικοινωνιών, το οποίο καλείται να καλύψει αυτές τις απαιτήσεις. Το δίκτυο πέμπτης γενιάς (5G) αναμένεται να αποτελέσει τη μελλοντική βάση δικτύων, αξιοποιώντας αναδυόμενες τεχνολογίες πρόσβασης και έναν συνδυασμό υπαρχόντων τεχνολογιών δικτύων. Παρακάτω παρουσιάζεται η ετήσια αύξηση του αριθμού των κινητών και των συσκευών τύπου «Machine To Machine - M2M» [115].



Εικόνα 4-1: Ρυθμός ανάπτυξης χρηστών διαδικτύου παγκοσμίως[18]

[18] Cisco Annual Internet Report (2018-2023) White Paper, Updated March 9, 2020.

4.2 Απαιτήσεις Απόδοσης 5G

Ο κύριος στόχος της τεχνολογίας 5G είναι η επίτευξη υψηλών συχνοτήτων μετάδοσης συνδυαστικά με μεγάλο εύρος ζώνης, όπως ορίζεται από τον πρότυπο IMT-2020[19] της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU). Τα μελλοντικά συστήματα τηλεπικοινωνιών 5G θα πρέπει να πληρούν αυτές τις απαιτήσεις ώστε να υπάρχει μία κοινή προσέγγιση για την ανάπτυξη υποδομών[20].

Η Διεθνής Ένωση Τηλεπικοινωνιών (International Telecommunications Union – ITU) έχει ορίσει τις κατηγορίες περίπτωσης χρήσης 5G ως (i) ενισχυμένη κινητή ευρυζωνική πρόσβαση (enhanced mobile broadband - eMBB), (ii) εξαιρετικά αξιόπιστες και χαμηλού χρόνου καθυστέρησης επικοινωνίες (ultra-reliable and low latency communications - URLLC) και (iii) μαζικές επικοινωνίες μηχανικού τύπου (massive Machine type Communications - mMTC). Ο φορέας 3GPP[21] έχει επίσης εντοπίσει αυτές τις περιπτώσεις χρήσης, αντίστοιχα ως: (i) ενισχυμένη ευρυζωνική κινητή, (ii) κρίσιμες επικοινωνίες και (iii) τεράστιο Internet of Things (mIoT) [118].

Τα συστήματα 5G αναμένεται να μειώσουν το κόστος ανάπτυξης δικτύου και να παρέχουν αυξημένη διαθεσιμότητα και κάλυψη σε σύγκριση με τα παλαιά συστήματα προηγούμενης γενιάς, ενώ θα ικανοποιούν τα αυξημένα προφίλ κινητικότητας, τα οποία κατηγοριοποιούνται ως: στάσιμο (0 km/h), πεζού / χαμηλής κινητικότητας (έως 10 km/h), οχήματος (10-120 km/h) και υψηλής ταχύτητας (120- 500 km/h). Επομένως, απαιτούνται νέες τεχνολογίες για την παροχή ασφαλών υπηρεσιών 5G που θα λειτουργούν απρόσκοπτα σε πολλά όρια δικτύου προσφέροντας ασφαλή λειτουργικότητα [121].

4.3 Αρχιτεκτονική Λειτουργίας Δικτύου 5G

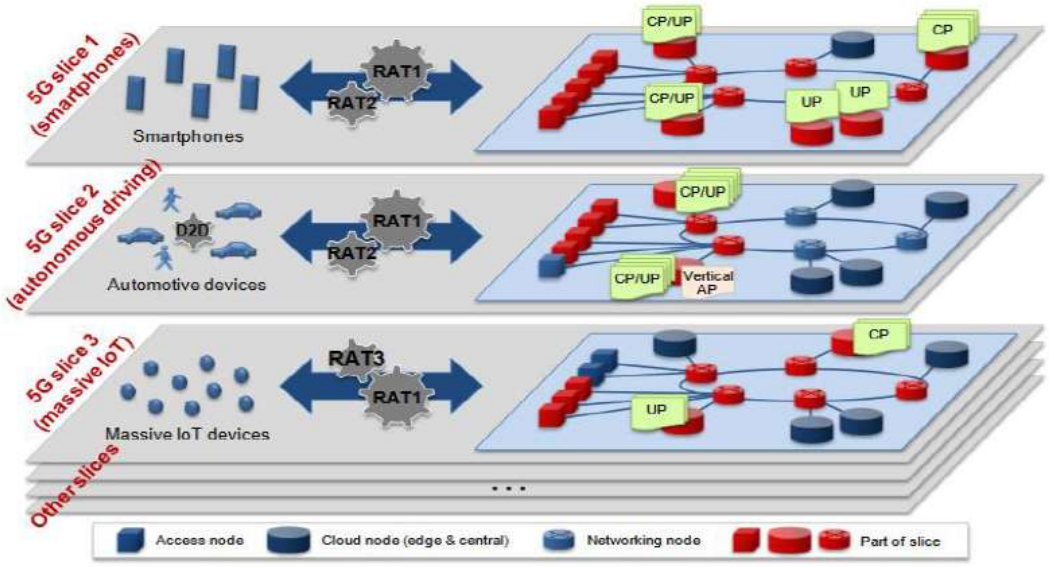
Ένας από τους στόχους και κινητήρια δύναμη της εξέλιξης της αρχιτεκτονικής του δικτύου 5G είναι η παροχή διαφοροποιημένων υπηρεσιών χρησιμοποιώντας δίκτυα κινητής τηλεφωνίας. Ο τεμαχισμός δικτύου (network slicing) είναι μία θεμελιώδης τεχνολογία για την επίτευξη αυτού του στόχου. Στην εποχή του 5G, ένα δίκτυο θα περιέχει πολλές λογικά διαχωρισμένες «φέτες» δικτύου (network slices). Κάθε φέτα διαθέτει συγκεκριμένη τοπολογία δικτύου, λειτουργία δικτύου και αντίστοιχο μοντέλο κατανομής πόρων. Τα δίκτυα 5G θα πρέπει να διαθέτουν δυνατότητες ευέλικτης λειτουργίας αυτό-εξυπηρέτησης. Οι υπηρεσίες τεμαχισμού δικτύου μπορούν να δημιουργηθούν, να διατηρηθούν ή να τερματιστούν αυτόματα σύμφωνα με τις απαιτήσεις των σχετικών υπηρεσιών, γεγονός που μειώνει σημαντικά τα λειτουργικά έξοδα του δικτύου. Οι καθετοποιημένοι τομείς της αγοράς (γνωστοί και ως “verticals”) μπορούν να εισάγουν συγκεκριμένες απαιτήσεις τεμαχισμού του δικτύου κινητής τηλεφωνίας σε μία πλατφόρμα λειτουργίας. Ο αρμόδιος χειριστής αναλύει τις απαιτήσεις των πελατών με βάση την τρέχουσα κατάσταση δικτύου. Αφού ολοκληρωθεί η διαδικασία συμφωνίας σε επίπεδο υπηρεσίας (Service Level

[19] Για περισσότερες πληροφορίες βλέπε, μεταξύ άλλων: https://en.wikipedia.org/wiki/IMT-2020

[20] ITU-R Recommendation M.2410 (2017-11): "Minimum requirements related to technical performance for IMT-2020 radio interface(s)". https://www.itu.int/pub/R-REP-M.2410-2017

[21] Για περισσότερες πληροφορίες βλέπε: https://www.3gpp.org/

Agreement - SLA), ο χειριστής χαρτογραφεί διάφορες απαιτήσεις υπηρεσίας σε απαιτήσεις δικτύου και επιλέγει πολλαπλά στοιχεία λειτουργίας δικτύου για να δημιουργήσει μία κατάλληλη δικτυακή φέτα. Σύμφωνα με τις δυνατότητες της υπηρεσίας και την ανάπτυξη κέντρων δεδομένων, ο χειριστής καθορίζει τους λογικούς κόμβους ανάπτυξης της λειτουργίας δικτύου και καθορίζει μία σχέση σύνδεσης, ειδικότερα μία μορφή τοπολογίας οριζόμενης από το λογισμικό (Software-defined Topology - SDT). Αφού καθοριστεί η τοπολογία τεμαχισμού δικτύου, καθορίζεται ένα πρωτόκολλο καθορισμένο από το λογισμικό (Software Defined Protocol – SDP). Σύμφωνα με τις απαιτήσεις της συναφούς υπηρεσίας-εφαρμογής, οι πόροι του δικτύου κατανέμονται καταλλήλως στη λογική τοπολογία για αντίστοιχες λογικές συνδέσεις. Τα SDT και SDP συνιστούν μία λίστα βασικών λειτουργιών που απαιτούνται για την Αυτόματη Δημιουργία Δικτύου με Στόχο την Εξυπηρέτηση της Υπηρεσίας (Service Oriented Network Auto Creation - SONAC) [122].



Εικόνα 4-2: Φέτες δικτύου 5G για διαφορετικές περιπτώσεις χρήσης [122]

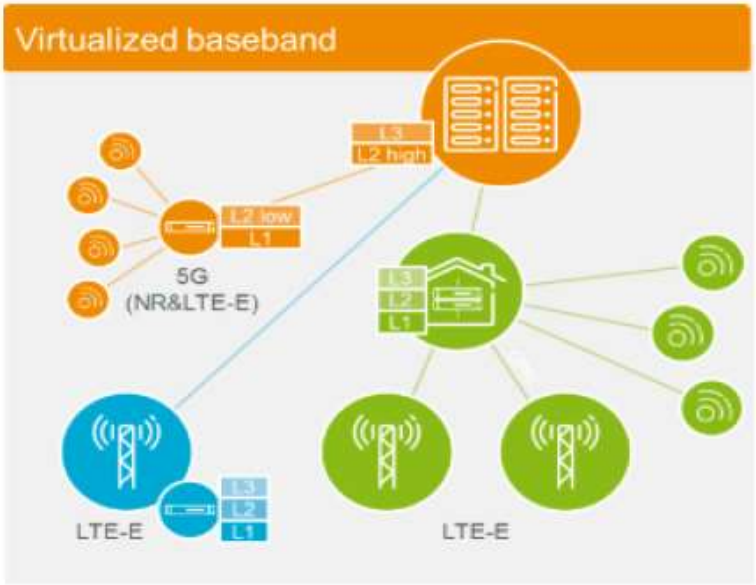
4.3.1 Αρχιτεκτονική C-RAN (Cloud-Radio Access Network)

Το 5G C-RAN (5G Ραδιοδίκτυο Νέφους) αποτελείται από μία μονάδα ζώνης βάσης (Base-Band Unit) και απομακρυσμένες κεφαλές εκπομπής ραδιοσήματος (Remote Radio Heads - RRHs). Το δίκτυο αυτό παρέχει στους χρήστες τη δυνατότητα σύνδεσης στον σταθμό βάσης, και κατ' επέκταση στο Διαδίκτυο. Το C-RAN μελετήθηκε πρώτη φορά από την εταιρεία IBM και αποτελεί μια βελτιωμένη έκδοση δικτύου που προβαίνει σε εκμετάλλευση της κεντρικοποίησης και της οπτικοποίησης[22].

Ωστόσο, όπως σε οποιαδήποτε άλλη νέα τεχνολογία δικτύου, η αρχιτεκτονική 5G C-RAN αντιμετωπίζει προκλήσεις, όπως η ανάπτυξη ενός αξιόπιστου και οικονομικού δικτύου fronthaul (πρόσθιου άκρου) με την απαιτούμενη χωρητικότητα και καθυστέρηση για μεγάλο αριθμό χρηστών [125].

[22] Για περισσότερα στοιχεία βλέπε επίσης: https://en.wikipedia.org/wiki/C-RAN

Με την αξιοποίηση του νέφους, καθίσταται δυνατός ο μερισμός (sharing) διαφορετικών τεχνολογιών ραδιοπρόσβασης στην ίδια φυσική υποδομή δικτύου. Στο C-RAN, η εκτέλεση των περισσοτέρων διαδικασιών του σταθμού βάσης πραγματοποιείται στο νέφος, διαχωρίζοντας τις διαδικασίες αυτές στο επίπεδο δεδομένων και στο επίπεδο ελέγχου (Data Plane (DP) – Control Plane (CP)). Έτσι, οι διαδικασίες στο επίπεδο δεδομένων εκτελούνται στους σταθμούς βάσης, ενώ οι διαδικασίες στο επίπεδο ελέγχου εκτελούνται στο cloud. Η αρχιτεκτονική της ραδιοπρόσβασης νέας γενιάς (5G C-RAN) εκμεταλλεύεται την τεχνική Εικονικοποίησης Δικτυακών Λειτουργιών (Network Function Virtualization – NFV) και τις επεξεργαστικές ικανότητες του κέντρου δεδομένων και έτσι ενεργοποιεί συντονισμό και κεντρικοποίηση στα δίκτυα [126].



Εικόνα 4-3: Αρχιτεκτονική 5G C-RAN[23]

4.3.2 Αρχιτεκτονική SDN/NFV

Μια άλλη «όψη» των αρχιτεκτονικών 5G είναι αυτή που συνδυάζει τις τεχνολογίες SDN και NFV. Βασίζεται στο διαχωρισμό του επιπέδου δεδομένων (DP) από το επίπεδο του ελέγχου (CP) έτσι ώστε ο δικτυακός εξοπλισμός να μπορεί να τύχει διαχείρισης εξωτερικά, από το λογισμικό διαχείρισης του αντίστοιχου εμπλεκόμενου παρόχου. Η οντότητα που χρειάζεται να πάρει αποφάσεις για την κίνηση του δικτύου (SDN Controller – Ελεγκτήρας SDN), δέχεται αιτήματα από τις διάφορες εφαρμογές και, ανάλογα ελέγχει τις διαδρομές δεδομένων (data paths) SDN. Η τεχνολογία SDN επιτρέπει στους διαχειριστές δικτύου να διαχειριστούν ή ακόμα και να βελτιστοποιήσουν το δίκτυο πολύ γρήγορα μέσω δυναμικών και αυτόματων SDN προγραμμάτων, τα οποία δεν εξαρτώνται από το υλισμικό, ενώ το NFV καθιστά δυνατό για διάφορες δικτυακές λειτουργίες το να πραγματοποιούνται σε υλισμικό γενικού σκοπού

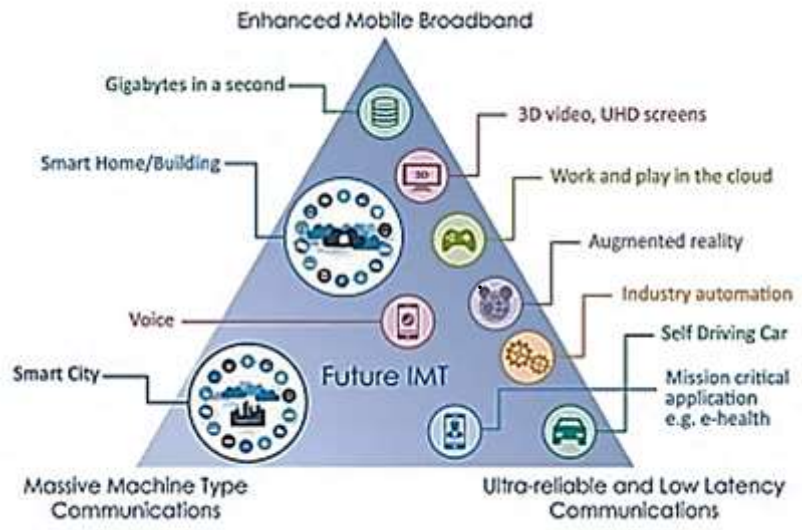
[23] White Paper: "Cloud RAN Architecture for 5G". A Telefonica White Paper prepared in collaboration with Ericsson. http://www.hit.bme.hu/~jakab/edu/litr/5G/WhitePaper_C-RAN_for_5G_-Telefonica_Ericsson.PDF.

(όπως π.χ. οι απλοί μεταγωγείς δικτύου να λειτουργούν ως δρομολογητές, δηλαδή ως ανωτέρου επιπέδου συσκευές).

Ένα άλλο παράδειγμα συνίσταται στο ότι θα μπορούσαν να αντικατασταθούν τα τείχη προστασίας (firewalls - FWs) ή ακόμα και άλλες συσκευές/εξοπλισμοί. Το NFV είναι διαφορετικό από το SDN, αλλά ουσιαστικά λειτουργεί ως συμπληρωματικό με αυτό. Είναι σημαντικό το να συνδυάζονται και να προσδίδουν ουσιαστικά σε μία αρχιτεκτονική τα βασικά τους πλεονεκτήματα. Μία άλλη σημαντική δυνατότητα, που παρέχεται από το NFV είναι το ότι καθίσταται εφικτό να προκύψουν σημαντικά οικονομικά οφέλη για νέες υπηρεσίες, οι οποίες διατίθενται γρηγορότερα στην αγορά [128].

4.4 Περιπτώσεις Χρήσης και Υπηρεσίες 5G

Το 5G υπόσχεται να προσφέρει υψηλότερες ταχύτητες λήψης, μικρότερο χρόνο καθυστέρησης και υψηλότερη χωρητικότητα. Ο στόχος της Βιομηχανίας 4.0[24] (Industry 4.0) είναι να μεγιστοποιήσει την αποδοτικότητά της χρησιμοποιώντας αυτές τις δυνατότητες σε όλες τις διαδικασίες και τα περιουσιακά στοιχεία της ανά πάσα στιγμή, και για να παρέχεται καλύτερη κατανόηση των διαδικασιών κατασκευής σε όλες τις τοποθεσίες παραγωγής, σε σχεδόν πραγματικό χρόνο. Με την αναμενόμενη αύξηση των απαιτήσεων δεδομένων που κυμαίνονται από κρίσιμη αποστολή έως μαζική συνδεσιμότητα μηχανών, η ανάπτυξη του 5G έχει δημιουργήσει προσδοκίες ότι θα ανοίξει νέες ευκαιρίες για την κατασκευή νέων επιχειρηματικών μοντέλων [129].



Εικόνα 4-4: Περιπτώσεις χρήσης 5G (ITU 2018)[25]

[24] Για περισσότερες σχετικές πληροφορίες βλέπε, π.χ.: https://www.i-scoop.eu/industry-4-0/

[25] Carugi, M. (2018). Key features and requirements of 5G/IMT-2020 networks, ITU Arab Forum on Emerging Technologies, Algiers – Algeria, 14-15 Feb. 2018. Accessible at: https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2018/RDF/Workshop%20Presentations/Session1/5G-%20IMT2020-presentation-Marco-Carugi-final-reduced.pdf

Η Τέταρτη Βιομηχανική Επανάσταση ή απλά η «Βιομηχανία 4.0» είναι ο τρόπος με τον οποίο η μεταποιητική βιομηχανία αναμένει να μεγιστοποιήσει τις καινοτομίες των ασύρματων επικοινωνιών 5G, αυτοματοποιώντας βιομηχανικές τεχνολογίες και χρησιμοποιώντας άλλες τεχνολογίες όπως η τεχνητή νοημοσύνη (AI) και η μηχανική μάθηση (Machine Learning - ML). Η βιομηχανία αναμένει ότι αυτό θα οδηγήσει σε ακριβέστερη λήψη αποφάσεων, όπως αυτοματοποίηση φυσικών εργασιών με βάση ιστορικές πληροφορίες και γνώσεις ή σε βελτιωμένα αποτελέσματα για ένα ευρύ φάσμα κάθετων αγορών όχι μόνο στη βιομηχανία αλλά και σε κλάδους όπως η γεωργία, η εφοδιαστική αλυσίδα εφοδιασμού, η υγειονομική περίθαλψη, η διαχείριση ενέργειας και ένας ολοένα αυξανόμενος αριθμός βιομηχανιών που συνειδητοποιούν περισσότερο τις δυνατότητες του 5G. Κάποιες περιπτώσεις χρήσης ίσως απαιτούν πολλαπλές διαστάσεις για βελτιστοποίηση ενώ άλλες εστιάζουν μόνο σε έναν δείκτη απόδοσης. Μία από τις κύριες προκλήσεις για τα δίκτυα κινητής 5ης γενιάς θα είναι το μπορούν να υποστηρίξουν διαφορετικές περιπτώσεις χρήσης (Use Cases - UCs) με όσο το δυνατό πιο ευέλικτους και αξιόπιστους τρόπους [132].

Οι υπηρεσίες που αναμένεται να προσφερθούν, ενδεικτικά κατηγοριοποιούνται ως: βελτιωμένη κινητή ευρυζωνικότητα (enhanced Mobility BroadBand - eMBB), μαζική επικοινωνία τύπου μηχανής (massive Machine Type Communication - mMTC) και αξιόπιστη και χαμηλής καθυστέρησης επικοινωνία (Ultra Reliable Low Latency Communication - URLLC)[26]. Συνοπτικά, οι υπηρεσίες αυτές αναλύονται στα παρακάτω κεφάλαια.

4.4.1 eMBB (Βελτιωμένη Κινητή Ευρυζωνική σύνδεση)

Το eMBB μπορεί αρχικά να αντιμετωπιστεί με την επέκταση σε υπάρχουσες υπηρεσίες 4G, καθώς στοχεύει στην εξυπηρέτηση πυκνοκατοικημένων μητροπολιτικών κέντρων με ταχύτητες κατερχόμενης ζεύξης που πλησιάζουν 1 Gbps (gigabits ανά δευτερόλεπτο) σε εσωτερικούς χώρους και 300 Mbps (megabit ανά δευτερόλεπτο) σε εξωτερικούς χώρους. Ένας τρόπος για να επιτευχθεί αυτό, είναι μέσω της εγκατάστασης κεραιών εξαιρετικά υψηλής συχνότητας (mm-Wave). Για αστικές περιοχές που είναι περισσότερο απομακρυσμένες και πέρα από αγροτικές (rural) περιοχές, το eMBB θα εργαστεί για την αντικατάσταση του τρέχοντος συστήματος LTE (Long-Term Evolution) του 4G, με ένα νέο δίκτυο παν-κατευθυντικών κεραιών χαμηλότερης ισχύος που θα παρέχουν υπηρεσία κατερχόμενης ζεύξης 50 Mbps. Η κίνηση eMBB μπορεί να θεωρηθεί ως προσθήκη στην ευρυζωνική υπηρεσία 4G η οποία διατίθεται σήμερα. Η eMBB είναι ικανή για μεγάλα ωφέλιμα φορτία και συσχετίζεται με ένα μοτίβο ενεργοποίησης ανά συσκευή, το οποίο μπορεί να παραμείνει σταθερό σε παρατεταμένο χρονικό διάστημα. Αυτό επιτρέπει στο δίκτυο να προγραμματίζει τη διάθεση ασύρματων πόρων σε συσκευές με δυνατότητα EMBB και να αποφεύγονται φαινόμενα διαμάχης (contention) μεταξύ δύο συναφών συσκευών που θα μπορούσαν να έχουν πρόσβαση στον ίδιο πόρο, ταυτόχρονα [133].

Η βελτιωμένη κινητή ευρυζωνική σύνδεση (eMBB), αναμένεται ότι θα προσφέρει[27]:

[26] Popovski, P., Trillingsgaard, K.F., Simeone, O., and Durisi, G. (2018): "5G wireless network slicing for eMBB, URLLC, and mMTC: A communication-theoretic view". IEEE Access, vol.6, pp.55765-55779.
[27] Ibid.

- Χωρητικότητα κίνησης έως και 10 Mbps ανά τετραγωνικό μέτρο σε κεντρικές (αστικές) περιοχές.

- Ταχύτητα μεταφοράς δεδομένων έως 1 Gbps, με μέγιστο ρυθμό μεταφοράς δεδομένων σε δεκάδες Gbps και χωρητικότητα μέγιστου όγκου κίνησης τουλάχιστον 1 Tbps ανά τετραγωνικό χιλιόμετρο.

- Καθυστέρηση τόσο χαμηλή όσο 1 ms για την ανταλλαγή δεδομένων.

- Πυκνότητα σύνδεσης έως και ένα εκατομμύριο συνδέσεις ανά τετραγωνικό χιλιόμετρο.

- Υψηλή κινητικότητα, διευκολύνοντας τη συνδεσιμότητα έως και 500 km/h σε τρένα υψηλής ταχύτητας και έως 1000 km/h σε αεροπλάνα, με βελτιωμένη εμπειρία χρήστη.

4.4.2 URLLC (Εξαιρετικά Αξιόπιστες Επικοινωνίες Χαμηλής Καθυστέρησης)

Ο τομέας εφαρμογών URLLC μπορεί να αντιμετωπίσει κρίσιμες ανάγκες επικοινωνιών, όπου το εύρος ζώνης δεν είναι τόσο κρίσιμο όσο η ταχύτητα (π.χ. καθυστέρηση από άκρο σε άκρο 1 ms ή μικρότερη). Ο σχεδιασμός μίας υπηρεσίας χαμηλής καθυστέρησης και υψηλής αξιοπιστίας περιλαμβάνει πολλά στοιχεία, όπως π.χ.: εξαιρετικά γρήγορη ανακύκλωση δεδομένων, αποτελεσματικό έλεγχο και κοινή χρήση πόρων δεδομένων, μετάδοση ανερχόμενης ζεύξης και προηγμένα σχήματα κωδικοποίησης καναλιών. Αυτό εγγυάται τη μείωση της καθυστέρησης μετάδοσης σήματος. Αυτές οι υπηρεσίες υποστηρίζονται από το πρότυπο 5G New Radio (NR)[28]. Το URLLC ως τεχνολογική υπηρεσία θα έχει εφαρμογή ιδίως στις εταιρίες αυτόνομων οχημάτων, όπου ο χρόνος απόφασης για αντίδραση σε πιθανό ατύχημα πρέπει να είναι σχεδόν ανύπαρκτος. Επίσης, το URLLC καθιστά το 5G μία εξαιρετικά ανταγωνιστική λύση έναντι δορυφόρου, κυρίως για υπηρεσίες παγκόσμιου εντοπισμού θέσης (GPS) [134].

[28] Η 5G NR (Νέα Ραδιοεπικοινωνία) είναι νέα τεχνολογία ραδιοπρόσβασης που αναπτύχθηκε από το 3GPP για το δίκτυο κινητής τηλεφωνίας πέμπτης γενιάς (5G). Σχεδιάστηκε για να είναι το παγκόσμιο πρότυπο για τη ραδιοδιεπαφή των δικτύων 5G. Η μελέτη της NR εντός του 3GPP ξεκίνησε το 2015 και η πρώτη προδιαγραφή διατέθηκε από τα τέλη του 2017. Ενώ η διαδικασία τυποποίησης του 3GPP ήταν σε εξέλιξη, η βιομηχανία είχε ήδη ξεκινήσει προσπάθειες για την υλοποίηση υποδομής συμβατής με το σχέδιο προτύπου, με την προσδοκία ότι η πρώτη μεγάλης κλίμακας εμπορική κυκλοφορία της 5G NR θα ήταν σε θέση ώστε να πραγματοποιηθεί το 2019. Πηγές: What is 5G New Radio (5G NR). 5g.co.uk.
«Making 5G New Radio (NR) a Reality – The Global 5G Standard - IEEE Communications Society». comsoc.org.

4.4.3 Μαζικές Επικοινωνίες Τύπου Μηχανής (mMTC)

Το 5G προσφέρει μαζική επικοινωνία τύπου μηχανής (massive Machine Type Communication - mMTC), η οποία στοχεύει να υποστηρίξει δισεκατομμύρια συσκευές με δυνατότητα δικτύου για ασύρματη σύνδεση. Τα σημερινά συστήματα επικοινωνίας εξυπηρετούν ήδη πολλές αντίστοιχες εφαρμογές. Ωστόσο, οι χαρακτηριστικές ιδιότητες του mMTC, δηλαδή ο τεράστιος αριθμός συσκευών και τα μικρά μεγέθη ωφέλιμου φόρτου, απαιτούν νέες προσεγγίσεις και ιδέες. Το 5G επιτρέπει πυκνότητα ενός εκατομμυρίου συσκευών ανά τετραγωνικό χιλιόμετρο. Το 5G θα μπορεί να μεταφέρει πολύ περισσότερα δεδομένα και να τα μεταφέρει πολύ πιο γρήγορα από το 4G LTE· ωστόσο, το γρηγορότερο δεν είναι πάντα καλύτερο ή ακόμη και απαραίτητο στον κόσμο του IoT, ειδικά όταν συνήθως απαιτεί περισσότερη ισχύ στην τελική συσκευή. Έτσι, το πρότυπο 5G NR θα εισάγει νέους τύπους συσκευών, όπως π.χ. το Cat-M1[29] (λειτουργεί σε εύρος ζώνης 1,4 MHz) και σε IoT στενής ζώνης[30] (NB-IoT). Τόσο οι συσκευές NB-IoT όσο και οι συσκευές Cat-M1 μπορούν να τεθούν σε λειτουργία «ύπνου» (sleep mode) για παρατεταμένα χρονικά διαστήματα με λειτουργίες εκτεταμένης ασυνεχούς λήψης (extended discontinuous reception) καθώς και λειτουργίες εξοικονόμησης ενέργειας (power-saving mode), οι οποίες μειώνουν σημαντικά την κατανάλωση ενέργειας της συσκευής. Αυτό θα επιτρέψει σε συσκευές με λιγότερες απαιτήσεις ενέργειας να λειτουργήσουν σε κατάσταση δικτύου με τη χρήση μπαταριών. Το 5G σε βιομηχανικό αυτοματισμό θα διευκολύνει τα ασύρματα δίκτυα αισθητήρων σε πραγματικό χρόνο, με εντοπισμό θέσης και στοιχείων. Τα δίκτυα 5G θα μπορούν τελικά να αντικαταστήσουν τις ενσύρματες συνδέσεις ακόμη και στις πιο απαιτητικές εφαρμογές, όπως ο αυτοματισμός και τα συστήματα υψηλής απόδοσης όρασης [135].

Κατηγορία περίπτωσης χρήσης	Στόχοι απόδοσης
eMBB	Υψηλός ρυθμός δεδομένων, χαμηλός χρόνος καθυστέρησης
mIoT/mMTC	Εξαιρετικά υψηλή πυκνότητα συσκευών, εξαιρετικά χαμηλή κατανάλωση ενέργειας
URLLC, κρίσιμες επικοινωνίες	Εξαιρετικά υψηλή αξιοπιστία, χαμηλός χρόνος καθυστέρησης, ισχυρή ασφάλεια

Πίνακας 4-2: Κατηγοριοποίηση των περιπτώσεων χρήσης 5G από την ITU και στόχοι αποδόσεων αυτών[31]

[29] Για περισσότερες πληροφορίες βλέπε, π.χ.: https://www.soracom.io/iot-definitions/what-is-cat-m1/
[30] Για περισσότερες πληροφορίες βλέπε: https://www.gsma.com/iot/narrow-band-internet-of-things-nb-iot/
[31] ITU-R Recommendation M.2410 (2017-11): "Minimum requirements related to technical performance for IMT-2020 radio interface(s)". https://www.itu.int/pub/R-REP-M.2410-2017

Περίπτωση Χρήσης	Κατηγορία	Απαίτηση
eMBB	Ανά σύνδεση καθόλη τη διάρκεια	1-10 Gbps
	Συγκεντρωτική κατερχόμενη ζεύξη κυψέλης καθόλη τη διάρκεια χρήσης	20 Gbps
	Συγκεντρωτική ανερχόμενη ζεύξη κυψέλης καθόλη τη διάρκεια χρήσης	10 Gbps
	Σύνδεση σε εσωτερικό χώρο ανά τετραγωνικό μέτρο	10 Mbps ανά τετραγωνικό μέτρο
	Κατερχόμενη ζεύξη καθόλη τη διάρκεια χρήσης ανά χρήστη	100 Mbps
	Ανερχόμενη ζεύξη καθόλη τη διάρκεια χρήσης ανά χρήστη	50 Mbps
	Καθυστέρηση επιπέδου χρήστη	4 ms
	Καθυστέρηση επιπέδου ελέγχου	10-20 ms
	Κινητικότητα (πυκνό αστικό πεδίο)	Έως 30 Km/h
	Κινητικότητα (αγροτική περιοχή)	Έως 500 Km/h
mMTC / mIoT	Αριθμός συνδεδεμένων συσκευών ανά τετραγωνικό χιλιόμετρο	1 εκατομμύριο
URLLC, κρίσιμες επικοινωνίες	Καθυστέρηση επιπέδου χρήστη	1 ms
	Καθυστέρηση επιπέδου ελέγχου	10-20 ms
	Αξιοπιστία	99.999%

Πίνακας 4-3: Ποσοτικοί στόχοι σχεδιασμού απόδοσης για περιπτώσεις χρήσης 5G[32]

[32] Ibid.

4.5 Μετάβαση του IoT στο 5G

Το μελλοντικό δίκτυο κινητών επικοινωνιών 5G θα πρέπει να υποστηρίξει τη ανάπτυξη του μαζικού IoT (mIoT) με δισεκατομμύρια συνδεδεμένων έξυπνων συσκευών και αισθητήρων, τα οποία θα αποτελούν τον παγκόσμιο ψηφιακό κόσμο. Το δίκτυο 5G NR το οποίο βρίσκεται υπό ανάπτυξη, αναμένεται να υποστηρίξει τόσο την περίπτωση του μαζικού όσο και του κρίσιμου IoT, καθώς οι απαιτήσεις για επικοινωνίες συνεχίζουν να αυξάνονται με ραγδαίο ρυθμό. Το Διαδίκτυο των αντικειμένων στο δίκτυο LTE (LTE IoT) αρχικά μελετήθηκε από τον οργανισμό 3GPP, στην Έκδοση 13 (Rel.13)[33]. Σε αυτό το πρότυπο, οι τεχνολογίες που αναπτύχθηκαν για επικοινωνία στο IoT, είναι τα πρότυπα LTE-Cat M1 και NB-IoT. Τα πρότυπα αυτά εντάσσονται στο LTE και αποτελούν τεχνολογίες κυψελών οι οποίες παρέχουν μια ενιαία πλατφόρμα συνδεσιμότητας στο IoT, εξασφαλίζοντας επικοινωνία σε μεγάλο πλήθος συνδέσεων και αποτελεσματική απόδοση ισχύος των συσκευών [136].

[33] Βλέπε: https://www.3gpp.org/ftp/Information/WORK_PLAN/Description_Releases/

5

Κρίσιμες Υποδομές

Η καθημερινή ζωή βασίζεται σε μεγάλο βαθμό στην αξιόπιστη και ασφαλή λειτουργία καθώς και στην έξυπνη διαχείριση κρίσιμων υποδομών μεγάλης κλίμακας. Οποιαδήποτε καταστροφή ή διακοπή αυτών των υποδομών θα προκαλούσε τεράστιες συνέπειες και θα είχε εκτενή αντίκτυπο στην ασφάλεια, την εθνική οικονομία, την εθνική δημόσια υγεία ή την ασφάλεια ή σε οποιονδήποτε συνδυασμό αυτών των ζητημάτων. Ως Κρίσιμες Υποδομές (ΚΥ) ή Υποδομές Ζωτικής Σημασίας (ΥΖΣ) νοούνται τα περιουσιακά στοιχεία, συστήματα ή μέρη αυτών που είναι ουσιώδη για την τήρηση των λειτουργιών ζωτικής σημασίας της κοινωνίας, της υγείας, της ασφάλειας, της οικονομικής και κοινωνικής ευημερίας των μελών της και των οποίων η διακοπή λειτουργίας ή η καταστροφή τους θα είχε σημαντικό αντίκτυπο για τη χώρα, ως αποτέλεσμα της αδυναμίας συνέχισης των λειτουργιών αυτών[34].

Χαρακτηριστικά παραδείγματα κρίσιμων υποδομών αποτελούν οι τομείς της Ηλεκτρικής Ενέργειας, των Τηλεπικοινωνιών και του Διαδικτύου, του Πετρελαίου και Φυσικού Αερίου (Oil & Gas), του Τραπεζοοικονομικού Συστήματος, των Κυβερνητικών Υπηρεσιών, των Μεταφορών, των Συστημάτων Διαχείρισης Νερού (Water Treatment Units), των Υπηρεσιών Υγείας και Άμεσης Ανάγκης (όπως π.χ. οι ευρωπαϊκοί αριθμοί 112, 119, 166 κλπ.), των Τροφίμων και της Γεωργίας αλλά και της Παραγωγής των διαφόρων Πρώτων Υλών (όπως π.χ. χαλκός, σίδερο, ατσάλι, αλουμίνιο, μάρμαρο, ξύλο κλπ.)

Όλοι οι τομείς υποδομών δεν είναι το ίδιο ζωτικοί/κρίσιμοι σε κάθε χώρα. Κάποιοι τομείς μπορούν να χαρακτηριστούν ως «κρίσιμοι» και κάποιοι ως «λιγότερο κρίσιμοι» ή ως «ελάχιστα σημαντικοί». Επιπλέον, δεν είναι όλες οι υπηρεσίες ενός τομέα/υποτομέα εξίσου κρίσιμες, γεγονός το οποίο δυσχεραίνει τον προσδιορισμό της αρχικής λίστας κρίσιμων τομέων σε στρατηγικό επίπεδο [141].

---

[34] Οδηγία 114/2008/ΕΚ του Ευρωπαϊκού Συμβουλίου της 8ης Δεκεμβρίου 2008 σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους. Επίσημη Εφημερίδα L345, σελ.75-82, 23.12.2008. https://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX%3A32008L0114

Τομέας	Περιγραφή	Υποτομέας ή υπηρεσία
I	Ενέργεια	1. Παραγωγή πετρελαίου και φυσικού αερίου, διύλιση, επεξεργασία, αποθήκευση, αγωγοί μεταφοράς 2. Παραγωγή ηλεκτρικής ενέργειας 3. Μεταφορά ηλεκτρικής ενέργειας, πετρελαίου και φυσικού αερίου 4. Διανομή ηλεκτρικής ενέργειας, πετρελαίου και φυσικού αερίου
II	Τεχνολογίες Πληροφορικής & Επικοινωνιών	5. Πληροφοριακά συστήματα & προστασία δικτύων 6. Συστήματα ελέγχου και αυτοματισμού (SCADA) 7. Διαδίκτυο 8. Παροχή σταθερών τηλεπικοινωνιών 9. Παροχή κινητών τηλεπικοινωνιών 10. Ραδιοεπικοινωνία και πλοήγηση 11. Δορυφορική Επικοινωνία 12. Εκπομπή & αναμετάδοση
III	Ύδατα	13. Παροχή πόσιμου νερού 14. Έλεγχος ποιότητας νερού 15. Φράγματα και έλεγχος ποσότητας νερού
IV	Τρόφιμα	16. Παραγωγή τροφίμων, υγιεινή και ασφάλεια τροφίμων
V	Υγεία	17. Ιατρική & νοσοκομειακή περίθαλψη 18. Φάρμακα, οροί, εμβόλια και φαρμακευτικά 19. Βιολογικά εργαστήρια και βιολογικοί παράγοντες
VI	Οικονομία	20. Υπηρεσίες πληρωμών – Δομές πληρωμών 21. Δημόσιες χρηματοπιστωτικές συναλλαγές
VII	Ασφάλεια & Δημόσια Τάξη	22. Ασφάλεια και τήρηση της δημόσιας τάξης 23. Διοίκηση, δικαιοσύνης και φυλακές
VIII	Δημόσια διοίκηση	24. Κυβερνητικές λειτουργίες 25. Ένοπλες Δυνάμεις 26. Υπηρεσίες πολιτικής διοίκησης 27. Υπηρεσίες έκτακτης ανάγκης
IX	Μεταφορές	29. Οδικές Μεταφορές 30. Σιδηροδρομικές Μεταφορές 31. Αεροπορικές Μεταφορές 32. Εσωτερικές Πλωτές Μεταφορές 33. Θαλάσσιες Μεταφορές (ποντοπόρα ναυτιλία και ακτοπλοΐα)
X	Χημική & Πυρηνική Βιομηχανία	34. Παραγωγή/αποθήκευση/επεξεργασία χημικών & πυρηνικών υλικών 35. Αγωγοί μεταφοράς επικίνδυνων προϊόντων (χημικών ουσιών)
XI	Διάστημα	36. Διάστημα 37. Διαστημική Έρευνα

Πίνακας 5-1: Αρχική Λίστα Κρίσιμων Τομέων και Υποτομέων/Υπηρεσιών[35]

[35] Στο στάδιο του προσδιορισμού των κρίσιμων τομέων, κάθε κυβέρνηση καταρτίζει μία αρχική λίστα εθνικών κρίσιμων τομέων, δηλαδή των τομέων που υφίστανται στα γεωγραφικά όρια της επικράτειάς της. Σύμφωνα με οδηγία της Ευρωπαϊκής Επιτροπής (EU Commission), το 2005 θεσπίστηκε ο παραπάνω πίνακας για το σύνολο των χωρών-μελών της Ε.Ε.

5.1 Κρίσιμες Υποδομές Πληροφορικής & Επικοινωνιών

Σύμφωνα με τον Φορέα της Ευρωπαϊκής Επιτροπής για την Κυβερνοασφάλεια[36] (ENISA – European Union Agency for Cybersecurity), υπάρχουν χώρες οι οποίες αναδεικνύουν δύο διαφορετικές προσεγγίσεις όσο αφορά στον τομέα των Κ.Υ, δηλαδή διαχωρίζουν τον τομέα των τηλεπικοινωνιών (Telecommunication) και τον τομέα πληροφορικής (Information Technologies), ενώ άλλες χώρες χειρίζονται και τους δύο τομείς ως ένα[37].

Στη παρούσα μελέτη, οι ως άνω δύο τομείς θα αντιμετωπιστούν ως ένας ενιαίος τομέας. Ο τομέας των επικοινωνιών πλέον αποτελεί βασικό στοιχείο για την οικονομία παγκοσμίως και σχεδόν όλες οι επιχειρήσεις στηρίζονται σε μεγάλο βαθμό σε αυτόν. Με την υποστήριξη των τεχνολογιών πληροφορικής και των δικτύων, πολλοί επιχειρηματικοί τομείς και βιομηχανικά συστήματα μπορούν να διασυνδέονται χρησιμοποιώντας ενσύρματα, δορυφορικά και ασύρματα συστήματα επικοινωνίας. Για την απρόσκοπτη και αδιάλειπτη λειτουργία τους, εκτός των πολλών φυσικών προκλήσεων που οφείλουν να αντιμετωπίσουν οι υποδομές τηλεπικοινωνιών (όπως π.χ. σεισμοί, τυφώνες, ακραίες καιρικές συνθήκες κλπ.) καλούνται επίσης να αντιμετωπίσουν με επιτυχία πολλές δολιοφθορές αλλά και μη εξουσιοδοτημένες δράσεις-ενέργειες του κυβερνοχώρου.

Οι προκλήσεις που παρουσιάζονται σε διάφορα συστήματα επικοινωνιών και πληροφορικής παρουσιάζουν μοναδικότητα λόγω της παγκόσμιας συνδεσιμότητας, εφόσον η τρωτότητα (vulnerability) των Κ.Υ. αυτών των σημείων μπορεί εύκολα και γρήγορα να επηρεάσει σχεδόν όλες τις διασυνδεμένες δομές που αλληλοεπιδρούν. Από μόνη της η τεχνολογία πληροφορικής και επικοινωνιών αποτελεί το ουσιαστικό και συνεκτικό μέρος σχεδόν όλων των υποδομών, εφόσον είναι ο συνδετικός κρίκος που διασυνδέει πολλά συστήματα ανταλλαγής πληροφοριών μεταξύ τους[38].

Στην Εικόνα 5-1 φαίνεται το υποθαλάσσιο δίκτυο μεταφορών οπτικών ινών της Νοτιοανατολικής Ασίας - Μέσης Ανατολής - Δυτικής Ευρώπης 4[39] (SEA-ME-WE 4) ως παράδειγμα μίας κρίσιμης υποδομής τηλεπικοινωνιών. Το SEA-ME-WE 4 είναι ένα καλώδιο οπτικών ινών μήκους περίπου 18.000 χιλιομέτρων το οποίο συνδέει την Σιγκαπούρη, τη Μαλαισία, την Ταϊλάνδη, το Μπαγκλαντές, την Ινδία, τη Σρι Λάνκα, το Πακιστάν, τα Ηνωμένα Αραβικά Εμιράτα, τη Σαουδική Αραβία, την Αίγυπτος, την Ιταλία, την Τυνησία, την Αλγερία και τη Γαλλία.

---

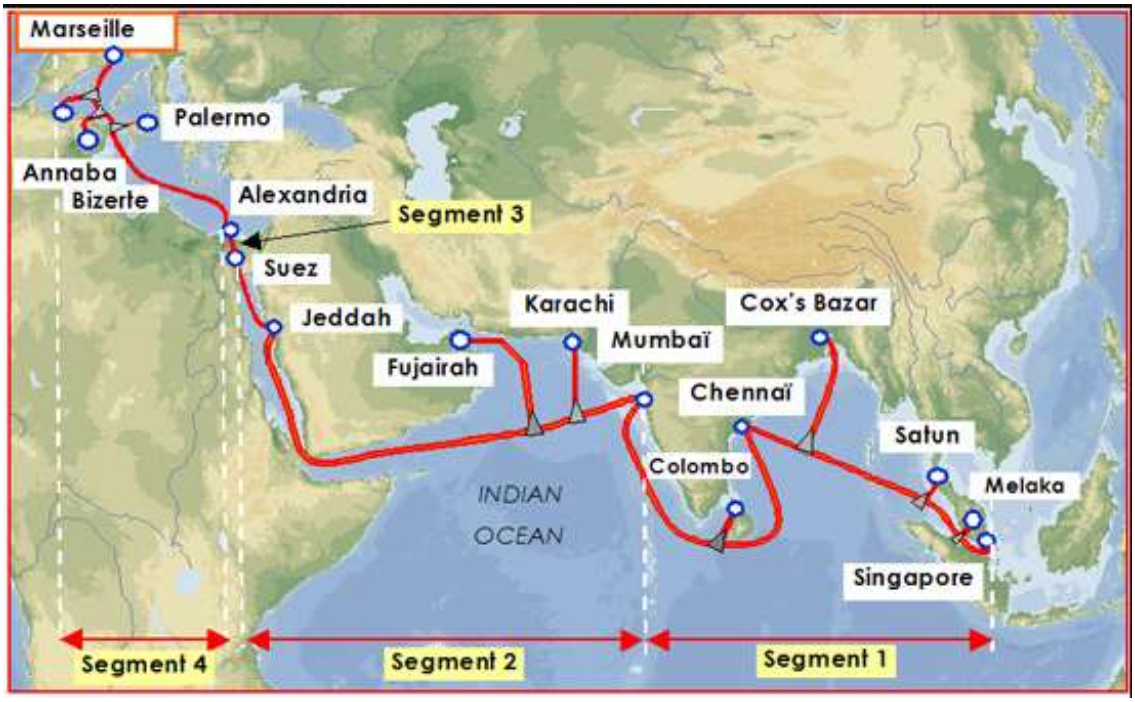
[36] Βλέπε: https://www.enisa.europa.eu/

[37] Βλέπε σχετικά στην Έκθεση της ENISA: https://www.enisa.europa.eu/news/enisa-news/enisa-maps-the-threat-landscape-for-internet-infrastructure-in-2014-and-provides-a-good-practice-guide-for-enhanced-security

[38] Σύμφωνα με την έκθεση της ENISA «Ασφαλής Χρήση του Cloud Computing στον Τομέα Οικονομικών» (www.enisa.europa.eu, 2020), η ευρωπαϊκή βιομηχανία τηλεπικοινωνιών θέτει τη συνεχιζόμενη ανησυχία για θέματα ασφάλειας που σχετίζονται με την απώλεια ελέγχου των δεδομένων, τον έλεγχο του λογαριασμού χρήστη, το κλείδωμα παρόχου, την συμμόρφωση και νομικά ζητήματα, την εμπιστευτικότητα δεδομένων, την διαθεσιμότητα, την ασφαλή διαγραφή, την απώλεια και παραβίαση δεδομένων, την παρακολούθηση και καταγραφή δραστηριοτήτων των εξουσιοδοτημένων χρηστών.

[39] https://en.wikipedia.org/wiki/SEA-ME-WE_4

Το σύστημα χρησιμοποιεί τεχνολογία πολυπλεξίας «Terabit DWDM» για να επιτύχει το μέγιστο εύρος ζώνης με ελάχιστο κόστος. Αυτό το καλώδιο συνδέει μεγάλο αριθμό χωρών και χρησιμοποιείται για τη μεταφορά δεδομένων τηλεφώνου, Διαδικτύου, πολυμέσων και για διάφορες ευρυζωνικές εφαρμογές δεδομένων, χρησιμοποιώντας ρυθμό μετάδοσης δεδομένων 1,28 Tbps[40].



Εικόνα 5-1: Υποθαλάσσιο σύστημα καλωδίων οπτικών ινών SEA-ME-WE 4 ως παράδειγμα κρίσιμης υποδομής τηλεπικοινωνιών[41]

5.2 Εξαρτήσεις Κρίσιμων Υποδομών

Στις Κρίσιμες Υποδομές παρατηρούνται δύο ειδών αλληλεξαρτήσεις, ήτοι: αυτές μεταξύ διαφορετικών επιπέδων της ίδιας Υποδομής (intra-dependency) και αυτές μεταξύ διαφορετικών Υποδομών (inter-dependency), ενώ συχνό φαινόμενο αποτελούν και οι αλληλεξαρτήσεις μεταξύ διαφορετικών τομέων (sectors), όπου Τομέας είναι ένα σύνολο Υποδομών με κοινά χαρακτηριστικά, όπως είδαμε σε προηγούμενο κεφάλαιο. Σε αυτήν την περίπτωση, συναντάμε τον όρο «δια-τομεακές αλληλεξαρτήσεις» (cross-sector interdependencies). Η ύπαρξη αλληλεξαρτήσεων αυξάνει την πολυπλοκότητα σε ένα δίκτυο

[40] SEA-ME-WE4: https://www.seamewe4.net/commonhtm.jsp?htm=htm/about_us.htm

[41] Η Fujitsu Limited ανακοίνωσε την κατασκευή του οπτικού υποβρυχίου καλωδιακού δικτύου για την κοινοπραξία SEA-ME-WE 4, με τον συνεργάτη Alcatel Submarine Networks of France τον Μάρτιο του 2004. Το οπτικό υποβρύχιο καλωδιακό δίκτυο, το οποίο συνδέει τις 14 χώρες προσφέρει καταλύτη για την ανάπτυξη βιομηχανιών πληροφορικής στις γειτονικές χώρες και ικανοποιεί επαρκώς την ταχέως αυξανόμενη ζήτηση για υπηρεσίες Διαδικτύου και ευρυζωνικών υπηρεσιών. Η πληροφορία εκδόθηκε σε επίσημο δελτίο τύπου από την εταιρεία Fujitsu τον Δεκέμβριο του 2005. Το δελτίο τύπου μπορεί να βρεθεί στον παρακάτω σύνδεσμο: https://www.fujitsu.com/global/about/resources/news/press-releases/2005/1213-01.html#1

Υποδομών και απαιτείται μία συλλογική αντιμετώπιση του προβλήματος. Οι υποδομές με κρίσιμη υπόσταση αποτελούν μία πολυδιάστατη αντιμετώπιση σε έναν ενδεχόμενο περιστατικό ασφαλείας [141].

Στη βιβλιογραφία[42] αναδεικνύονται περιπτώσεις αλληλεξάρτησης των Κ.Υ. όπως για παράδειγμα η φυσική (physical) αλληλεξάρτηση, η ψηφιακή (cyber) αλληλεξάρτηση, η γεωγραφική (geographical) αλληλεξάρτηση και η λογική (logical) αλληλεξάρτηση. Η φυσική αλληλεξάρτηση υποδηλώνει ότι η κατάσταση της κάθε Υποδομής (είσοδος) εξαρτάται από την υλική έξοδο μιας άλλης. Για παράδειγμα, ένα σιδηροδρομικό δίκτυο και ένα εργοστάσιο παραγωγής ηλεκτρικής ενέργειας με καύση άνθρακα ανήκουν σε αυτή την κατηγορία καθώς η κάθε μία παρέχει αγαθά που η άλλη έχει ανάγκη για να λειτουργήσει σωστά. Η ψηφιακή (κυβερνοχωρική) εξάρτηση ενώνει δύο Υποδομές μέσω ηλεκτρονικών, πληροφοριακών συνδέσμων, ενώ το αγαθό που παράγεται ή υπόκειται σε επεξεργασία από τη μία και εν συνεχεία μεταφέρεται στην άλλη είναι η πληροφορία. Η συγκεκριμένη αλληλεξάρτηση έχει προκύψει με τη ραγδαία εξάπλωση της τεχνολογίας και αποτελεί μία από τις πιο συχνές μορφές. Η γεωγραφική εξάρτηση εμφανίζεται σε περιπτώσεις κατά τις οποίες τα στοιχεία διαφόρων Υποδομών βρίσκονται σε στενή χωρική εγγύτητα, όπως όταν γραμμές ηλεκτρικής ενέργειας και οπτικές ίνες βρίσκονται κάτω από μία γέφυρα, όπου σε αυτή την περίπτωση, μία καταστροφή της τελευταίας, θα οδηγήσει σε ζημία-βλάβη στον τομέα της ηλεκτρικής ενέργειας, αλλά και σε αυτόν της επικοινωνίας.

Τέλος η λογική εξάρτηση δεν σχετίζεται με καμία από τις παραπάνω κατηγορίες, καθώς αφορά σε περιπτώσεις όπου παράγοντες όπως νομικά ή ρυθμιστικά πλαίσια τα οποία αφορούν μια Υποδομή, επιφέρουν συνέπειες και σε άλλες. Για παράδειγμα, η περίπτωση στην οποία λόγω της χαμηλής τιμής στα καύσιμα αυξάνεται η κινητικότητα στους δρόμους, με κίνδυνο δημιουργίας κυκλοφοριακής συμφόρησης [142].

Στην παρούσα μελέτη, θα μας απασχολήσουν οι απειλές που ενδέχεται να προκαλέσουν απώλεια ή ζημία στις Κ.Υ. τηλεπικοινωνιών, οι οποίες μπορεί να είναι είτε φυσικές είτε ανθρωπογενείς. Ο αριθμός των αποτυχιών που έχει παρατηρηθεί λόγω των αλληλεξαρτήσεων είναι μεγάλος, γεγονός που μαρτυρά την ελλιπή αντιμετώπιση τους.
Προτεραιότητα δίνεται στην Προστασία των Κρίσιμων Τηλεπικοινωνιακών και Πληροφοριακών Υποδομών, δηλαδή στην πρόληψη εμφάνισης περιστατικών παραβίασης της ασφάλειας, προκειμένου να διασφαλιστεί η διαθεσιμότητα των χρήσιμων πληροφοριών που πρέπει να εξαχθούν για την λειτουργία όλων των συστημάτων αλλά και άλλων υποδομών οι οποίες αλληλοεπιδρούν με τις ανωτέρω. Έτσι, κρίνεται επιτακτική η ανάγκη υιοθέτησης μηχανισμών ενίσχυσης της «επανατακτικότητας» των Κ.Υ. τηλεπικοινωνιών ενώ δίνεται έμφαση στις συνέπειες μίας ενδεχόμενης αποτυχίας και στο πώς μπορεί αυτή να τύχει αντιμετώπισης. Αξίζει ωστόσο να αναφερθεί ότι ο συνδυασμός της προστασίας και της επανατακτικότητας αποτελεί τον ιδανικό τρόπο αντιμετώπισης του δυναμικού περιβάλλοντος των σημερινών Κρίσιμων Τηλεπικοινωνιακών Υποδομών.

[42] Rinaldi S., Peerenboom J., and Kelly T. (2001): "Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies". IEEE Control Systems Magazine, vol.21, No.6, pp.11-25.

5.3 Βασικές Έννοιες σχετικά με την Ασφάλεια Κρίσιμων Υποδομών

Κάθε χώρα που επιθυμεί να προστατεύσει τις Κ.Υ. που διαθέτει θα πρέπει να αναπτύξει κατάλληλους μηχανισμούς άμυνας και προστασίας. Η ανάγκη δημιουργίας ανθεκτικών Κ.Υ., ειδικότερα όσο αφορά στον τομέα των τηλεπικοινωνιών (ICT), έχει επισημανθεί πολλές φορές στη βιβλιογραφία ([143], [144]). Οι περισσότερες υποδομές που θεωρούνται κρίσιμες χρησιμοποιούν σύγχρονες τεχνολογίες όπως για παράδειγμα το σύστημα SCADA[43] και κατά συνέπεια, εκτός των φυσικών ευπαθειών γίνονται επιρρεπείς και σε κυβερνοεπιθέσεις[44].

Οι βασικές έννοιες τις οποίες διαπραγματευόμαστε σχετικά με την ασφάλεια των Κ.Υ., επεξηγούνται συνοπτικά παρακάτω:

Ευπάθεια-τρωτότητα (Vulnerability): Έτσι ορίζεται ένα ελάττωμα ή μία αδυναμία στις διαδικασίες ασφάλειας ενός συστήματος, το οποίο μπορεί κατά λάθος ή σκόπιμα να χρησιμοποιηθεί και να οδηγήσει σε ένα ρήγμα ασφάλειας (security breach) ή σε παραβίαση της πολιτικής ασφάλειας του συστήματος [144].

Απειλή (Threat): Είναι το ενδεχόμενο μία πηγή απειλής (threat source) να εκμεταλλευτεί κατά λάθος ή σκόπιμα μία δυνητική ευπάθεια [144].

Συνέπεια (Consequence): Είναι το αποτέλεσμα ενός γεγονότος ασφαλείας, το οποίο εκφράζεται ποιοτικά ή ποσοτικά και μπορεί να είναι μία απώλεια, ένας τραυματισμός, μία οικονομική ζημία κλπ. Οι επιδράσεις των συνεπειών μπορεί να αφορούν στην ανθρώπινη υγεία και ζωή, στο περιβάλλον, σε οικονομικούς παράγοντες κ.α. [145].

Αντίκτυπος (Impact): Είναι η αρνητική μεταβολή των επιχειρησιακών στόχων που έχουν επιτευχθεί, είτε αυτοί είναι ποιοτικοί είτε ποσοτικοί [145].

Κίνδυνος Ασφάλειας Πληροφοριών (Information Security Risk): Το ενδεχόμενο ότι μία δεδομένη απειλή θα εκμεταλλευτεί τις ευπάθειες ενός αγαθού ή ενός οργανισμού, με αποτέλεσμα να προκαλέσει ζημία. Αυτό συνήθως εκφράζεται ως συνδυασμός της πιθανότητας ενός συμβάντος και των συνεπειών αυτού [146].

---

[43] Ο όρος SCADA (Supervisory Control And Data Acquisition) περιγράφει μία κατηγορία συστημάτων βιομηχανικού αυτομάτου ελέγχου και τηλεμετρίας. Το χαρακτηριστικό των συστημάτων SCADA είναι ότι αποτελούνται από τοπικούς ελεγκτές, που ελέγχουν επί μέρους στοιχεία και μονάδες μίας εγκατάστασης, συνδεδεμένους σε ένα κεντρικό Master Station (Κύριο Σταθμό Εργασίας). Ο κεντρικός σταθμός εργασίας μπορεί κατόπιν να επικοινωνεί τα δεδομένα που συλλέγει από την εγκατάσταση σε ένα πλήθος από σταθμούς εργασίας σε τοπικό LAN ή/και να μεταδίδει τα δεδομένα της εγκατάστασης σε μακρινά σημεία μέσω κάποιου συστήματος τηλεπικοινωνίας (π.χ. μέσω του ενσύρματου τηλεφωνικού δικτύου ή μέσω κάποιου ασύρματου δικτύου). Επίσης είναι δυνατό ο κάθε ένας τοπικός ελεγκτής να βρίσκεται σε απομακρυσμένη θέση και να μεταδίδει τα δεδομένα προς τον Σταθμό Εργασίας μέσω απλού καλωδίου ή μέσω ασύρματου πομποδέκτη, πάντα με σύνολο από τοπικούς ελεγκτές συνδεδεμένους σε τοπολογία αστέρα προς έναν Σταθμό Εργασίας.
Πηγή: Bailey, D., and Wright, E. (2003): Practical SCADA for Industry. Elsevier.

[44] European Commission (2009): "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM(2009)149 final, Brussels, 30.03.2009.

Ετοιμότητα (Preparedness): Είναι το σύνολο των μέτρων που καλούμαστε να λάβουμε ώστε να διασφαλίσουμε ότι οι οργανισμοί είναι ικανοί να αντιμετωπίσουν τις επιδράσεις των έκτακτων περιστατικών ασφαλείας [146].

5.3.1 Ευρωπαϊκό Πρόγραμμα για την Προστασία των Κρίσιμων Υποδομών

Η ποιότητα ζωής των πολιτών της Ευρωπαϊκής Ένωσης (ΕΕ) και η ασφάλειά τους, καθώς και η ορθή και αποτελεσματική λειτουργία της αγοράς, εξαρτώνται από την παροχή βασικών υπηρεσιών μέσω διαφορετικών υποδομών ζωτικής σημασίας σε ένα ευρύ φάσμα τομέων. Είναι επομένως επιτακτική ανάγκη οι κρίσιμες υποδομές να προστατεύονται επαρκώς από ένα εκτενές φάσμα απειλών, τόσο φυσικών όσο και ανθρωπογενών, ακούσιων και κακόβουλων προθέσεων. Όπου αυτό αποτυγχάνει και παρόλα αυτά ακολουθούν διαταραχές, οι υποδομές ζωτικής σημασίας πρέπει να είναι «ανθεκτικές», δηλαδή να μπορούν να ανακάμψουν γρήγορα μέσα σε ένα αποδεκτό χρονικό διάστημα. Ως αντανάκλαση της σημασίας αυτού του ζητήματος, η Ευρωπαϊκή Επιτροπή (European Commission) συνέστησε το 2006 το Ευρωπαϊκό Πρόγραμμα για την Προστασία των Κρίσιμων Υποδομών (European Programme for Critical Infrastructure Protection – EPCIP), το οποίο καθορίζει ένα πλαίσιο ευρωπαϊκού επιπέδου για όλους τους κινδύνους για την προστασία των υποδομών ζωτικής σημασίας[45].

Ένας από τους κεντρικούς πυλώνες του EPCIP είναι η Οδηγία 2008/114/ΕΚ, η οποία θεσπίζει μία διαδικασία για τον εντοπισμό των ευρωπαϊκών Κ.Υ. εάν συμβεί διατάραξη του πλαισίου ασφαλείας ή ενδεχόμενη φυσική καταστροφή. Η Οδηγία προβλέπει επίσης μία κοινή προσέγγιση για την αξιολόγηση της ανάγκης βελτίωσης της φυσικής προστασίας των καθορισμένων Κ.Υ.

Ωστόσο, μια αναθεώρηση της Οδηγίας για τις ECIs (European Critical Infrastructures) δείχνει ότι το ισχύον πλαίσιο είναι ανεπαρκές υπό το φως των αυξανόμενων αλληλεξαρτήσεων εντός και μεταξύ κρίσιμων τομέων υποδομής, καθώς και των εξελισσόμενων κινδύνων που αντιμετωπίζουν. Καθώς αυτές οι υποδομές αναπτύσσονται ολοένα και περισσότερο, οι διαταραχές σε έναν τομέα έχουν τη δυνατότητα να δημιουργήσουν άμεσες και – σε ορισμένες περιπτώσεις – μακροχρόνιες επιπτώσεις σε άλλους τομείς όπου αλληλοεπιδρούν, με ζημιογόνα αποτελέσματα. Καταστάσεις όπως οι παραπάνω μπορεί να έχουν σοβαρές συνέπειες για την ασφάλεια, τόσο σε μεμονωμένα κράτη μέλη όσο και σε ολόκληρη την Ευρωπαϊκή Ένωση και μπορούν να οδηγήσουν σε αβεβαιότητα ή να υπονομεύσουν την εμπιστοσύνη στις αρμόδιες Αρχές και τους παρόχους βασικών υπηρεσιών [147].

[45] Commission of the European Communities, "Communication from the Commission on a European Programme for Critical Infrastructure Protection", Brussels, 12.12.2006, COM(2006) 786 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN

Η πρόταση της Ευρωπαϊκής Επιτροπής για πρόσθετα μέτρα για την προστασία των υποδομών Κ.Υ., η οποία περιλαμβάνεται στο Πρόγραμμα Εργασίας της Ευρωπαϊκής Επιτροπής 2020[46] (CWP 2020 - Παράρτημα), θα αναπτυχθεί σε συντονισμό με άλλες προγραμματισμένες πρωτοβουλίες σε συναφείς τομείς. Για παράδειγμα, η πρόταση συστήνει απαραίτητα μέτρα για την επιχειρησιακή επανατακτικότητα στον κυβερνοχώρο και τον τομέα της πολιτικής προστασίας, καθώς και τη συνεχιζόμενη αναθεώρηση της Οδηγίας 2016/1148/ΕΚ[47] σχετικά με μέτρα για υψηλό κοινό επίπεδο δικτύων και συστημάτων πληροφοριών σε ολόκληρη την Ευρωπαϊκή Ένωση[48].

Ο γενικός στόχος αυτής της πρωτοβουλίας είναι να ενισχυθεί περαιτέρω η προστασία, αλλά και η επανατακτικότητα των Κ.Υ. στην ΕΕ, λαμβάνοντας υπόψη τον ολοένα και πιο «βαθύ» χαρακτήρα τομεακών αλληλεξαρτήσεων και τους εξελισσόμενους κινδύνους που αντιμετωπίζουν οι κρίσιμες υποδομές. Πιο συγκεκριμένα, η πρωτοβουλία στοχεύει στα εξής:

- Εξασφάλιση μεγαλύτερης συνοχής, με τη συνολική προσέγγιση της Ε.Ε. για την προστασία και την επανατακτικότητα των κρίσιμων υποδομών.

- Διεθνή συνεργασία και εξασφάλιση ισότιμων όρων ανταγωνισμού για τους φορείς εκμετάλλευσης σε ολόκληρη την Ε.Ε. παρέχοντάς τους συνεπείς απαιτήσεις, συμπεριλαμβανομένων των μηχανισμών αναφοράς.

- Διασφάλιση ότι όλοι οι σχετικοί τομείς που είναι υπεύθυνοι για την παροχή διαφορετικών τύπων βασικών υπηρεσιών περιλαμβάνονται στην αναθεωρημένη προσέγγιση για την προστασία και την επανατακτικότητα των κρίσιμων υποδομών και για την αποτελεσματική διαχείριση των διατομεακών/διασυνοριακών διαταραχών.

- Θέσπιση νέων/βελτιωμένων υφιστάμενων μηχανισμών με στόχο την περαιτέρω ενίσχυση της ικανότητας των κρατών μελών να προστατεύουν και να διασφαλίζουν την επανατακτικότητα των κρίσιμων υποδομών που θεωρούνται ζωτικής σημασίας σε εθνικό επίπεδο.

- Εξασφάλιση υψηλότερου επιπέδου κατανόησης των κινδύνων/απειλών που αντιμετωπίζουν οι Κ.Υ τώρα και ενδέχεται να αντιμετωπιστούν στο μέλλον, καθώς και τα μέσα αντιμετώπισής τους [148].

---

[46] Για περισσότερες πληροφορίες σχετικά με το CWP-2020 βλέπε το αναλυτικό κείμενο στον ακόλουθο σύνδεσμο: https://ec.europa.eu/info/sites/default/files/cwp-2020-publication_en.pdf

[47] Βλέπε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016L1148

[48] Η Ευρωπαϊκή Επιτροπή δημοσίευσε το ετήσιο πρόγραμμα εργασίας της τον Ιανουάριο του 2020. Καθορίζει τις σημαντικότερες πρωτοβουλίες για το πρώτο έτος της θητείας της Επιτροπής και είχε ως στόχο να μετατρέψει τις πολιτικές κατευθυντήριες γραμμές που δημοσίευσε ο Πρόεδρος της Ευρωπαϊκής Επιτροπής σε απτά οφέλη για τους ευρωπαίους πολίτες, τις επιχειρήσεις και την κοινωνία, και να αναδείξουν τις κύριες προτεραιότητες για το Ευρωπαϊκό Κοινοβούλιο και εκείνες που περιλαμβάνονται στη στρατηγική ατζέντα του Ευρωπαϊκού Συμβουλίου για την περίοδο 2019-2024. Σχετικές πληροφορίες μπορούν να βρεθούν στον σύνδεσμο https://www.europeansources.info/record/commission-work-programme-2020-a-union-that-strives-for-more/

5.3.2 Οικογένεια Προτύπων Διαχείρισης Ασφαλείας BS-7799

Το ευρέως διαδεδομένο πρότυπο διαχείρισης ασφαλείας υποδομών πληροφοριών, το οποίο στηρίζεται σε πόρους πληροφορικής (IT Asset-based framework) ονομάζεται BS-7799 [149], θεσπίζεται από το BSI Group[49] και οποίο χωρίζεται σε δύο μέρη:

1. **BS 7799-1 Information technology – Code of practice for information security management**[50] (Τεχνολογία Πληροφοριών - Κώδικας Πρακτικών για τη Διαχείριση Ασφάλειας των Πληροφοριών) [BSI-EN, 2001]. Το πρώτο μέρος είναι επίσης γνωστό ως BS ISO/IEC 17799[51], υιοθετήθηκε από τον οργανισμό ISO σχεδόν αυτούσιο [ISO 17799, 2000] και περιγράφει ένα σύνολο από βέλτιστες πρακτικές – οδηγίες για την εφαρμογή ενός συστήματος διαχείρισης της ασφάλειας των πληροφοριών (Information Security Management System). Ο ακρογωνιαίος λίθος για τον καθορισμό των επαρκών μέτρων ασφάλειας είναι η αναγνώριση των κινδύνων και των επιπτώσεών τους, οι οποίοι είναι το μόνο εύλογο κριτήριο για τη δικαιολόγηση του κόστους της διαχείρισης κινδύνων από έναν οργανισμό. Προς την επίτευξη αυτού του στόχου, σημαντικοί αρωγοί είναι η συστηματική αποτίμηση των κινδύνων του οργανισμού, καθώς επίσης οι νομικές και ρυθμιστικές απαιτήσεις που υπαγορεύονται από το περιβάλλον μέσα στο οποίο ο εν λόγω οργανισμός δραστηριοποιείται[52].

2. **BS 7799-2 Information Security Management Systems – Specification with guidance for use**[53] (Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών – Προδιαγραφές με καθοδήγηση για τη χρήση). Το δεύτερο μέρος του προτύπου περιγράφει τον τρόπο οργάνωσης ενός δομημένου συστήματος ελέγχου και αναφορών (**ISMS**) προκειμένου να αποτιμηθεί το επίπεδο διαχείρισης ασφάλειας σε ένα πληροφοριακό σύστημα (το οποίο ακολουθεί ένα σύστημα διαχείρισης ασφάλειας). Τα μέτρα ασφάλειας που υιοθετούνται ενδέχεται να προέρχονται από το πρότυπο BS ISO/IEC 17799, χωρίς κάτι τέτοιο να είναι υποχρεωτικό. Το πρότυπο αυτό μπορεί να χρησιμοποιηθεί για σκοπούς ελέγχου και πιστοποίησης [BSI-EN, 2002]. Το πρότυπο αυτό προωθεί την υιοθέτηση μίας διαδικαστικής προσέγγισης για την ανάπτυξη, την εφαρμογή και τη βελτίωση της αποδοτικότητας ενός συστήματος διαχείρισης της ασφάλειας των πληροφοριών (ISMS) ενός οργανισμού. Ένας οργανισμός θα πρέπει να αναγνωρίζει και να διαχειρίζεται πολλές δραστηριότητες για να λειτουργεί αποδοτικά. Κατά το εν λόγω πρότυπο, μία διεργασία πληροφορικής ορίζεται ως μία διαχειριζόμενη δραστηριότητα που χρησιμοποιεί

---

[49] Το British Standards Institution (BSI) είναι ο εθνικός οργανισμός τυποποίησης του Ηνωμένου Βασιλείου. Το BSI παράγει τεχνικά πρότυπα σε ένα ευρύ φάσμα προϊόντων και υπηρεσιών και παρέχει επίσης υπηρεσίες πιστοποίησης και σχετικές με πρότυπα σε επιχειρήσεις. Για περισσότερα στοιχεία βλέπε: https://www.bsigroup.com/

[50] Βλέπε επίσης, μεταξύ άλλων: https://en.wikipedia.org/wiki/BS_7799

[51] Βλέπε επίσης: https://www.iso.org/standard/39612.html

[52] Όπως για παράδειγμα το Sarbanes-Oxley Act 404 (SOX 404), που εκδόθηκε από την Κεφαλαιαγορά των Ην. Πολιτειών (Securities and Exchange Commission – SEC, http://www.sec.gov) το 2002 και αφορά στην ποιότητα του συστήματος εσωτερικού ελέγχου όσον αφορά τις οικονομικές καταστάσεις των εταιρειών που είναι εισηγμένες στην SEC.

[53] Για περισσότερες σχετικές πληροφορίες βλέπε: https://shop.bsigroup.com/products/information-security-management-specification-with-guidance-for-use?pid=000000000030049529

πόρους πληροφορικής, ούτως ώστε να μετατρέπει τις εισόδους της επεξεργασίας σε εξόδους. Το πρότυπο εισάγει το μοντέλο Plan-Do-Check-Act[54] (PDCA) ([BSI-EN, 2002] ως ένα μέρος μίας προσέγγισης διαχείρισης συστημάτων για την ανάπτυξη, την εφαρμογή και τη βελτίωση της αποδοτικότητας ενός ISMS, μέσα στο επιχειρησιακό πλαίσιο των κινδύνων πληροφορικής που αντιμετωπίζει ένας οργανισμός.

Εικόνα 5-2: Κύκλος Plan-Do-Check-Act (PDCA)[55]

Όπως είδαμε στις προηγούμενες ενότητες, η ασφάλεια των Κ.Υ. τηλεπικοινωνιών και πληροφορικής αφορά μία διαδικασία η οποία βρίσκεται σε συνεχή εξέλιξη. Η μέθοδος PDCA μπορεί να χρησιμοποιηθεί για να διασφαλιστεί η συνεχής προσαρμογή του πλαισίου ασφάλειας.

Η χρήση τέτοιων εργαλείων στη σχεδίαση και υλοποίηση οποιασδήποτε εφαρμογής ασφαλείας, είτε αυτή αφορά σε φυσική είτε σε ψηφιακή ασφάλεια, προσδίδει μεγαλύτερη αξία καθώς από την μία μεριά η μέτρηση στοιχείων κατά την φάση "Check" συστήνει την συνεχή επαγρύπνηση και βελτίωση των χρησιμοποιούμενων μεθόδων, και από την άλλη μεριά, κατά τον επαναπροσδιορισμό των στόχων ποιότητας, μπορούν να χρησιμοποιηθούν οι προηγούμενες τακτικές οι οποίες επέφεραν τα καλύτερα αποτελέσματα (best practices) [150].

---

[54] Για περισσότερα πληροφοριακά στοιχεία βλέπε επίσης, μεταξύ άλλων: https://en.wikipedia.org/wiki/PDCA

[55] Σε κάθε φάση της διαδικασίας διαχείρισης, οι επόμενες ενέργειες λαμβάνουν χώρα (βλ. και [BSI-EN, 2002]):

- Plan – Σχεδιασμός (Καθορισμός του πλαισίου του ISMS): Καθορισμός των πολιτικών ασφαλείας, των στόχων, των διεργασιών και των διαδικασιών σχετικών με τον έλεγχο των κινδύνων και της βελτίωσης της ασφάλειας της πληροφορίας.
- Do – Εφαρμογή (Σχεδιασμός και Υλοποίηση): Εφαρμογή και λειτουργία των πολιτικών ασφάλειας.
- Check – Έλεγχος (Κριτικές και Συμβουλές): Μέτρηση και αποτίμηση της απόδοσης των διεργασιών σε σχέση με τις πολιτικές, τους στόχους του οργανισμού και την πρακτική εμπειρία καθώς δημιουργία αναφοράς των αποτελεσμάτων στους υπεύθυνους.
- Act – Δράση (Βελτίωση): Λήψη διορθωτικών και αποτρεπτικών αποφάσεων για περαιτέρω βελτίωση της απόδοσης των διεργασιών.

5.4 Αποτυχία Κρίσιμων Υποδομών

Η λειτουργία ενός συστήματος κρίσιμων υποδομών απειλείται συνεχώς από ένα ευρύ φάσμα απειλών σε σχέση με την ασφάλεια. Αυτές οι απειλές μπορούν, γενικά, να κατηγοριοποιηθούν σε πέντε βασικές ομάδες ως εξής:

- Κλιματολογικές απειλές (συμπεριλαμβανομένων φυσικών καταστροφών όπως π.χ. πλημμύρες, ανεμοστρόβιλοι, βαριές χιονοπτώσεις ή εκτεταμένες πυρκαγιές).
- Γεωλογικές απειλές (π.χ. σεισμοί, ηφαιστειακή δραστηριότητα, κατολισθήσεις).
- Βιολογικές απειλές (π.χ., πανδημίες).
- Τεχνολογικές απειλές (συμπεριλαμβανομένων τεχνολογικών καταστάσεων έκτακτης ανάγκης όπως συμβάντα ραδιενέργειας, επικίνδυνες χημικές διαρροές, πλημμύρες που προκαλούνται από ζημιές σε υδραυλικές κατασκευές, εκτεταμένες διαταραχές στα δίκτυα μηχανικής, έκτακτες ανάγκες δημόσιας ύδρευσης ή μεγάλα οδικά, σιδηροδρομικά ή αεροπορικά ατυχήματα).
- Εγκληματικές απειλές (π.χ. τρομοκρατία, εγκληματική δραστηριότητα, ένοπλες συγκρούσεις) [154].

Οι επιπτώσεις που προκαλούνται από αυτές τις απειλές σε ένα σύστημα κρίσιμης υποδομής – ή στα υποσυστήματά του – μπορούν να προκαλέσουν ανεπιθύμητα συμβάντα τα οποία με τη σειρά τους μπορούν να οδηγήσουν σε διακοπές και/ή σε ακραίες περιπτώσεις, αποτυχίες διαφορετικών υποσυστημάτων. Αυτό συνεπάγεται, ειδικότερα, διαταραχές στις λειτουργικές παραμέτρους που προκαλούν μείωση της απόδοσης συγκεκριμένων στοιχείων όπου η «πτώση» είναι άμεσα ανάλογη με την ένταση της έκτακτης ανάγκης και τον βαθμό επανατακτικότητας του αντίστοιχου κρίσιμου στοιχείου υποδομής.

Με την πάροδο του χρόνου όλο και περισσότερες Κρίσιμες Υποδομές εξαρτώνται από την Τεχνολογία της Πληροφορίας και των Επικοινωνιών, με αποτέλεσμα μία αποτυχία είτε λόγω ατυχήματος είτε σκόπιμα, να διαδίδεται και σε άλλες υποδομές, υποβαθμίζοντας ή διαταράσσοντας τη λειτουργικότητα αυτών. Με την ίδια λογική, μία αποτυχία σε Κ.Υ. μπορεί επίσης να διαδοθεί στην υποδομή τηλεπικοινωνίας και πληροφορικής και έτσι να επηρεάσει τη λειτουργία των διαφόρων διασυνδεδεμένων συστημάτων (γνωστό ως «συμβάν αποτυχίας κατεξάπλωσης» - “cascading failure event”). Πολλές από αυτές τις αποτυχίες ίσως οδηγήσουν σε σοβαρές διαταραχές, με αποτέλεσμα να καθίσταται όλο και πιο επιτακτική η ανάγκη για μία ασφαλή και αξιόπιστη λειτουργία των Κ.Υ.. Βασική προϋπόθεση για την ομαλή αυτή λειτουργία είναι η κατανόηση των μορφών αλληλεξαρτήσεων. Αξίζει να αναφερθεί ότι η τεχνικής φύσεως πολυπλοκότητα που συναντάται στις σημερινές υποδομές δυσχεραίνει ακόμη περισσότερο την αναγνώριση αλληλεξαρτήσεων και ευπαθειών, με αποτέλεσμα την εξάπλωση μίας αρχικά ασήμαντης αποτυχίας. Μελετώντας την προέλευση των αποτυχιών λόγω αλληλεξαρτήσεων (αποτυχία που συσχετίζεται με τις αλληλεπιδράσεις – interdependencies - related failure) και τον τρόπο με τον οποίο αυτές διαδίδονται, μπορούμε να κατανοήσουμε καλύτερα τις εξαρτήσεις και συνεπώς, *λαμβάνοντας τις κατάλληλες αποφάσεις*, να σχεδιάσουμε πιο αποδοτικά το σύστημά μας, από πλευράς κόστους, ασφάλειας και αξιοπιστίας [155].

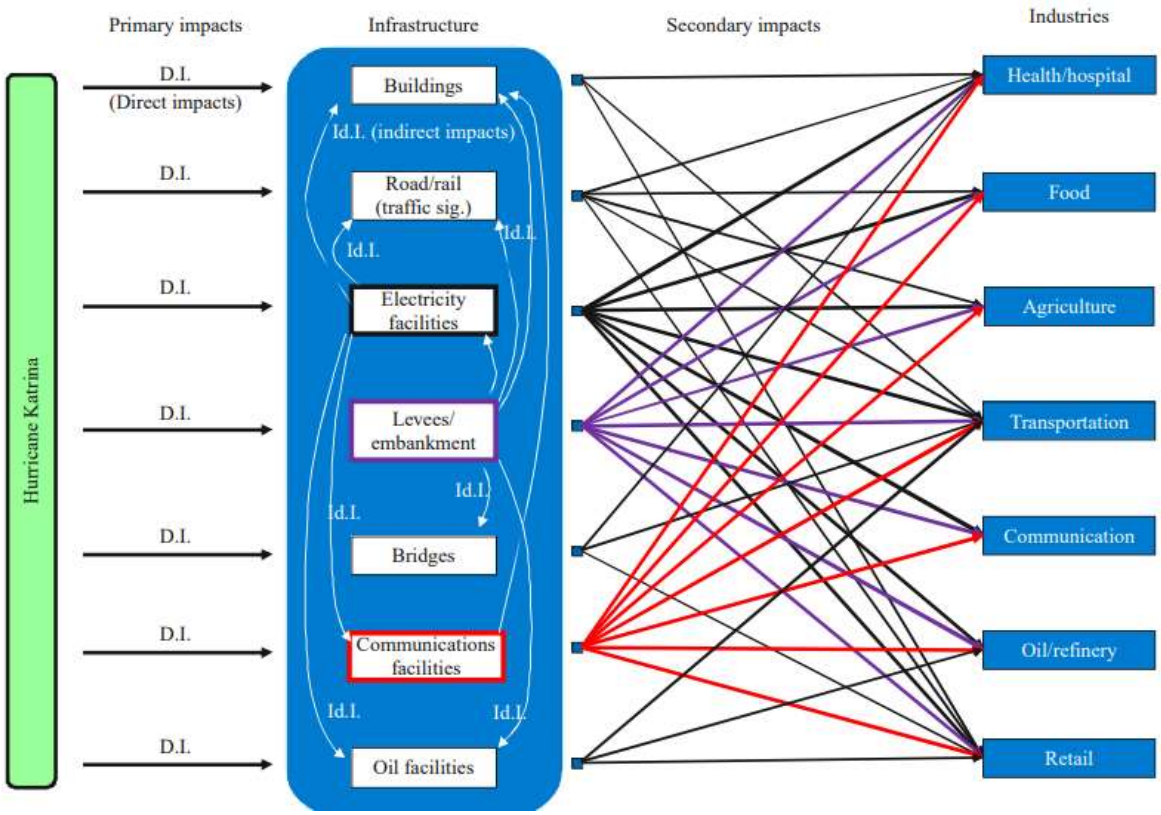
5.4.1 Περιστατικά Αποτυχιών

Ανάλογα με την κατηγορία των απειλών, τρεις τύποι καταστάσεων έκτακτης ανάγκης, που στη συνέχεια δημιουργούν αποτυχίες, μπορούν να προκύψουν σε ένα σύστημα Κρίσιμης Υποδομής. Αυτές περιλαμβάνουν: (1) εκ προθέσεως ανθρωπογενή γεγονότα (δηλ. τρομοκρατία, δολιοφθορά και εγκληματική δραστηριότητα), (2) ακούσια ανθρωπογενή γεγονότα (δηλαδή, τεχνολογικές καταστάσεις έκτακτης ανάγκης όπως βλάβες) και (3) φυσικά γεγονότα (δηλαδή κλιματολογικές, γεωλογικές και βιολογικές απειλές). Μόλις δημιουργηθούν, οι αποτυχίες μπορούν να επεκταθούν περαιτέρω σε ένα σύστημα Κ.Υ. και να παράγουν αρνητικές επιπτώσεις διαφορετικού χαρακτήρα, έντασης και αποτελέσματος.

Παρόλο που στις μέρες μας η τεχνολογία έχει βοηθήσει στη βελτίωση της ασφάλειας, ένα αρχικά ασήμαντο γεγονός μπορεί να οδηγήσει σε μία ακολουθία καταστροφικών περιστατικών, όχι μόνο για την ίδια την Υποδομή και τις εξαρτώμενες από αυτήν, αλλά και για την κοινωνία, στο σύνολό της. Η βλάβη σε μια υποδομή ύδρευσης, ενδεχομένως ως μεμονωμένο συμβάν, ενδέχεται να μην προκαλεί έντονη ανησυχία αλλά εάν αναλογιστεί κανείς τις πιθανές επεκτάσεις αυτού του συμβάντος, όπως π.χ. σε ενδεχόμενη περίπτωση πυρκαγιάς, τότε μπορεί να γίνει καταληπτή η πολυδιάστατη όψη ενός αρχικά μη σημαντικού περιστατικού [156].

Ενδεικτικά θα αναφέρουμε μια περίπτωση μελέτης, η οποία αφορά στον τύπο αποτυχίας “cascading” (κατεξάπλωση):
Σε διακοπές ηλεκτρικού ρεύματος στην Καλιφόρνια των ΗΠΑ το 2005, κατά την επίδραση του τυφώνα Κατρίνα (hurricane Katrina), λόγω των τότε συνθηκών όσον αφορά στο εμπόριο του ηλεκτρικού ρεύματος και στις ισχύουσες νομοθεσίες, προέκυψε οικονομική κρίση σε εταιρείες ηλεκτρικού ρεύματος οι οποίες αδυνατούσαν να παράγουν επαρκώς ηλεκτρικό ρεύμα. Έτσι, οι κατά διαστήματα διακοπές ηλεκτρικού ρεύματος, μείωσαν την παραγωγή φυσικού αερίου (1ης τάξης επίδραση), η οποία επηρέασε άμεσα τις προμήθειες αερίου και κατά συνέπεια τις μονάδες παραγωγής ηλεκτρικού ρεύματος που λειτουργούσαν με τη βοήθεια αερίου, το οποίο επιδείνωσε τα υπάρχοντα προβλήματα ενέργειας, δημιουργώντας ένα βρόχο ανάδρασης (feedback loop). Επιπλέον, μονάδες παραγωγής που λειτουργούσαν με τη βοήθεια αερίου, επηρεάστηκαν από τα μειωμένα διαθέσιμα αποθέματα, μειώνοντας την παραγωγή τους η οποία χρησίμευε στην παραγωγή πετρελαίου (2ης τάξης επίδραση). Με τον τρόπο αυτό, επηρεάστηκε και η παραγωγή πετρελαίου (3ης τάξης επίδραση). Κατά συνέπεια, οι διακοπές ηλεκτρικού ρεύματος επηρέασαν τη μεταφορά βενζίνης και καυσίμων αεροπορίας (jet fuel), με αποτέλεσμα τη δημιουργία μεγαλύτερης ποσότητας αποθεμάτων στα διυλιστήρια σε σχέση με τη ζήτηση και την αύξηση των λειτουργικών εξόδων (Operational Expenses - OPEX) στις εταιρείες. Επίσης επηρεάστηκε η προμήθεια από τους τερματικούς σταθμούς των προϊόντων, συμπεριλαμβανομένων αρκετών σημαντικών αεροδρομίων της Καλιφόρνιας. Το τελευταίο επηρέασε και τις εναέριες μεταφορές, οι οποίες θα έπρεπε να υιοθετούν πλάνα εκτάκτου ανάγκης, ενώ η λειτουργία των διυλιστηρίων επηρέασε και τις υποδομές μεταφορών, λόγω της έλλειψης της ειδικής μορφής βενζίνης που χρησιμοποιείτο στην Καλιφόρνια. Φυσικά δεν έλειψαν και οι διακοπές στις αντλίες μεταφοράς νερού για άρδευση καλλιεργειών, με άμεση επίπτωση τόσο στον αγροτικό όσο και στον οικονομικό τομέα.
Όλες οι προαναφερθείσες επιδράσεις αναπτύχθηκαν αλυσιδωτά και επηρέασαν ένα πλήθος αλληλοεπιδρώμενων τομέων (cross-sectoral) [157].

Στην παρακάτω εικόνα, φαίνεται η πολυπλοκότητα της αποτυχίας αλληλοεπιδρώμενων τομέων μετά από την αποτυχία μιας Κ.Υ.



Εικόνα 5-3: Επιπτώσεις σε αλληλοεπιδρώσες Κρίσιμες Υποδομές στην περίπτωση του τυφώνα «Κατρίνα»

Οι βασικοί τρόποι διάδοσης αποτυχίας σε ένα σύστημα κρίσιμης υποδομής συνίστανται στα κάτωθι:

- Μία διαδοχική αποτυχία συμβαίνει όταν μία ενδεχόμενη διακοπή σε μία υποδομή προκαλεί αποτυχία ενός στοιχείου σε μία δεύτερη υποδομή, η οποία στη συνέχεια προκαλεί διακοπή στη δεύτερη υποδομή (π.χ., η διακοπή ηλεκτρικής ενέργειας θα μπορούσε να δημιουργήσει διακοπή σε άλλες υποδομές).

- Μία κλιμακούμενη αποτυχία συμβαίνει όταν μία υπάρχουσα διακοπή σε μία υποδομή επιδεινώνει μία ανεξάρτητη διακοπή μίας δεύτερης υποδομής (π.χ., η διακοπή στο δίκτυο τηλεπικοινωνιών μπορεί να κλιμακωθεί σε διαταραχή στο δίκτυο οδικών μεταφορών).

- Μία κοινή αιτία συμβαίνει όταν δύο ή περισσότερα δίκτυα υποδομής υποφέρουν από διακοπές ταυτόχρονα, λόγω κάποιου κοινού αιτίου (π.χ. δράση φυσικής καταστροφής σε όλες τις τοπικές υποδομές) [158].

Όπως είδαμε, σε περίπτωση διακοπής ενός συστήματος Κ.Υ., οι επιπτώσεις εξαπλώνονται σε δύο άξονες. Στην πρώτη περίπτωση περιλαμβάνονται επιπτώσεις στο σύστημα όπου η αποτυχία ενός υποσυστήματος προκαλεί βλάβη ενός άλλου υποσυστήματος με αυτό που είναι γνωστό ως διαδοχικό αποτέλεσμα. Οι επιπτώσεις αυτές μπορούν να ταξινομηθούν ως άμεσες ή έμμεσες. Η άμεση επίδραση ενός διαταραγμένου υποσυστήματος σε ένα άλλο υποσύστημα ή απευθείας στην κοινωνία, συμβαίνει ανάμεσα σε δύο αμιγώς αλληλεξαρτώμενα συστήματα προκαλώντας διαδοχικές βλάβες από το πρώτο στο δεύτερο (domino effect). Αντίθετα, οι έμμεσες επιπτώσεις συμβαίνουν οπουδήποτε, ανεξάρτητα από το εάν επηρεάζουν ή όχι ένα άλλο υποσύστημα. Οι έμμεσες επιπτώσεις μπορεί να είναι δευτερεύουσες (μέσω ενός υποσυστήματος) ή πολύ-διαρθρωτικές (μέσω διαφόρων υποσυστημάτων).

Οι κρίσιμες βλάβες ενός συστήματος κρίσιμων υποδομών προκαλούν στη συνέχεια αρνητικές επιπτώσεις, οι οποίες μπορούν να επεκταθούν περαιτέρω όχι μόνο εντός του κρίσιμου συστήματος υποδομής (μεταξύ εξαρτημένων υποσυστημάτων), αλλά και εκτός του αρχικού συστήματος και μπορούν να επηρεάσουν την κοινωνία, συμπεριλαμβανομένων σημαντικών εθνικών παραγόντων σταθερότητας όπως είναι η κρατική ασφάλεια και η οικονομία.

Πολλές επιστημονικές εργασίες και μελέτες που δημοσιεύθηκαν, προσπάθησαν να επεξεργαστούν και να αντιμετωπίσουν το ζήτημα της διάδοσης αποτυχίας σε ένα σύστημα κρίσιμης υποδομής, υπό διαφορετικές απόψεις-θεωρήσεις. Σε αυτές περιλαμβάνονται η οπτικοποίηση της αποτυχίας κρίσιμης υποδομής, τα διαδοχικά αποτελέσματα των αποτυχιών κοινής αιτίας σε κρίσιμες υποδομές, η ανάλυση της αποτυχίας κρίσιμης υποδομής με ένα μοντέλο επανατακτικότητας εισόδου-εξόδου ή/και η ανάλυση εξάρτησης κρίσιμης υποδομής βάσει χρόνου για μεγάλης κλίμακας και διατομεακές αποτυχίες [159].

5.4.2 Προσαρμοστικότητα/Επανατακτικότητα (Resilience) Κρίσιμων Υποδομών

Η εξάρτηση των Κρίσιμων Υποδομών από τα επιτεύγματα της τεχνολογίας έχει καταστήσει τον παράγοντα της διαθεσιμότητας (availability) ως καθοριστικό για την ομαλή λειτουργία τους. Η μεταβλητή φύση όμως της τεχνολογίας, έχει επηρεάσει την αξιοπιστία (reliability) των Κρίσιμων Υποδομών. Έτσι, η δημιουργία επανατακτικών (resilient) Κ.Υ. αποτελεί πρόκληση.
Η προσαρμοστικότητα/επανατακτικότητα εστιάζει στην αποτροπή εμφάνισης αποτυχιών ή στην ελαχιστοποίηση του αντίκτυπου τους, εάν αυτές εκδηλωθούν. Πρόκειται για την ικανότητα μίας υποδομής να αντισταθεί στις επιπτώσεις μίας απειλής (εξωτερικής ή εσωτερικής) και να διατηρήσει τη βασική λειτουργικότητά της, δηλαδή να απορροφήσει, να ανακάμψει και να προσαρμοστεί επιτυχώς σε αντιξοότητες ή σε αλλαγή των φυσιολογικών συνθηκών λειτουργίας[56] [160].

[56] Παρόμοιες προσεγγίσεις σχετικά με το ορισμό της επανατακτικότητας των Κ.Υ., όπου η επανατακτικότητα ταυτίζεται με την ικανότητα του συστήματος να προσαρμοστεί και να διορθωθεί γρήγορα, συναντάμε στην βιβλιογραφία, και συγκεκριμένα στις εξής αναφορές:

Ως προσαρμοστικότητα/επανατακτικότητα μίας Κ.Υ. σε άλλες περιπτώσεις ορίζεται η ύπαρξη στιβαρότητας (robustness) αναφορικά με την απειλή για καταστροφή των στοιχείων της, έτσι ώστε να αποτραπεί η διάδοση μίας αποτυχίας και οι σοβαρές επιπτώσεις αυτής. Με άλλα λόγια, αποτρέπεται η δημιουργία σημείου αποτυχίας. Σε αυτήν την περίπτωση, η προσαρμοστικότητα/επανατακτικότητα ορίζεται με βάση τρείς παραμέτρους: τη στιβαρότητα (robustness), δηλαδή την ικανότητα μιας Κ.Υ. να αντισταθεί σε μία απειλή, την ανάκαμψη/ανάκτηση (recovery), δηλαδή την ικανότητα να ανακάμψει μετά από μία κρίση και την ύπαρξη πόρων (resourcefulness), τόσο για την αποφυγή μίας αποτυχίας όσο και για τη γρήγορη ανάκαμψη από αυτή [161].

Η προσαρμοστικότητα/επανατακτικότητα άρχισε σταδιακά να ορίζεται υπό γενικούς όρους για οποιοδήποτε σύστημα, συμπεριλαμβανομένων των συστημάτων πληροφορικής. Ωστόσο, η προσαρμοστικότητα/επανατακτικότητα μιας Κ.Υ. περιεγράφηκε για πρώτη φορά από τον Αμερικανικό Οργανισμό Κυβερνοασφάλειας και Ασφάλειας Υποδομών (CISA – Cybersecurity & Infrastructure Security Agency)[57] σε ένα έγγραφο με τίτλο “Critical Infrastructure Resilience - Final Report and Recommendations” («Προσαρμοστικότητα/Επανατακτικότητα Κρίσιμων Υποδομών – Τελική Έκθεση και Συστάσεις») όπου ορίστηκε ως η ικανότητα απορρόφησης, προσαρμογής και ταχείας ανάκαμψης από ένα αποδιοργανωτικό συμβάν. Στη συνέχεια μετεξελίχθηκε στην ικανότητα μείωσης του μεγέθους και/ή της διάρκειας ενός αποδιοργανωτικού συμβάντος. Ο ορισμός αυτός έχει παραμείνει ως ο επικρατέστερος σχετικά με επανατακτικότητα των Κ.Υ. [162]. Αυτοί οι ορισμοί δείχνουν σαφώς το τι συνιστά την προσαρμοστικότητα/επανατακτικότητα και το ποια χαρακτηριστικά ενισχύουν την προσαρμοστικότητα/επανατακτικότητα ενός συστήματος Κ.Υ.

5.5 Γενική Προσέγγιση Εκτίμησης Κρισιμότητας

Η βασική προσέγγιση για την εκτίμηση της επικινδυνότητας δίνει έμφαση στα πιθανά λειτουργικά αποτελέσματα σε έναν τομέα (sector) ή σε έναν υπό-τομέα (subsector) ή στην κοινωνία, εάν εμφανιστούν παράγοντες κινδύνου σε μία υποδομή. Εξετάζοντας τις αλληλεξαρτήσεις καθώς και τη σημαντικότητα του αντίκτυπου που θα προκύψει από την παρουσία απειλών ασφάλειας, μία υποδομή χαρακτηρίζεται ως Κρίσιμη Υποδομή για την κοινωνία ή για τον τομέα στον οποίο ανήκει. Οι παράγοντες αντικτύπου (impact factors) ή

- Kasthurirangan, G., and Srinivas, P. (2010): “Sustainable and Resilient Critical Infrastructure Systems Simulation, Modeling, and Intelligent Engineering”, Springer.
- National Infrastructure Advisory Council (2010): “A Framework for Establishing Critical Infrastructure Resilience Goals”, Final Report and Recommendations by the Council, October 19, 2010.

[57] Ο Οργανισμός για την Ασφάλεια στον Κυβερνοχώρο και τις Υποδομές (CISA) είναι ένας αυτόνομος ομοσπονδιακός οργανισμός των Ηνωμένων Πολιτειών, ένας λειτουργικός παράγοντας υπό την εποπτεία του Υπουργείου Εσωτερικής Ασφάλειας. Η CISA ιδρύθηκε στις 16 Νοεμβρίου 2018, όταν ο Πρόεδρος Ντόναλντ Τραμπ υπέγραψε νόμο σχετικά με αναθεώρηση του νόμου για την ασφάλεια στον κυβερνοχώρο και την ασφάλεια των υποδομών του 2018. Ο αναμενόμενος ρόλος της CISA είναι να βελτιώσει την ασφάλεια στον κυβερνοχώρο σε όλα τα επίπεδα διακυβέρνησης, να συντονίσει τα προγράμματα ασφάλειας στον κυβερνοχώρο με τις πολιτείες των ΗΠΑ και να βελτιώσει την κυβερνοπροστασία στον κυβερνοχώρο, έναντι ιδιωτών και εθνικών κρατικών hackers.
Πηγή: "About CISA". Department of Homeland Security. November 19, 2018. Archived from the original on July 6, 2019. Retrieved December 16, 2018.

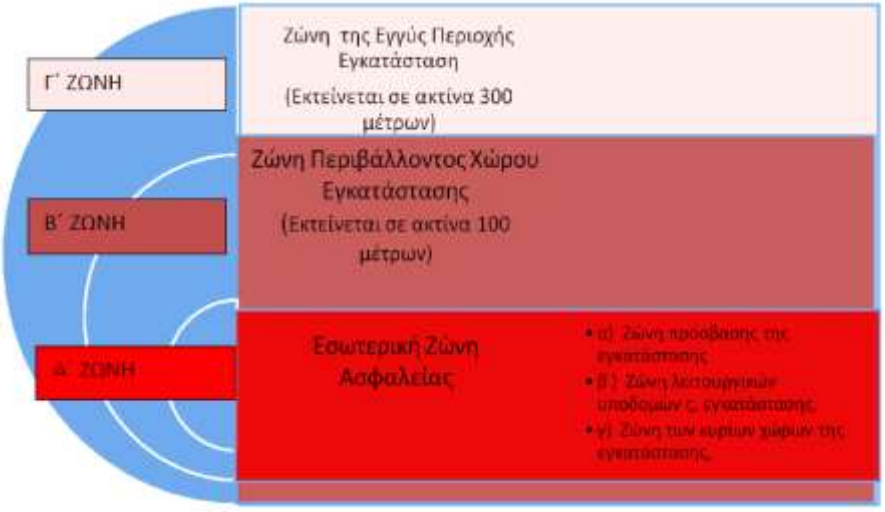
οι παράγοντες κρίσιμων αγαθών (critical asset factors), αποτελούν κριτήρια που χρησιμοποιούνται έτσι ώστε να κατηγοριοποιηθούν οι συναφείς κρίσιμες υποδομές [163].

Η μεθοδολογία για ανάλυση κρισιμότητας που προτείνεται στη βιβλιογραφική παραπομπή [164], απαρτίζεται από τα παρακάτω βήματα:

1. **Προσδιορισμός των Κρίσιμων Αγαθών**
   Ο προσδιορισμός των Κρίσιμων Αγαθών είναι μία διαδικασία στην οποία καταγράφονται τα αγαθά της υπό εξέταση Υποδομής καθώς και τα ιδιαίτερα χαρακτηριστικά αυτών (π.χ. εκρηκτικές ύλες), ενώ ταυτόχρονα διερευνώνται οι αλληλεξαρτήσεις των αγαθών αυτών. Για παράδειγμα, εάν η προς εξέταση υποδομή αφορά σε μία αποθήκη πρώτων υλών τροφίμων, τότε θα πρέπει να εξεταστεί η αλυσίδα διανομής και διάθεσης η οποία εξαρτάται από την υποδομή αυτή, καθώς και το αντίκτυπο 2^{ου} και 3^{ου} βαθμού σε περίπτωση απειλής.

2. **Καθορισμός των Αλληλεξαρτήσεων**
   Οι αλληλεξαρτήσεις χωρίζονται σε δύο κατηγορίες, ήτοι: των εξαρτώμενων Κ.Υ., δηλαδή των υποδομών που εξαρτώνται από την υπό εξέταση υποδομή και των απαιτούμενων, δηλαδή των υποδομών που απαιτούνται από την υπό εξέταση υποδομή για τη λειτουργία της. Στην ανάλυση κρισιμότητας οι διασυνδεδεμένες Κ.Υ. θα πρέπει να λαμβάνονται υπόψη, ακόμη και στην περίπτωση που δεν επιφέρουν ή δεν επιδέχονται κάποιο κίνδυνο από ή προς την εξεταζόμενη υποδομή.

3. **Εκτίμηση του Αντικτύπου Κρισιμότητας (Criticality Impact)**
   Οι Παράγοντες Αντικτύπου (Impact Factors) δίνουν έμφαση στο κοινωνικό παρά στον εσωτερικό αντίκτυπο και η εκτίμησή τους γίνεται με βάση την έκταση, τη σοβαρότητα και το χρόνο. Για παράδειγμα, μία έκρηξη εκρηκτικών υλών μίας αποθήκης μπορεί να επηρεάζει μεγάλη ακτίνα μέτρων γύρω από την εγκατάσταση, ενώ μία διακοπή ρεύματος θα επηρεάσει την εσωτερική εγκατάσταση του κτηρίου. Στην παρακάτω εικόνα, φαίνονται σχηματικά οι ζώνες επιρροής.



Εικόνα 5-4: Σχηματική κατάτμηση σε ζώνες επικινδυνότητας μιας υποδομής [165]

4. **Καθορισμός Απειλών**
   Καθώς η ανάλυση κρισιμότητας βασίζεται στις διασυνδεδεμένες Κρίσιμες Υποδομές, θα πρέπει να δημιουργηθεί μία λίστα των εν δυνάμει απειλών. Ενδεικτικά θα αναφέρουμε την προσποίηση ενός μη εξουσιοδοτημένου χρήστη (masquerading attack), την μη εξουσιοδοτημένη χρήση πόρων, την εισαγωγή κακόβουλου λογισμικού, την εκτροπή ή παραποίηση επικοινωνιών, τις αποτυχίες επικοινωνίας, τις αποτυχίες τεχνικής φύσεως, τις διακοπές ρεύματος, τις αποτυχίες λογισμικού, τα λειτουργικά σφάλματα, τα σφάλματα συντήρησης, τα σφάλματα χρηστών, τη φωτιά, τις φυσικές καταστροφές, τις ελλείψεις προσωπικού και την τρομοκρατία.

5. **Εκτίμηση του Επιπέδου Απειλών και Ευπαθειών**
   Οι πιθανές απειλές αφορούν τόσο στο εσωτερικό της υπό εξέταση υποδομής, αλλά και σε όλη την έκταση των διασυνδέσεων και εξαρτήσεων αυτής. Η πιθανότητα της απειλής μπορεί να βασιστεί στο ιστορικό προηγούμενων περιστατικών, στην υπάρχουσα βιβλιογραφία και σε συνεντεύξεις με ειδικούς. Οι απειλές που συναντώνται σε μία Κρίσιμη Υποδομή είναι ένα γενικότερο σύνολο των απειλών που συναντάμε σε μία αξιολόγηση κινδύνου (risk assessment).

Ο πίνακας που ακολουθεί περιέχει ορισμένα βασικά κριτήρια που λαμβάνονται υπόψη στην αποτίμηση επικινδυνότητας [164].

	ΚΡΙΤΗΡΙΑ ΑΠΟΤΙΜΗΣΗΣ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ		
	Έκταση	**Σπουδαιότητα**	**Χρόνος**
ΠΑΡΑΓΟΝΤΕΣ	• Πληγής πληθυσμός • Συγκέντρωση πληθυσμού • Εμβέλεια αντίκτυπου	• Οικονομικός αντίκτυπος • Αλληλεξάρτηση • Δημόσια εμπιστοσύνη • Διεθνείς σχέσεις (διατάραξη σχέσεων) • Δημόσια Τάξη (διατάραξη δημόσιας τάξης) • Πολιτική και λειτουργία των δημοσίων υπηρεσιών • Ασφάλεια πολιτών • Εθνική άμυνα	• Διάρκεια ανάκαμψης • Στιγμή μέγιστου αντίκτυπου (Impact Peak) • Μεταβολή κρισιμότητας (Critical Time Frame)

Πίνακας 5-2: Παράγοντες Αντίκτυπου (Impact Factor) για τον προσδιορισμό της Κρισιμότητας Υποδομών

5.5.1 Ασφάλεια Τηλεπικοινωνιών & Πληροφοριακών Συστημάτων

Ο ιδιωτικός φορέας, που σήμερα διευθύνει ή διαχειρίζεται ένα ευρύ πλέγμα κρίσιμων υποδομών, θα πρέπει να διαβουλεύεται με τις εθνικές Αρχές σχετικά με το πλαίσιο των ελάχιστων μέτρων ασφάλειας που θα πρέπει να λαμβάνει στην καθημερινότητα καθώς και στις έκτακτες ανάγκες. Η προστασία των δημοσίων και ιδιωτικών Κ.Υ., καθώς και τα μέτρα ασφάλειας που θα λαμβάνονται, αποτελούν ευθύνη των ιδίων των ιδιοκτητών ή διαχειριστών των υποδομών αυτών. Η Ευρωπαϊκή Επιτροπή, χρηματοδοτεί Μελέτες Τρωτότητας – Ευπάθειας, καθώς και Μελέτες Επικινδυνότητας κρίσιμων υποδομών, σε τοπικό, περιφερειακό και εθνικό επίπεδο. Το ποσοστό χρηματοδότησης προβλέπεται να φθάσει μέχρι το 85% του κόστους.

Στην Ελλάδα, αναγνωρίσθηκαν και προσδιορίστηκαν οι σημαντικές Εθνικές Κρίσιμες Υποδομές, ενώ εκπονήθηκαν ειδικές Μελέτες Ανάλυσης Πληροφοριών, Αξιολόγησης του Κινδύνου και Εκτίμησης της Ασφάλειας από έμπειρα στελέχη των Υπηρεσιών Ασφάλειας. Με δεδομένο ότι ο τομέας Προστασίας των Υποδομών δεν είναι ένα στατικό γεγονός αλλά συνιστά μία διαρκή, εξελισσόμενη διαδικασία και με αφορμή την παρακολούθηση των εξελίξεων για την προστασία των κρίσιμων υποδομών της Ελλάδας που παρουσιάζουν ευρωπαϊκό ενδιαφέρον, στα τέλη του 2005, συγκροτήθηκε Μόνιμη Διυπουργική Ομάδα Εργασίας που λειτουργεί υπό την αιγίδα της Γενικής Γραμματείας Πολιτικής Προστασίας. Ο συγκεκριμένος φορέας θεσμικά φέρει, *αφενός μεν* την ευθύνη για το διυπουργικό συντονισμό σε θέματα προληπτικής προστασίας κρίσιμων υποδομών, *αφετέρου δε* την ευθύνη συντονισμού των κρατικών και μη φορέων, όταν εκδηλώνονται μεγάλης έκτασης και έντασης καταστάσεις έκτακτης ανάγκης [165].

Η έννοια της προστασίας των Κρίσιμων Υποδομών (CIP - Critical Infrastructure Protection) αποτελεί ένα μεγαλύτερο σύνολο της έννοιας της προστασίας Κρίσιμων Υποδομών Τηλεπικοινωνιών και Πληροφορικής (CIIP - Critical Information Infrastructure Protection). Η εστίαση αποκλειστικά σε κυβερνοαπειλές στον τομέα CIIP αγνοεί τον κρίσιμο παράγοντα των φυσικών απειλών (physical threats) και έτσι αφήνει σημαντικά κενά ασφαλείας σε μια Κ.Υ.. Σε συνέχεια των προσεγγίσεων που είδαμε σε προηγούμενα κεφάλαια, αλλά και της σύγχρονης βιβλιογραφίας όσον αφορά στις απειλές σε Κ.Υ., η οποιαδήποτε υιοθετούμενη προσέγγιση θα πρέπει να λαμβάνει υπόψη και να αξιοποιεί και τις δύο οπτικές, ώστε να θεωρείται επαρκής. Ο λόγος που συμβαίνει αυτό είναι γιατί οι δύο έννοιες δεν μπορούν – και δεν πρέπει – να εξετάζονται ως εντελώς ξεχωριστές.

Παρόλα αυτά, υπάρχει τουλάχιστον ένα χαρακτηριστικό για να διαχωρίσουμε τις δύο έννοιες: δηλαδή, ενώ η προστασία κρίσιμων υποδομών εξετάζει όλους τους τομείς ενδιαφέροντος που περιλαμβάνουν κρίσιμες υποδομές, η προστασία κρίσιμων πληροφοριακών υποδομών περιλαμβάνει ένα υποσύνολο αυτών, καθώς εστιάζει σε μέτρα προστασίας της κρίσιμης πληροφοριακής υποδομής.

Γενικά, μία κρίσιμη πληροφοριακή και επικοινωνιακή υποδομή αποτελεί μέρος πολλών εθνικών υποδομών οι οποίες είναι απαραίτητες για την παροχή κρίσιμων υπηρεσιών, όπως είδαμε και σε προηγούμενα κεφάλαια σχετικά με τις αλληλεξαρτήσεις. Οι Κ.Υ. Τηλεπικοινωνιών και Πληροφορικής, αποτελούν μέρος του κρίσιμου τομέα των Τεχνολογιών Πληροφοριών και Επικοινωνιών (ΤΠΕ) που περιλαμβάνει τις τεχνολογίες των

τηλεπικοινωνιών, της πληροφορικής και των υπολογιστών, του λογισμικού, του διαδικτύου, των δορυφορικών επικοινωνιών, των οπτικών ινών, της μεταφοράς σημάτων κ.α. Ο όρος χρησιμοποιείται επίσης για το σύνολο των διασυνδεδεμένων υπολογιστών και δικτύων καθώς και των κρίσιμων ροών πληροφορίας μεταξύ αλληλεξαρτώμενων υποδομών. Ακριβώς λόγω αυτού του ρόλου διασύνδεσης, οι Κ.Υ. τηλεπικοινωνιών αποτελούν στόχους κακόβουλων ενεργειών. Εφόσον λοιπόν αυτές οι Κ.Υ. θεωρούνται η «ραχοκοκαλιά» των Κ.Υ., η ανταλλαγή δεδομένων επιβάλλεται να είναι συνεχώς διαθέσιμη και αξιόπιστη, καθώς είναι απαραίτητη για τη λειτουργία των υποδομών και των αντίστοιχων υπηρεσιών τους [168].

Η διαφύλαξη των πόρων και η προστασία των δεδομένων δεν προσδιορίζεται αόριστα, αλλά επί τη βάσει των τριών (3) θεμελιωδών ιδιοτήτων της Ασφάλειας Πληροφοριών, που είναι οι εξής [167]:

1. **Διαθεσιμότητα (Availability)**: Η διαθεσιμότητα (availability) των δεδομένων και των υπολογιστικών πόρων είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους.

2. **Ακεραιότητα (Integrity)**: Η ακεραιότητα (integrity) αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μία γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και την αποτροπή της πρόσβασης ή χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια.
   Για παράδειγμα, μια εφημερίδα που δημοσιεύει τα άρθρα της και η οποία στο Διαδίκτυο θα ήθελε αυτά τα άρθρα να είναι ασφαλή από μετατροπές ενός χάκερ που επιθυμεί να εισάγει λανθασμένες πληροφορίες στα κείμενα. Ακριβώς αυτό συνέβη το 1995, όταν άγνωστα άτομα κατάφεραν να εξουδετερώσουν τα μέτρα ασφάλειας της εφημερίδας Ελευθεροτυπία και να εισαγάγουν πρωτοσέλιδο άρθρο για τον πρόωρο θάνατο του Ανδρέα Παπανδρέου, που εκείνη τη στιγμή νοσηλευόταν στο Ωνάσειο[58].

3. **Εμπιστευτικότητα (Confidentiality):** Η εμπιστευτικότητα ορίζει ότι ευαίσθητες πληροφορίες δεν θα έπρεπε να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα. Ζητούμενο είναι η διασφάλιση του μερισμού των πληροφοριών που διακινούνται σε μία πληροφοριακή και επικοινωνιακή υποδομή χωρίς την άδεια του ιδιοκτήτη τους.

[58] Πηγή: Αθηναϊκό ειδησεογραφικό πρακτορείο, «Πειρατές στο Ίντερνετ Ξαναχτυπούν, ΜΠΕ» (10/1996). http://www.hri.org/info/articles/96-10-07.elot.html

Εκτός όμως από τις παραπάνω βασικές ιδιότητες, η ασφάλεια στις Κ.Υ. τηλεπικοινωνιών και πληροφορικής συσχετίζεται με την επιτυχημένη εφαρμογή και των ακόλουθων μηχανισμών [167]:

- **Αναγνώριση (Identification):** Αφορά στη διαδικασία παρουσίασης της ταυτότητας μίας οντότητας (π.χ. πελάτη) στο σύστημα (π.χ. εξυπηρετητή).

- **Αυθεντικοποίηση/επαλήθευση ταυτότητας (Authentication)**: Αφορά στη διαδικασία επιβεβαίωσης της ταυτότητας που έχει παρουσιάσει μία οντότητα στο σύστημα.

- **Εξουσιοδότηση (Authorization):** Αφορά στη διαδικασία λήψης απόφασης σχετικά με την αποδοχή ή την απόρριψη ενός αιτήματος πρόσβασης μίας αυθεντικοποιημένης οντότητας στο σύστημα, επί τη βάσει των δικαιωμάτων πρόσβασης που της έχουν ήδη εκχωρηθεί και της πολιτικής ελέγχου πρόσβασης του συστήματος.

- **Αδυναμία αποποίησης/μη αποποίηση (Non-Repudiation):** Αφορά στη διαδικασία αδιαμφισβήτητου καταλογισμού ευθύνης για την επιτέλεση μίας ενέργειας στο σύστημα (αναφορικά με την τήρηση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των κάθε είδους πόρων μίας πληροφοριακής και επικοινωνιακής υποδομής).

Μία κατάσταση, όπου υπάρχει το ενδεχόμενο πρόκλησης απωλειών ή ζημιών, όπως υποκλοπή (interception) αγαθού, μεταβολή (modification) αγαθού, πλαστογραφία (fabrication) αγαθού ή διακοπή (interruption) της κανονικής λειτουργίας του συστήματος, αποτελεί απειλή (threat) για το σύστημα. Οι απειλές μπορούν να κατηγοριοποιηθούν ως εξής [169]:

1. **Φυσικές απειλές**, είναι αυτές που προκύπτουν από τη φύση των συστημάτων ή από το περιβάλλον μέσα στο οποίο αναπτύσσονται και λειτουργούν.

2. **Εκούσιες απειλές**, είναι αυτές που προκύπτουν από εσκεμμένες κακόβουλες ενέργειες των χρηστών.

3. **Ακούσιες απειλές**, είναι αυτές που προκύπτουν από λανθασμένες (ακούσιες) ενέργειες των χρηστών.

Οι ζημίες προκαλούνται μετά από επιθέσεις (attacks). Μία επίθεση προκαλείται ως αποτέλεσμα της εκμετάλλευσης μίας ή περισσότερων ευπαθειών/τρωτοτήτων του συστήματος. Μία ευπάθεια (vulnerability) μπορεί να αφορά σε μία αδυναμία στις ρυθμίσεις ή στη διαχείριση του συστήματος ή σε ένα ευάλωτο σημείο σε ένα υποσύστημα ασφάλειας.

Ορισμένες κατηγορίες και χαρακτηριστικά παραδείγματα ευπαθειών είναι:

- **Ανθρώπινες Ευπάθειες (Human)**: Αποτελούν την κρισιμότερη κατηγορία για την ασφάλεια ενός Πληροφοριακού Συστήματος (ΠΣ) και μπορεί να προκαλέσουν τις χειρότερες επιπτώσεις, καθώς προέρχονται εκ των έσω (insiders), δηλαδή από νόμιμους χρήστες που γνωρίζουν καλά το σύστημα και τους μηχανισμούς ασφάλειας.

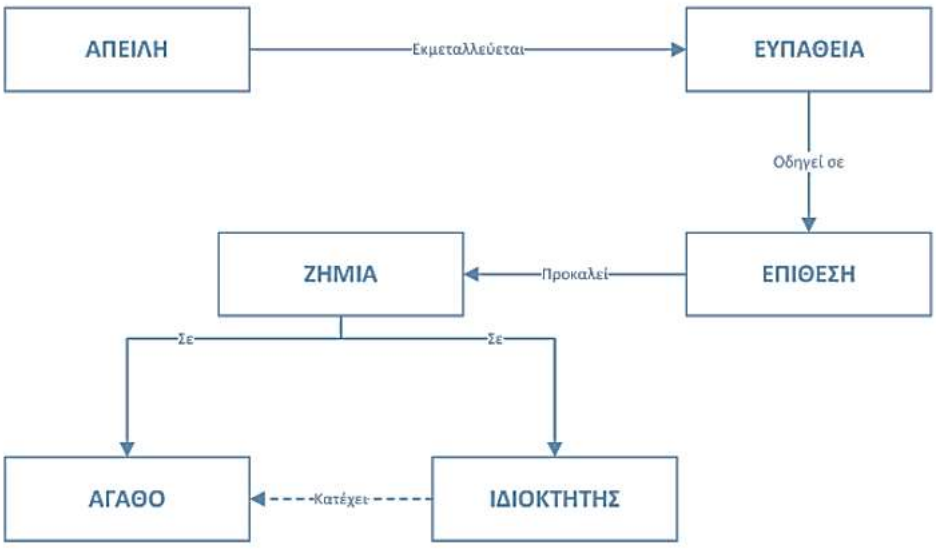
- **Ευπάθειες Υλισμικού και Λογισμικού:** Αφορούν σε προβληματική κατασκευή, καθώς και σε λανθασμένες ρυθμίσεις και δυσλειτουργίες του υλισμικού (hardware) και του λογισμικού (software).

- **Ευπάθειες Μέσων (Media):** Αφορούν ΣΕ προβληματικές διαδικασίες διαχείρισης που μπορεί να οδηγήσουν σε κλοπή ή καταστροφή μαγνητικών, οπτικών ή έντυπων μέσων αποθήκευσης δεδομένων.

- **Ευπάθειες Επικοινωνιών (Communications):** Αφορούν σε κατασκευαστικές αδυναμίες, λανθασμένες ρυθμίσεις καθώς και σε δυσλειτουργίες των δικτυακών συνδέσεων.

- **Φυσικές Ευπάθειες (Physical):** Αφορούν στο φυσικό χώρο όπου αναπτύσσονται και λειτουργούν τα συστήματα (π.χ. data centers).

- **Εκ φύσεως Ευπάθειες (Natural):** Αφορούν σε φυσικά φαινόμενα (π.χ. φυσικές καταστροφές), περιβαλλοντικές εξαρτήσεις κ.α.).



Εικόνα 5-5: Συσχέτιση βασικών εννοιών στην προστασία Κ.Υ. [169]

Οι επιπτώσεις που μπορεί να προκαλέσει μία επιτυχημένη επίθεση, αφορούν κυρίως στη μείωση της αξίας των αγαθών ή/και στη πρόκληση προσωρινής δυσλειτουργίας ή διακοπής της λειτουργίας του συστήματος. Η αντιμετώπιση των απειλών επιτυγχάνεται με μέτρα προστασίας (controls) ή αντίμετρα (countermeasures), τα οποία συνίστανται σε προληπτικά κυρίως μέτρα (π.χ. πράξη, συσκευή, διαδικασία ή μέθοδος) τεχνικής και διαχειριστικής φύσης που αποσκοπούν στη μείωση ή εξάλειψη των γνωστών ευπαθειών του συστήματος. Η απόκτηση και εφαρμογή των μέτρων προστασίας συνεπάγεται ένα πρόσθετο κόστος λειτουργίας του οικείου οργανισμού [169].

Κατά τις πρώιμες προσπάθειες προστασίας κρίσιμων υποδομών, η τρωτότητα κατευθυνόταν κυρίως προς άγνωστους κινδύνους οι οποίοι προέρχονταν από τον κυβερνοχώρο (cyberspace). Η παγκόσμια πληροφοριακή υποδομή φαινόταν να ευνοεί ανώνυμες επιθέσεις από οπουδήποτε στον κόσμο, δρώντας παράλληλα ως ανεξάντλητη πηγή εργαλείων για επιθέσεις για τον οποιοδήποτε. Με βάση αυτή την οπτική, στις Η.Π.Α. θεσπίστηκε πολιτική για την προστασία των Κ.Υ. τηλεπικοινωνιών, όπως αυτή περιγράφεται στην έκθεση του Προέδρου της Επιτροπής Ασφαλείας σχετικά με την προστασία των Κ.Υ. [PCCIP, 1997][59].

Η πολιτική αυτή προσανατολιζόταν κυρίως προς την ασφάλεια πληροφοριών, ενώ την ίδια προσέγγιση υιοθέτησαν και άλλες χώρες, εστιάζοντας στο τηλεπικοινωνιακό και πληροφοριακό μέρος των Κ.Υ. Η πρώτη έκδοση του International Critical Infrastructure Protection (CIP) Handbook μελετά είκοσι (20) εθνικές και έξι (6) διεθνείς σχετικές προσεγγίσεις[60]. Ωστόσο, μετά τα ειδικά εγκλήματα βίας της 11ης Σεπτέμβρη του 2001, υπήρξε μία μεταστροφή από την κλασσική προσέγγιση της πληροφοριακής απειλής, η οποία παραπέμπει έντονα στην ασφάλεια των πληροφοριών. Η εστίαση μετατοπίστηκε κυρίως σε δομικές απειλές, οι οποίες προκύπτουν μη τυχαία αλλά εσκεμμένα, με την αντιτρομοκρατική στρατηγική να παίζει κυρίαρχο ρόλο. Θέματα της φυσικής προστασίας των κρίσιμων υποδομών αποκτούν μεγαλύτερο βάρος, σε αντιδιαστολή με την πληροφοριακή ή τη δικτυακή τους ασφάλεια[61]. Ακόμα και σήμερα, η ορολογία και ο διαχωρισμός μεταξύ προστασίας κρίσιμων υποδομών (Critical Infrastructure Protection - CIP) και προστασίας κρίσιμων πληροφοριακών και επικοινωνιακών υποδομών (Critical Information Infrastructure Protection – CIIP) δεν είναι ξεκάθαρος. Στην υπάρχουσα βιβλιογραφία, χρησιμοποιείται πιο συχνά ο όρος «προστασία κρίσιμων υποδομών (CIP)», ακόμα και σε περιπτώσεις όπου γίνεται αναφορά στις πληροφοριακές προεκτάσεις του θέματος .

---

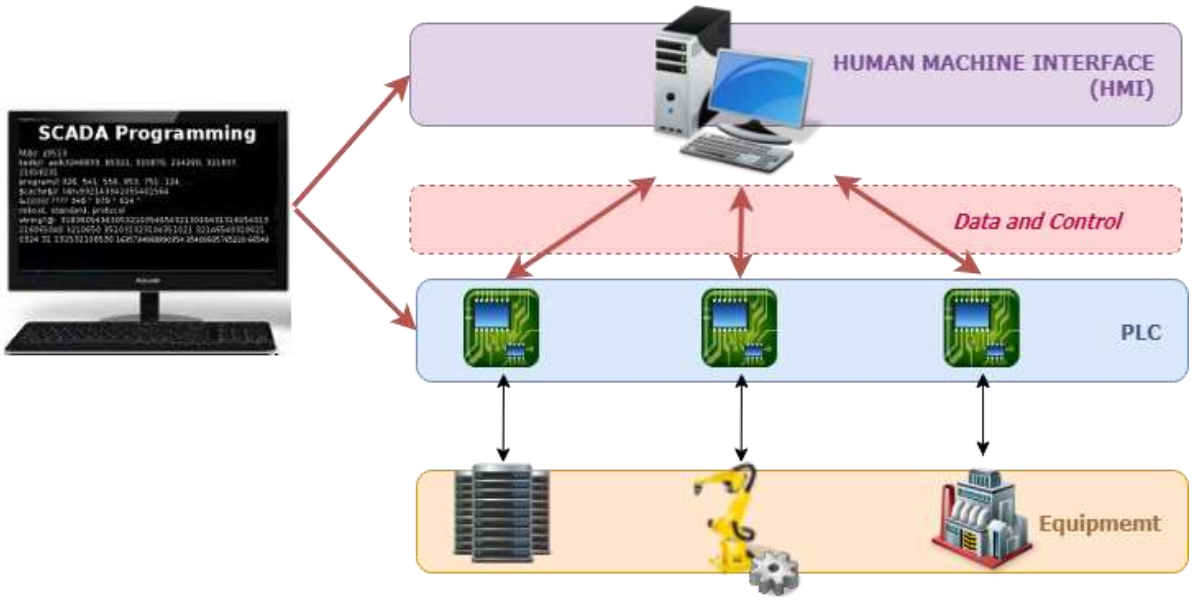
[59] Βλέπε, π.χ.: https://www.hsdl.org/?abstract&did=487492

[60] Βλέπε επίσης τις πληροφορίες που αναφέρονται στον σύνδεσμο: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf

[61] Μία από τις βασικές αποστολές του Υπουργείου Εσωτερικής Ασφάλειας (DHS) των Η.Π.Α. είναι η ενίσχυση την ικανότητας του κράτους και των τοπικών κυβερνήσεων να προλαμβάνουν, να προστατεύουν και να αναπτύσσουν την ικανότητα ανάκαμψης από τρομοκρατικές επιθέσεις και άλλες καταστροφές. Η Ομοσπονδιακή Υπηρεσία Διαχείρισης Καταστάσεων (FEMA) πρότεινε μια ολοκληρωμένη σειρά προγραμμάτων επιχορήγησης η οποία αποτελεί σημαντικό μέρος μιας προσπάθειας ενίσχυσης της ετοιμότητας για την ασφάλεια των Η.Π.Α. Σε αυτά τα προγράμματα δίνεται η παραπάνω προσέγγιση καθώς μετά το 9/11 υλοποιούνται στόχοι που αναφέρονται σε μια σειρά νόμων, στρατηγικών, έγγραφων οδηγιών και σχεδίων Εσωτερικής Ασφάλειας (Homeland Security Presidential Directives - HSPDs).

5.5.1.1 Ασφάλεια Συστημάτων SCADA

Κεντρικά ηλεκτρονικά συστήματα, τα οποία φέρουν την ονομασία SCADA (Supervisory, Control, and Data Acquisition), χρησιμοποιούνται ευρέως για την εποπτεία και τον έλεγχο υποδομών, είτε τοπικά είτε με απομακρυσμένο τρόπο.
Συνοπτικά, τα συστήματα SCADA αποτελούνται από τοπικούς ελεγκτές, που ελέγχουν επί μέρους στοιχεία και μονάδες μίας εγκατάστασης, συνδεδεμένους σε ένα Κεντρικό Σταθμό Εργασίας (Master Station). Ο κεντρικός σταθμός εργασίας μπορεί κατόπιν να επικοινωνεί τα δεδομένα που συλλέγει από την εγκατάσταση σε ένα πλήθος από σταθμούς εργασίας σε τοπικό δίκτυο (LAN – Local Area Network) ή και να μεταδίδει τα δεδομένα της εγκατάστασης σε μακρινά σημεία μέσω κάποιου συστήματος τηλεπικοινωνίας, π.χ. μέσω του ενσύρματου τηλεφωνικού δικτύου ή μέσω κάποιου ασύρματου δικτύου. Επίσης είναι δυνατό ο κάθε ένας τοπικός ελεγκτής να βρίσκεται σε απομακρυσμένη τοποθεσία και να μεταδίδει τα δεδομένα προς τον master station μέσω απλού καλωδίου ή μέσω ασύρματου πομποδέκτη, πάντα με σύνολο από τοπικούς ελεγκτές συνδεδεμένους σε τοπολογία αστέρα προς έναν master station [170].



Εικόνα 5-6: Διάγραμμα βασικών στοιχείων συστήματος SCADA[62]

[62] Η αρχιτεκτονική ενός SCADA περιλαμβάνει την συλλογή αναλογικών δεδομένων και την μετατροπή τους σε ψηφιακά, πχ την μέτρηση της θερμοκρασίας ενός μηχανήματος. Το κανάλι επικοινωνίας μπορεί να είναι αναλογικό (T202, POTS) ή ψηφιακό (RS485, TCP / IP). Η τοπολογία δικτύου SCADA συνήθως περιλαμβάνει επίσης κάποιο είδος επικύρωσης μεταφοράς. Τα δεδομένα που συλλέγονται υποβάλλονται σε επεξεργασία, οργανώνονται και παρουσιάζονται για τους διαχειριστές συστημάτων ώστε να λαμβάνουν τις κατάλληλες αποφάσεις απόκρισης και ελέγχου. Η παρουσίαση μπορεί να ποικίλει από παρουσίαση σε πίνακα των καταγεγραμμένων συμβάντων έως γραφική παρουσίαση σε χαρτογράφηση ή υπόβαθρα εικόνας. Εάν απαιτούνται αποφάσεις ελέγχου και το σύστημα υποστηρίζει έξοδο, μπορούν να αποσταλούν κατάλληλες εντολές για να επηρεάσουν συγκεκριμένες αλλαγές λειτουργίας ή διαμόρφωσης. Οι περισσότερες ενέργειες ελέγχου εκτελούνται από PLC (Programmable Logic Controller) και RTUs (Remote Telemetry Units).
Πηγή: https://www.dpstele.com/scada/how-systems-work.php

Τα συστήματα SCADA δεν χαρακτηρίζονται ως τα πλέον ασφαλή, καθώς ο εξοπλισμός ο οποίος τα αποτελεί είναι δικτυακός και βασισμένος σε διαδικτυακά πρωτόκολλα (IP-based), τα οποία απαιτούν τη χρήση του διαδικτύου ως μέσο διασύνδεσης, γεγονός που αυξάνει την πιθανότητα εξωτερικών ψηφιακών απειλών, εκτός από τον ενυπάρχοντα κίνδυνο άλλων φυσικών απειλών ή «εκ των έσω» κινδύνων (insider threats) [170].

Στα συστήματα αυτά, οι πιθανοί τρόποι επιθέσεων ποικίλλουν. Αυτές περιλαμβάνουν κυβερνο-επιθέσεις, αλλά και τη φυσική καταστροφή ιδιωτικών ή στρατιωτικών εγκαταστάσεων. Πιο συγκεκριμένα, έχουν αναφερθεί αρκετά περιστατικά που σχετίζονται με δικτυακές επιθέσεις σε ιδιωτικές ή δημόσιες υποδομές παροχής ηλεκτρικής ενέργειας και ύδρευσης, οι οποίες χρησιμοποιούν πληροφοριακά και επικοινωνιακά συστήματα ελέγχου της λειτουργίας τους (SCADA). Σύμφωνα με την ετήσια έκθεση ασφαλείας της N. Ζηλανδίας (PGG Wrightson Annual Report[63]) χαρακτηριστικά παραδείγματα επιθέσεων περιλαμβάνουν τις παρακάτω περιπτώσεις:

- Επίθεση στο εταιρικό δίκτυο SCADA του εθνικού φορέα παροχής ηλεκτρικής ενέργειας της Βραζιλίας, χωρίς όμως επιτυχή εισβολή στο επίπεδο λειτουργιών του (Βραζιλία, Νοέμβριος 2009).
- Μέρος μεγάλης μονάδας πυρηνικής ενέργειας (Brown's Ferry nuclear power plant) σταμάτησε να λειτουργεί λόγω βλάβης σε δύο αντλίες κυκλοφορίας ύδατος, όπου κατά την διερεύνηση του περιστατικού εντοπίστηκε ως αιτία διακοπής η υπερχείλιση δεδομένων στο εσωτερικό δίκτυο ελέγχου. (Αλαμπάμα, ΗΠΑ, Αύγουστος 2006).
- Επιτυχής εγκατάσταση μη εξουσιοδοτημένου λογισμικού πραγματοποιήθηκε σε σύστημα SCADA το οποίο έλεγχε την πορεία των υδάτων στον ποταμό Σακραμέντο (Καλιφόρνια, ΗΠΑ, 2007).
- Ένας hacker κατάφερε να αποκτήσει έλεγχο του υπολογιστικού συστήματος που έλεγχε κρίσιμα συστήματα ελέγχου υδάτων (water treatment plant), μέσω του φορητού υπολογιστή ενός υπαλλήλου, στην Πενσυλβάνια, ΗΠΑ (Οκτώβριος 2006).
- Μια κυβερνοεπίθεση προκάλεσε πλήρη διακοπή ηλεκτροδότησης σε τρεις πόλεις βόρεια του Ρίο ντε Τζανέιρο, επηρεάζοντας δεκάδες χιλιάδες πολιτών (Βραζιλία, 2005).
- Τον Μάιο του 2001, 400.000 σπίτια στην Καλιφόρνια έμειναν χωρίς ηλεκτρική ενέργεια για δύο ημέρες, μετά από την επιτυχή επίθεση σε δύο εξυπηρετητές ενός τοπικού παρόχου (California Independent System Operator). Οι επιτιθέμενοι βρίσκονταν στο δίκτυο της εταιρείας από τις 25 Απρίλιου μέχρι 11 Μαΐου (Καλιφόρνια, ΗΠΑ, 2001).
- Την ίδια χρονιά στο Σαιντ Λούις, της πολιτείας Μιζούρι, μία ασυμβατότητα στις ενδείξεις του φράγματος Sauk Water Storage Dam οδήγησαν στην απώλεια δις γαλονιών νερού (Μιζούρι, ΗΠΑ, 2001).
- Ένας ιός (Slammer worm) διέκοψε τη λειτουργία της πυρηνικής εγκατάστασης Davis Besse στο Οχάιο, ΗΠΑ (Ιανουάριος 2003).

[63] Βλέπε: https://www.pggwrightson.co.nz/Investors/Company-Reports

Όπως είδαμε, οι τηλεπικοινωνιακές και πληροφοριακές Κρίσιμες Υποδομές αποτελούν υποσύνολο των υποδομών, ενώ σε πολλές περιπτώσεις, μία πληροφοριακή και επικοινωνιακή υποδομή μπορεί να αποτελέσει και τμήμα μίας ευρύτερης υποδομής. Το σύστημα SCADA, το οποίο ελέγχει τη λειτουργία μίας υποδομής καθώς αποτελείται από υπο-συστήματα και δίκτυα, θα μπορούσε έστω και έμμεσα να θεωρηθεί ως μία μορφή ολοκληρωμένης τηλεπικοινωνιακής υποδομής. Η ασφάλεια SCADA είναι η πρακτική προστασίας των δικτύων εποπτικού ελέγχου και απόκτησης δεδομένων σε κρίσιμες υποδομές αλλά και σε βιομηχανικές κρίσιμες εγκαταστάσεις. Όπως είδαμε στα προηγούμενα παραδείγματα καταστροφών, αυτά τα δίκτυα είναι υπεύθυνα για την παροχή αυτοματοποιημένου ελέγχου και απομακρυσμένης ανθρώπινης διαχείρισης βασικών προϊόντων και υπηρεσιών, όπως νερό, φυσικό αέριο, ηλεκτρικό ρεύμα και μεταφορά σε εκατομμύρια ανθρώπους και, *όπως και οποιοδήποτε άλλο δίκτυο*, απειλούνται από επιθέσεις στον κυβερνοχώρο που θα μπορούσαν να καταστρέψουν οποιοδήποτε μέρος μίας εθνικής κρίσιμης υποδομής, γρήγορα και με τρομερές συνέπειες. Οι κεφαλαιουχικές δαπάνες είναι ένα άλλο βασικό μέλημα καθώς τα συστήματα SCADA μπορούν να κοστίσουν για έναν οργανισμό από δεκάδες χιλιάδες έως εκατομμύρια ευρώ. Για αυτούς τους λόγους, είναι σημαντικό οι οργανισμοί να εφαρμόζουν ισχυρά μέτρα ασφαλείας για την προστασία της υποδομής αλλά και των πολλών ανθρώπων που θα επηρεαστούν από τυχόν διαταραχές που θα προκληθούν από μία εξωτερική επίθεση ή ένα εσωτερικό σφάλμα.

Η ασφάλεια των SCADA έχει εξελιχθεί δραματικά τα τελευταία χρόνια. Πριν από τους υπολογιστές, ο μόνος τρόπος παρακολούθησης ενός δικτύου SCADA ήταν να ορίσουμε ανθρώπους σε κάθε σταθμό για να αναφέρουν την κατάσταση του κάθε συστήματος. Σε πιο πολυσύχναστους σταθμούς, οι τεχνικοί διορίζονταν σε μόνιμη 24ωρη βάση, για την επιτήρηση της λειτουργίας του δικτύου αλλά και της επικοινωνίας μέσω καλωδίων τηλεφώνου. Η εισαγωγή του τοπικού δικτύου (LAN) αλλά και οι βελτιώσεις στον τομέα των δικτύων έφεραν πρόοδο στην ανάπτυξη SCADA, όπως το κατανεμημένο δίκτυο SCADA. Στη συνέχεια τα δικτυωμένα συστήματα ήταν σε θέση να επικοινωνούν μέσω δικτύου ευρείας περιοχής (WAN) και να συνδέουν περισσότερα στοιχεία μαζί. Έτσι, οι απειλές για την ασφάλεια των δικτύων SCADA οροθετούνται στις συνήθεις απειλές που μπορούν να προσβάλλουν οποιοδήποτε σύστημα το οποίο βασίζεται στο πρωτόκολλο Διαδικτύου (IP) [171].

Οι συγκεκριμένες απειλές για τα δίκτυα SCADA περιλαμβάνουν τα ακόλουθα [171]:

- **Χάκερ (hacker)**: Άτομα ή ομάδες με κακόβουλη πρόθεση θα μπορούσαν να προσβάλλουν ένα δίκτυο SCADA. Με την απόκτηση πρόσβασης σε βασικά στοιχεία SCADA, οι hackers θα μπορούσαν να εξαπολύσουν χάος σε έναν οργανισμό.

- **Κακόβουλο λογισμικό:** Το κακόβουλο λογισμικό, συμπεριλαμβανομένων ιών, spyware και ransomware μπορεί να αποτελέσει κίνδυνο για τα συστήματα SCADA. Παρόλο που το κακόβουλο λογισμικό ενδέχεται να μην μπορεί να στοχεύσει συγκεκριμένα στο ίδιο το δίκτυο, μπορεί ακόμα να αποτελέσει απειλή για την βασική υποδομή που βοηθά στη διαχείριση του δικτύου SCADA. Αυτό περιλαμβάνει κινητές εφαρμογές SCADA που χρησιμοποιούνται για την παρακολούθηση και διαχείριση των συστημάτων.

- **Τρομοκράτες**: Όπου οι hackers συνήθως παρακινούνται από κέρδος, οι τρομοκράτες οδηγούνται από την επιθυμία να προκαλέσουν όσο το δυνατόν περισσότερη καταστροφή και ζημία.

- **Υπάλληλοι:** Οι εσωτερικές απειλές μπορεί να είναι εξίσου καταστροφικές με τις εξωτερικές απειλές.

Η διαχείριση των δικτύων SCADA μπορεί να είναι μία εξαιρετικά σύνθετη πρόκληση, δίχως τις κατάλληλες προφυλάξεις ασφαλείας. Πολλά δίκτυα εξακολουθούν να μην διαθέτουν τα απαραίτητα συστήματα ανίχνευσης και παρακολούθησης και αυτό τα αφήνει ευάλωτα είτε σε φυσικές είτε σε ψηφιακές επιθέσεις. Θα μπορούσαμε να ορίσουμε τα μέτρα ασφαλείας των συστημάτων SCADA σύμφωνα με τα όσα είδαμε στα προηγούμενα κεφαλαία σχετικά με την ασφάλεια των Κρίσιμων Υποδομών τηλεπικοινωνιών. Επειδή οι επιθέσεις στο δίκτυο SCADA εκμεταλλεύονται τόσο τις ευπάθειες στον κυβερνοχώρο όσο και τη φυσική ευπάθεια, είναι κρίσιμο να ευθυγραμμιστούν αυτοί οι δύο άξονες ασφάλειας. Αυτό θα μπορούσε να γίνει λαμβάνοντας υπόψη τόσο τα φυσικά μέτρα προστασίας των υποδομών (με την χρήση κατάλληλων προστατευτικών διατάξεων που θα δούμε στο επόμενο κεφάλαιο), όσο και τα ψηφιακά μέτρα προστασίας των δικτύων επικοινωνίας με την χρήση ισχυρού τείχους προστασίας το οποίο κρυπτογραφεί την κυκλοφορία, απορρίπτει την μη εξουσιοδοτημένη πρόσβαση και προστατεύει το απόρρητο [171].

6

Εφαρμογές Ασφαλείας με WSNs

Η προηγμένη τεχνολογία των ασύρματων δικτύων και των ενσωματωμένων συστημάτων (embedded systems) μας δίνει σήμερα τη δυνατότητα να εντοπίσουμε, όχι μόνο να μετρήσουμε αλλά και να ελέγξουμε αναλογικά μεγέθη του περιβάλλοντος τα οποία σχετίζονται είτε με τον χώρο είτε με τον χρόνο, σε βαθμό τέτοιο που παλιότερα θα χαρακτηρίζονταν ως «επιστημονική φαντασία». Η πολύ σημαντική δυνατότητα που μας παρέχουν οι νέες τεχνολογίες ασύρματων δικτύων προσεγγίζει υπάρχοντα προβλήματα τα οποία έμεναν άλυτα ή αντιμετωπίζονταν ανεπαρκώς για χρόνια (όπως για παράδειγμα το πρόβλημα της παρακολούθησης μεγάλων στρατιωτικών περιοχών). Η οργάνωση μίας στρατιωτικοποιημένης ζώνης (militarized zone) με κατανεμημένους αισθητήρες ήταν η αρχική ιδέα πίσω από το πρόγραμμα Igloo White[64] στο Βιετνάμ.

Σήμερα, ειδικοί επίγειοι ασύρματοι αισθητήρες (Unattended Ground Sensors - UGSs) μπορούν να ανιχνεύσουν και να εκτιμήσουν την κατεύθυνση κίνησης ενός οχήματος-εισβολέα σε μία περιοχή. Την ίδια στιγμή, άλλοι αισθητήρες μπορούν να βρίσκονται τοποθετημένοι κατά μήκος ενός κτηρίου ή μίας διαδρομής και να ανταποκρίνονται σε σεισμικές δονήσεις, σε διαρροές ή υπερχειλίσεις υγρών ή επικίνδυνων αερίων, σε ακουστικά κύματα, στην υπέρυθρη εκπεμπόμενη ενέργεια, στις αλλαγές του μαγνητικού πεδίου κλπ., προς τον εντοπισμό εχθρικών ή κακόβουλων δραστηριοτήτων, αποστέλλοντας δεδομένα προς επεξεργασία είτε τοπικά είτε απομακρυσμένα μέσω ραδιοφωνικών εκπομπών. Στο τέλος τα μηνύματα αυτά αποδιαμορφώνονται, αποκωδικοποιούνται,

[64] Η επιχείρηση Igloo White ήταν μία κρυφή κοινή στρατιωτική επιχείρηση ηλεκτρονικού πολέμου που διεξήχθη από τα τέλη Ιανουαρίου 1968 έως τον Φεβρουάριο του 1973, κατά τη διάρκεια του πολέμου του Βιετνάμ. Αυτές οι αποστολές πραγματοποιήθηκαν από την 553d Reconnaissance Wing, μονάδα Πολεμικής Αεροπορίας των ΗΠΑ και έφεραν το τροποποιημένο αεροσκάφος EC-121R Warning Star. Αυτή η υπερσύγχρονη, για την εποχή, τροποποίηση (θα μπορούσαμε να πούμε ότι προσέγγιζε την ιδέα του μη επανδρωμένου αεροσκάφους) χρησιμοποιούσε ηλεκτρονικούς αισθητήρες, υπολογιστές και ασύρματα ρελέ επικοινωνίας σε μια προσπάθεια αυτοματοποίησης της συλλογής πληροφοριών. Στη συνέχεια, οι πληροφορίες αυτές θα εξυπηρετούσαν προς την ανεύρεση των στόχων επιθέσεων από αέρος. Πηγή: Correll, John T. (November 2004). "Igloo White". Air Force Magazine. 87 (11): 56–61. Retrieved 30 October 2009.

υπόκεινται σε επεξεργασίας και αξιολογούνται κατάλληλα από ειδικά διαμορφωμένους αλγόριθμους (όπως είναι π.χ. οι αλγόριθμοι Video Analytics (VA) στα συστήματα παρακολούθησης εικόνας), ώστε να ενημερώσουν τον χρήστη σχετικά με τις σχετιζόμενες απειλές ή ακόμα και να ενεργοποιήσουν δευτερεύοντες μηχανισμούς προστασίας (όπως για παράδειγμα ακουστικά μέσα συναγερμού) ή για να ενημερώσουν απευθείας τον χρήστη ή για να ειδοποιήσουν κάποιον κεντρικό σταθμό λήψης σημάτων, ο οποίος παρακολουθεί απομακρυσμένα το σύστημα [172].

6.1 Ασύρματα Συστήματα Εντοπισμού σε Πραγματικό Χρόνο (RTLS)

Ένα σύστημα προσδιορισμού τοποθεσίας σε πραγματικό χρόνο (Real-Time Location System - RTLS) επιτρέπει στον χρήστη να παρακολουθεί, να διαχειρίζεται, να αναλύει και να χρησιμοποιεί τις πληροφορίες τοποθεσίας των υπό παρακολούθηση στοιχείων. Είναι σαφές το πόσο πολύτιμη θα ήταν μία ακριβής και αξιόπιστη τεχνολογία RTLS για μία μεγάλη ποικιλία εφαρμογών ασφαλείας (σε ένα εύρος δράσεων που αφορά στις τηλεπικοινωνιακές υποδομές, στην υγειονομική περίθαλψη, στις κατασκευές, στο λιανικό εμπόριο, στις επιχειρήσεις και στις κατασκευές κλπ.). Η παρακολούθηση και ο έγκαιρος εντοπισμός περιουσιακών στοιχείων (assets) σε επίπεδο υλισμικού είναι ο κύριος στόχος της τεχνολογίας αυτής, μετρώντας ως παράγοντα επιτυχίας την πρόληψη απώλειας ενός συστήματος υλισμικού/εξοπλισμού ή την αλλαγή της θέσης του. Ένα ιδανικό σύστημα RTLS θα μπορούσε να εντοπίσει και να αποδώσει με ακρίβεια εκατοστών τη θέση ενός ή περισσότερων αντικειμένων, βελτιστοποιώντας έτσι τη διαχείριση και την ασφάλεια των περιουσιακών στοιχείων ενός οργανισμού και διασφαλίζοντας ότι το στοιχείο αυτό θα είναι πάντα εκεί που απαιτείται. Η προειδοποίηση των αρμόδιων προσωπικού όταν ένα περιουσιακό στοιχείο μετακινείται σε μία μη εξουσιοδοτημένη τοποθεσία, θα μπορούσε να βελτιώσει δραματικά την πρόληψη της απώλειας και να μειώσει το άμεσο και έμμεσο κόστος [173].

Υπάρχουν διαφορετικά επίπεδα λειτουργικότητας ενός RTLS, τα οποία ποικίλλουν αναλόγως με την πολυπλοκότητα, τον όγκο της απαιτούμενης υποδομής και την ακρίβεια που μπορεί να παρέχεται. Τα επίπεδα αυτά συνοπτικά είναι τα εξής [173]:

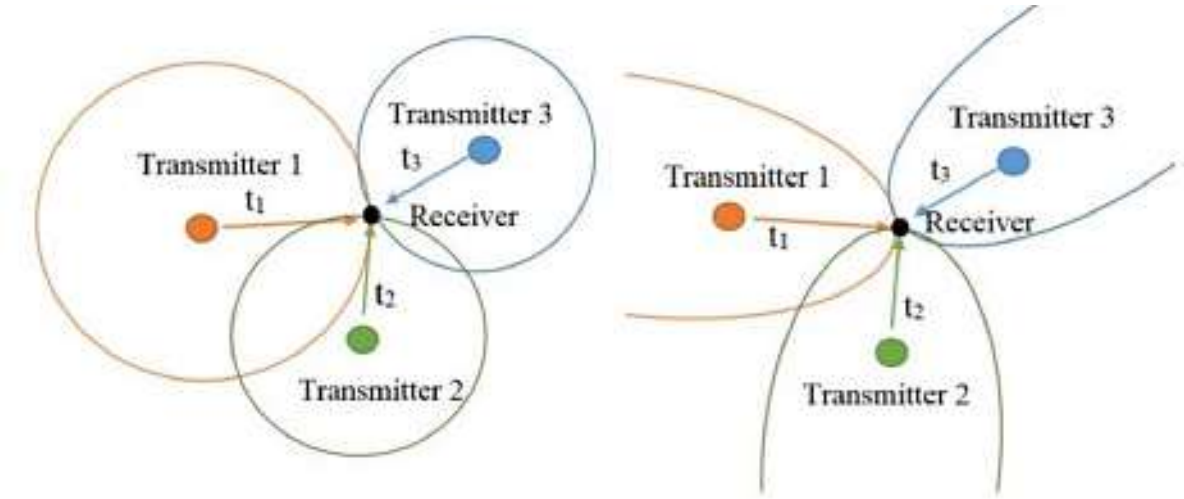
- **Εντοπισμός βάσει παρουσίας**: Το RTLS αντιλαμβάνεται εάν μια ετικέτα είναι ή δεν υπάρχει στην ορισμένη περιοχή παρακολούθησης (“you are here”).
- **Εντοπισμός σε επίπεδο δωματίου**: Το RTLS αντιλαμβάνεται σε ποιο δωμάτιο υπάρχει μία ετικέτα (“you are near here”).
- **Εντοπισμός σε σημεία ενεργοποίησης συναγερμού (choke points)**: Η θέση της ετικέτας καθορίζεται από την παρατήρηση ετικετών που κινούνται μέσω «σημείων πνιγμού» (choke points) (πόρτες, είσοδοι και εξόδους) υποθέτοντας ότι οι μόνες διαδρομές που μπορούν να ληφθούν περνούν από αυτά τα σημεία αυτά.
- **Εντοπισμός με συσχέτιση**: Η τοποθεσία της ετικέτας επιστρέφεται κοντά σε άλλη ετικέτα.
- **Εντοπισμός με ακρίβεια**: Το RTLS επιστρέφει τη μετρημένη θέση ετικέτας σε χώρο 2D/3D και επικαλύπτει έναν χάρτη της περιοχής παρακολούθησης.

Ο καθορισμός της καλύτερης ισορροπίας μεταξύ του επιπέδου λεπτομέρειας που επιστρέφεται από το σύστημα RTLS και της απαιτούμενης πολυπλοκότητας και υποδομής είναι πολύ σημαντικός. Ένα ακριβές σύστημα εντοπισμού μπορεί να παραμένει ανεκμετάλλευτο, εάν το μόνο που χρειάζεται είναι να γνωρίζουμε το εάν μία ετικέτα είναι ή δεν υπάρχει σε μία συγκεκριμένη τοποθεσία. Επίσης, *σε κάθε περίπτωση*, κάθε προσπάθεια απλοποίησης της αρχιτεκτονικής για ελαχιστοποίηση του κόστους και της κατανάλωσης ενέργειας για συμβατότητα συλλογής ενέργειας είναι θεμιτή [173].

Οι διαφορετικοί τύποι RTLS χρησιμοποιούν ασύρματα σήματα για τον προσδιορισμό της απόστασης μεταξύ 2 ή περισσότερων σημείων όπως υπέρυθρες ακτίνες, οπτικά σήματα, ήχο (υπέρηχους) ή ηλεκτρομαγνητικά κύματα (RFID, WLAN ή και διαφορετικές τεχνολογίες βασισμένες σε RF). Τα περισσότερα RTLS λειτουργούν με μία πολύ απλή αρχή, ήτοι: Τα αντικείμενα που παρακολουθούνται ονομάζονται «ετικέτες», οι οποίες είναι οι ίδιοι πομποδέκτες με μοναδικό αναγνωριστικό. Για την παρακολούθηση αυτών των ετικετών, πολλοί πομποδέκτες που ονομάζονται «άγκυρες» (anchors) έχουν ρυθμιστεί με σταθερές θέσεις στην περιοχή παρακολούθησης. Για συστήματα που απαιτούν μόνο εντοπισμό εγγύτητας (επίπεδο δωματίου, επιμέρους δωματίου) απαιτείται μόνο να πραγματοποιείται σύνδεση μεταξύ ετικέτας και σημείου αγκύρωσης (anchor point) ώστε να προσδιοριστεί ότι η ετικέτα βρίσκεται σε μικρή απόσταση από τη θέση αυτής της αγκύρωσης [173].

Για ακριβή παρακολούθηση θέσης σε εσωτερικούς χώρους πρέπει να χρησιμοποιούνται πιο σύνθετες μέθοδοι. Με βάση τις γεωμετρικές ιδιότητες των τριγώνων, ο τριγωνισμός είναι ο τυπικός αλγόριθμος εντοπισμού για τον προσδιορισμό της θέσης ενός αντικειμένου ή μίας ετικέτας σε σχέση με το σύνολο των αγκυρώσεων που υποθέτουμε ότι μπορούν να επικοινωνούν ασύρματα με τις ως άνω ετικέτες. Στην μέθοδο του τριγωνισμού ή τριμερισμού (Trilateration), χρησιμοποιώντας μία από τις τεχνολογίες RTLS που είδαμε προηγουμένως, θα πρέπει να είναι δυνατή η ακτινική απόσταση ενός αντικειμένου από κάποιο σταθερό σημείο αγκύρωσης. Εάν η απόσταση από τρία ή περισσότερα ξεχωριστά σημεία αγκύρωσης είναι γνωστή, τότε μπορεί να χρησιμοποιηθεί ένας απλός αλγόριθμος για την εύρεση της κατά προσέγγιση θέσης ενός αντικειμένου [173].

Μία άλλη μέθοδος που βασίζεται σε τριγωνισμό είναι η «γωνίωση» (angulation) όπου οι λαμβανόμενες εκπομπές σήματος μπορούν να χρησιμοποιηθούν για τον προσδιορισμό της γωνίας προσβολής του ίδιου του σήματος. Αυτό μπορεί να γίνει μέσω της μεθόδου Angle of Arrival (AOA) όπου μία σειρά κεραιών στην άγκυρα μετράει την ώρα άφιξης ή τη φάση του σήματος που φθάνει στην πρώτη κεραία, την συγκρίνει με την ώρα άφιξης στη δεύτερη κεραία και ούτω καθεξής. Εάν αυτή η διαφορά μπορεί να μετρηθεί με ακρίβεια, τότε μπορεί να προσδιοριστεί και η γωνία άφιξης του εκπεμπόμενου σήματος. Εάν τα σήματα είναι ακριβώς τα ίδια, τότε η κατεύθυνση διάδοσης πρέπει να είναι κάθετη προς την κατεύθυνση της διάταξης κεραίας. Όσο μεγαλύτερη είναι η καθυστέρηση χρόνου ή η καθυστέρηση φάσης μεταξύ των λαμβανόμενων σημάτων στις κεραίες τόσο μεγαλύτερη είναι η γωνία πρόσπτωσης [173].



Εικόνα 6-1: Ανίχνευση θέσης με βάση τον τριμερισμό,
TOA (αρ.) και TDOA (δεξ.) μέθοδος[65]

Υπάρχουν διάφορες προσεγγίσεις σύνδεσης των επί μέρους αγκυρών στο δίκτυο, προκειμένου να επεξεργαστούμε τα δεδομένα που λαμβάνονται από αυτές. Ένας κοινός τρόπος είναι το να επικοινωνούν οι άγκυρες με έναν σταθμό βάσης για την εκτέλεση των αλγορίθμων, για τον προσδιορισμό της θέσης κάθε ετικέτας εντός της περιοχής παρακολούθησης. Η βάση μπορεί να έχει την μορφή ενός λογισμικού που εκτελείται σε έναν υπολογιστή και το ίδιο διασυνδέεται με ένα σύνολο δεδομένων όπου αναγράφονται όλες οι τρέχουσες ετικέτες και η τοποθεσία τους, ενημερώνοντας κάθε φορά που λαμβάνεται μία νέα ενημέρωση θέσης από μία ετικέτα. Μία άλλη προσέγγιση σε αυτό μπορεί να είναι η εκτέλεση των αλγορίθμων στην ετικέτα που συνήθως γίνεται όταν το αντικείμενο που παρακολουθείται είναι μία έξυπνη συσκευή (όπως π.χ. ένα κινητό τηλέφωνο) όπου η υπολογιστική ισχύς δεν προκαλεί προβληματισμό. Αντί λοιπόν να στέλνει σήμα στις άγκυρες, η ετικέτα - τηλέφωνο περιμένει σήματα από τις άγκυρες και χρησιμοποιεί οποιαδήποτε από τις μεθόδους που αναφέρονται παραπάνω για να υπολογίσει τη θέση της στον εσωτερικό χώρο [173].

[65] Υπάρχουν διαφορετικές υπο-μέθοδοι που χρησιμοποιούνται στη διαμόρφωση τριμερισμού για να λάβουμε την απόσταση από κάθε σημείο αγκύρωσης. Το πιο συνηθισμένο από αυτά είναι η χρήση της ισχύος λήψης σήματος (Radio Signal Strength - RSS). Βασικά δεδομένα σχετικά με το πώς αλλάζει η ισχύς σήματος μίας ετικέτας σχετικά με την απόσταση από την άγκυρα, μπορεί να χρησιμοποιηθούν για να εξαχθεί μία εκτίμηση της απόστασής της από την εν λόγω άγκυρα. Μία άλλη κοινή μέθοδος είναι να το να χρησιμοποιηθεί ο χρόνος άφιξης (Time of Arrival - TOA) του σήματος, γνωρίζοντας ότι η ταχύτητα διάδοσης των ηλεκτρομαγνητικών σημάτων είναι η ταχύτητα του φωτός και ότι τα ακουστικά σήματα είναι η ταχύτητα του ήχου στον αέρα, οπότε μπορεί κανείς να επιστρέψει για να βρει την απόσταση. Παρόμοια με αυτή την μέθοδο είναι η χρήση της διαφοράς του χρόνου άφιξης (Time Difference of Arrival - TDOA) που χρησιμοποιεί τη διαφορά στην ώρα άφιξης μεταξύ αρκετών φάρων οι οποίοι μπορούν να προσφέρουν ακριβέστερα και περισσότερο αξιόπιστα αποτελέσματα από την τεχνική RSS, σε πραγματικές εφαρμογές. Πηγή: Segers, L., Van Bavegem, D., et al. (2015): An ultrasonic multiple-access ranging core based on frequency shift keying towards indoor localization. Sensors 15.8, pp.18641-18665.

6.1.1 Χαρακτηριστικά RTLS

Τα κύρια χαρακτηριστικά που λαμβάνονται υπόψη κατά τη σύγκριση της σχετικής απόδοσης των συστημάτων RTLS περιγράφονται συνοπτικά παρακάτω [174]:

- **Ακρίβεια (accuracy):** Η ακρίβεια είναι το πιο σημαντικό χαρακτηριστικό με την μέτρηση του οποίου κρίνουμε εκ πρώτης όψεως τα συστήματα εντοπισμού θέσης. Ο τρόπος με τον οποίο προσδιορίζεται το σφάλμα ακρίβειας στα RTLS, βασίζεται στον υπολογισμό της μέσης απόστασης μεταξύ της εκτιμώμενης θέσης και της πραγματικής θέσης ενός αντικειμένου. Ενώ γενικά όσο πιο ακριβές είναι το σύστημα τόσο το καλύτερο, συχνά μπορεί να υπάρχουν «αντισταθμίσεις» μεταξύ της ακρίβειας και άλλων χαρακτηριστικών (όπως πολυπλοκότητα, κόστος, κατανάλωση ενέργειας, επεκτασιμότητα, απαιτούμενη υποδομή κλπ.). Εξαιτίας αυτού, υπάρχει κάποιο είδος συμβιβασμού μεταξύ της ακρίβειας και των άλλων παραγόντων. Η ακρίβεια εξετάζει το πόσο σταθερά λειτουργεί το σύστημα και έτσι είναι μία πολύ καλή ένδειξη για το πόσο στιβαρό είναι ένα σύστημα RTLS.

- **Πολυπλοκότητα (complexity):** Το χαρακτηριστικό της πολυπλοκότητας ενός συστήματος RTLS μπορεί να αναφέρεται στο υλισμικό, στο λογισμικό ή στη λειτουργία του συστήματος. Ωστόσο, η υπολογιστική πολυπλοκότητα του αλγορίθμου θέσης μπορεί να προσδώσει την έννοια της πολυπλοκότητας σε ένα RTLS. Κάθε διαφορετική μέθοδος, όπως RSS, TOA, TDOA, κλπ. χρησιμοποιεί διαφορετικούς αλγορίθμους για να μετατρέψει τα ανεπεξέργαστα δεδομένα (ένταση σήματος, ώρα άφιξης κλπ.) σε θέση, σε 2D ή 3D χώρο. Εάν ο αλγόριθμος θέσης για κάθε ετικέτα εκτελείται από την πλευρά του διακομιστή, τότε η πολυπλοκότητα συνήθως δεν αποτελεί πρόβλημα. Σε περιπτώσεις όμως που η ετικέτα επεξεργάζεται τα ίδια τα δεδομένα αυτό μπορεί να είναι ενδεχόμενο πρόβλημα, και για το λόγο αυτό συνήθως οι ετικέτες είναι εφοδιασμένες με μικροεπεξεργαστές χαμηλής ισχύος, οι οποίοι χειρίζονται γρήγορα αρκετά πολύπλοκους αλγορίθμους. Αυτό θα δώσει χαμηλό μέγιστο ποσοστό εντοπισμού θέσης εάν η πολυπλοκότητα είναι πολύ υψηλή. Εάν είναι επιθυμητός ένας ρυθμός εντοπισμού θέσης υψηλής συχνότητας, για αυτή τη ρύθμιση απαιτείται αλγόριθμος χαμηλής πολυπλοκότητας για την ελαχιστοποίηση της μέσης ισχύος επεξεργασίας.

- **Ευρωστία (robustness):** Ένα ισχυρό σύστημα εντοπισμού είναι ένα σύστημα το οποίο δεν επηρεάζεται από τη μη διαθεσιμότητα ορισμένων σημάτων ή ορισμένων ληφθέντων σημάτων. Ορισμένες φορές ένας πομπός μπορεί να αποτυγχάνει να αποστείλει προσωρινά ή κατά διαστήματα τα σήματα από μία ετικέτα (π.χ. άτομα, περιουσιακά στοιχεία, μηχανήματα κλπ.) που κινείται. Είναι επιθυμητό ώστε κάτι τέτοιο να μην διαταράσσει το σύστημα, το οποίο θα πρέπει να μπορεί να λειτουργήσει με ελλιπείς εισερχόμενες πληροφορίες ή υπό άλλου είδους λειτουργικές διαταραχές όπως είναι οι EM (Electro-Magnetic) παρεμβολές στο περιβάλλον από μία μεγάλη ποικιλία πηγών (κινητά τηλέφωνα, καταιγίδες, ο ήλιος κλπ.).

- **Κλιμακοθετησιμότητα (scalability):** Έχοντας ένα σύστημα εντοπισμού θέσης που είναι κλιμακοθετήσιμο σημαίνει ότι η λειτουργία παραμένει η ίδια από ένα μικρότερο επίπεδο προς ένα μεγαλύτερο, δηλαδή η παρακολούθηση μίας μόνο ετικέτας σε ένα μικρό δωμάτιο έχει την ίδια λειτουργία με την παρακολούθηση χιλιάδων γύρω από ένα μεγάλο εργοστάσιο. Η κλιμακοθετησιμότητα καλύπτει δύο ξεχωριστές ιδιότητες, ήτοι: γεωγραφική κλίμακα και κλίμακα πυκνότητας. Η γεωγραφική κλιμάκωση ασχολείται με την περιοχή ή τον όγκο στον οποίο μπορεί να υπόκεινται σε παρακολούθηση οι ετικέτες, ενώ η κλιμάκωση πυκνότητας αφορά στο πόσες ετικέτες μπορούν να «χωρέσουν» στην περιοχή παρακολούθησης. Η αύξηση της πυκνότητας μπορεί να προκαλέσει την κυκλοφοριακή συμφόρηση των καναλιών ασύρματου σήματος, επομένως απαιτείται μεγαλύτερη υποδομή και χρειάζονται περισσότεροι υπολογισμοί ανά δευτερόλεπτο για την παρακολούθηση της κάθε επιμέρους ετικέτας.

- **Κόστος (cost):** Το κόστος ενός RTLS συστήματος τοποθέτησης θα πρέπει να περιλαμβάνει όχι μόνο το ίδιο το σύστημα αλλά και το κόστος που σχετίζεται με τον χρόνο που απαιτείται για την εγκατάσταση και τη συντήρηση του. Με ορισμένες τεχνολογίες υπάρχει αντιστάθμιση μεταξύ της εφικτής ακρίβειας και του απαραίτητου ποσού υποδομής. Ορισμένες μέθοδοι μπορεί να απαιτούν μεγάλο αριθμό υποδομών για την καλύτερη δυνατή ακρίβεια, ενώ άλλες μπορεί να απαιτούν λιγότερες και να αποδίδουν εξίσου καλά. Η προσπάθεια που απαιτείται για τη συντήρηση του συστήματος είναι ένας άλλος παράγοντας κόστους, καθώς η τακτική συντήρηση πολλών ετικετών θα μπορούσε να είναι μια χρονοβόρα και κοστοβόρα διαδικασία.

- **Κατανάλωση ενέργειας (energy consumption):** Δεδομένου ότι πρόκειται για ασύρματο σύστημα, οποιαδήποτε ενεργή ετικέτα χρειάζεται πηγή τροφοδοσίας, συνήθως με τη μορφή μπαταρίας. Στην ιδανική περίπτωση, η μπαταρία σε μία ετικέτα θα είναι πολύ μικρή (μέγεθος νομισμάτων) και θα διαρκέσει για αρκετά χρόνια. Εάν η ενεργή ετικέτα καταναλώνει πολλή ενέργεια, τότε η μπαταρία της ετικέτας θα πρέπει να αλλάζει συχνά, κάτι που δεν θα ήταν διαχειρίσιμο για ένα σύστημα με χιλιάδες ετικέτες. Ή εναλλακτικά το μέγεθος της μπαταρίας θα έπρεπε να αυξηθεί, καθιστώντας τον παράγοντα μορφής της ετικέτας μεγαλύτερο που είναι επίσης ανεπιθύμητο στις περισσότερες περιπτώσεις.

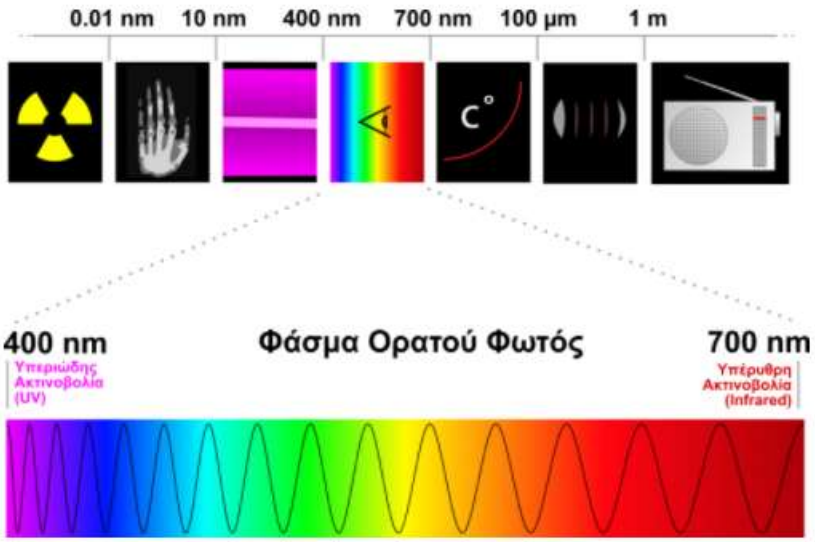
6.2 Προστασία από Φυσική Εισβολή με Ανίχνευση Κίνησης

Η παρακολούθηση στόχου ο οποίος κινείται μέσα σε ένα ασύρματο δίκτυο αισθητήρων είναι μία πολύ σημαντική και ταυτόχρονα δύσκολη εφαρμογή, καθώς εμφανίζονται προκλήσεις όπως είναι ο εντοπισμός των κινούμενων αντικειμένων, η εύρεση της μέσης ταχύτητάς τους ή ακόμα και η αλλαγή κατεύθυνσής τους. Η τεχνική που χρησιμοποιείται για την ανίχνευση των αντικειμένων αυτών βασίζεται στη λήψη και στην ψηφιοποίηση αναλογικών μεγεθών, με την χρήση μετατροπέων αναλογικού σε ψηφιακού (Analog to Digital Converter - ADC) [175].

Η τεχνολογία που μας επιτρέπει την ανίχνευση της κίνησης σε έναν χώρο, βασίζεται στην λειτουργία παθητικών αισθητήρων υπέρυθρου φωτός (Passive InfraRed sensors – PIR). Το αντικείμενο παρακολουθείται από αισθητήρες PIR. Στη καρδιά μίας τέτοιας μονάδας βρίσκεται ένα ζεύγος αισθητήρων, οι οποίοι είναι φτιαγμένοι από υλικά τα οποία είναι ευαίσθητα στην υπέρυθρη ακτινοβολία, όπως κοβάλτιο, φθαλοκυανίνη, νιτρίδιο γαλλίου κ.α. Οι δύο αυτοί αισθητήρες βρίσκονται κλεισμένοι ερμητικά μέσα σε ένα μεταλλικό κυτίο, το οποίο έχει ένα παράθυρο από σιλικόνη και από το οποίο μπορεί να περάσει η υπέρυθρη ακτινοβολία. Το μεταλλικό κουτί είναι τοποθετημένο στην πλακέτα της μονάδας και καλύπτεται από ένα πλαστικό περίβλημα που αποτελείται από φακούς Φρενέλ (Fresnel)[66].
Οι αισθητήρες PIR χαρακτηρίζονται ως «παθητικοί» γιατί δεν εκπέμπουν κάποιο σήμα για να προχωρήσουν στην ανίχνευση της επιστροφής του, όπως συμβαίνει για παράδειγμα με τους αισθητήρες υπερήχων (στέλνουν υπερήχους και περιμένουν να τους λάβουν πίσω) ή τους αισθητήρες αποφυγής εμποδίων (στέλνουν υπέρυθρες ακτίνες και περιμένουν να τις λάβουν πίσω). Η φύση των υλικών από τα οποία αποτελούνται δημιουργεί μικρά ηλεκτρικά φορτία, όταν αυτά εκτίθενται σε υπέρυθρες ακτίνες. Οι δυο αισθητήρες είναι συνδεδεμένοι μεταξύ τους με τέτοιον τρόπο ώστε όταν ο ένας λαμβάνει διαφορετική ποσότητα υπέρυθρης ακτινοβολίας από τον άλλο, παράγεται ένα ηλεκτρικό σήμα το οποίο αποστέλλεται από την έξοδο της μονάδας προς το ADC. Όταν ο χώρος που εποπτεύει ο αισθητήρας παραμένει σταθερός και δεν υπάρχει κίνηση αντικειμένων που μεταδίδουν θερμότητα, δεν ανιχνεύονται διαφορές στην υπέρυθρη ακτινοβολία ανάμεσα στα δυο στοιχεία. Όταν όμως κάποιο θερμό σώμα (π.χ. άνθρωπος ή ζώο) περάσει μπροστά από τον αισθητήρα, τότε θα δημιουργηθεί κάποια στιγμή μία διαφορά στην ποσότητα της υπέρυθρης ακτινοβολίας που ανιχνεύει το κάθε στοιχείο και ο αισθητήρας θα παράγει ηλεκτρικό σήμα στην έξοδο του. Ο αισθητήρας PIR με την χρήση των φακών Φρενέλ έχει ωφέλιμη γωνία ανίχνευσης περίπου 120 μοίρες και μπορεί να ανιχνεύσει κινήσεις σε απόσταση 7 έως 10 μέτρων [176].

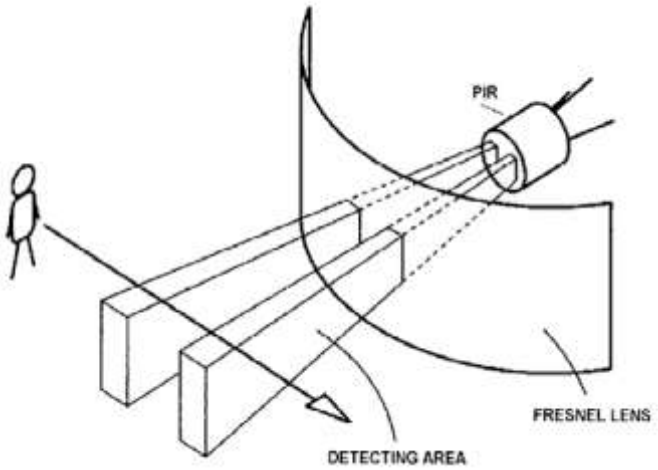
Σε ένα σύστημα πρόληψης και ελέγχου φυσικής εισβολής, οι αισθητήρες τοποθετούνται σε στατικές θέσεις εντός του χώρου. Η χρήση των πληροφοριών που συλλέγονται από τους αισθητήρες κίνησης μπορεί να μας δώσει προβλέψεις για την διαδρομή της κίνησης, την μέση ταχύτητα και τη διεύθυνση του αντικειμένου που παρακολουθούμε. Ωστόσο ο παθητικός αισθητήρας υπέρυθρων χρησιμοποιείται για να προσδιορίσει εάν ο εισβολέας είναι άνθρωπος ή όχι.

[66] Ο Ογκιστέν-Ζαν Φρενέλ (Augustin-Jean Fresnel, 10 Μαΐου 1788 - 14 Ιουλίου 1827) ήταν Γάλλος φυσικός και εφευρέτης. Ασχολήθηκε κυρίως με την πόλωση, την διάθλαση, την διπλή ανάκλαση του φωτός καθώς και με την κυματοειδή του διάδοση. Έγινε μέλος της Γαλλικής Ακαδημίας των Επιστημών (1823) και της Αγγλικής Βασιλικής Εταιρίας των Επιστημών. Ο Φρενέλ αντιλήφθηκε την ανάγκη της χρησιμοποίησης των επιπεδόκυρτων φακών στις μηχανές των φάρων. Ασχολούμενος με την έρευνα αυτή εφηύρε τη μέθοδο κατασκευής αυτών με τη χρήση αντί ολόσωμων φακών δακτυλιοειδών επάλληλων διοπτρικών στοιχείων, επιτρέποντας έτσι την δημιουργία μεγάλων διαμέτρων και μικρής διαμέτρου και μάλιστα με πολύ μικρή δαπάνη. Η δημιουργία του πρώτου τέτοιου «φαρικού οπτικού» που τοποθετήθηκε προς δοκιμή στα πρόσγεια του Μπορντώ, στον Φάρο του Κορντουάν, γενίκευσε την χρήση της επινόησης του Φρενέλ. Η μέθοδός του χρησιμοποιείται ακόμα και σήμερα αποκλειστικά σε όλους τους φάρους του κόσμου, που για αυτό το λόγο ονομάζονται «καταδιοπτρικοί».



Εικόνα 6-2: Το φάσμα του ορατού φωτός είναι ένα μικρό μέρος του φάσματος της ηλεκτρομαγνητικής ακτινοβολίας (*από την Βικιπαίδεια*)

Ο αισθητήρας παθητικών υπέρυθρων (Passive Infrared - PIR) είναι ένας χαμηλού κόστους και ισχύος αξιόπιστος αισθητήρας. Ως εκ τούτου, θεωρήθηκε ότι ένα σύστημα ασφαλείας βασισμένο σε αισθητήρα PIR που αποτελείται από τον αισθητήρα, ένα σύστημα φωτισμού και ένα σύστημα εγγραφής (κάμερα Web και το λογισμικό για την αποθήκευση του βίντεο) θα μπορούσε να ικανοποιήσει ή και να ξεπεράσει ορισμένα ή όλα από τα προβλήματα φυσικής ασφάλειας υποδομών, όπως αναφέρθηκαν σε προηγούμενα κεφάλαια. Ο αισθητήρας χρησιμοποιώντας την αρχιτεκτονική που περιεγράφηκε παραπάνω, μπορεί να ανιχνεύσει την παρουσία εισβολέων ενώ κατά την ανίχνευση υπέρυθρης ακτινοβολίας στον χώρο εποπτείας του, ο αισθητήρας PIR παράγει έξοδο με τη μορφή ηλεκτρικού σήματος [175].



Εικόνα 6-3: Λειτουργία ανιχνευτή κίνησης PIR [175]

6.2.1 Ασύρματοι Ανιχνευτές Κίνησης PIR

Όπως είδαμε στο προηγούμενο κεφάλαιο, η επεξεργασία και ανάλυση δεδομένων διαδραματίζουν σημαντικό ρόλο στην εφαρμογή ανίχνευσης κίνησης, ενώ το σύστημα επιλογής είναι η μία κεντρική εφαρμογή υπολογιστή που αναγνωρίζει την κίνηση ανθρώπων σε μία συγκεκριμένη περιοχή, χρησιμοποιώντας αισθητήρες PIR. Προκειμένου όμως να εντάξουμε το σύστημα σε ένα ευρύτερο δίκτυο επικοινωνίας, στοχεύουμε στον σχεδιασμό του χρησιμοποιώντας ένα ασύρματο δίκτυο αισθητήρων. Αυτή η εφαρμογή πρέπει να είναι σε θέση να εντοπίσει καθώς και να παρακολουθήσει ανθρώπους, συμπεριλαμβανομένης της κατεύθυνσης και της ταχύτητάς τους, μεταφέροντας τα δεδομένα αυτά σε έναν κεντρικό σταθμό βάσης. Έτσι, ο ανθρώπινος εισβολέας ανιχνεύεται από έναν ή περισσότερους παθητικούς αισθητήρες υπέρυθρων, ενώ αυτοί συνδέονται ταυτόχρονα σε κόμβους αισθητήρων MICAz[67] προκειμένου να αναμεταδώσουν τα δεδομένα τους.

Εικόνα 6-4: Ασύρματος στεγανός ανιχνευτής κίνησης της εταιρείας Paradox με διπλό PIR και ενσωματωμένο MICAz

Ο αισθητήρας που χρησιμοποιείται για αυτήν την εφαρμογή είναι ένα “all-in-one” πακέτο, το οποίο αποτελείται από έναν αισθητήρα PIR, ορισμένα κυκλώματα (συμπεριλαμβανομένου ενισχυτή τάση εξόδου) και φακό Φρενέλ. Ο αισθητήρας PIR χρησιμοποιείται για τη λήψη σημάτων υπέρυθρου φάσματος ενώ συνδέεται με τον κόμβο

[67] Το MICAz είναι μία μονάδα Mote 2,4 GHz η οποία χρησιμοποιείται για ενεργοποίηση ασύρματης σύνδεσης χαμηλής ισχύος σε ένα WSN. Ένας σταθμός βάσης επιτρέπει τη συγκέντρωση δεδομένων δικτύου αισθητήρων σε υπολογιστή ή άλλη πλατφόρμα υπολογιστή. Κάθε MICAz Mote μπορεί να λειτουργεί ως σταθμός βάσης όταν είναι συνδεδεμένος σε μία τυπική διεπαφή υπολογιστή.

MICAz χρησιμοποιώντας μία σύνδεση 51 ακίδων (pin). Ο αισθητήρας PIR που χρησιμοποιείται στην εφαρμογή χρειάζεται 3 έως 12V τάση λειτουργίας με 1,5 mA κατανάλωσης, η οποία μπορεί να αντληθεί από ένα ζεύγος μπαταριών AA στον κόμβο του αισθητήρα. Ο αισθητήρας έχει έξοδο που χρησιμοποιείται για να δείξει το ότι είτε συμβαίνει μία κίνηση είτε όχι, ρυθμίζοντας ανάλογα μία τάση αναφοράς. Για την ανίχνευση κίνησης, η τοποθέτηση του αισθητήρα παίζει σημαντικό ρόλο. Ο αισθητήρας PIR έχει άμεση οπτική επαφή για ανίχνευση και δεν είναι παντοκατευθυντικός. Η τοποθέτηση του αισθητήρα εξαρτάται κυρίως από την τοπολογία του δικτύου. Για τη συγκεκριμένη εφαρμογή, οι αισθητήρες πρέπει να μπορούν να ακολουθούν τοπολογία γραμμής, δηλαδή να συνδέονται σειριακά, ενώ τα συγκεντρωτικά δεδομένα αποστέλλονται στον σταθμό βάσης με τη βοήθεια των ενδιάμεσων κόμβων MICAz [175].

Οι ασύρματες εκδόσεις των ανιχνευτών PIR μπορούν εύκολα να μεταδώσουν πληροφορίες έως και 30 μέτρα (πολύ περισσότερο σε ανοιχτό πεδίο). Η χρήση ανιχνευτών διπλής τεχνολογίας (PIR και μικροκυμάτων) θα αυξήσει την απόδοση την αξιοπιστία ώστε να αποφευχθούν οι ψευδείς συναγερμοί (false alarms). Σε αυτή την τεχνολογία, η λειτουργία AND[68] μεγιστοποιεί την αποφυγή σφάλματος λόγω ψευδών σημάτων του αισθητήρα PIR. Στον ανιχνευτή διπλής τεχνολογίας μπορεί να ρυθμιστεί ανεξάρτητα η ευαισθησία των αισθητήρων PIR και μικροκυμάτων. Το κόστος του θα είναι φυσικά υψηλότερο, είναι όμως μια τιμή η οποία μεταφράζεται σε μεγαλύτερη ακρίβεια.

6.2.2 Ασύρματο Σύστημα Συναγερμού Εισβολής

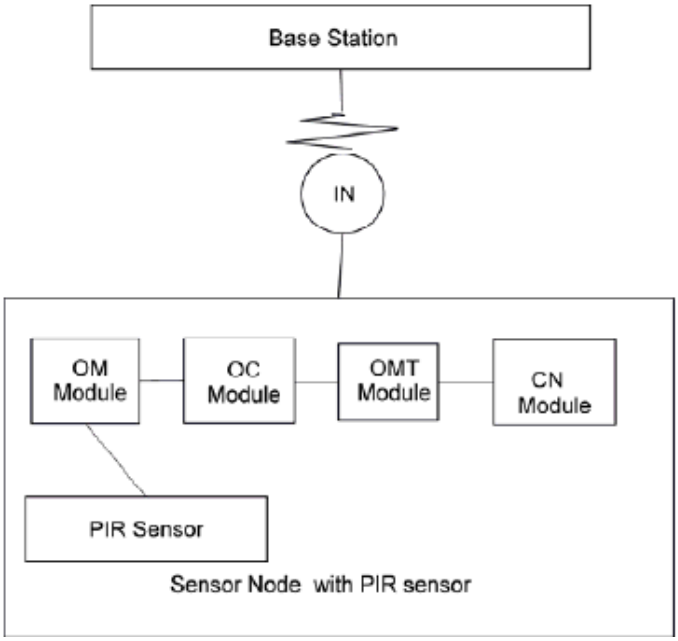
Ένα σύστημα συναγερμού και προστασίας από εισβολή μπορεί πρώτα να ταξινομηθεί στις εξής λειτουργικές κατηγορίες:

- Ενσύρματο σύστημα.
- Ασύρματο σύστημα
- Υβριδικό σύστημα.

Τα περισσότερα συστήματα συναγερμού εισβολέων (intruder alarm systems) είναι ενσύρματα συστήματα, επειδή τα ασύρματα συστήματα χρειάζονται εφεδρική πηγή ενέργειας (μπαταρία) και, ακόμη και με προστασία κατά της εμπλοκής (RF Jamming supervision), εξακολουθούν να μπορούν να επηρεαστούν από ηλεκτρομαγνητικές παρεμβολές. Τα ασύρματα συστήματα χρησιμοποιούνται κυρίως όταν δεν υπάρχει καλωδίωση και λειτουργούν στα 433MHz ή 868MHz. Τα υβριδικά συστήματα συναγερμού επιτρέπουν ταυτόχρονα την εγκατάσταση ενσύρματων και ασύρματων ανιχνευτών και είναι τα περισσότερο ευέλικτα [177].

[68] Η λειτουργία AND είναι μια ψηφιακή λογική λειτουργία βασισμένη σε πύλη AND, η οποία εφαρμόζει τη λογική σύνδεση δύο στοιχείων (Λ) από τη μαθηματική λογική. Μια τάση εξόδου η οποία αντιστοιχεί σε ψηφιακό σήμα HIGH (1), προκύπτει μόνο εάν όλες οι είσοδοι σε μια πύλη AND είναι ενεργοποιημένες (HIGH (1)). Στην περίπτωση ενός ανιχνευτή κίνησης διπλής τεχνολογίας, αυτό σημαίνει ότι τόσο το αισθητήριο παθητικού υπέρυθρου (PIR) όσο και το αισθητήριο μικροκυμάτων (MW) πρέπει να παράγουν ένα ηλεκτρικό σήμα, ώστε η τάση εξόδου του ανιχνευτή να λάβει θετικό πρόσημο. Πηγή: Wikipedia AND gate: https://en.wikipedia.org/wiki/AND_gate

Ωστόσο, ένα τυπικό ασύρματο σύστημα συναγερμού, ακόμη και εάν εντάσσεται σε ευρωπαϊκές πιστοποιήσεις συστημάτων ασφαλείας, δεν μπορεί να μας παρέχει πληροφορίες σχετικά με την κατεύθυνση ή την ταχύτητα κίνησης ενός εισβολέα.
Σε αυτή την περίπτωση, ένα ασύρματο δίκτυο ανιχνευτών βασισμένο σε MICAz, μπορεί να παρέχει τις ζητούμενες πληροφορίες σε έναν σταθμό βάσης, ακολουθώντας την αρχιτεκτονική της παρακάτω εικόνας (6-5) [175].



Εικόνα 6-5: Υλοποίηση συστήματος συναγερμού εισβολής με χρήση WSN

Αυτή η προσέγγιση βασίζεται στην επικοινωνία των αισθητήρων PIR έχοντας ως τελικό στόχο την παρακολούθηση της κίνησης ανθρωπίνων σωμάτων μεταξύ των κόμβων του δικτύου. Οι λειτουργίες του συστήματος που απεικονίζεται στην Εικόνα 6-5, περιγράφονται συνοπτικά παρακάτω [176]:

- **Παρακολούθηση αντικειμένου (δομοστοιχείο OM - Object Monitoring**): Το δομοστοιχείο (module) αυτό «διαβάζει» τα δεδομένα τα οποία εξάγει ο ανιχνευτής PIR και τα μετατρέπει σε ψηφιακά μέσω του ενσωματωμένου μετατροπέα ADC. Όταν ένας εισβολέας ανιχνευτεί εντός της περιοχής ανίχνευσής του αισθητήρα PIR, τότε η στάθμη σήματος στην έξοδο του μεταβάλλεται, το νέο σήμα ψηφιοποιείται ξανά από το δομοστοιχείο OM προκειμένου να περάσει στο επόμενο στάδιο.

- **Σύλληψη αντικειμένου (δομοστοιχείο OC - Object Catching)**: Μόλις ληφθούν τα δεδομένα από το δομοστοιχείο παρακολούθησης, το δομοστοιχείο σύλληψης (catching) θα αποφασίσει για την έναρξη και τη διακοπή της διαδικασίας σύλληψης συμβάντων, με βάση το εσωτερικό προγραμματισμένο χρονόμετρο (Internal clock) και τον αριθμό των δειγμάτων. Μετά από το χρονικό διάστημα που ορίζεται από το δομοστοιχείο () OC (ουσιαστικά είναι αυτό που μεσολαβεί μεταξύ της αποστολής

δύο σημάτων από το OM στο OC), ο εισβολέας ο οποίος κινείται εντός του πεδίου ανίχνευσης θα «συλληφθεί» από διαφορετικό κόμβο PIR και η διαδικασία θα ξεκινήσει από την αρχή. Με αυτόν τον τρόπο, το σύστημα αντιλαμβάνεται την κατεύθυνση και την ταχύτητα κίνησης. Φυσικά, για να πετύχουμε την αποτελεσματική λειτουργία του συστήματος, όλοι οι κόμβοι πρέπει να γνωρίζουν τους γείτονές τους. Έτσι, στην δομή του μηνύματος που μεταφέρεται στον σταθμό βάσης, περιέχονται οι λεπτομέρειες θέσης κόμβου (x, y συντεταγμένες), κατεύθυνση (αριστερά, δεξιά), κόμβος, ταχύτητα (αριθμός κόμβων> 1).

- **Ανίχνευση κίνησης αντικειμένων (δομοστοιχείο OMT - Object Movement Tracing):** Αυτό το δομοστοιχείο θα λειτουργήσει ως συντονιστική ενότητα, η οποία θα φροντίσει την επικοινωνία μεταξύ διαφορετικών κόμβων και την αναφορά προς τον σταθμό βάσης. Βασικά, οι δύο λειτουργίες που εκτελεί αυτή το δομοστοιχείο αφορούν στον συντονισμό επικοινωνίας μεταξύ των κόμβων και μεταξύ των κόμβων με τον σταθμό βάσης.

- **Δομοστοιχείο επικοινωνίας (CN Module – Communication Module):** Αυτό το δομοστοιχείο χρησιμοποιείται για την αποστολή μηνύματος σε μία ομάδα κόμβων. Χρησιμοποιείται για την αποστολή του ίδιου μηνύματος σε πολλαπλούς κόμβους ταυτόχρονα και για τον συντονισμό της επικοινωνίας με αυτήν την ομάδα. Η αποστολή του ίδιου του μηνύματος πολλές φορές και η υπερχείλιση των μηνυμάτων μπορεί να αποφευχθούν με τη χρήση αυτού του δομοστοιχείου.

Ο σταθμός βάσης (Base Station - BS) αναφέρει τα συμβάντα έναν υπολογιστή, χρησιμοποιώντας το εργαλείο XSniffer[69] ώστε το ληφθέν μήνυμα να είναι σε αναγνώσιμη μορφή και να αποθηκεύεται ένα αρχείο Excel. Τα δεδομένα αυτά μπορούν να χρησιμοποιηθούν για τη δημιουργία σημάτων συναγερμού ή ειδοποίησης μηνυμάτων που αποστέλλονται σε κινητά τηλέφωνα μέσω διαποδιαμορφωτών GSM ή email κλπ.

6.3 Έλεγχος Πρόσβασης με RFID Ταυτότητες ή Βιομετρικά Στοιχεία

Τα συστήματα Ελέγχου Πρόσβασης (Access Control) μπορούν να προσδιοριστούν ως η διαδικασία με την οποία το προσωπικό ασφαλείας ελέγχει πότε και ποιος εισέρχεται ή εξέρχεται σε μία περιοχή ελέγχου, σε ένα κτίριο ή σε κάποιο χώρο. Η παγκόσμια αγορά ελέγχου πρόσβασης είχε προβλεφθεί να φθάσει σε τζίρο τα 10,4 δισεκατομμύρια δολάρια το 2020, καθώς αυξάνεται με μέσο ετήσιο ρυθμό 10,6%, σύμφωνα με έρευνα της Markets and Markets[70].

[69] https://el.wikipedia.org/wiki/Packet_sniffer

[70] Η εταιρεία MarketsandMarkets™ παρέχει ποσοτικοποιημένη έρευνα B2B σχετικά με 30.000 αναπτυσσόμενες ευκαιρίες / απειλές υψηλής ανάπτυξης που θα επηρεάσουν το 70% έως 80% των εσόδων των παγκόσμιων εταιρειών. Επί του παρόντος εξυπηρετούν 7.500 πελάτες παγκοσμίως, συμπεριλαμβανομένου του 80% των εταιρειών globalFortune 1.000 ως πελάτες. Βλέπε επίσης: https://www.marketsandmarkets.com/AboutUs-8.html

Όσον αφορά στις Κρίσιμες Υποδομές, ο έλεγχος πρόσβασης οφείλει να είναι αυστηρότερος και έτσι περιλαμβάνει μηχανικά μέσα (όπως π.χ. ηλεκτρομαγνητικές κλειδαριές), αλλά και εξελιγμένα ηλεκτρονικά τουρνικέ, μαγνητικές πύλες ελέγχου, ασύρματες κλειδαριές και άλλα μέσα ελέγχου.
Τα κλειδιά μπορεί να χαθούν, να κλαπούν και να αντιγραφούν, αφήνοντας ευάλωτα τα περιουσιακά στοιχεία ενός οργανισμού, ενώ συνοδεύονται με την απαίτηση για μία ακριβή αλλαγή των κλειδαριών. Αντίθετα, όταν μία κάρτα ηλεκτρονικής πρόσβασης χαθεί ή κλαπεί, τότε τα δικαιώματα πρόσβασης μπορούν να αποσυρθούν άμεσα, καθιστώντας συνεπώς την κάρτα ανενεργή. Τα σύγχρονα συστήματα Ελέγχου Πρόσβασης προσφέρουν επίσης ευέλικτα δικαιώματα πρόσβασης. Για παράδειγμα, ενώ όλοι οι υπάλληλοι μπορούν να αποκτήσουν πρόσβαση μέσω της κύριας εισόδου ενός κτιρίου, η πρόσβαση σε ορισμένες εσωτερικές περιοχές μπορεί να περιορίζεται σε επιλεγμένους υπαλλήλους. Η πρόσβαση μπορεί επίσης να περιορίζεται σε συγκεκριμένες χρονικές περιόδους.

Η πλαστική κάρτα πρόσβασης είναι εδώ και καιρό η κυρίαρχη μορφή της επαλήθευσης ταυτότητας. Αν και εξακολουθεί να χρησιμοποιείται στα περισσότερα εγκατεστημένα συστήματα, οι βιομετρικές λύσεις – επικύρωση ταυτότητας μέσω αναγνώρισης προσώπου, δακτυλικών αποτυπωμάτων και αναγνώρισης της ίριδας – καθίστανται όλο και περισσότερο αξιόπιστες, οικονομικά προσιτές και περισσότερο διαδεδομένες [179].

Ένα τεχνολογικό παράδειγμα, είναι το RTLS που είδαμε σε προηγούμενη παράγραφο, όπου καρταναγνώστες RFID μπορούν να χρησιμοποιηθούν για τον έλεγχο ετικετών RFID οι οποίες συνδέονται στα υπό έλεγχο αντικείμενα και μεταφέρονται από άτομα που κινούνται στο περιβάλλον. Για να πετύχουμε τη βέλτιστή χρήση ενός συστήματος ελέγχου πρόσβασης και την ολοκλήρωση (integration) με υπολογιστικά συστήματα, το RFID του μέλλοντος πρέπει να εξελιχθεί από τη φιλοσοφία του κλειστού βρόχου και να εξεταστεί η εφαρμογή ανοικτού βρόχου μέσα από μια νέα αρχιτεκτονική. Στην βιβλιογραφία [180], προτείνεται ένα σύστημα ελέγχου πρόσβασης που βασίζεται σε RFID σύστημα και στο φιλτράρισμα πακέτων στο επίπεδο δικτύου.

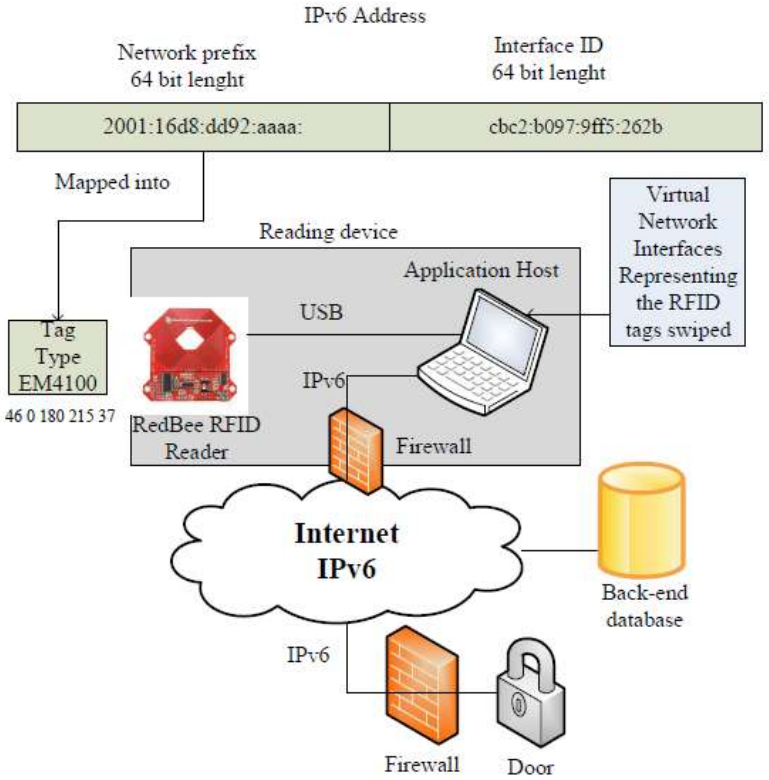
Τα περισσότερα αντικείμενα στο περιβάλλον μας δεν είναι εξοπλισμένα με μικροεπεξεργαστές και ως εκ τούτου δεν μπορούν να συνδεθούν απευθείας σε ένα ασύρματο δίκτυο υπολογιστών. Ωστόσο, αυτά τα αντικείμενα μπορούν να εξοπλιστούν με χαμηλού κόστους, παθητικές ετικέτες RFID είτε ως ενσωματωμένες ετικέτες είτε κολλημένες στο αντικείμενο και με αυτόν τον τρόπο να υπάρχει επικοινωνία. Οι Dominikus, Aiger και Kraxberger[71] προτείνουν έναν τρόπο ενσωμάτωσης παθητικών συστημάτων RFID στο Internet of Things, χρησιμοποιώντας αναγνώστες που λειτουργούν ως IPv6 δρομολογητές και καθορίζοντας ένα σχήμα διευθύνσεων IPv6, ώστε να μετατραπούν οι ετικέτες (tag IDs) σε διευθύνσεις δικτύου. Ο ηλεκτρονικός κωδικός προϊόντος (EPC) της ετικέτας, ο οποίος είναι ταυτότητα, σε αυτή την περίπτωση γίνεται μέρος της στοίβας IPv6. Η προτεινόμενη λύση χωρίζεται σε δύο βασικά λειτουργικά στοιχεία. Το πρώτο στοιχείο είναι υπεύθυνο για τη χαρτογράφηση ετικετών RFID σε διευθύνσεις IPv6. Το άλλο στοιχείο εφαρμόζει τη λειτουργία ελέγχου πρόσβασης του στο σύστημα (physical access control). Με αυτόν τον

[71] Dominikus, S., Aiger, M.J., and Kraxberger, S. (2010). “Passive RFID Technology for the Internet of Things”. In Proceedings of the International Conference for Internet Technology and Secured Transactions (ICITST), pp.1-8, November 2010.

τρόπο, παρέχεται η δυνατότητα πρόσβασης εξουσιοδοτημένων χρηστών σύροντας τις ανέπαφες ταυτότητες εγγύτητας (proximity cards) που φέρουν το RFID στοιχείο, μπροστά από τον αναγνώστη. Τα στοιχεία αναλύονται σε ένα υπολογιστή ο οποίος δίνει την εντολή πρόσβασης σε μία ελεγχόμενη θύρα. Ταυτόχρονα το σύστημα καταγράφει την κίνηση των χρηστών και εκτυπώνει ένα αρχείο (log file) στον διαχειριστή [180].

1. Ενσωμάτωση Ετικετών RFID στο Διαδίκτυο

Το πρώτο σκέλος της λύσης χρησιμοποιεί έναν αναγνώστη RFID και μία εφαρμογή σε κεντρικό υπολογιστή, ο οποίος λειτουργεί ως διακομιστής μεσολάβησης για τις ετικέτες που θέλουμε να ελέγξουμε. Στον υπολογιστή, μέσω σειριακού διαύλου (usb), συνδέεται μία συσκευή ανέπαφης ανάγνωσης ετικετών RFID (αναγνώστης) (Εικόνα 6-6). Ο διακομιστής μπορεί να δημιουργήσει μία εικονική αναπαράσταση της παθητικής ετικέτας με RFID στο Διαδίκτυο, δημιουργώντας μια Διεπαφή Εικονικού Δικτύου (Virtual Network Interface - VNI) με διεύθυνση IPv6, στην οποία μπορεί να αποδοθεί κάθε ετικέτα που βρίσκεται μέσα στο ηλεκτρικό πεδίο ενός αναγνώστη. Ως εκ τούτου, οι ετικέτες δεν τερματίζουν απευθείας την κίνηση IPv6 αλλά απλώς επικοινωνούν με μία οντότητα που αντιπροσωπεύει την ετικέτα (φυσικό αντικείμενο), με το οποίο θέλουμε να επικοινωνήσουμε. Η συσκευή ανάγνωσης επικοινωνεί με μία κεντρική βάση δεδομένων που βρίσκεται στο διαδίκτυο. Έτσι, χρησιμοποιώντας την έννοια της εικονικοποίησης (virtualization), μπορούμε να έχουμε αναπαραστάσεις ετικετών RFID στο Διαδίκτυο.



Εικόνα 6-6: Δικτυακές, παθητικές ετικέτες RFID για έλεγχο πρόσβασης[72]

[72] Η ετικέτα εδώ έχει την ταυτότητα: 46 0 180 215 37. Ο αναγνώστης RFID (RedBee RFID Reader) στέλνει έναν παλμό στην ετικέτα και ακούει την απόκριση της ετικέτας. Η ετικέτα ανιχνεύει αυτήν την ενέργεια και στέλνει

Οι ετικέτες μπορεί να σχετίζονται με εικονικές αναπαραστάσεις με τη μορφή λογισμικού το οποίο είναι σε θέση να ανταποκριθεί σε αιτήματα που προέρχονται από αντίστοιχους κόμβους, ενεργώντας ως πληρεξούσιο (proxy) για λογαριασμό των επισημασμένων αντικειμένων. Για συστήματα ελέγχου πρόσβασης, τα αντικείμενα με ετικέτα (tagged objects) είναι οι ανέπαφες κάρτες εγγύτητας (proximity cards), όμως αυτό μπορεί να γενικευτεί σε οτιδήποτε φέρει παθητική RFID ετικέτα.

Το σύστημα ελέγχου πρόσβασης χρησιμοποιεί και έναν Προσωπικό Αριθμό αναγνώρισης (Personal Identification Number - PIN) στα σημεία ελέγχου. Η ταυτότητα RFID μαζί με το PIN χρησιμοποιείται στη συνέχεια για την κατασκευή μίας κρυπτογραφημένης διεύθυνσης η οποία αντιπροσωπεύει την ταυτότητα του χρήστη που θέλει πρόσβαση σε μία ασφαλή ζώνη.

Προκειμένου να προστατευθούν τα συστήματα από τις απειλές ενός ανοιχτού δικτύου, ορίζονται συγκεκριμένα ασφαλή κανάλια επικοινωνίας μεταξύ αναγνωστών και κλειδαριών θυρών καθώς και μεταξύ αναγνωστών και βάσης δεδομένων (back-end database). Οι κρυπτογραφικά παραγόμενες διευθύνσεις, είναι IPv6 διευθύνσεις που κατασκευάζονται μέσω μίας κρυπτογραφικής συνάρτησης κατακερματισμού (hash function) μονής κατεύθυνσης.

2. Λειτουργία Ελέγχου Πρόσβασης

Τα συστήματα ελέγχου πρόσβασης λειτουργούν με διαφορετικούς τύπους και τεχνολογίες αναγνωστών, όπως αναγνώστες RFID, σαρωτές αμφιβληστροειδούς, δακτυλικού αποτυπώματος κλπ., ενώ ορισμένες φορές απαιτείται ο συνδυασμός βιομετρικών χαρακτηριστικών και εισαγωγή αριθμού PIN για μεγαλύτερη ασφάλεια. Στους χρήστες παραχωρείται εξουσιοδότηση πρόσβασης στον υπό προστασία χώρο, σύροντας τις ανέπαφες κάρτες ταυτότητας (ή εισάγοντας άλλο βιομετρικό χαρακτηριστικό) μπροστά από τον αναγνώστη και έπειτα εισάγοντας το σωστό PIN. Αυτές οι πληροφορίες, δηλαδή η ταυτότητα ετικετών RFID και το PIN, υποβάλλονται σε επεξεργασία τοπικά. Η ετικέτα (επίσης γνωστή ως αναμεταδότης) διατηρεί τα δεδομένα που μεταδίδονται στον αναγνώστη όταν η ετικέτα αναγιγνώσκεται από τον αναγνώστη. Η ετικέτα περιέχει εσωτερική κεραία και μικροτσίπ. Το μικροτσίπ αποθηκεύει τα δεδομένα που ορίζουν και διακρίνουν κάθε ετικέτα. Υπάρχουν τρεις τύποι ετικετών σε χρήση: ενεργές ετικέτες, παθητικές ετικέτες και ημι-παθητικές ετικέτες. Οι ενεργές ετικέτες ενσωματώνουν μία μπαταρία μαζί με την κεραία και το μικροτσίπ. Η μπαταρία επηρεάζει το κόστος και το μέγεθος των ενεργών ετικετών. Κατά συνέπεια, οι ενεργές ετικέτες δεν χρησιμοποιούνται πολύ συχνά. Οι παθητικές ετικέτες δεν έχουν ενσωματωμένη μπαταρία. Οι απαιτήσεις ισχύος μίας παθητικής ετικέτας παράγονται από τα ηλεκτρικά ή μαγνητικά πεδία που παράγονται από τον αναγνώστη RFID. Οι παθητικές ετικέτες είναι πολύ φθηνές και μικρότερες από τις ενεργές ετικέτες. Ως αποτέλεσμα χρησιμοποιούνται κατά την εγγραφή παρακολούθησης. Οι ημι-παθητικές ετικέτες έχουν ενσωματωμένη πηγή ισχύος και

μία απόκριση που περιέχει τον σειριακό αριθμό της και πιθανώς και άλλες πληροφορίες (π.χ. σειριακό αριθμό). Ο αναγνώστης μεταφέρει την ταυτότητα της ετικέτας στον διακομιστή, ο οποίος δημιουργεί την εικονική αναπαράστασή της στο Διαδίκτυο.

ενδέχεται να έχουν ενσωματωμένους αισθητήρες. Η ενσωματωμένη πηγή ισχύος παρέχει μία συνεχή πηγή ισχύος για τους αισθητήρες. Αυτό επιτρέπει στις ημι-παθητικές ετικέτες να μεταφέρουν δεδομένα ακόμη και εν απουσία αναγνώστη RFID. Οι ημι-παθητικές έχουν επίσης αυξημένο εύρος ανάγνωσης. Το κόστος των ημι-παθητικών ετικετών κυμαίνεται μεταξύ του κόστους των ενεργών και των παθητικών ετικετών [181].

Στην λύση που παρακολουθήσαμε, το πλεονέκτημα έγκειται στο ότι ο ίδιος ο αναγνώστης μπορεί να χρησιμοποιηθεί ως ένα ολοκληρωμένο σύστημα ελέγχου πρόσβασης, όπου ένα τείχος προστασίας παρέχοντας τη λειτουργία ελέγχου πρόσβασης, αποκλείει την επικοινωνία με το δίκτυο εάν ο χρήστης δεν είναι εξουσιοδοτημένος [180].

Η συσκευή ανάγνωσης μπορεί επίσης να λειτουργήσει και ως αυτόνομος (standalone) αναγνώστης ελέγχου πρόσβασης, στον οποίο αποστέλλονται κανόνες πρόσβασης από έναν εξωτερικό υπολογιστή. Αυτοί οι κανόνες είναι ουσιαστικά ένα σύνολο κανόνων πολιτικής τείχους προστασίας οι οποίοι αποθηκεύονται στη συσκευή ανάγνωσης. Η διανομή των αλλαγών σε μία ζώνη ή περιοχή ασφαλείας μπορεί να γίνει με πολλαπλή διανομή των νέων κανόνων πρόσβασης σε όλες τις συσκευές που βρίσκονται στην ζώνη, με ενημέρωση από τον εξωτερικό συνδεδεμένο υπολογιστή.

Το σύστημα ανταποκρίνεται σε έναν χρήστη στον οποίο έχει παραχωρηθεί πρόσβαση σε μία συγκεκριμένη ζώνη ασφαλείας και η ετικέτα του έχει προστεθεί στο σύστημα μέσω του διαχειριστή διαμόρφωσης τείχους προστασίας. Τελικά, ο χρήστης αποκτά πρόσβαση στη συγκεκριμένη ζώνη ασφαλείας ενώ ο παράγοντας διαμόρφωσης της πολιτικής είναι η διεπαφή. Έτσι, οι διαχειριστές μπορούν να προσθέσουν ή να αφαιρέσουν κανόνες φίλτρου πακέτων οι οποίοι λειτουργούν ως ο μηχανισμός ελέγχου πρόσβασης.

6.4 Συστήματα Επιτήρησης και Καταγραφής (CCTV)

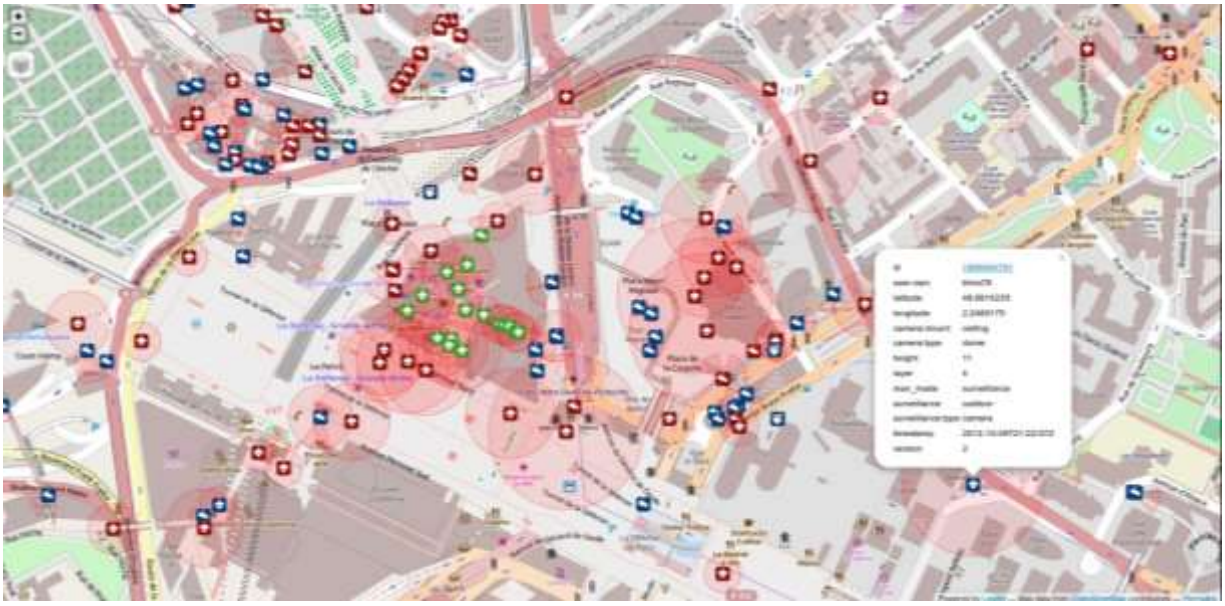
Ένα σύστημα επιτήρησης έχει σαν βασικό σκοπό την επιτήρηση μίας υποδομής, δίνοντας παράλληλα την δυνατότητα καταγραφής των συμβάντων σε κάποιο αποθηκευτικό μέσο, όπου ο χρήστης μπορεί να ανατρέξει όποτε χρειαστεί προκειμένου να εντοπίσει κάποιο συμβάν. Με τον όρο Κλειστό Κύκλωμα Τηλεόρασης (Closed Circuit TV – CCTV) εννοούμε ένα σύστημα παρακολούθησης αποτελούμενο από εικονολήπτες (κάμερες) συνδεδεμένο με οθόνη ή υπολογιστή για την παρακολούθηση κάποιου χώρου. Ο ψηφιακός εγγραφέας (Digital Video Recorder – DVR), ως θεμελιώδες συστατικό του κυκλώματος αναλαμβάνει την καταγραφή της εικόνας και την αποθήκευσή της.

Η χρήση του CCTV είναι κοινή σε πολλές περιοχές σε όλο τον κόσμο, ενώ νέες τεχνολογίες αναδύονται συνεχώς. Τα τελευταία χρόνια, η χρήση βιντεοκάμερας που φέρεται στο σώμα έχει εισαχθεί ως μία νέα μορφή επιτήρησης, η οποία χρησιμοποιείται συχνά στην επιβολή του νόμου, με κάμερες που βρίσκονται στο στήθος ή στο κεφάλι ενός αστυνομικού. Σε βιομηχανικές εγκαταστάσεις, ο εξοπλισμός CCTV μπορεί να χρησιμοποιηθεί για την παρακολούθηση τμημάτων μίας διαδικασίας, για παράδειγμα όταν το περιβάλλον δεν είναι κατάλληλο για ανθρώπους. Τα συστήματα CCTV μπορούν να λειτουργούν συνεχώς ή μόνο όπως απαιτείται για την παρακολούθηση ενός συγκεκριμένου συμβάντος. Μία πιο προηγμένη μορφή CCTV, χρησιμοποιώντας ψηφιακές συσκευές εγγραφής βίντεο (DVR),

παρέχει εγγραφή για πιθανώς πολλά χρόνια, με ποικιλία επιλογών ποιότητας και απόδοσης και επιπλέον δυνατοτήτων όπως ανίχνευση κίνησης και ειδοποιήσεις μέσω email [182].

Στη σύγχρονη μορφή του CCTV, αποκεντρωμένες ή ασύρματες δικτυακές κάμερες εξοπλισμένες με αισθητήρες megapixel, υποστηρίζουν εγγραφή απευθείας σε συσκευές αποθήκευσης συνδεδεμένες στο δίκτυο ή σε εσωτερική μνήμη για εντελώς αυτόνομη λειτουργία. Σύμφωνα με μία σχετική εκτίμηση, περισσότερες από 1 δισεκατομμύριο κάμερες παρακολούθησης θα χρησιμοποιηθούν παγκοσμίως έως το 2030, οι περισσότερες εκ των οποίων θα βρίσκονται εγκατεστημένες στην Ασία. Οι κάμερες αυτές θα μπορούν να τροφοδοτούνται από εναλλακτικές πηγές ενέργειας και να συνδέονται στα ασύρματα δίκτυα 4ης και 5ης γενιάς, αποτελώντας έναν μεγάλο διαδραστικό ιστό παρακολούθησης και καταγραφής συμβάντων [183].

Ο πλέον αναπτυσσόμενος κλάδος στο CCTV αφορά στις κάμερες πρωτοκόλλου διαδικτύου (κάμερες IP). Οι κάμερες IP χρησιμοποιούν το πρωτόκολλο Internet (IP) που χρησιμοποιείται από τα περισσότερα τοπικά δίκτυα (LAN) για τη μετάδοση βίντεο σε δίκτυα δεδομένων σε ψηφιακή μορφή. Η IP διεύθυνση μπορεί προαιρετικά να μεταδοθεί στο δημόσιο διαδίκτυο, επιτρέποντας στους χρήστες να βλέπουν τις κάμερές τους από απόσταση σε υπολογιστή ή τηλέφωνο μέσω σύνδεσης στο Διαδίκτυο. Για επαγγελματικές ή δημόσιες εφαρμογές υποδομών, το βίντεο IP περιορίζεται σε ιδιωτικό δίκτυο (VPN). Οι κάμερες IP θεωρούνται μέρος του Internet of Things (IoT) και έχουν πολλά από τα ίδια οφέλη και κινδύνους ασφαλείας με άλλες συσκευές με δυνατότητα IP [184].



Εικόνα 6-7: Χάρτης με κάμερες CCTV κοντά στο Grande Arche (Γαλλία) χρησιμοποιώντας δεδομένα OpenStreetMap[73]

[73] Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) είναι ένας ευρωπαϊκός κανονισμός που τέθηκε σε ισχύ στις 25 Μαΐου 2018 και αντικαθιστά τον Νόμο περί Προστασίας Δεδομένων 1998 με τον Νόμο Προστασίας Δεδομένων 2018 (DPA). Στα πλαίσια του GDPR, οι δημόσιες ενεργές κάμερες εντός της Ευρωπαϊκής Ζώνης θα πρέπει να δηλώνονται στην εκάστοτε υπηρεσία προσωπικών δεδομένων και να

Οι κύριοι τύποι καμερών IP περιλαμβάνουν: σταθερές κάμερες, κάμερες με κλίση κλίσης (Pan-Tilt-Zoom - PTZ[74]) και κάμερες πολλαπλών αισθητήρων. Η ανάλυση της σταθερής κάμερας μπορεί να διαφέρει ανάλογα με την περιοχή εφαρμογής, αλλά συνήθως δεν υπερβαίνει τα 20 megapixel. Το κύριο χαρακτηριστικό ενός PTZ είναι η δυνατότητα απομακρυσμένης κατεύθυνσης και οπτικού zoom (εστίασης). Με κάμερες πολλαπλών αισθητήρων, μπορούν να παρακολουθούνται ευρύτερες περιοχές και να επιτυγχάνεται ανάλυση εκατοντάδων megapixel. Από το 2008, οι κατασκευαστές παρακολούθησης βίντεο IP μπορούν να χρησιμοποιήσουν τυποποιημένη διεπαφή δικτύου (Open Network Video Interface Forum - ONVIF[75]) για να υποστηρίξουν τη συμβατότητα μεταξύ συστημάτων. Πολλοί καταναλωτές στρέφονται σε ασύρματες κάμερες ασφαλείας, καθώς οι ασύρματες κάμερες δεν απαιτούν καλώδια για τη μετάδοση βίντεο/ήχου. Οι ασύρματες κάμερες είναι επίσης εύκολες και φθηνές στην εγκατάσταση, ενώ οι σύγχρονες κάμερες χρησιμοποιούν ψηφιακή τεχνολογία που παρέχει πιο καθαρό ήχο, ευκρινέστερο βίντεο και ασφαλές σήμα χωρίς παρεμβολές. Οι ασύρματες κάμερες μπορούν αν ενσωματωθούν σε ένα ευρύτερο πλέγμα ασύρματων αισθητήρων, μεταδίδοντας και παραλαμβάνοντας δεδομένα μέσω ασύρματων τηλεφωνικών δικτύων 4ης και 5ης γενιάς [184].

6.4.1 Ασύρματα Συστήματα CCTV

Ως μη επεμβατική τεχνολογία, η απεικόνιση παίζει σημαντικό ρόλο στις κινητές συσκευές ανίχνευσης. Πολλαπλές κάμερες οι οποίες παρατηρούν μία ίδια σκηνή από διαφορετικές οπτικές γωνίες, μπορούν να αποτελέσουν ένα σύστημα επιτήρησης υψηλής απόδοσης. Ωστόσο, η χαμηλή κατανάλωση ενέργειας σε αντίστροφη αναλογία με την υψηλής ποιότητας απεικόνιση, αποτελεί πρόκληση για τα δίκτυα ασύρματων έξυπνων καμερών. Οι Kleihorst και Schueler συστήνουν μία ασύρματη έξυπνη κάμερα η οποία βασίζεται σε επεξεργαστή ανάλυσης βίντεο SIMD και μικροελεγκτή 8051 ως τοπικό κεντρικό υπολογιστή [190].

Η ασύρματη επικοινωνία γίνεται μέσω του Προτύπου IEEE802.15.476, ενώ πολλαπλές κάμερες μπορούν να δημιουργήσουν ένα δίκτυο ομότιμων στοιχείων (peer-to-peer) και να αναλύσουν τη σκηνή με κατανεμημένο τρόπο από αρκετές απόψεις ταυτόχρονα.

απεικονίζονται σε χάρτη. Το εργαλείο OpenStreetMap είναι ψηφιακός χάρτης του κόσμου υπό άδεια ελεύθερης χρήσης, το οποίο μεταξύ άλλων εξυπηρετεί και την απεικόνιση αυτή.

[74] https://en.wikipedia.org/wiki/Pan%E2%80%93tilt%E2%80%93zoom_camera

[75] Ένας κοινός όρος που μπορεί να συναντήσετε στη βιομηχανία βίντεο IP είναι το ONVIF. Το ONVIF (Open Network Video Interface Forum) είναι ένα παγκόσμιο φόρουμ όσο και ένα παγκόσμιο πρωτόκολλο που επιτρέπει σε διαφορετικές συσκευές παρακολούθησης και ασφάλειας από διαφορετικούς κατασκευαστές να λειτουργούν απρόσκοπτα. Για περισσότερα στοιχεία βλέπε: https://www.onvif.org/

[76] Για περισσότερα στοιχεία βλέπε: https://en.wikipedia.org/wiki/IEEE_802.15.4

Καθώς η χαμηλή κατανάλωση ενέργειας και οι ταυτόχρονες υψηλές επιδόσεις είναι δύσκολο να επιτευχθούν και ιδιαίτερα εφόσον η συσκευή λειτουργεί με εφεδρική πηγή ενέργειας (μπαταρίες), η λειτουργικότητα θα μπορούσε να μετατοπιστεί προς έναν υπολογιστή που τροφοδοτείται με ρεύμα μετά από την μετάδοση των ακατέργαστων (raw) δεδομένων βίντεο. Ωστόσο, αυτό απαιτεί ισχύ της τάξης των 400mWatts για την ασύρματη μετάδοση ενός έγχρωμου βίντεο, ροής 15 πλαισίων ανά δευτερόλεπτο (frame per second – FPS). Στην πραγματικότητα, για μετάδοση μικρών αποστάσεων, το μεγαλύτερο μέρος της ενέργειας εκπομπής καταναλώνεται στον μετατροπέα DAC παρά στον πομπό. Η τεχνολογία αυτών των μετατροπέων είναι πολύ κοντά στο χαμηλότερο δυνατό όριο κατανάλωσης ενέργειας, το οποίο υποδεικνύεται από τον θερμικό θόρυβο.

Εικόνα 6-8: Ασύρματο mote έξυπνης κάμερας με ενσωματωμένους αισθητήρες εικόνας VGA και σύστημα όρασης υψηλής απόδοσης [190]

Η επεξεργασία και μετάδοση βίντεο σε πραγματικό χρόνο, με χαμηλό κόστος και χαμηλή κατανάλωση ενέργειας, καθίστανται πλέον δυνατή χάρη στην πρόοδο στις τεχνικές ενσωμάτωσης μικροεπεξεργαστών (embedded microchips). Οι δύο τύποι προγραμματιζόμενων μικροεπεξεργαστών που προτείνουν οι Kleihorst και Schueler στην αρχιτεκτονική της έξυπνης κάμερας είναι ο επεξεργαστής πολλαπλών ενιαίων οδηγιών (Single Instruction Multiple Data - SIMD) και η συστοιχία (ενός ή περισσότερων) επεξεργαστών ψηφιακού σήματος (Digital Signal Processor – DSP) γενικής χρήσης [190].

Πέρα από την προτεινόμενη λύση, οι ασύρματες κάμερες ασφαλείας 5G, είναι οι κάμερες εκείνες που περιλαμβάνουν κυψελοειδές πομπό και λειτουργούν στο δίκτυο 5G για την μετάδοση σήματος βίντεο. Παρόμοια με τις 3G/4G κυψελοειδείς κάμερες ασφαλείας, οι 5G απαιτούν ένα πρόγραμμα κινητής υπηρεσίας για να λειτουργήσουν, ενώ η αξιοπιστία τους μπορεί να επηρεαστεί από τις συνθήκες του δικτύου. Παρά το γεγονός ότι το δίκτυο 5G είναι ακόμα στα πρώτα στάδια εμπορικής διάθεσης-ανάπτυξης, πολλές χώρες και φορείς έχουν συμμετάσχει στον έντονο ανταγωνισμό για την κυριαρχία στο 5G. Χωρίς καμία αμφιβολία, οι κάμερες IP ακόμη και πάνω από τεχνολογία 5G, θα είναι η επόμενη νέα τάση στην αγορά CCTV [191].

Με βάση το δίκτυο κινητής τηλεφωνίας 5G, με μεγαλύτερη ταχύτητα και μικρότερη καθυστέρηση, οι κάμερες ασφαλείας 5G μπορούν να προσφέρουν τα ακόλουθα πλεονεκτήματα [192]:

- **Δεν απαιτείται σύνδεση WiFi και εξωτερική τροφοδοσία**. Λειτουργώντας σε 5G, οι ασύρματες κάμερες ασφαλείας 5G μπορούν να παρέχουν μία αξιόπιστη λύση ασφάλειας για περιοχές χωρίς σύνδεση WiFi και πηγή ενέργειας, όπως π.χ. αχυρώνες, αγροκτήματα, εργοτάξια, εξοχικές κατοικίες, κάμπινγκ, RVs, σκάφη κλπ.

- **Ταχύτερες ταχύτητες λήψης και μεταφόρτωσης.** Το 5G αναμένεται να προσφέρει ταχύτητες Internet για κινητά άνω των 10 gigabits ανά δευτερόλεπτο, που είναι έως και 1000 φορές αυτές των τωρινών δικτύων 4G. Αυτό σημαίνει ότι το βίντεο υψηλής ανάλυσης της κάμερας ασφαλείας 5G μπορεί να ανέβει στο cloud μέσα σε λίγα δευτερόλεπτα.

- **Ομαλή ροή με μικρή καθυστέρηση**. Βασισμένες στην ταχύτερη ταχύτητα του δικτύου, οι ασύρματες κάμερες ασφαλείας 5G μπορούν να μειώσουν σημαντικά την καθυστέρηση ή τους χρόνους ψηφιακής απόκρισης. Αυτό καθιστά δυνατή την παρακολούθηση ζωντανής (real time) προβολής, σχεδόν με μηδενική καθυστέρηση.

- **Βίντεο υπέρ υψηλής ανάλυσης (Full HD)**. Ενώ το δίκτυο 3G και 4G αποτυγχάνει να υποστηρίξει τη μετάδοση βίντεο 1080p Full HD, οι κάμερες κινητής ασφάλειας 5G είναι κατάλληλες για ροή βίντεο υψηλής ανάλυσης διατηρώντας παράλληλα την ποιότητα και τις λεπτομέρειες της εικόνας.

- **Μεγαλύτερος χρόνος αναμονής και λιγότερη κατανάλωση ενέργειας**. Τα συστήματα ασφαλείας 5G τροφοδοτούνται από εναλλακτικές πηγές ενέργειας και μπαταρίες. Χάρη στη γρήγορη ταχύτητα αποστολής της εικόνας και τη μικρή καθυστέρηση, τα συστήματα καμερών 5G μπορούν να λειτουργήσουν καταναλώνοντας λιγότερη ενέργεια, όντας για περισσότερο χρόνο σε κατάσταση αναμονής.

- **Αμφίδρομη επικοινωνία υψηλής ποιότητας**. Για τις κάμερες ασφαλείας 5G με ενσωματωμένο μικρόφωνο και ηχείο, είναι δυνατή η εμπειρία αμφίδρομης επικοινωνίας ομιλίας ή άλλου χειρισμού.

Δεν είναι μόνο τα συστήματα επιτήρησης που θα ενισχυθούν με τις δυνατότητες απόδοσης του 5G. Τα συστήματα ασφαλούς πόλης θα ενισχυθούν περαιτέρω, ώστε το βίντεο να μπορεί να χρησιμοποιηθεί για μία σειρά εφαρμογών, όπως η δημόσια ασφάλεια, η διαχείριση της κυκλοφορίας, ο εντοπισμός πυρκαγιάς, η διαχείριση πλήθους, ο έλεγχος πρόσβασης και ο εντοπισμός εισβολέων. Αυτό θα ισχύει εάν αυτές οι ροές βίντεο προέρχονται είτε από συμβατικές εξωτερικές κάμερες είτε από μόνο ασύρματες.

Φυσικά, εκτός της κατηγορίας των σταθερά τοποθετημένων ασύρματων καμερών τις οποίες γνωρίζουμε ως μέσο καταστολής και επιτήρησης εγκληματικών ενεργειών, η ασύρματη τεχνολογία επιφέρει επιπλέον κάμερες που φέρονται στο σώμα (wearables) καθώς και κάμερες τοποθετημένες σε οχήματα. Η δυνατότητα τεμαχιοποίησης του δικτύου (network slicing) που προσφέρεται στα δίκτυα 5ης γενιάς, μπορεί να προσφέρει αποκλειστικά τμήματα χωρητικότητας δικτύου για συγκεκριμένες εφαρμογές, καταργώντας την ανάγκη κοινής χρήσης χωρητικότητας με πολλούς χρήστες [191].

Εικόνα 6-9: Ασύρματη κάμερα 4G της εταιρείας HikVision, με αυτόνομη τροφοδοσία από φωτοβολταϊκό πάνελ[77]

6.4.2 Αλγόριθμοι Ανάλυσης Εικόνας (Video Analytics)

Οι κάμερες τεχνολογίας IP που ελέγχονται από υπολογιστή μπορούν να αναγνωρίσουν, να παρακολουθήσουν και να κατηγοριοποιήσουν αντικείμενα στο οπτικό τους πεδίο. Η ανάλυση περιεχομένου βίντεο, επίσης αναφερόμενη ως ανάλυση βίντεο (Video Analytics), είναι η δυνατότητα αυτόματης ανάλυσης βίντεο για τον εντοπισμό και τον προσδιορισμό χρονικών γεγονότων που δεν βασίζονται σε μία μόνο εικόνα, αλλά σε ταξινόμηση αντικειμένων, για παράδειγμα σύμφωνα με το χρώμα. Την τελευταία δεκαετία έχουν αναπτυχθεί βελτιωμένα χαρακτηριστικά VCA (Video Content Analysis). Πέρα από την

[77] Το “Solar-Powered Security Camera Setup” αφορά την πρόταση της Κινεζικής εταιρείας Hikvision για περιοχές όπου χρειάζεται ισχυρή απόδοση, αλλά τα τροφοδοτικά και τα καλώδια δικτύου δεν μπορούν να φτάσουν. Στην κάμερα παρέχεται εφεδρική ισχύς για την επίλυση διακοπών παρακολούθησης λόγω διακοπών ρεύματος σε οποιοδήποτε σενάριο τροφοδοσίας, πράγμα που σημαίνει ότι η κάμερα μπορεί να τροφοδοτηθεί από εξωτερική τροφοδοσία 12V ή να λειτουργήσει εντελώς αυτόνομα λαμβάνοντας ενέργεια από τον ήλιο. Την ίδια στιγμή η μετάδοση γίνεται μέσω 4G δικτύου, με ενσωματωμένη κάρτα SIM στην κάμερα, ενώ τα δεδομένα εικόνας μεταφέρονται σε σταθμό βάσης, προς επεξεργασία. Αυτά τα προηγμένα συστήματα καμερών είναι ιδανικά για αγροκτήματα και δάση, καθώς και για έργα υποδομής και προσωρινές αθλητικές ή πολιτιστικές εκδηλώσεις. Η κάμερα υποστηρίζει LTE-TDD/LTE-FDD/WCDMA/GSM 4G δίκτυο.
Πηγή:https://www.hikvision.com/en/products/IP-Products/Network-Cameras/solar-powered-security-camera-setup/ds-2xs6a25g0-i-ch20s40/

αναγνώριση συγκεκριμένων σχημάτων και χρωμάτων, οι εφαρμογές VCA μπορούν τώρα να αναλύσουν πιο πολύπλοκα σενάρια.

Σε αυτήν την παράγραφο, θα δοθεί έμφαση στις ενότητες ενός συστήματος επιτήρησης, οι οποίες είναι υπεύθυνες για τη «μετάφραση» των ακατέργαστων δεδομένων βίντεο σε συγκεκριμένες δομημένες πληροφορίες. Οι πιο συνηθισμένες δραστηριότητες σε αυτόν τον τομέα είναι η ανίχνευση προσώπου, η αναγνώριση προσώπου, η ταυτοποίηση αντικειμένων και η παρακολούθηση αντικειμένων.

Α. Ανίχνευση Προσώπου

Ο εντοπισμός προσώπων μέσα σε μία σκηνή είναι ένα πρόβλημα στην περιοχή της όρασης του υπολογιστή. Αυτό συμβαίνει επειδή η ανίχνευση προσώπου είναι μία από τις πιο ευρέως χρησιμοποιούμενες διαδικασίες στα συστήματα επιτήρησης, καθώς απαιτείται από πολλές εφαρμογές όπως αναγνώριση προσώπου, παρακολούθηση προσώπου και ανάλυση προσώπου για εξαγωγή συμπεριφορικής γνώσης. Ωστόσο, αναδύονται συνεχώς νέες εφαρμογές, όπως το Human Computer Interaction[78] (HCI), το οποίο απαιτεί πιο στιβαρές και ακριβείς λύσεις. Ο στόχος της ανίχνευσης προσώπου είναι πρώτα να καθορίσει εάν κάποια πρόσωπα απεικονίζονται σε μία σκηνή και δεύτερον να υπολογίσει και να επιστρέψει τις συντεταγμένες των ανιχνευόμενων προσώπων [186]. Το καινοτόμο έργο των Viola και Jones[79] άλλαξε τον τρόπο για την ανίχνευση προσώπου και προτείνει ότι οι αλγόριθμοι ανίχνευσης προσώπων πρέπει να κατηγοριοποιούνται σε αλγόριθμους που βασίζονται σε άκαμπτα πρότυπα και σε αλγόριθμους που αναπτύσσουν μοντέλο βασισμένο σε παραμορφώσιμα μέρη, για να μοντελοποιήσουν πιθανές παραμορφώσεις μεταξύ των σημείων του προσώπου. Οι Viola και Jones πρότειναν έναν ανιχνευτή προσώπου που βασίζεται στην ολοκληρωμένη εικόνα και την ταξινόμηση της μάθησης με το AdaBoost[80]. Μετά από αυτήν την ιδέα, έχουν προταθεί νέα χαρακτηριστικά εικόνας προκειμένου να βελτιωθεί η ακρίβεια των αλγορίθμων. Τέτοιες δυνατότητες είναι κοινές λειτουργίες Haar[81], οι οποίες βασίζονται στη συνύπαρξη πολλαπλών χαρακτηριστικών τύπου Haar και των αδύναμων ταξινομητών που βασίζονται στην ταξινόμηση και το Regression Tree[82] (CART). Ένα άλλο κοινό χαρακτηριστικό για την ανίχνευση προσώπου βασίζεται σε περιφερειακές στατιστικές όπως ιστογράμματα, με το Histogram of Oriented Gradients[83] (HOG) να είναι το πιο δημοφιλές. Όσον αφορά τα σχήματα ταξινόμησης, τα νευρωνικά δίκτυα[84] (neural networks) χρησιμοποιούνται ευρέως, όπως ένα περιορισμένο γενετικό μοντέλο (ένα αυτό-συσχετισμένο, πλήρως συνδεδεμένο πολυεπίπεδο perceptron με τρία μεγάλα στρώματα βάρους) και προσεγγίσεις βασισμένες σε συνελικτικό νευρωνικό δίκτυο (Convolutional Neural Network - CNN[85]). Όσον αφορά στα Παραμορφώσιμα Μέρη-Μοντέλα (γνωστά και ως μοντελοποίηση εικονογραφικών δομών), αποτελούν μία από τις βασικές επιλογές για

[78] Για περισσότερες πληροφορίες βλέπε, ενδεικτικά: https://www.interaction-design.org/literature/topics/human-computer-interaction

[79] Viola P., Jones M. (2001): Rapid object detection using a boosted cascade of simple features. Computer vision and pattern recognition (CVPR 2001) Kauai, HI, USA, 2001.

[80] Βλέπε: https://en.wikipedia.org/wiki/AdaBoost

[81] Βλέπε, π.χ.: https://el.wikitechpro.com/925615-haar-wavelet-TLYIHO

[82] https://www.solver.com/regression-trees

[83] Για περισσότερα στοιχεία βλέπε: https://en.wikipedia.org/wiki/Histogram_of_oriented_gradients

[84] Βλέπε επίσης, μεταξύ άλλων: https://en.wikipedia.org/wiki/Neural_network

[85] Βλέπε επίσης: https://en.wikipedia.org/wiki/Convolutional_neural_network

την ανάπτυξη γενικών ανιχνευτών αντικειμένων. Ενώ έχουν προταθεί απλά μοντέλα, πιο σύνθετες προσεγγίσεις έχουν προσφέρει ισχυρές λύσεις [186].

Β. Αναγνώριση Προσώπου

Η αναγνώριση προσώπου αποτελεί το πρόβλημα της αναγνώρισης ενός προσώπου έναντι μίας προκαθορισμένης βάσης δεδομένων γνώσεων προσώπων. Το πρόβλημα αναγνώρισης προσώπου συνεπάγεται ότι ένα πρόσωπο έχει ήδη ανιχνευθεί σε μία σκηνή, γεγονός που καθιστά την ανίχνευση προσώπου μία απαραίτητη διαδικασία για την αναγνώριση προσώπου. Αυτό το ζήτημα προβληματίζει τους ερευνητές για περισσότερα από σαράντα χρόνια, προσπαθώντας να παράγει ισχυρές, ακριβείς και πραγματικές λύσεις σε πραγματικό χρόνο. Οι πρώτες τεκμηριωμένες προσεγγίσεις προσπάθησαν να μοντελοποιήσουν το πρόβλημα αναγνώρισης προσώπου ως ένα πρόβλημα δύο διαστάσεων, υπολογίζοντας «σημαντικές» αποστάσεις των χαρακτηριστικών του προσώπου, όπως η απόσταση μεταξύ των ματιών και του μήκους των χειλιών. Σήμερα, μπορεί κανείς να ταξινομήσει τις μεθόδους αναγνώρισης προσώπου σε τρεις κατηγορίες, ήτοι: ολιστικές μέθοδοι αντιστοίχισης, μέθοδοι που βασίζονται σε χαρακτηριστικά και υβριδικές μέθοδοι. Οι μέθοδοι που βασίζονται σε φυσικά χαρακτηριστικά προσπαθούν να εξάγουν γεωμετρικά χαρακτηριστικά του προσώπου, όπως το στόμα, τα χείλη, η μύτη και τα μάτια. Αυτές οι λειτουργίες χρησιμοποιούνται ως «είσοδος» στους ταξινομητές, με στόχο την ανίχνευση της αντιστοίχισης που βρίσκεται πιο κοντά στο πρόσωπο που εντοπίστηκε. Έχουν προταθεί μέθοδοι εκτίμησης χαρακτηριστικών, αξιοποιώντας κυρίως τους δομικούς περιορισμούς προσώπου. Για παράδειγμα, στη βιβλιογραφία[86] προτείνεται μία νέα προσέγγιση για την αναγνώριση προσώπου που ενσωματώνει πληροφορίες υφής και σχήματος για να αναπαριστά πρόσωπα. Ένα πρόσωπο χωρίζεται αρχικά σε μικρά τετράγωνα από τα οποία εξάγονται τα χαρακτηριστικά του τοπικού δυαδικού μοτίβου και τα οποία ακολούθως ενώνονται σε ένα ιστόγραμμα με ένα μόνο χαρακτηριστικό, που αντιπροσωπεύει το πρόσωπο. Τα τελευταία χρόνια, οι αλγόριθμοι αναγνώρισης προσώπων έχουν φτάσει σε επίπεδο ωριμότητας οπότε μπορούν να χρησιμοποιηθούν σε πραγματικές εφαρμογές και σε μη ελεγχόμενα περιβάλλοντα. Αυτό το γεγονός έφερε την ανάγκη για ανάπτυξη νέων προσεγγίσεων, όπως το πρόβλημα της «λίστας παρακολούθησης». Σύμφωνα με αυτήν την εκδοχή του εν λόγω προβλήματος, το σύστημα πρέπει να διακρίνει μεταξύ ενός πολύ μεγάλου αριθμού ατόμων μόνο εκείνα τα άτομα που ανήκουν σε μία προκαθορισμένη λίστα [187].

Γ. Επιβεβαίωση Ταυτότητας

Το πρόβλημα επιβεβαίωσης ταυτότητας εμφανίζεται σε συστήματα παρακολούθησης πολλαπλών καμερών, όπου οι άνθρωποι περπατούν γύρω από το πεδίο προβολής πολυάριθμων καμερών. Σε τέτοιες περιπτώσεις, ένα σύστημα επιτήρησης θα πρέπει να έχει τη δυνατότητα ώστε να παρακολουθεί άτομα σε πολλές κάμερες, εκτελώντας έτσι ανάλυση κίνησης πλήθους και ανίχνευση δραστηριότητας. Ο επαναπροσδιορισμός είναι ζωτικής σημασίας για τη δημιουργία αξιόπιστων πληροφοριών που επισημαίνουν άτομα σε πολλές κάμερες ή ακόμη και μέσα στην ίδια κάμερα, ιδίως όταν εμφανίζονται ασυνέχειες και

[86] Ahonen T., Hadid A., Pietikäinen M. (2004): Face recognition with local binary patterns. In proceedings of the European Conference on Computer Vision (ECCV 2004) Prague, pp.469-481.

«τυφλά» σημεία. Ο επαναπροσδιορισμός ταυτότητας συνιστά ιδιαίτερη πρόκληση λόγω της οπτικής ασάφειας ή της χρονικής αβεβαιότητας στην εμφάνιση ενός ατόμου σε διαφορετικές κάμερες, ενώ οι δυσκολίες αυτές ενισχύονται από εικόνες χαμηλής ανάλυσης είτε από ροές βίντεο κακής ποιότητας. Θέματα όπως αυτά ανάγκασαν την ερευνητική κοινότητα να εστιάσει στο πρόβλημα αναγνώρισης ταυτότητας τα τελευταία χρόνια, με στόχο να παράγει ισχυρούς και ευρέως εφαρμοζόμενους αλγόριθμους [187].

Δ. Ανίχνευση και Παρακολούθηση Αντικειμένων

Η ανίχνευση και παρακολούθηση αντικειμένων είναι οι πιο συνηθισμένες εφαρμογές στα συστήματα παρακολούθησης βίντεο. Η ανίχνευση αντικειμένου αποτελεί το πρόβλημα της απομόνωσης, σε μία συγκεκριμένη περιοχή, μίας ροής βίντεο με βάση τις παραμέτρους του συστήματος, ενώ η παρακολούθηση αντικειμένων είναι μια διαδικασία παρακολούθησης της κίνησης της προαναφερθείσας περιοχής. Κάποιος μπορεί να ταξινομήσει τους αλγόριθμους ανίχνευσης αντικειμένων σε τέσσερις κατηγορίες, ήτοι: αφαίρεση φόντου, χρονική διαφοροποίηση, διαφοροποίηση πλαισίου και οπτική ροή. Οι αλγόριθμοι που χρησιμοποιούν τεχνικές φόντου προσπαθούν να διαχωρίσουν αντικείμενα σε πρώτο πλάνο από το φόντο της σκηνής. Για να επιτευχθεί αυτό, η μοντελοποίηση υποβάθρου (μοντέλο αναφοράς) είναι υποχρεωτική. Όσο πιο ακριβές και προσαρμοστικό είναι το υπόβαθρο, τόσο πιο ακριβής είναι ο αλγόριθμος ανίχνευσης. Οι αλγόριθμοι χρονικής διαφοροποίησης υπολογίζουν τη διαφορά (σε επίπεδο pixels) μεταξύ διαδοχικών καρέ βίντεο, προκειμένου να ανιχνεύσουν το κινούμενο αντικείμενο. Αυτοί οι αλγόριθμοι είναι σε θέση ώστε να προσαρμόζονται γρήγορα σε εξαιρετικά δυναμικές αλλαγές σκηνής. Ωστόσο, υποφέρουν από σημαντικά μειονεκτήματα: Το πιο σημαντικό από αυτά είναι η απώλεια ανίχνευσης όταν το αντικείμενο σταματά να κινείται και όταν η χρωματική υφή του αντικειμένου είναι παρόμοια με τη σκηνή (καμουφλάζ). Επίσης, η ανίχνευση ψευδών αντικειμένων μπορεί να συμβεί όταν τα αντικείμενα της σκηνής τείνουν να κινούνται (π.χ. φύλλα ενός δέντρου, όταν φυσάει ο αέρας). Μία απλή προσέγγιση της χρονικής διαφοροποίησης είναι η διαφορά πλαισίου, όπου οι χρονικές πληροφορίες υποδεικνύουν τα κινούμενα αντικείμενα της σκηνής. Σε τέτοιες μεθόδους, η κινητικότητα καθορίζεται με τον υπολογισμό της διαφοράς (επίπεδο pixel) δύο διαδοχικών καρέ βίντεο. Τέλος, η οπτική ροή είναι το μοτίβο της κίνησης των αντικειμένων σε μία οπτική σκηνή που προκαλείται από τη σχετική κίνηση μεταξύ ενός παρατηρητή και της σκηνής. Οι μέθοδοι οπτικής ροής χρησιμοποιούν μερική παραγωγή σε σχέση με τις χωρικές και χρονικές συντεταγμένες κατά σειρά, για να υπολογιστεί η κίνηση μεταξύ δύο πλαισίων εικόνας. Λόγω του υπολογιστικού χρόνου που απαιτείται και της ανοχής του θορύβου, οι μέθοδοι οπτικής ροής είναι ακατάλληλες για σενάρια πραγματικού (ή σχεδόν πραγματικού) χρόνου.

6.4.3 Cloud CCTV

Η τεχνολογία νέφους (cloud) φαίνεται να ταιριάζει απόλυτα με τα συστήματα επιτήρησης, καθώς μπορεί να προσφέρει τόσο τις ελλείπουσες υπολογιστικές δυνατότητες ανάλυσης βίντεο όσο και τη χωρητικότητα αποθήκευσης που συνήθως χρειάζεται ένα σύστημα παρακολούθησης. Υποδομές cloud διευκολύνουν την εγκατάσταση και τη διαχείριση συστημάτων επιτήρησης, αλλάζοντας το παράδειγμα από αυτόνομη εφαρμογή σε

εφαρμογή τύπου Software-as-a-Service[87] (SaaS). Αυτό επιτρέπει στα συστήματα επιτήρησης να χρησιμοποιούν διαφορετικές αναλύσεις βίντεο και μηχανισμούς ειδοποίησης όταν απαιτείται και για το χρονικό διάστημα που απαιτείται. Έχοντας υπόψη το κόστος μετάδοσης ενός βίντεο σε ένα σύστημα cloud και το αντίστοιχο κόστος της αποθήκευσης στο cloud, πρέπει να σχεδιαστούν νέοι αλγόριθμοι συμπίεσης, οι οποίοι θα διατηρήσουν την ακρίβεια των αλγορίθμων ανάλυσης βίντεο, μειώνοντας παράλληλα το προαναφερθέν κόστος.

Η τεχνολογία cloud, μπορεί να υποστηριχθεί και να επεκταθεί με υπολογιστές ομίχλης (fog computing[88]) και υπολογισμούς στο άκρο (edge) του δικτύου. Πιο συγκεκριμένα, ο υπολογιστής ομίχλης και άκρων μπορεί να αντιμετωπίσει την καθυστέρηση που επιβαρύνουν συνήθως οι υπηρεσίες cloud σε ένα σύστημα παρακολούθησης, μεταφέροντας την υπολογιστική ισχύ πιο κοντά στην πηγή του συμβάντος. Με τον υπολογισμό των χαρακτηριστικών και των αναλυτικών στοιχείων κοντά στους αισθητήρες μειώνεται το απαιτούμενο εύρος ζώνης δικτύου και αυξάνεται ο χρόνος απόκρισης του συστήματος. Έτσι, αυτές οι προσεγγίσεις μπορούν να χρησιμοποιηθούν για προσεγγίσεις αιχμής όπως η αυτόματη πλοήγηση με drone ή η αυτόματη αναδιάταξη του οπτικού πεδίου.

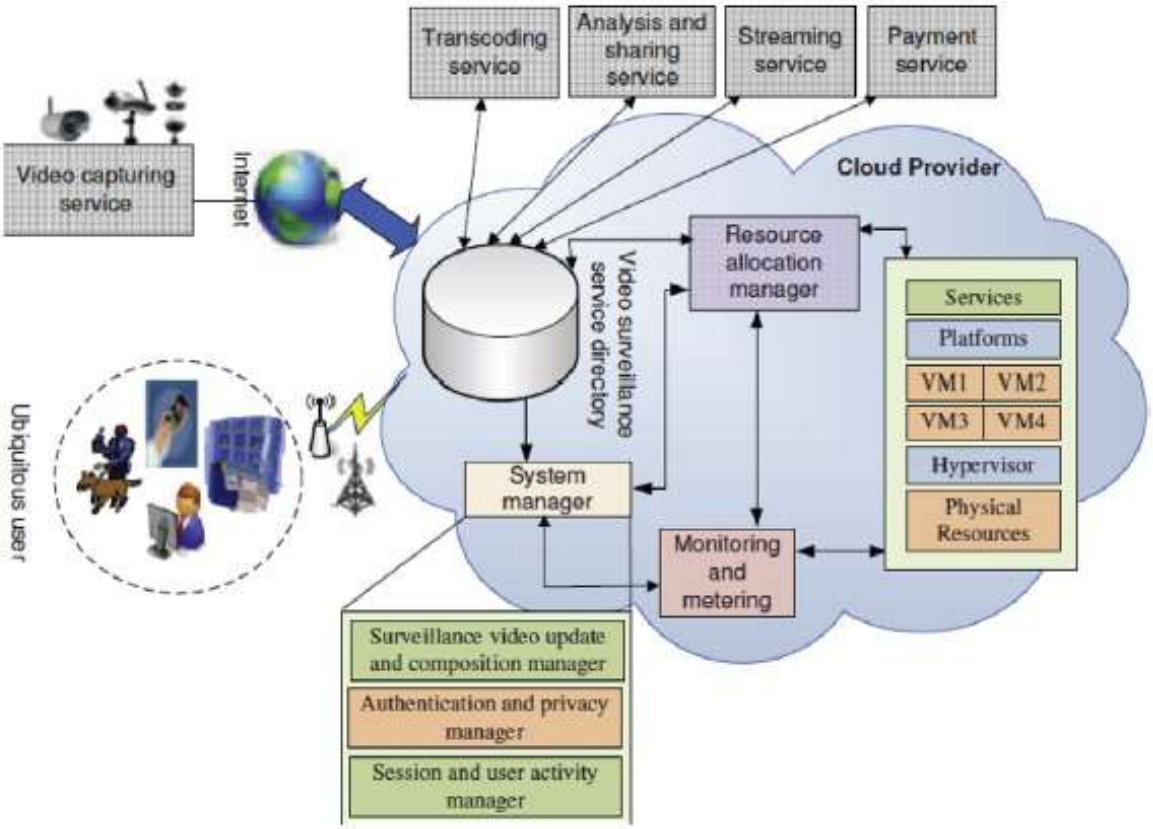
Η απόκριση σε πραγματικό χρόνο – ή σχεδόν σε πραγματικό χρόνο – είναι ίσως ο πιο σημαντικός παράγοντας όσον αφορά στα συστήματα παρακολούθησης. Η αυτόματη ειδοποίηση για ένα συγκεκριμένο συμβάν είναι πολύτιμη μόνο όταν πραγματοποιείται εντός ενός χρονικού διαστήματος μετά το πραγματικό συμβάν. Σήμερα, έχουν σχεδιαστεί και αναπτυχθεί συστήματα παρακολούθησης που πληρούν τις προαναφερθείσες απαιτήσεις σε όλο τον κόσμο. Ωστόσο, η φύση των γεγονότων που αναγνωρίζονται αυτόματα από τα συστήματα είναι μάλλον ασήμαντη, συμπεριλαμβανομένης της μετακίνησης αντικειμένων, της ύπαρξης πυρκαγιάς ή της αναγνώρισης αντικειμένων. Παρόλα αυτά, τα συστήματα επιτήρησης αντιμετωπίζουν σήμερα μία σειρά προκλήσεων, οι οποίες περιλαμβάνουν ανίχνευση τροχαίων ατυχημάτων, πρόβλεψη τρομοκρατικών δραστηριοτήτων ή ανάλυση συμπεριφοράς πολλαπλών χρήσεων. Αυτά τα συμβάντα απαιτούν σημαντικά μεγαλύτερους υπολογιστικούς πόρους, καθώς περιλαμβάνουν πολύπλοκους υπολογισμούς και μη γραμμικά μοντέλα. Επιπλέον, οι σύγχρονοι αισθητήρες βίντεο είναι σε θέση ώστε να καταγράφουν πλάνα υψηλής ανάλυσης, τα οποία διευκολύνουν τους αλγόριθμους και τα χειριστήρια ανίχνευσης συμβάντων, π.χ. σε κάποιο σημείο, με κακές συνθήκες φωτισμού κλπ.

Το αποτέλεσμα της ενσωμάτωσης τέτοιων αισθητήρων σε συστήματα επιτήρησης είναι ο πολλαπλασιασμός των παραγόμενων ρυθμών δεδομένων και κατά συνέπεια η αύξηση του απαιτούμενου μεγέθους αποθήκευσης. Και οι δύο απαιτήσεις για πρόσθετες υπολογιστικές δυνατότητες και αύξηση του μεγέθους αποθήκευσης θα μπορούσαν να αντιμετωπιστούν με την ολοκλήρωση συστημάτων παρακολούθησης, με υποδομές cloud. Όσο ελπιδοφόρα ακούγεται αυτή η δυνατότητα, δεν υπάρχουν πολλά αναφερόμενα συστήματα παρακολούθησης στη βιβλιογραφία, τα οποία χρησιμοποιούν υπηρεσίες cloud, είτε ως SaaS

[87] Βλέπε επίσης, μεταξύ άλλων: https://en.wikipedia.org/wiki/Software_as_a_service
[88] https://en.wikipedia.org/wiki/Fog_computing

(Λογισμικό ως υπηρεσία), ως PaaS (Πλατφόρμα ως υπηρεσία) είτε ως IaaS (Υποδομή ως υπηρεσία)[89].

Ένα σχήμα κατανομής πόρων για τη διαχείριση υπηρεσιών σε συστήματα παρακολούθησης που βασίζονται σε cloud περιγράφεται από τους Hossain & Mehedi[90], όπου οι πόροι VM (Εικονικές μηχανές) συντονίζονται με βάση τις απαιτήσεις QoS, όπως απεικονίζεται στο παρακάτω σχήμα.



Εικόνα 6-10: Προτεινόμενη εννοιολογική αρχιτεκτονική νέφους για CCTV

Ένα από αυτά τα έργα αναφέρεται στην βιβλιογραφία [189], όπου η προτεινόμενη υποδομή cloud χρησιμοποιείται ως SaaS και επικεντρώνεται κυρίως σε ζητήματα αποθήκευσης, χρησιμοποιώντας την πλατφόρμα Amazon S3[91]. Στο ίδιο θέμα, περιγράφεται ένα σύστημα παρακολούθησης για συστήματα αστικής κυκλοφορίας, το οποίο είναι σε θέση να επεξεργάζεται τεράστια δεδομένα πλωτών αυτοκινήτων που προέρχονται από ταξί της

[89] Για περισσότερα στοιχεία βλέπε επίσης την προσέγγιση που παρατίθεται στην ιστοσελίδα: https://www.redhat.com/en/topics/cloud-computing/iaas-vs-paas-vs-saas?sc_cid=7013a000002pgRXAAY&gclid=EAIaIQobChMIxunO69eX8wIVVYODBx2mQAmWEAAYASAAEgJXmvD_BwE&gclsrc=aw.ds

90 Rodríguez-Silva, D.A., Adkinson-Orellana, L., González-Castaño, F.J., Armiño-Franco, I., and González-Martínez, D. (2012): Video surveillance based on cloud storage. In Proceedings of the IEEE fifth International Conference on Cloud Computing, pp.991-992. Honolulu, HI, USA, 2012.

[91] Περισσότερα σχετικά στοιχεία μπορούν να βρεθούν στον ιστότοπο https://aws.amazon.com/es/s3/

πόλης. Το Bigtable και το MapReduce διερευνώνται ως τεχνολογίες cloud όχι μόνο για σκοπούς αποθήκευσης αλλά και για υπολογιστικές διαδικασίες [187].

6.5 Ανίχνευση Σεισμικών Δονήσεων

Πρόγνωση σεισμού είναι η πρόβλεψη, με σιγουριά, ότι συγκεκριμένου μεγέθους σεισμός πρόκειται να συμβεί σε συγκεκριμένο τόπο και σε συγκεκριμένο χρονικό πλαίσιο. Η πρόγνωση που αφορά τους σεισμούς που γεννώνται με φυσικές διαδικασίες στον γήινο φλοιό δεν έχει επιτευχθεί ως σήμερα, υπήρξαν και υπάρχουν όμως προσπάθειες προς την κατεύθυνση αυτή. Θεωρείται, *από μερίδα επιστημόνων*, απίθανο να υπάρξει πρόβλεψη σεισμών με χρονική ακρίβεια μεγαλύτερη του ενός ή δύο ετών ή ίσως και χρονική ακρίβεια δεκαετίας και από πολλούς τίθεται επίσης υπό αμφισβήτηση η ίδια η σκοπιμότητα πιο βραχυπρόθεσμων προβλέψεων. Η προσπάθεια για βραχυπρόθεσμη πρόγνωση έχει επικεντρωθεί κυρίως στην αναζήτηση και μελέτη των αξιοποιήσιμων παραμέτρων πρόδρομων σεισμικών φαινομένων, όπως είναι η ανίχνευση δονήσεων, η αλλαγή ηλεκτρομαγνητικά προσεισμικών σημάτων και ο έλεγχος απόκλισης της αναμενόμενης θερμοκρασίας του εδάφους με δορυφόρους [193].

Τα τελευταία χρόνια, οι σεισμολόγοι έχουν υιοθετήσει τους αισθητήρες επιτάχυνσης χαμηλούς κόστους που βρίσκονται ενσωματωμένοι στα έξυπνα κινητά, για την ανίχνευση σεισμών. Η εφαρμογή "Myshake"[92] είναι μία από τις πιο πρόσφατες συνεισφορές που χρησιμοποιεί το έξυπνο κινητό, στην ανίχνευση σεισμών. Ο αισθητήρας του κινητού τηλεφώνου καταγράφει τα δεδομένα χρησιμοποιώντας το τηλέφωνο του χρήστη, στη συνέχεια τα επεξεργάζεται και χρησιμοποιώντας το ασύρματο δίκτυο κινητής τηλεφωνίας τα στέλνει σε έναν κεντρικό διακομιστή. Η εφαρμογή MyShake εκτελείται σε smartphone εθελοντών στους οποίους ζητείται να εγκαταστήσουν την εφαρμογή και είναι το πρώτο παγκόσμιο σύστημα συναγερμού σεισμού που χρησιμοποιεί ασύρματους αισθητήρες έξυπνων κινητών τηλεφώνων. Ωστόσο, επειδή το MyShake βασίζεται σε μεγάλο βαθμό στα εθελοντικά smartphone, όταν τα smartphone είναι σε ενεργή λειτουργία, δεν μπορούν να χρησιμοποιηθούν ως σεισμικός σταθμός ή ανιχνευτής σεισμών. Επιπλέον, το μοντέλο ανίχνευσης σεισμών που έχει βασιστεί σε ανθρώπινες δραστηριότητες, δεν μπορεί να διακρίνει ανάμεσα σε σεισμούς και διάφορους τύπους δονήσεων που δημιουργούνται από κτίρια [194].

Παρομοίως, το Quake-Catcher Network [195] το οποίο ξεκίνησε από το Πανεπιστήμιο του Στάνφορντ χρησιμοποιεί μικρό-ηλεκτρομηχανικούς αισθητήρες (MicroElectric Mechanical Sensors – MEMS) επιτάχυνσης χαμηλού κόστους για την ανίχνευση σεισμών. Αισθητήρες εγκαταστάθηκαν σε κτίρια κατοικιών σε όλη την Καλιφόρνια και ανιχνεύουν σεισμικές δονήσεις αποστέλλοντας τα δεδομένα σε κεντρικούς διακομιστές για περαιτέρω επεξεργασία. Σημαντικό και αξιοσημείωτο πλεονέκτημα είναι το χαμηλό κόστος των αισθητήρων MEMS. Άλλες χώρες όπως η Ιαπωνία, η Ιταλία και η Ταϊβάν έχουν αναπτύξει επίσης συστήματα έγκαιρης προειδοποίησης όπου χρησιμοποιούν αισθητήρες MEMS, όπως το HSN (Home Seismometer Network) που αναπτύχθηκε από την Ιαπωνική Μετεωρολογική

[92] Για περισσότερα στοιχεία βλέπε επίσης: https://myshake.berkeley.edu/

Υπηρεσία (Japan Meteorological Agency[93] - JMA) και το δίκτυο αισθητήρων MEMS από το INGV (Intituto Nazionale di Geofisica e Vulcanologia[94]) στην Ιταλία.

6.5.1 Ανίχνευση Κραδασμών με Χρήση Ανιχνευτών Επιτάχυνσης

Εκτός της πρόγνωσης της σεισμικής δραστηριότητας, μία από τις τεχνολογίες που χρησιμοποιούνται για την επίβλεψη της ασφάλειας υποδομών είναι η παρακολούθηση κραδασμών. Οι αισθητήρες κραδασμών μπορούν να χρησιμοποιηθούν για να δώσουν πληροφορίες σχετικά στοιχεία που σχετίζονται με βλάβη μηχανικών εξοπλισμών, επιτρέποντας την πρόληψη κατάρρευσης μεγάλων κρίσιμων μονάδων. Η παρακολούθηση της κατάστασης ενός μηχανήματος σημαίνει τη χρήση προηγμένων τεχνολογιών, προκειμένου να καθοριστεί η κατάσταση του εξοπλισμού και ενδεχομένως να προβλεφθεί πιθανή αποτυχία χρήσης. Προς το παρόν, το πεδίο μίας τέτοιας παρακολούθησης περιορίζεται από το κόστος, είτε αυτό αφορά στο κόστος μόνιμης εγκατάστασης αισθητήρων είτε στο κόστος συλλογής δεδομένων. Νέες εξελίξεις στην εφαρμογή ασύρματων αισθητήρων για καταγραφή κραδασμών προσφέρουν τη δυνατότητα μίας πιο οικονομικά αποδοτικής προσέγγισης, η οποία θα μπορούσε να αλλάξει δραματικά την παρακολούθηση κραδασμών [196].

Ένα επιταχυνσιόμετρο είναι ένας αισθητήρας δόνησης ο οποίος μετρά την επιτάχυνση ανάλογα με τη δύναμη που ασκείται σε ένα αντικείμενο και που το κάνει να αλλάξει τη θέση ή την ταχύτητά του. Τα επιταχυνσιόμετρα παρέχουν πληροφορίες σχετικά με τις δυνάμεις που ένας αισθητήρας βιώνει κατά τη διάρκεια μίας κρουστικής δραστηριότητας. Επίσης, είναι εύχρηστοι αισθητήρες μικρού μεγέθους, συνήθως <100 mm, έτσι ώστε να μπορούν εύκολα να τοποθετηθούν σε βασικές θέσεις σε μία δομή. Τα σήματα επιτάχυνσης μπορούν να ληφθούν από έναν υπολογιστή, ο οποίος θα επεξεργαστεί και θα εξομαλύνει τον θόρυβο και ακολούθως θα εξάγει συμπεράσματα σχετικά με το κατώφλι ασφαλείας που έχει οριστεί.

Ένα ασύρματο δίκτυο αισθητήρων έχει αναπτυχθεί για το ερευνητικό έργο που ονομάζεται WiVib και αφορά στην ανίχνευση κραδασμών [197]. Ένας κόμβος μετρά περιοδικά τη δόνηση ενός κινητήρα και μεταδίδει τα δεδομένα σε έναν σταθμό βάσης, χρησιμοποιώντας το πρότυπο WirelessHART το οποίο είναι βασισμένο στην τεχνολογία ασύρματης μετάδοσης IEEE802.15.4 στο εύρος ζώνης 2.4GHz. Ο κόμβος αισθητήρα περιέχει ηλεκτρονικά που επεξεργάζονται το ακατέργαστο σήμα και τα οποία μειώνουν την ποσότητα των δεδομένων που πρέπει να διαβιβαστούν. Η ανάλυση πραγματοποιείται από τον διακομιστή, ο οποίος χρησιμοποιεί ένα εργαλείο οπτικοποίησης του ασύρματου δικτύου και ένα λογισμικό ανάλυσης των δεδομένων.

Εκτός από το υψηλό κόστος εγκατάστασης για ενσύρματες και υπάρχοντες ασύρματες λύσεις, η τιμή ανά μονάδα αισθητήρα είναι επίσης σημαντική. Οι σημερινές λύσεις χρησιμοποιούν συμβατικούς αισθητήρες, είτε επιτάχυνσης είτε πιεζοηλεκτρικούς. Αυτοί οι αισθητήρες είναι κατάλληλοι όσον αφορά στην απόδοση, αλλά είναι αρκετά ογκώδεις και

[93] https://www.jma.go.jp/jma/indexe.html
[94] https://www.ingv.it/

δαπανηροί. Στο πλαίσιο αυτό αυξάνεται το ενδιαφέρον για αντικατάσταση τέτοιων συμβατικών αισθητήρων με αισθητήρες MEMS, οι οποίοι πλεονεκτούν ως προς την απόδοση αλλά και ως προς το δυναμικό εύρος και την μέγιστη μετρήσιμη επιτάχυνση. Ο αισθητήρας MEMS μπορεί να παρακολουθεί την κατάσταση ενός κινητήρα και να μετράει ένα ευρύ φάσμα κραδασμών. Για παράδειγμα, εάν σε έναν κινητήρα υπάρχουν ελαττωματικά ρουλεμάν θα εμφανιστεί ένα σήμα χαμηλής συχνότητας, συνήθως στην περιοχή 1–5 Hz [196].

6.6 Ανίχνευση Πλημμυρών με τη Χρήση WSN

Η ακριβής εκτίμηση της πλημμύρας είναι ένα σημαντικό πρόβλημα για τις υποδομές οι οποίες βρίσκονται σε παράκτιες περιοχές. Σε υπεράκτιες περιοχές, τα ακριβή παλιρροιακά δεδομένα είναι πολύ χρήσιμα για μία επιτυχημένη πολιτική ασφαλείας και τα ασύρματα δίκτυα αισθητήρων μπορεί να παρέχουν ποικιλία εφαρμογών. Σε μία στοχευμένη περιοχή, όλοι οι κόμβοι είναι έμμεσα συνδεδεμένοι και επιπλέον, η ανταλλαγή δεδομένων πραγματοποιείται με σύστημα επικοινωνίας πολλαπλών αλμάτων (hops). Οι περιβαλλοντικές καταστροφές είναι τυχαίες και «γιγαντώνονται» σε πολύ σύντομα χρονικά διαστήματα, επομένως, η τεχνολογία που χρησιμοποιείται πρέπει να είναι ικανή να συλλάβει κατάλληλα σήματα, με ελάχιστη διακοπή λειτουργίας. Έτσι, ο ασύρματος αισθητήρας είναι μία από τις σύγχρονες τεχνολογίες που μπορεί να αντιδρά γρήγορα σε απόκριση ταχείας παραλλαγής δεδομένων, και να στέλνει τα δεδομένα αυτά σε κέντρο ανάλυσης δεδομένων, σε περιοχές όπου δεν είναι δυνατή η καλωδίωση.

Το βυθιζόμενο δίκτυο αισθητήρων (Underwater Wireless Sensor Network[95] – UWSN) μπορεί να χρησιμοποιηθεί για παρακολούθηση δεδομένων σε πραγματικό χρόνο, με βυθιζόμενους στεγανούς ασύρματους αισθητήρες που επικοινωνούν συνεχώς με τον σταθμό ελέγχου και προειδοποιούν για μεταβολές κυματισμού στην στάθμη υγρών μέσων ή θαλάσσιων περιοχών. Ωστόσο, αυτός ο τύπος ασύρματης επικοινωνίας ξοδεύει πάρα πολύ ενέργεια λόγω των υποθαλάσσιων μεταδόσεων που απαιτούν μεγάλη ισχύ, και έτσι εάν και τα πακέτα δεδομένων είναι μεγάλα, η λύση μπορεί να εφαρμοστεί μόνο σε μικρές αποστάσεις [198].

Εκτός των συστημάτων ανίχνευσης παράκτιας πλημμύρας η παλίρροιας, πολλά από τα νέα έξυπνα δίκτυα ενσωματώνουν ανιχνευτές διαρροής νερού και υγρών γενικά. Αυτοί οι αισθητήρες μπορούν να τοποθετηθούν κοντά σε σημαντικές συσκευές που πρέπει να προστατεύονται ή σε πηγές πιθανής διαρροής όπως βιομηχανικά μηχανήματα, πλυντήρια, δεξαμενές, ψυκτικά μηχανήματα, σωλήνες δικτύων υδροδότησης, τα οποία βρίσκονται σε κάθε χώρο και η σημασία της έγκαιρης ανίχνευσης διαρροής είναι ζωτικής σημασίας για αποφυγή κρίσιμων καταστάσεων. Οι περισσότεροι ασύρματοι έξυπνοι αισθητήρες διαρροής, λειτουργούν με μπαταρία και περιλαμβάνουν χαμηλής ισχύος ασύρματη τεχνολογία. Το WSN εξαλείφει την ανάγκη ενσύρματων κόμβων αισθητήρων και μειώνει την εγκατάσταση και το κόστος συντήρησης.

[95] Βλέπε: https://encyclopedia.pub/3316

Ένας κόμβος αισθητήρα διαρροής περιλαμβάνει όλα τα απαραίτητα κυκλώματα για τον εντοπισμό της παρουσίας νερού, δηλαδή μια μπαταρία, έναν μικροελεγκτή 16bit για τον έλεγχο του αναλογικού σήματος, έναν ακροδέκτη για την εκτέλεση αναλογικών μετρήσεων και την ανίχνευση της στάθμης του νερού, μία μονάδα εκπομπής RF (ραδιοσυχνότητα) και ένα βομβητή για να προειδοποιήσει τον χρήστη τοπικά κατά την παρουσία νερού. Η συσκευή μπορεί επίσης να περιέχει έναν ηλεκτρονικό διακόπτη προστασίας για ανοίγματος στο καπάκι ή μεταφοράς της συσκευής (tamper). Και στην περίπτωση τέτοιων ανιχνευτών, για τον σχεδιασμό του ασύρματου κόμβου λαμβάνεται υπόψη το χαμηλό κόστος, η κατανάλωση της ενέργειας και το μικρό μέγεθος [199].

6.7 Συστήματα Πυρανίχνευσης

Το ευρωπαϊκό πρότυπο EN 54 έχει συνταχθεί από την Ευρωπαϊκή Επιτροπή Τυποποίησης CEN/TC72[96] (Comité Européen de Normalization - CEN) και αποτελείται από μία σειρά παραγράφων που περιλαμβάνουν πρότυπα προϊόντων και οδηγίες εφαρμογής για συστήματα πυρανίχνευσης και συναγερμού πυρκαγιάς, καθώς και για συστήματα φωνητικής προειδοποίησης[97]. Τα πρότυπα προϊόντων καθορίζουν τα χαρακτηριστικά του προϊόντος, τις μεθόδους δοκιμής και τα κριτήρια απόδοσης βάσει των οποίων μπορεί να αξιολογηθεί και να δηλωθεί η αποτελεσματικότητα και η αξιοπιστία κάθε στοιχείου του συστήματος πυρανίχνευσης και συναγερμού πυρκαγιάς.

Ένα σύγχρονο σύστημα πυρανίχνευσης περιλαμβάνει απαραίτητα ένα επαρκές δίκτυο ανιχνευτών, που θα είναι κατάλληλοι για την κάθε περίπτωση και θα εξασφαλίζουν επαρκή αξιοπιστία. Η πυρανίχνευση (δηλαδή η διέγερση ενός κατάλληλου αισθητηρίου συστήματος), θα έχει σαν άμεσο αποτέλεσμα τη σήμανση (οπτική, ακουστική κλπ.) και παράλληλα, εάν υπάρχει σχετική εγκατάσταση, θα θέσει σε λειτουργία κάποιον μηχανισμό κατασβέσεως. Η πυρανίχνευση βασίζεται σε ειδικούς ανιχνευτές (ιονισμού, θερμοκρασίας, φλόγας, ορατού καπνού ή θερμοδιαφορικούς) και σε κομβία (μπουτόν) που είναι τοποθετημένα σε επίκαιρα σημεία και επιτρέπουν χειροκίνητη ενεργοποίηση του συστήματος [200].

Οι ανιχνευτές αυτοί και τα κομβία συναγερμού πυρκαγιάς, συνδέονται με ηλεκτρικούς αγωγούς με τα κέντρα ανιχνεύσεως. Τα κέντρα ανιχνεύσεως τοποθετούνται σε επιλεγμένα σημεία μετά από προσεκτική μελέτη του συγκεκριμένου κτιριακού συγκροτήματος ή των συγκροτημάτων. Ο ανιχνευτές πυρκαγιάς τοποθετούνται επί της οροφής του χώρου τον οποίο πρόκειται να προστατεύσουν. Κάθε ομάδα ανιχνευτών αποτελεί μία ιδιαίτερη ζώνη ή βρόχο κυκλώματος που καταλήγει στο κέντρο ανιχνεύσεως πυρκαγιάς και το κύκλωμα διαρρέεται μονίμως από τάση συνεχούς ρεύματος. Ομοίως ανά ομάδες, ανεξάρτητες από αυτές των ανιχνευτών, είναι συνδεδεμένα τα κομβία χειροκίνητης αναγγελίας, ώστε και αυτά να καταλήγουν στο κέντρο ανιχνεύσεως πυρκαγιάς.

Μόλις οι ανιχνευτές ή τα κομβία που είναι συνδεδεμένα στο σύστημα ενεργοποιηθούν, στον κεντρικό πίνακα αναγγέλλεται κατάσταση «συναγερμού» (Alarm) ο οποίος εκφράζεται

[96] Βλέπε επίσης: https://standards.iteh.ai/catalog/tc/cen/6c7335ad-adf5-4c3f-a2b6-ee55036462f3/cen-tc-72
[97] BSI Shop - Buy British Standards. https://shop.bsigroup.com/

μέσω των συνδεδεμένων φάρων και σειρήνων, οπτικά και ακουστικά. Ο συναγερμός μπορεί επίσης να μεταδοθεί είτε σε άλλο επαναληπτικό πίνακα ή απευθείας στην Πυροσβεστική Υπηρεσία.

Τα είδη των ανιχνευτών πυρκαγιάς που θα συναντήσουμε σε ένα σύστημα είναι συνοπτικά τα παρακάτω [200]:

- **Ανιχνευτές ιονισμού:** Αντιδρούν χημικά στα ορατά και αόρατα προϊόντα (ιόντα) της καύσεως. Οι ανιχνευτές ιονισμού έχουν ευρύτατες εφαρμογές, π.χ. μεγάλα καταστήματα, βιομηχανίες, ξενοδοχεία, νοσοκομεία, δημόσια κτίρια κλπ.

- **Ανιχνευτές ορατού καπνού:** Αντιδρούν ανιχνεύοντας οπτική διάθλαση λόγω καπνού (ή άλλου μέσου στην ατμόσφαιρα).

- **Ανιχνευτές θερμικού ορίου**: Αντιδρούν όταν η θερμοκρασία του αέρα ενός χώρου φθάσει ένα προκαθορισμένο σημείο (ανάλογα με τη χρήση), π.χ. 70°C. Οι δυνατότητες εφαρμογής τους είναι περιορισμένες. Για να φθάσει η θερμοκρασία σε αυτό το ύψος, χρειάζεται συνήθως να προχωρήσει η διαδικασία της καύσεως και έτσι οι ανιχνευτές αυτοί χρησιμοποιούνται σε σπάνιες περιπτώσεις. Μία πιθανή εφαρμογή τους είναι σε μηχανοστάσια κεντρικής θέρμανσης.

- **Θερμοδιαφορικοί ανιχνευτές**: Αντιδρούν όταν ο ρυθμός αύξησης της θερμοκρασίας αυξάνεται με συγκεκριμένη ταχύτητα (π.χ. η θερμοκρασία μέσα σε προκαθορισμένα χρονικά όρια ανεβαίνει, κατά 10°C). Και εδώ συναντώνται τα ίδια μειονεκτήματα όπως στους ανιχνευτές μέγιστης θερμοκρασίας, χρειάζεται δηλαδή φωτιά σχετικά μεγάλων διαστάσεων ώστε να γίνει ανίχνευση της αυξανόμενης θερμοκρασίας και έτσι χρησιμοποιούνται μόνο εκεί όπου ένας οπτικός ανιχνευτής δεν ενδείκνυται, για λόγους που σχετίζονται με τη χρήση του χώρου και τις συνθήκες λειτουργίας των εγκαταστάσεων (π.χ. σκόνη).

- **Ανιχνευτές φλόγας:** Ανιχνεύουν οπτικά τη φλόγα και αντιδρούν στη συχνότητα της πόλωσης που παρουσιάζει. Χρησιμοποιούνται πάντα σε συνδυασμό με άλλους ανιχνευτές για την αύξηση του επιπέδου ασφαλείας σε ένα σύστημα πυρανίχνευσης.

Όσο αφορά στην μετάβαση των οικοσυστημάτων πυρανίχνευσης στην τάση που πλέον ονομάζεται 4η βιομηχανική επανάσταση[98] (Industry 4.0), εντός της επόμενης δεκαετίας θα συναντήσουμε τα παρακάτω χαρακτηριστικά [201]:

Τεχνητή Νοημοσύνη

Η τεχνητή νοημοσύνη, τα συνδεδεμένα συστήματα και η αρχιτεκτονική των έξυπνων πόλεων θα προκαλέσουν μία δημιουργική επανάσταση στα συστήματα πυρανίχνευσης, τα

[98] Βλέπε επίσης τα στοιχεία που παρατίθενται στον ιστότοπο: https://el.wikipedia.org/wiki/%CE%92%CE%B9%CE%BF%CE%BC%CE%B7%CF%87%CE%B1%CE%BD%CE%AF%CE%B1_4.0

οποία πλέον θα λειτουργούν ως ενιαία συστήματα και τα οποία ενώ θα βρίσκονται αρκετά απομακρυσμένα το ένα από το άλλο θα μπορούν να ανταλλάσσουν πληροφορίες σε περιβάλλον cloud και να αλληλοεπιδρούν.

IoT στα Συστήματα Πυρανίχνευσης

Η πυρασφάλεια είναι ένας από τους τεχνολογικούς τομείς που μπορούν να πραγματοποιήσουν τα εξαιρετικά πλεονεκτήματα του Internet of Things. Το Διαδίκτυο των πραγμάτων οδήγησε μεγάλο μέρος του κόσμου να γίνει πιο έξυπνο και συνδεδεμένο. Με το IoT, οι ειδοποιήσεις ασφαλείας θα μπορούν να σταλούν σε εκατοντάδες άτομα, γρήγορα και αποτελεσματικά. Αρκετές κορυφαίες εταιρείες πυρανίχνευσης έχουν ήδη ξεκινήσει ανιχνευτές πυρκαγιάς με δυνατότητα σύνδεσης στο IoT.

IoT Αυτόνομοι Ανιχνευτές Μονοξειδίου του Άνθρακα

Υπάρχουν πολλές κορυφαίες εταιρείες στην αγορά που προσφέρουν συνδεδεμένους ανιχνευτές καπνού και ανιχνευτές μονοξειδίου του άνθρακα, για οικιακή χρήση. Αυτοί οι συνδεδεμένοι ανιχνευτές λειτουργούν ως αυτόνομες μονάδες συνδεδεμένες σε παροχή 220V και είναι σε θέση ώστε να επικοινωνούν με τον άλλες συσκευές IoT του χώρου και να αλληλοεπιδρούν. Για παράδειγμα σε επικοινωνία με τον θερμοστάτη μπορούν να κλείσουν τον λέβητα θέρμανσης σε περίπτωση πυρκαγιάς ή διαρροής μονοξειδίου του άνθρακα. Οι ανιχνευτές είναι προσβάσιμοι οπουδήποτε, χρησιμοποιώντας εφαρμογές για κινητά. Σε περίπτωση συναγερμού, οι ανιχνευτές ηχούν έναν τοπικό συναγερμό και στέλνουν ειδοποιήσεις στο κινητό τηλέφωνο του χρήστη.

Διασυνδεδεμένα Συστήματα

Όλο και περισσότεροι ιδιοκτήτες και διαχειριστές εγκαταστάσεων συνειδητοποιούν τα οφέλη της διασύνδεσης-ενοποίησης (integration) όλων των κτιριακών συστημάτων, όπως τα συστήματα μαζικής ειδοποίησης και ασφάλειας. Ένα ενοποιημένο σύστημα μαζικής ειδοποίησης (MNS) ορίζεται ως πλατφόρμα για την παράδοση ενός μηνύματος σε μία μικρή ή μεγάλη ομάδα ανθρώπων. Παραδοσιακά, αυτά τα συστήματα προσέφεραν μονόδρομη παράδοση μηνυμάτων μέσω email, γραπτού μηνύματος ή μηχανισμών κλήσεων. Με την ενοποίηση αυτών των συστημάτων, οι χρήστες μπορούν να έχουν την εποπτεία και τη διαχείριση πολλαπλών συστημάτων όπως πυρανίχνευση, CCTV, σύστημα αντικλεπτικού συναγερμού, HVAC, από ένα μόνο σημείο ελέγχου.

Δεδομένα Μεγάλης Κλίμακας (Big Data)

Με τα εργαλεία που μας παρέχει η ανάλυση δεδομένων μεγάλης κλίμακας (Big Data) και με άλλες προηγμένες τεχνολογίες, μπορούν να επιτευχθούν βελτιώσεις στον σχεδιασμό δράσης έκτακτης ανάγκης. Τα δεδομένα των αισθητήρων και των ανιχνευτών συλλέγονται και αναλύονται και με την χρήση αλγορίθμων βοηθούν στην προετοιμασία αποτελεσματικότερων σχεδίων έκτακτης ανάγκης ή εκκένωσης. Η ανάλυση μπορεί να εξετάσει διάφορους παράγοντες, όπως ο αριθμός των ατόμων στο κτίριο, οι χάρτες κτιρίων, η τοποθεσία της πυρκαγιάς, ο ρυθμός με τον οποίο εξαπλώνεται η φωτιά και η κατεύθυνση της πυρκαγιάς για να προκύψουν καλύτερα σχέδια εκκένωσης τα οποία αποτρέπουν την συμφόρηση και διασφαλίζουν γρήγορη και αποτελεσματική εκκένωση ενός χώρου.

Ασύρματες Τεχνολογίες

Η ασύρματη τεχνολογία συνεχίζει να εξαπλώνεται ευρέως στον κλάδο της ασφάλειας, ενώ ο συναγερμός πυρκαγιάς δεν αναμένεται να παραμείνει στο περιθώριο. Σήμερα, οι ασύρματοι ανιχνευτές καπνού έρχονται σε πιο συμπαγή και απλοποιημένα σχέδια που μπορούν να είναι πιο ελκυστικά αισθητικά.

Στην παρούσα εργασία, μας απασχολεί η συμβολή των WSN στον τομέα της φυσικής ασφάλειας, στον οποίο περιέχονται και τα πολύ σημαντικά συστήματα πυρανίχνευσης. Στα επόμενο κεφάλαιο θα δούμε πως μπορεί να υλοποιηθεί ένα σύστημα πυρανίχνευσης βασισμένο στα ασύρματα δίκτυα και στο IoT.

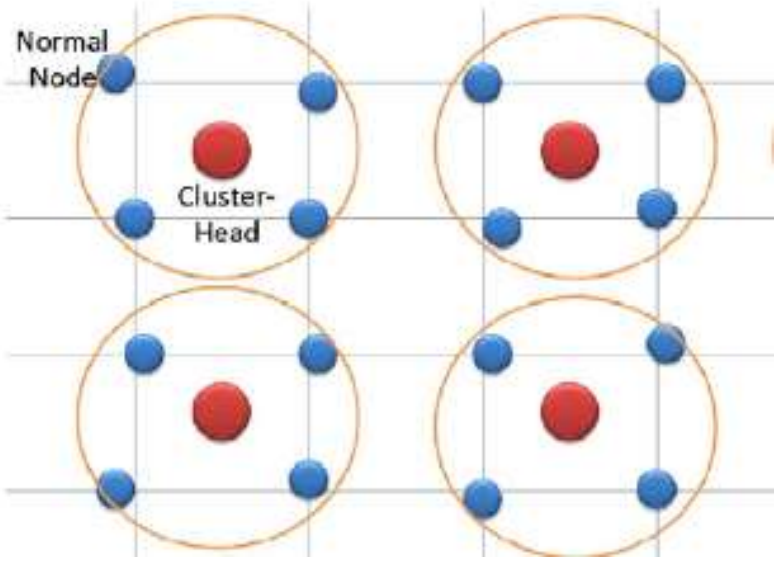
6.7.1 Συστήματα Πυρανίχνευσης βασισμένα σε WSNs

Ως μία πολλά υποσχόμενη εναλλακτική λύση, τα ασύρματα δίκτυα αισθητήρων (WSNs) είναι μία αναδυόμενη τεχνολογία που μπορεί να χρησιμοποιηθεί για την ανίχνευση δασικών πυρκαγιών και συναφών δραστηριοτήτων. Όπως ήδη γνωρίζουμε, ένα ασύρματο δίκτυο αισθητήρων αποτελείται από μικρούς αισθητήρες με μπαταρία και χαμηλού κόστους κόμβους που έχουν τη δυνατότητα ανίχνευσης, επεξεργασίας και ασύρματης σύνδεσης επικοινωνίας (Shyam & Kumar, 2010). Ασύρματοι κόμβοι αισθητήρων που αναπτύσσονται σε ένα δάσος μπορούν να συλλέγουν δεδομένα και να τα αποδίδουν σε ακατέργαστη ή επεξεργασμένη μορφή σε ένα κέντρο μέσω ενός σταθμού βάσης, όπου τα εισερχόμενα δεδομένα μπορούν να αναλυθούν αυτόματα. Σαν αποτέλεσμα, μπορούν να εντοπιστούν πυρκαγιές και κάποια άλλα συναφή συμβάντα χωρίς να απαιτούνται χειροκίνητες, ανθρωποκεντρικές λειτουργίες [202].

Ωστόσο, υπάρχουν πολλά ζητήματα που πρέπει να λάβουμε υπόψη και να επιλύσουμε κατά τη χρήση της ασύρματης σύνδεσης δίκτυών αισθητήρων για την παρακολούθηση και την ανίχνευση δασικών πυρκαγιών. Εκτός των περιορισμένων ενεργειακών πόρων που έχουν πολλές φορές αναφερθεί στην παρούσα διατριβή, ένα άλλο παράδειγμα είναι οι περιβαλλοντικές συνθήκες σε μία κατάσταση πυρκαγιάς οι οποίες μπορούν να περιορίσουν την επιτυχία του εκτεταμένου συστήματος πυρανίχνευσης που βασίζεται σε ασύρματα δίκτυα αισθητήρων. Έτσι, απαιτείται συνεχής επιτήρηση ολόκληρης της προστατευόμενης περιοχής και αυτό μπορεί να προκαλέσει υπερβολική κατανάλωση ενέργειας, εάν δεν σχεδιαστεί προσεκτικά. Αν ξεπεράσουμε τους παραπάνω προβληματισμούς με επιτυχία, τότε το WSN μπορεί να ανιχνεύσει και να προβλέψει αποτελεσματικότερα τη δασική πυρκαγιά σε σύγκριση με την παραδοσιακή δορυφορική προσέγγιση, καθώς η παρακολούθηση της πυρκαγιάς μέσω δορυφορικής απεικόνισης είναι μεν μία δημοφιλής τεχνική, αλλά ο μεγάλος χρόνος σάρωσης και η χαμηλή ανάλυσή της μπορούν να περιορίσουν την αποτελεσματικότητα της δορυφορικής μεθόδου ανίχνευσης πυρκαγιάς. Επιπλέον, το δορυφορικό σύστημα δεν μπορεί να προβλέψει τη δασική πυρκαγιά πριν από τη διάδοση της φωτιάς.

Σε ένα ασύρματο δίκτυο αισθητήρων, μεγάλος αριθμός αισθητήρων αναπτύσσεται πυκνά στη δασική περιοχή. Οι κόμβοι αισθητήρα συλλέγουν τα δεδομένα που ανιχνεύονται όπως

θερμοκρασία, υγρασία, καπνός κλπ. και στέλνουν τις πληροφορίες που συλλέγονται από αυτά τα δεδομένα στον σχετικό κόμβο συμπλέγματος (cluster node), ο οποίος στέλνει περαιτέρω τα δεδομένα στην κεφαλή συμπλέγματος (cluster head) σχηματίζοντας ένα δίκτυο. Οι κόμβοι αισθητήρα που αναπτύσσονται στο πεδίο επικοινωνούν μεταξύ τους χρησιμοποιώντας συνδέσμους RF. Η κεφαλή του συμπλέγματος μέσα από μια ασύρματη πύλη (gateway) αποστέλλει τα δεδομένα στο νέφος (cloud). Η πύλη είναι υπεύθυνη για τις κινητές επικοινωνίες (GPRS[99]) και επιτρέπει σε έναν απομακρυσμένο χρήστη να έχει πρόσβαση ή να παρακολουθεί τα δεδομένα πεδίου σε πραγματικό χρόνο.



Εικόνα 6-11: Δείγμα διάταξης WSN σε τετράγωνη ανάπτυξη [202]

Οι συσκευές που είναι εξοπλισμένες με αισθητήρες είναι διασκορπισμένες σε διαφορετικές τοποθεσίες ανάλογα με την περιοχή ενδιαφέροντος η οποία μπορεί να αποτελείται από οικήματα, μεμονωμένα κτίρια ή ακόμη και απομακρυσμένα βουνά και δάση. Μετά την ανάλυση των δεδομένων, μπορεί να δημιουργηθεί ένα μήνυμα κατάλληλης προειδοποίησης (π.χ. προειδοποίησης πυρκαγιάς). Το σενάριο των εκδηλώσεων πυρκαγιάς έχει διερευνηθεί από διάφορες οπτικές γωνίες μαζί με διαφορετικές ερευνητικές τάσεις όπως οι τεχνολογίες IoT, Future Internet, κλπ.

Οι Hartung και Han [203] ανέπτυξαν ένα φορητό ασύρματο σύστημα παρακολούθησης των περιβαλλοντικών συνθηκών, ιδιαίτερα για δασικές πυρκαγιές. Συνδύασαν θερμικές κάμερες[100] παρακολούθησης με δυνατότητα σύνδεσης στο Διαδίκτυο, με ασύρματους

[99] Το General Packet Radio Service (GPRS) είναι ένα πρότυπο πακέτων δεδομένων κινητής τηλεφωνίας στο παγκόσμιο σύστημα κινητής επικοινωνίας του δικτύου κινητής τηλεφωνίας 2G και 3G (GSM). Το GPRS ιδρύθηκε από το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI) ως απάντηση στις παλαιότερες τεχνολογίες CDPD και i-mode. Το πρότυπο GPRS επιτηρείται από το Πρόγραμμα Συνεργασίας 3ης Γενιάς (3GPP).

[100] Οι θερμικές κάμερες φιλτράρουν όλα τα υπόλοιπα είδη ακτινοβολίας και κρατούν μόνο την υπέρυθρη, δηλαδή καταγράφουν την υπέρυθρη ακτινοβολία που εκπέμπουν σώματα και αντικείμενα και τη μετατρέπουν σε ορατή εικόνα. Η τελική εικόνα που λαμβάνουμε είναι συνήθως σε αποχρώσεις του γαλάζιου και πράσινου και δεν έχει την λεπτομέρεια που προσφέρει μια συμβατική κάμερα. Στην πράξη, οι θερμικές κάμερες μας δίνουν ένα σημαντικό συγκριτικό πλεονέκτημα έναντι των συμβατικών καμερών, γιατί μπορούμε να δούμε μια φιγούρα ενός ανθρώπου, ζώου ή θερμού αντικειμένου πολύ καθαρά, σε συνθήκες απόλυτου σκοταδιού,

κόμβους αισθητήρων, ώστε το σύστημα να παρέχει σε πραγματικό χρόνο δεδομένα καιρού από μία δασική περιοχή. Έτσι, τρία διαφορετικά δίκτυα αισθητήρων αναπτύσσονται σε διαφορετικά μέρη ενός δάσους και για τη μεταξύ τους επικοινωνία τα δίκτυα ενεργοποιούνται από ισχυρές ασύρματες συσκευές που μπορούν να στείλουν δεδομένα έως και δέκα χιλιόμετρα. Με το ασύρματο δίκτυο αισθητήρων γύρω από μία ενεργή φωτιά, μετρούν την μεταβολή των περιβαλλοντικών συνθηκών (θερμοκρασία, υγρασία κλπ.), ενώ παράλληλα οι κάμερες χρησιμοποιούνται για τη λήψη οπτικών δεδομένων της ζώνης πυρκαγιάς. Τα δεδομένα που συλλέγονται από τους κόμβους αισθητήρων και από τις κάμερες συγκεντρώνονται σε έναν σταθμό βάσης ο οποίος έχει τη δυνατότητα να παρέχει επικοινωνία μεγάλων αποστάσεων, χρησιμοποιώντας δορυφόρους. Περιοδικά, οι κόμβοι αισθητήρων μετρούν τη θερμοκρασία, τη σχετική υγρασία, την ταχύτητα και την κατεύθυνση ανέμου, ενώ κάμερες ιστού παρέχουν συνεχή οπτικά δεδομένα στον σταθμό βάσης.

Το βασισμένο σε WSN σύστημα ανίχνευσης πυρκαγιάς που περιγράφεται από τους Hartung και Han προσδιορίζεται από τα παρακάτω σημαντικά σημεία και δυνατότητες, τα οποία οφείλει να έχει ένα ασύρματο δίκτυο αισθητήρων ώστε να είναι σε θέση να παρακολουθεί επιτυχώς ένα δάσος και να ανιχνεύει φωτιές [203]:

1. **Ενεργειακή απόδοση[101]:** Οι κόμβοι αισθητήρων τροφοδοτούνται με μπαταρίες. Ως εκ τούτου, ένα ασύρματο δίκτυο αισθητήρων που έχει αναπτυχθεί για τον εντοπισμό πυρκαγιάς, θα πρέπει να καταναλώνει την ελάχιστη δυνατή ενέργεια. Συνήθως, εάν η περιοχή ανάπτυξης είναι πολύ μεγάλη, μπορεί να χρειαστούν εκατοντάδες κόμβοι αισθητήρων και επομένως η ενδεχόμενη αντικατάσταση μπαταριών μπορεί να είναι δαπανηρή, μη πρακτική ή ακόμη και αδύνατη.
2. **Έγκαιρη ανίχνευση και ακριβής εντοπισμός**: Είναι σημαντικό να ανιχνεύεται μία πυρκαγιά όσο το δυνατόν νωρίτερα, ώστε να εκτιμήσει κανείς την θέση της με μεγάλη ακρίβεια. Η ακριβής εκτίμηση της θέσης της πυρκαγιάς είναι σημαντική για την αποστολή του πυροσβεστικού προσωπικού στο σωστό σημείο, στο συντομότερο δυνατό χρονικό διάστημα.

3. **Δυνατότητα πρόβλεψης**: Το σύστημα πρέπει να είναι σε θέση να προβλέψει την κατεύθυνση εξάπλωσης ενώ η ταχύτητα είναι σημαντική για τον σχεδιασμό της πυρόσβεσης και για την κινητοποίηση πόρων και προειδοποιήσεων των γύρω περιοχών. Η ακριβής πρόβλεψη απαιτεί ακριβή και «φρέσκα» αισθητήρια δεδομένα για να φτάσουν στο κέντρο αποφάσεων και ελέγχου από όλα τα σημεία του δάσους,

---

μέσα από καπνό ή ομίχλη και μάλιστα ακόμη και από απόσταση χιλιομέτρων. Συνεπώς, οποιοδήποτε αντικείμενο στη φύση έχει θερμοκρασία, ακτινοβολεί ηλεκτρομαγνητικά κύματα στις θερμικές κάμερες που έχουν τοποθετηθεί. Όσο υψηλότερη είναι η θερμοκρασία της επιφάνειας του αντικειμένου, τόσο μεγαλύτερη είναι η υπέρυθρη ακτινοβολία. Πηγή: https://www.securitymanager.gr/egkairi-anichneysi-pyrkagion-me-thermikes-kameres-tis-mobotix/

[101] Παρατηρούμε εδώ ότι η ελαχιστοποίηση της κατανάλωσης ενέργειας είναι ένα κοινό σημείο αναφοράς για όλα τα ασύρματα δίκτυα αισθητήρων, ανεξαρτήτως της χρήσης για την οποία προορίζονται. Όσο πιο εκτεταμένο είναι ένα δίκτυο ασύρματων αισθητήρων, τόσο μεγαλύτερο είναι το κόστος που προκύπτει στην ενδεχόμενη αντικατάσταση μπαταριών και αυτό είναι μια σημαντική παράμετρος που θα πρέπει να λαμβάνεται σοβαρά υπόψη, σε οποιονδήποτε αντίστοιχο σχεδιασμό.

ειδικά από και γύρω την περιοχή όπου έχει σημειωθεί η πυρκαγιά (δηλαδή τις αποκαλούμενες ως κρίσιμες ζώνες).

4. **Προσαρμογή σε σκληρά περιβάλλοντα**: Ένα δίκτυο αισθητήρων για δάση λειτουργεί συνήθως σε σκληρά περιβάλλοντα (κυρίως αυξομειώσεις θερμοκρασίας/υγρασίας) και ως εκ τούτου θα πρέπει να είναι σε θέση να αντιμετωπίζει και να προσαρμόζεται στις συνθήκες αυτές. Επίσης θα πρέπει να είναι σε θέση να ανακτήσει γρήγορα την λειτουργία του από σφάλματα όπως ζημίες κόμβων, σφάλματα σύνδεσης, υψηλή θερμοκρασία, υγρασία, πίεση, κλπ.

Εκτός από αυτούς τους στόχους, μπορεί να υπάρχουν κάποιες άλλες κρίσιμες απαιτήσεις για ένα ασύρματο δίκτυο αισθητήρων το οποίο είναι σχεδιασμένο για ανίχνευση πυρκαγιάς, όπως είναι η ασφάλεια δικτύου από κυβερνοεπιθέσεις, η αντιμετώπιση βανδαλισμού και δολιοφθοράς, η ενσωμάτωση μηχανισμών αυτο-θεραπείας και αυτο-οργάνωσης. Στην συνέχεια της διατριβής αυτής, θα μελετηθούν διεξοδικά ορισμένοι τρόποι προστασίας των οντοτήτων που ονομάζουμε ως ασύρματα δίκτυα αισθητήρων, εστιάζοντας κυρίως στις κυβερνοεπιθέσεις οι οποίες αποτελούν και την πιο σημαντική απειλή για αυτά.

6.8 Πλατφόρμες Διαχείρισης Συστημάτων (PSIM)

Το λογισμικό Ενοποιημένης Διαχείρισης Συστημάτων Ασφάλειας (Physical Security Integration Management – PSIM software) ή Διαχείριση πληροφοριών φυσικής ασφάλειας είναι μία πλατφόρμα λογισμικού που ενσωματώνει συστήματα ασφαλείας και τα παρακολουθεί μέσω μίας διεπαφής. Οι πλατφόρμες PSIM συλλέγουν και συσχετίζουν συμβάντα από συστήματα ασφαλείας και πληροφοριών (βίντεο, αναλυτικά στοιχεία, έλεγχο πρόσβασης, αισθητήρες, συστήματα κτιρίων κλπ.) και είναι σε θέση να υποστηρίξουν το προσωπικό ασφαλείας προκειμένου να εντοπίσουν και να επιλύσουν κρίσιμες καταστάσεις σύμφωνα με τις πολιτικές του αντίστοιχου οργανισμού [204].

Μία πλατφόρμα PSIM μπορεί να:

- Συλλέγει δεδομένα από οποιονδήποτε αριθμό διαφορετικών συσκευών ή συστημάτων ασφαλείας.
- Αναλύει και συσχετίζει δεδομένα, συμβάντα και συναγερμούς, προκειμένου να προσδιορίσει την πραγματική κατάσταση και την προτεραιότητά της.
- Υποστηρίζει τον χειριστή, για ταχύτερη επαλήθευση τυχόν κρίσιμης κατάστασης.
- Παρέχει τις απαραίτητες οδηγίες βάσει των πολιτικών του οργανισμού, για την υποστήριξη της επίλυσης της κρίσιμης κατάστασης κάθε περιστατικού.
- Δημιουργεί αυτόματες και αναλυτικές αναφορές και να υποστηρίζει σε βάθος την ανάλυση έρευνας.

Κάθε κατασκευαστής συνήθως περιλαμβάνει τα δικά του διαχειριστικά εργαλεία που μπορεί να κρίνονται επαρκή για ομογενείς εγκαταστάσεις αλλά δεν μπορούν να καλύψουν τις απαιτήσεις εγκαταστάσεων βασισμένων σε μεικτές λύσεις και με γεωγραφικά κατανεμημένα συστήματα. Οι μεγάλοι οργανισμοί που δραστηριοποιούνται στους τομείς

των τραπεζών, του λιανεμπορίου και της παροχής υπηρεσιών, και οι οποίοι διαθέτουν πολλά υποκαταστήματα γεωγραφικώς κατανεμημένα ή κρίσιμες υποδομές, συνήθως διαθέτουν οι ίδιοι είτε τους παρέχεται από κάποια εξειδικευμένη εταιρεία ένα κέντρο ελέγχου στο οποίο εξουσιοδοτημένοι χρήστες παρακολουθούν σε 24ωρη βάση την τήρηση της πολιτικής ασφαλείας και επεμβαίνουν άμεσα σε συναγερμούς που υποδηλώνουν παραβιάσεις αυτής.

Η παρακολούθηση και η άμεση αντίδραση σε συμβάντα ασφαλείας σε κρίσιμες και μεγάλες υποδομές αλλά και σε σύνθετα συστήματα απαιτεί αναλυτική και στοχευμένη πληροφόρηση στους επιφορτισμένους με την τήρηση της πολιτικής ασφάλειας, μέσω εργαλείων που αναλύουν την σημασία ενός συμβάντος και την αντίδραση ανάλογα την σημαντικότητα του. Απαιτεί επίσης την καταγραφή των ενεργειών των χρηστών ώστε να είναι εφικτός ο μεταγενέστερος έλεγχος [205].

Η επιλογή του κατάλληλου λογισμικού Ενοποιημένης Διαχείρισης Συστημάτων Ασφάλειας όλων των υποδομών ενός οργανισμού, θα μπορέσει να υποστηρίξει την λήψη αποφάσεων, τόσο σε τακτικό-καθημερινό επίπεδο από τον Υπεύθυνο Ασφάλειας, όσο και σε στρατηγικό πεδίο στο επίπεδο της Διοίκησης, μέσω της αναθεώρησης των σχεδίων ασφάλειας-πυρασφάλειας, της εκπαίδευσης του προσωπικού και της επέκτασης-αναβάθμισης του εξοπλισμού. Σε συνδυασμό με τη δυνατότητα ενοποιημένης διαχείρισης και του κτιριακού αυτοματισμού, ενημερώνονται άμεσα οι υπεύθυνοι συντηρήσεων σε περιπτώσεις υπερβάσεων κρίσιμων κατωφλίων θερμοκρασίας, υγρασίας, ενεργειακών δεδομένων κ.α.

Για να επιτύχει στην αποστολή της, η Ενοποίηση Συστημάτων θα πρέπει να υπηρετεί τρεις βασικούς άξονες [205]:

1. Ενοποίηση των «διάσπαρτων» πηγών δεδομένων ασφάλειας ενός οργανισμού, έτσι ώστε να αξιοποιηθούν στον μέγιστο βαθμό οι υπάρχουσες υποδομές, παράλληλα με τις νέες επενδύσεις σε υλικοτεχνικές υποδομές.
2. Διάθεση των κατάλληλων διαδικασιών που θα επιτρέψουν τον μετασχηματισμό των συλλεγόμενων δεδομένων σε αξιοποιήσιμες πληροφορίες, με το μικρότερο δυνατό κόστος. Για το σκοπό αυτό, η ενοποίηση συστημάτων ασφάλειας θα πρέπει να είναι εξοπλισμένη με υψηλό βαθμό αυτοματοποίησης και να διαθέτει «ευφυΐα».
3. Υποστήριξη της ενοποιημένης διαχείρισης συστημάτων για τον μεγαλύτερο δυνατό βαθμό ανάληψης δράσης, από τις δομές και τους χρήστες της εγκατάστασης. Για παράδειγμα, μέσα από την ενοποιημένη πλατφόρμα θα πρέπει να ειδοποιούνται οι κατάλληλοι άνθρωποι με την κατάλληλη πληροφορία, μέσα από το κατάλληλο επικοινωνιακό μέσο και στον κατάλληλο χρόνο, ενώ στη συνέχεια θα πρέπει να υποστηρίζεται η επικοινωνία και η συνεργασία μεταξύ διαφορετικών χρηστών, υπευθύνων και διευθύνσεων σε κάθε βήμα του διαχειριστικού κύκλου συμβάντος συναγερμού ή ελέγχου πρόσβασης, μέχρι την τελική επίλυση των θεμάτων και την αξιολόγηση των αποτελεσμάτων.

Με την εξέλιξη της τεχνολογίας και την σταδιακή υποστήριξη ανοιχτών πρωτοκόλλων επικοινωνίας εξοπλισμού διαφορετικών κατασκευαστών, η επιλογή του κατάλληλου λογισμικού ενοποιημένης διαχείρισης αυξάνει την ζητούμενη αποτελεσματικότητα, ενισχύοντας παράλληλα την αξιοπιστία της επένδυσης σε βάθος χρόνου.

6.9 Διαχείριση Συστημάτων σε Πλατφόρμες Cloud

Η ραγδαία εξέλιξη των υπηρεσιών Cloud ήρθε ως απάντηση των περιορισμών που έχουν τα συστήματα και οι ηλεκτρονικές συσκευές. Η τεράστια επεξεργαστική δυνατότητα που προσφέρουν οι φάρμες διακομιστών (Servers), σε συνάρτηση με τη σημαντική αύξηση της ταχύτητας του Διαδικτύου μέσω ευζωνικής, κινητής ακόμα και δορυφορικής επικοινωνίας, επέτρεψε στα συστήματα να αποκτήσουν δυνατότητες που δεν είχαμε φανταστεί.

Τα τελευταία χρόνια ήρθε και η σειρά των συστημάτων συναγερμού, αφού υπάρχουν ήδη εφαρμογές από κατασκευαστές που επιτρέπουν στον χρήστη πρόσβαση στις βασικές λειτουργίες όπως ενεργοποίησης και απενεργοποίησης από το κινητό του. Το κύριο όφελος ασφαλείας που προέκυψε από την ένωση ενός συστήματος στο δίκτυο, είναι η απρόσκοπτη επικοινωνία με τα κέντρα λήψεως σημάτων. Η επικοινωνία είναι άμεση και δίνεται η δυνατότητα συνεχούς παρακολούθησης, σε αντίθεση με τις παραδοσιακές τηλεφωνικές γραμμές που επικοινωνούν σε συγκεκριμένο χρόνο για παρακολούθηση της κατάστασης του συστήματος. Αυτό έδωσε τη δυνατότητα στα κέντρα λήψεως σημάτων, ώστε να δημιουργήσουν υπηρεσίες βασισμένες στη συνεχή παρακολούθηση της κατάστασης συστημάτων με διαφορετικές χρεώσεις. Ιδέες εφαρμογής υπάρχουν πολλές και οι τεχνικές εταιρείες μπορούν εύκολα να διαφοροποιηθούν από τον ανταγωνισμό σχεδιάζοντας διαφορετικές υπηρεσίες. Για παράδειγμα, με τον ίδιο τρόπο που οι αυτοκινητοβιομηχανίες «προσέχουν» τα οχήματα πριν να παρουσιάσουν βλάβη, οι εγκαταστάτες συστημάτων ασφαλείας μπορούν να προσέχουν τα συστήματα συναγερμού σε τεχνικό επίπεδο με ένα μηνιαίο συνδρομητικό κόστος, παρακολουθώντας την κατάσταση των συστημάτων των πελατών συνδρομητών τους και να ενημερώνονται για πιθανές βλάβες πριν ακόμα το αντιληφθεί ο ίδιος ο πελάτης.

Όπως ήταν αναμενόμενο όμως, οι νέες δυνατότητες έφεραν και νέες προκλήσεις ασφαλείας, που πρέπει να αναλογιστούμε πριν προτείνουμε ή χρησιμοποιήσουμε την σύνδεση ενός συστήματος σε υπηρεσίες Cloud. Η ευθύνη λειτουργίας του Cloud που χρησιμοποιούμε για να ενωθούμε στο όποιο σύστημα, ανήκει στην εταιρεία κατασκευής του συστήματος. Συχνά παρέχεται ως υπηρεσία από εξωτερικό συνεργάτη λόγω έλλειψης τεχνογνωσίας του κατασκευαστή, οπότε προκύπτουν σημαντικά ερωτήματα όπως εάν ο κατασκευαστής ή ο συνεργάτης τηρούν τα διεθνή πρότυπα ασφαλείας [178].

Το IoT περιέχει δισεκατομμύρια έξυπνα αντικείμενα και κάθε έξυπνο αντικείμενο στέλνει τεράστια ποσότητα δεδομένων σε άλλα αντικείμενα. Ένα έξυπνο αντικείμενο πρέπει να πιστοποιείται και να διαθέτει μηχανισμούς ασφαλείας για την ασφάλεια χρηστών, συσκευών και υπηρεσιών. Ταυτόχρονα, χρησιμοποιούνται μηχανισμοί ασφαλείας για την αποτροπή απειλών και επιθέσεων για πρόσβαση σε δεδομένα ή υπηρεσίες. Αυτή η λειτουργία ονομάζεται ασφάλεια End-to-End (E2E). Ο τομέας της ασφάλειας End-to-End περιλαμβάνει συσκευές IoT, πύλες IoT, πρόσβαση και σύνδεση δικτύου, εφαρμογές IoT, πλατφόρμες και χρήστες. Οι κύριες απαιτήσεις ασφάλειας End-to-End είναι οι διαδικασίες ελέγχου ταυτότητας, ελέγχου πρόσβασης και κρυπτογράφησης. Όταν οποιοδήποτε έξυπνο αντικείμενο θέλει να συνδεθεί σε άλλο, και τα δύο πρέπει να είναι αντικείμενα ελέγχου ταυτότητας. Μόλις γίνει έλεγχος ταυτότητας ενός έξυπνου αντικειμένου, αυτό μπορεί να στείλει και να λάβει δεδομένα ή εντολές. Στη συνέχεια, ένα έξυπνο αντικείμενο μπορεί να συνδεθεί απευθείας στο cloud. Ο υπεύθυνος του cloud παρέχει διαδικασία ελέγχου

ταυτότητας και ελέγχει τα μηνύματα μεταξύ έξυπνων αντικειμένων. Μετά την εφαρμογή ελέγχου ταυτότητας και ελέγχου, ένα έξυπνο αντικείμενο συνδέεται στο Διαδίκτυο μέσω της πύλης. Στη συνέχεια, η διαδικασία κρυπτογράφησης χρησιμοποιείται για την κρυπτογράφηση μηνυμάτων που ανταλλάσσονται μεταξύ έξυπνων αντικειμένων.

Ο μηχανισμός ελέγχου ταυτότητας παίζει σημαντικό ρόλο στην ασφάλεια του IoT και μπορεί να εφαρμοστεί με πολλές μεθόδους όπως η ταυτότητα, ο κωδικός πρόσβασης και η υποδομή δημόσιου κλειδιού[102]. Η διαχείριση ταυτότητας χρησιμοποιείται για τον καθορισμό των συνδέσεων έξυπνων αντικειμένων. Περιλαμβάνει συνδεσιμότητα, τομείς δικτύου και εφαρμογές στην πλατφόρμα IoT. Οι μηχανισμοί εξουσιοδότησης και ελέγχου πρόσβασης παρέχουν στους χρήστες πρόσβαση σε πόρους και υπηρεσίες δικτύου. Ο έλεγχος ταυτότητας και η πρόσβαση εμποδίζουν τους μη εξουσιοδοτημένους χρήστες να αποκτήσουν πρόσβαση σε πόρους δικτύου. Όπως αναφέρθηκε παραπάνω, οι συσκευές IoT έχουν περιορισμένη χωρητικότητα και ισχύ αποθήκευσης, οπότε η εφαρμογή μεθοδολογιών ελέγχου και πρόσβασης δεν είναι εύκολη αποστολή. Εκτός από την ετερογένεια και την πολυπλοκότητα των συσκευών, οι μεθοδολογίες εξουσιοδότησης και ελέγχου πρόσβασης ενδέχεται να μην ισχύουν για το σύστημα IoT [206].

[102] https://en.wikipedia.org/wiki/Public-key_cryptography

7

Ασφάλεια Ασύρματων Δικτύων

Τα ζητήματα ασφαλείας είναι ζωτικής σημασίας σε ασύρματα δίκτυα που χρησιμοποιούνται για την ασφάλεια κρίσιμων υποδομών, όπου σύμφωνα με όσα είδαμε στα προηγούμενα κεφάλαια, οι απαιτήσεις αξιοπιστίας και διαθεσιμότητας είναι ιδιαίτερα αυξημένες. Η ασφάλεια ενός δικτύου WSN αποσκοπεί στην ακεραιότητα του ίδιου του δικτύου και στην αντιμετώπιση δυσμενών καταστάσεων, οι οποίες σχετίζονται με το ρίσκο (διακινδύνευση) της ακεραιότητας δεδομένων, τις υποκλοπές και παρεμβολές μεταδιδόμενης πληροφορίας, την είσοδο και μετάδοση στο σύστημα ψεύτικων ή τροποποιημένων μηνυμάτων πληροφοριών καθώς επίσης και την απώλεια ή κατασπατάληση πόρων του δικτύου. Ένα ασφαλές σύστημα προϋποθέτει τη συμμετοχή σε αυτό οντοτήτων (συσκευές, μηχανισμοί κλπ.), οι οποίες είναι σχεδιασμένες με επίκεντρο την ασφάλεια. Κάθε παρέκκλιση από αυτή την αρχή αφήνει περιθώρια σε υπόπτους ώστε να ενεργήσουν με κακόβουλο τρόπο κατά του δικτύου [207].

7.1 Ζητήματα Ασφαλείας σε WSNs

Παρά την καταλληλότητα των ασύρματων τεχνολογιών για πολλές εφαρμογές και για διαφορετικά πεδία, δεν αναιρείται το γεγονός ότι η φύση της ασύρματης επικοινωνίας καθιστά τα ασύρματα δίκτυα περισσότερο ευάλωτα σε επιθέσεις από ό,τι τα ενσύρματα δίκτυα. Επιπλέον, τα WSNs αναπτύσσονται συχνά σε μη ελεγχόμενα περιβάλλοντα, τα οποία τελικά τα καθιστούν ευαίσθητα σε φυσικές αλλοιώσεις. Οι προβληματισμοί σχετικά με την ασφάλεια των υλισμικών υποδομών ενός WSN, συνοπτικά αναφέρονται παρακάτω [207]:

- **Αξιοπιστία μέσου μετάδοσης:** Εξαιτίας της ασύρματης σύνδεσης των κόμβων και των ασυρμάτων μέσων και υποδομών μετάδοσης, οι υποδομές δικτύου είναι ευαίσθητες σε επιθέσεις και κακόβουλες ενέργειες τρίτων. Ως εκ τούτου, είναι απαραίτητη λήψη κατάλληλων μέτρων, ώστε κάθε επιμέρους κόμβος να είναι σε θέση να αντιμετωπίσει τις απειλές. Η ανάγκη αυτή ενισχύεται και από το γεγονός ότι

η μετάδοση της πληροφορίας βασίζεται σε δρομολόγηση με πολλαπλά άλματα μέσω των κόμβων (multi-hop routing).

- **Περιορισμοί πόρων λόγω κόστους:** Ο σχεδιασμός των κόμβων ενός WSN είναι υπολογισμένος σύμφωνα με το χαμηλότερο δυνατό κόστος υλισμικού, εγκατάστασης και συντήρησης, συχνά με περιορισμένες δυνατότητες υπολογισμών και αποθήκευσης και με σημαντικούς περιορισμούς σε ενεργειακά αποθέματα. Οι περιορισμοί αυτοί πολλές φορές θέτουν θέματα αξιοπιστίας στο δίκτυο.

- **Ευρωστία**: Η εφαρμογή δικτύων WSN τις περισσότερες φορές υλοποιείται και παραμένει σε λειτουργία χωρίς την ύπαρξη ανθρώπινης επίβλεψης και παρέμβασης, συνήθως για μεγάλο χρονικό διάστημα. Το γεγονός αυτό καθιστά τα δίκτυα WSN ευαίσθητα σε καιρικές συνθήκες και σε αντίξοα περιβάλλοντα λειτουργίας. Επομένως, σε αυτές τις περιπτώσεις θα πρέπει να προβλεφθούν όλοι οι αστάθμητοι φυσικοί παράγοντες που μπορούν να επηρεάσουν τη λειτουργία ενός ή περισσότερων κόμβων.

- **Επικοινωνία και συγχρονισμός συσκευών δικτύου**: Η επικοινωνία και ο συγχρονισμός των συσκευών ενός WSN είναι κρίσιμης σημασίας και αφορά στη διαθεσιμότητα του δικτύου. Ωστόσο, η επίτευξη της ομαλής επικοινωνίας και συγχρονισμού δυσχεραίνονται εξαιτίας της δρομολόγησης πακέτων με πολλαπλά άλματα (απαίτηση συγχρονισμού κάθε συσκευής που συμμετέχει στη δρομολόγηση).

Από την άλλη μεριά, όσο αφορά στις κύριες απειλές που συσχετίζονται με την ακεραιότητα των μεταδιδόμενων δεδομένων σε ένα WSN, συνοπτικά θα συναντήσουμε τις εξής κατηγορίες απειλών [208]:

- **Επίθεση τροποποίησης δεδομένων:** Ένας εισβολέας τροποποιεί την τιμή μίας ή περισσοτέρων αναγνώσεων δεδομένων, είτε εισβάλλοντας στον αισθητήρα αποστολέα είτε εισάγοντάς τον μεταξύ του αποστολέα και των δεκτών.

- **Εισαγωγή ψευδών δεδομένων:** Μπορεί να θέσει σε κίνδυνο τους υπάρχοντες κόμβους και να εισάγει ένα ψευδές μήνυμα με ψευδείς πληροφορίες. Είναι επίσης πιθανό να προσθέσει νέους κόμβους στα δίκτυα αισθητήρων που τροφοδοτούν τα ψευδή δεδομένα. Μία τέτοια επίθεση καταναλώνει επίσης τους ενεργειακούς πόρους άλλων κόμβων αισθητήρων.

- **Διαγραφή δεδομένων:** Η επίθεση διαγραφής δεδομένων μπορεί να πραγματοποιηθεί με την απόρριψη μεμονωμένων αναγνώσεων δεδομένων ή την απόρριψη μίας ή περισσότερων ομάδων και την παρεμπόδισή τους να φτάσουν στον επιδιωκόμενο παραλήπτη.

- **Άρνηση υπηρεσίας (Denial of Service - DoS):** Οι επιθέσεις άρνησης υπηρεσίας σε ασύρματο δίκτυο αισθητήρων ενδέχεται να λάβουν διάφορες μορφές, όπως π.χ. διακοπή της ραδιοφωνικής σύνδεσης, εσφαλμένη διέλευση δεδομένων αισθητήρα ή πόρων κόμβου [208].

Οι στόχοι ασφαλείας παραμένουν οι ίδιοι για οποιαδήποτε εφαρμογή ασύρματων δικτύων και ιδιαίτερα για τα WSNs που σχετίζονται με και που επηρεάζουν άμεσα την ασφάλεια κρίσιμων υποδομών και κατ' επέκταση της χώρας ή την ευρύτερη οικονομική ανάπτυξη. Οι τεχνικές ασφαλείας μπορεί να είναι προαιρετικές σε ορισμένες εφαρμογές του WSN. Από την άλλη πλευρά όμως, τα WSNs είναι απαραίτητα για πολλές εφαρμογές όπως τα στρατιωτικά πεδία, η παρακολούθηση της διαρροής ακτινοβολίας πυρηνικών εγκαταστάσεων, η εξάπλωση επιδημιών και βιολογικών και χημικών όπλων, η παρακολούθηση και ο έλεγχος των καλλιεργειών τεράστιων περιοχών γεωργικής, περιβαλλοντικής παρακολούθησης, η έγκαιρη ανίχνευση δασικών πυρκαγιών κλπ. Σε αυτούς τους τομείς των εφαρμογών των WSNs δεν υπάρχει υποκατάστατο για τη χρήση τεχνικών ασφαλείας υψηλής απόδοσης. επίσης, η ασφάλεια είναι ένα σημαντικό ζήτημα για ad hoc δίκτυα, ειδικά για εκείνες τις εφαρμογές που είναι ευαίσθητες ως προς αυτή την απαίτηση. Για να διασφαλιστεί η επάρκεια της λειτουργίας ενός ad hoc δικτύου, λαμβάνονται υπόψη τα ακόλουθα χαρακτηριστικά που, όπως είδαμε σε προηγούμενα κεφάλαια, διασφαλίζουν την ασφάλεια δεδομένων και είναι τα εξής: διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα και μη αποποίηση [209].

7.2 Επιθέσεις και Μοντέλα Επιθέσεων

Ως «επιθέσεις ασφαλείας» ("security attacks") ορίζονται οι κακόβουλες ενέργειες εξωτερικών οντοτήτων με σκοπό την πρόκληση δυσμενών συνεπειών (ήτοι υποκλοπή, τροποποίηση, εισαγωγή ή διαγραφή μηνυμάτων) στη λειτουργία του δικτύου WSN, με στόχο τη διατάραξη των θεμελιωδών ιδιοτήτων της Ασφάλειας Πληροφοριών (βλ. κεφ. 5.5.1), δηλαδή της διαθεσιμότητας, της ακεραιότητας και της εμπιστευτικότητας [210]. Στη βιβλιογραφία συχνά οι επιθέσεις αναφέρονται και ως απειλές, ενώ στο Λεξικό Ασφαλείας Διαδικτύου (Internet Security Glossary) [209] γίνεται διαχωρισμός των δύο εννοιών όπως παρακάτω:

Απειλή (threat): Είναι η δυνατότητα παραβίασης της ασφάλειας, η οποία δίνεται όταν υπάρχει κάποιο περιστατικό, ενέργεια ή συμβάν που επιτρέπει την εκμετάλλευση μίας ευπάθειας του συστήματος, με πιθανές αρνητικές συνέπειες.

Επίθεση (attack): Είναι η προσβολή της ασφάλειας του συστήματος που προκύπτει ως αποτέλεσμα μίας απειλής, δηλαδή είναι η πράξη που αποτελεί σκόπιμη απόπειρα με την έννοια της μεθόδου ή της τεχνικής, για την παράκαμψη των υπηρεσιών ασφαλείας και την παραβίαση ενός συστήματος.

Οι επιθέσεις μπορούν να διαχωριστούν σε ενεργητικής και παθητικής μορφής:

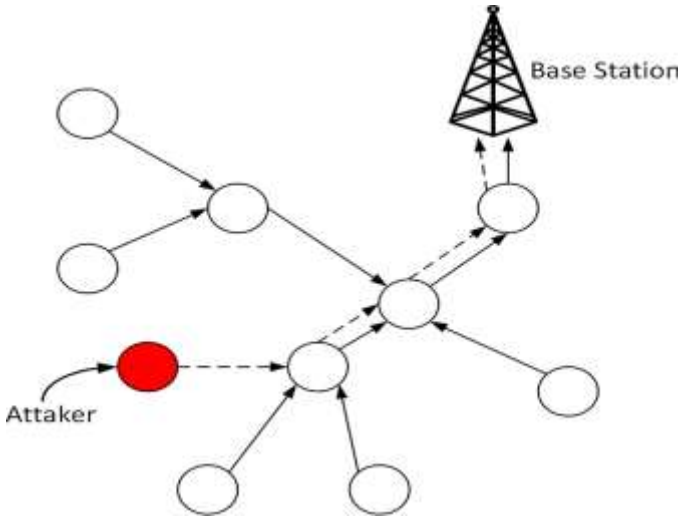
- **Ενεργές Επιθέσεις (active attacks):** Ο επιτιθέμενος στοχεύει επιπλέον στην ακεραιότητα και διαθεσιμότητα δεδομένων (τροποποίηση δεδομένων ή δημιουργία ψεύτικων δεδομένων, άρνηση εξυπηρέτησης), παρακολουθώντας και τροποποιώντας τη ροή δεδομένων στο κανάλι επικοινωνίας. Σε αυτό τον τύπο επίθεσης, ο επιτιθέμενος έχει ενεργό ρόλο, προσποιούμενος ότι αποτελεί έναν έγκυρο και λειτουργικό κόμβο.

- **Παθητικές επιθέσεις (passive attacks)**: Ο επιτιθέμενος δεν εκπέμπει εντός του δικτύου ψευδή ή τροποποιημένα δεδομένα, αλλά στοχεύει στη μείωση της εμπιστευτικότητας στο δίκτυο (υποκλοπή δεδομένων): Ένας κακόβουλος, μη εξουσιοδοτημένος κόμβος παρακολουθεί ένα κανάλι επικοινωνίας, με στόχο να συγκεντρώσει εμπιστευτικής διαβάθμισης πληροφορίες και να προετοιμαστεί για μία ενεργή επίθεση. Αυτός ο τύπος επίθεσης είναι δύσκολο να εντοπιστεί, αφού ο εισβολέας δεν συνεισφέρει δεδομένα στο κανάλι επικοινωνίας. Συνήθεις επιθέσεις παθητικής μορφής είναι η υποκλοπή (eavesdropping) και η παρακολούθηση (monitoring) μίας ασύρματης ζεύξης.

Μία επιπλέον κατηγοριοποίηση των επιθέσεων ασφαλείας είναι η ταξινόμησή τους σε **εσωτερικές** και **εξωτερικές**. Οι εσωτερικές επιθέσεις προέρχονται από συσκευές του δικτύου που έχουν κακόβουλα προσβληθεί και είναι δυσκολότερη η ανίχνευσή τους. Στις εξωτερικές επιθέσεις, μία εκτός δικτύου συσκευή παρακολουθεί τα διακινούμενα πακέτα ή εισάγει στο δίκτυο μη έγκυρα πακέτα με σκοπό τη διατάραξη των λειτουργιών του [210].

7.2.1 Επιθέσεις Άρνησης Υπηρεσίας (Denial of Service – DoS)

Μία επίθεση άρνησης υπηρεσίας (DoS) είναι μία προσπάθεια ώστε να γίνει ένα σύστημα (διακομιστής/πελάτης) ή κάποιος άλλος δικτυακός πόρος απρόσιτος για τους αυθεντικούς χρήστες. Αυτή η επίθεση «πλημμυρίζει» το σύστημα από πάρα πολλά αιτήματα επικοινωνίας και, εξαιτίας αυτού, το «πολιορκημένο» σύστημα δεν μπορεί να ανταποκριθεί στους αυθεντικούς χρήστες του ή θα ανταποκριθεί πολύ αργά, εξασθενίζοντας δραστικά τη διαθεσιμότητα του. Εν τέλει μπορεί να αντικαταστήσει το θύμα ή να απορροφήσει σχεδόν όλους τους πόρους του, αποτρέποντας την επικοινωνιακή του πορεία.



Εικόνα 7-1: Επίθεση DoS με σκοπό την αύξηση της κίνησης δικτύου[103]

[103] Διατηρώντας μη εξουσιοδοτημένη πρόσβαση και έλεγχο σε έναν κόμβο αισθητήρα, δίνεται στον επιτιθέμενο η δυνατότητα να επηρεάσει το σημαντικό χαρακτηριστικό της ισχύος μετάδοσής του και κατ' επέκταση της ζωής της πηγής ενέργειάς του (δηλαδή της μπαταρίας του) [210].

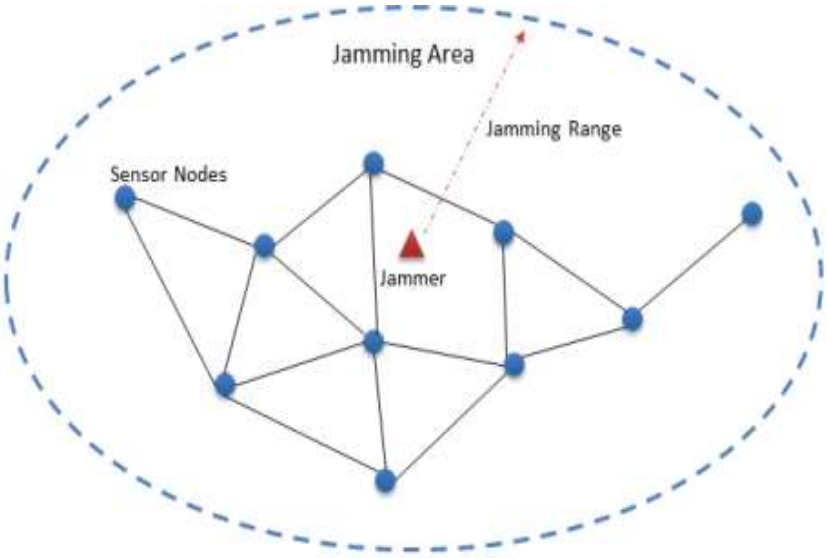
Αυτού του είδους η επίθεση μειώνει την απόδοση του συστήματος προκαλώντας απώλεια ή καθυστέρηση πακέτων και αναγνώριση αυτών. Επίσης καταναλώνει χρόνο μνήμης, εύρος ζώνης και χρόνο επεξεργασίας CPU, ενώ μπορεί να αφαιρέσει ή/και να αλλάξει πληροφορίες δρομολόγησης στο WSN, όπως επίσης και να αλλάξει την περίοδο λειτουργίας του πρωτοκόλλου ελέγχου μετάδοσης ή ακόμα και να εμποδίσει την επικοινωνία μεταξύ των κόμβων [211].

Επιθέσεις DoS θα συναντήσουμε στο φυσικό στρώμα (physical layer) ενός WSN, το οποίο αφορά στις υποδομές και στα υλισμικά που απαρτίζουν το ίδιο το δίκτυο. Ωστόσο, DoS επιθέσεις επίσης θα συναντήσουμε στο στρώμα δικτύου (network layer), στο στρώμα μεταφοράς (transport layer) και στο στρώμα εφαρμογής (application layer) [211].

Φυσικό Στρώμα (Physical layer)

Σε ένα WSN, το φυσικό επίπεδο (Physical layer) είναι υπεύθυνο για τη διαμόρφωση του σήματος και για τη μετάδοση της πληροφορίας. Οι κοινές επιθέσεις DoS Physical Layer που αφορούν στα WSN είναι οι επιθέσεις παρεμβολής (Jamming) και οι επιθέσεις παραβίασης κόμβων (node tampering).

Η επίθεση παρεμβολής εκπέμπει σήμα στο ίδιο δίκτυο και εύρος συχνοτήτων, με σκοπό ο επιτιθέμενος να δημιουργήσει θόρυβο και για να διαταράξει την ορθή ανταλλαγή μηνυμάτων μεταξύ των κόμβων, είτε σε ολόκληρο το δίκτυο είτε σε ένα επιμέρους τμήμα του.



Εικόνα 7-2: Επίθεση παρεμβολής (Jamming attack)[104]

[104] Στο σχήμα απεικονίζονται ελεγχόμενες από τον επιτιθέμενο συσκευές (jammers), οι οποίες εκπέμπουν εντός του δικτύου δημιουργώντας παρεμβολές στους παραλήπτες των απεσταλμένων πακέτων Πηγή: Ünsal, E., & Çebi, Y. (2013): Denial of service attacks in WSN. In Proceedings of the International Symposium on Computing in Science & Engineering (p.24). Gediz University, Engineering and Architecture Faculty. https://www.researchgate.net/publication/270885540_DENIAL_OF_SERVICE_ATTACKS_IN_WSN

Για τον εντοπισμό επιθέσεων παρεμβολών σε μία περιοχή WSN, σε μία μορφή αντιστοίχισης, μπορούν να χρησιμοποιηθούν αλγόριθμοι εντοπισμού υπερχείλισης σημάτων (back-flooding), ενώ άλλοι μηχανισμοί αντιμετώπισης της συγκεκριμένης επίθεσης είναι οι τεχνικές μεταπήδησης συχνότητας FHSS (Frequency Hopping Spread Spectrum)[105] και εξάπλωσης κώδικα (code spreading).

Στην κατηγορία των επιθέσεων παρεμβολών θα συναντήσουμε επίσης την επίθεση εξάντλησης πόρων (exhaustion attack) η οποία είναι δυνατόν να προκληθεί από επαναλαμβανόμενες συμφορήσεις δεδομένων που προκαλούνται από κόμβους «φαντάσματα» (“ghost” nodes). Οι συμφορήσεις αυτές οδηγούν τους εκτιθέμενους κόμβους σε επαναλαμβανόμενες εκπομπές πακέτων με αποτέλεσμα την κατασπατάληση των ενεργειακών πόρων. Μέτρο πρόληψης τέτοιων επιθέσεων μπορεί να προσφέρει η χρήση πολλαπλής πρόσβασης διαίρεσης χρόνου (Time Division Multiple Access - TDMA), η δρομολόγηση πακέτων μόνο μετά από αυθεντικοποίηση του αποστολέα και η φραγή πακέτων με μέγεθος που υπερβαίνει το μέγεθος πακέτων της εφαρμογής.

Η επίθεση παραβίασης (node tampering) στοχεύει στη φυσική καταστροφή των κόμβων, ωφελούμενη από την απομακρυσμένη λειτουργία τους, πολλές φορές σε δυσπρόσιτες περιοχές. Από την παραβίαση ενός κόμβου, μπορεί να υποκλαπούν ευαίσθητα δεδομένα (όπως για παράδειγμα κρυπτογραφικά κλειδιά, με σκοπό την ανάληψη του ελέγχου του κόμβου από τον επιτιθέμενο, ώστε να δημιουργηθεί δολιοφθορά και διαταραχή στην αποστολή δεδομένων (data collision – σύγκρουση δεδομένων)). Τρόποι άμυνας σε αυτού του τύπου τις επιθέσεις είναι η χρήση μηχανισμών προστασίας από παραβίαση (tamper switches), οι μικροί σε μέγεθος κόμβοι και η φυσική τους απόκρυψη.

Γενικότερα, σε μία περίπτωση επίθεσης DoS, οι κόμβοι ενός WSN μπορούν να τεθούν σε κατάσταση αναστολής λειτουργίας, μέχρι το τέλος της επίθεσης. Ωστόσο, η ανταλλαγή δεδομένων δεν θα μπορεί να πραγματοποιηθεί κατά τη διάρκεια αυτής της μεθόδου πρόληψης.

Στρώμα Δικτύου (Network layer)

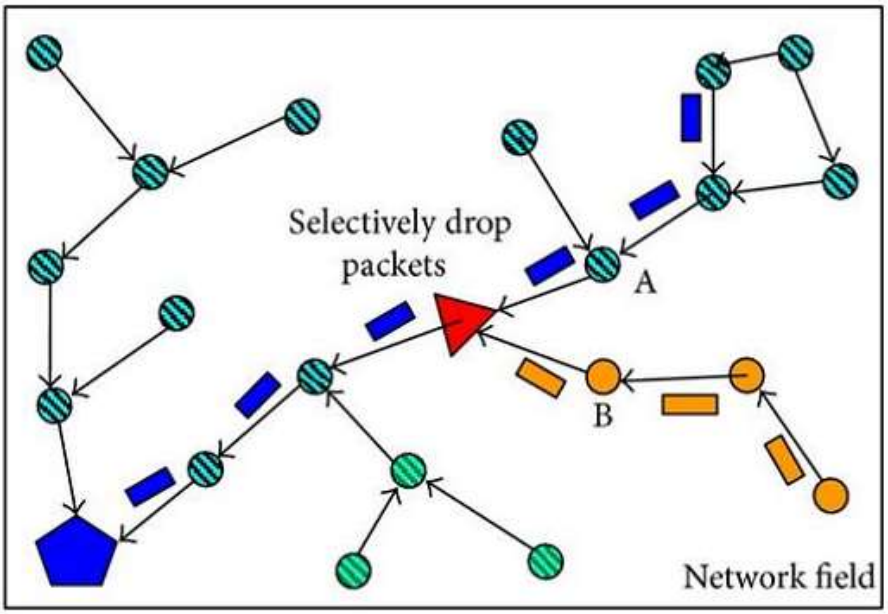
Το στρώμα Δικτύου είναι υπεύθυνο για τη δρομολόγηση των σημάτων, την ανακάλυψη των γειτονικών κόμβων και την ανάκτηση συνδέσμων. Οι συνηθισμένοι τύποι επιθέσεων DoS στο επίπεδο δικτύου σε ένα WSN ταξινομούνται στις κατηγορίες των επιθέσεων Υποκλοπής-Παραπλάνησης (Spoofing), Επιλεκτικής Προώθησης (selective forwarding), Επιστροφής (homing) και Μαύρης Τρύπας (Black-hole), όπως θα δούμε παρακάτω.

- *IP Spoofing:* Η συγκεκριμένη επίθεση λαμβάνει χώρα κατά των προτύπων που προβλέπουν ανταλλαγή μηνυμάτων αναγνώρισης. Με την αλλοίωση αυτών των μηνυμάτων, ο επιτιθέμενος στοχεύει στη δημιουργία δυσλειτουργιών στη διακίνηση πληροφοριών στο δίκτυο. Ο εισβολέας εκτελεί “ping” σε διάφορους κόμβους και η

[105] Liu, F., Marcellin, M. W., Goodman, N. A., & Bilgin, A. (2014, March): Compressive Detection of Multiple Frequency-Hopping Spread Spectrum Signals. In 2014 Data Compression Conference (pp. 415-415). IEEE. doi: 10.1109/DCC.2014.18.

διεύθυνση προέλευσης στο “ping” περιέχει τη διεύθυνση του κόμβου του θύματος. Έτσι, όλες οι απαντήσεις εκτρέπονται στον κόμβο του θύματος.

- *Επιλεκτική προώθηση*: Ένας κόμβος δικτύου, λαμβάνοντας ένα πακέτο από γειτονικό του κόμβο, το προωθεί σε έναν άλλο γειτονικό του κόμβο, σύμφωνα με το μονοπάτι πολλαπλών αλμάτων που έχει καθορίσει το πρωτόκολλο δρομολόγησης. Ένας κόμβος που έχει προσβληθεί θα προωθήσει με επιλεκτικό τρόπο ορισμένα πακέτα, απορρίπτοντας τα υπόλοιπα τα οποία χάνονται. Επέκταση της επίθεσης επιλεκτικής προώθησης θεωρείται η επίθεση «μαύρης τρύπας» (blackhole attack), στην οποία ο επιτιθέμενος κόμβος απορρίπτει κάθε πακέτο που λαμβάνει, χωρίς να το προωθεί στον επόμενο κόμβο, παρακάμπτοντας τις κατευθύνσεις του αλγόριθμου δρομολόγησης.



Εικόνα 7-3: Επίθεση DoS Επιλεκτικής προώθησης (selective forwarding)

- *Homing*: Σε ένα WSN υπάρχουν κόμβοι με αυξημένες αρμοδιότητες όπως για παράδειγμα ο συντονιστικός κόμβος, οι κεφαλές συστάδων (cluster heads), οι δρομολογητές κλπ. Η συγκεκριμένη επίθεση παρακολουθεί τη δρομολόγηση πακέτων στο δίκτυο και, όταν ανιχνεύσει τους κρίσιμους κόμβους, δίνει τη δυνατότητα στον επιτιθέμενο να στοχεύσει κακόβουλα κατά αυτών.

Στρώμα Μεταφοράς (Transport layer)

Το στρώμα μεταφοράς είναι υπεύθυνο για την αξιόπιστη σύνδεση μεταξύ δύο κόμβων από άκρο-σε άκρο (end-to-end).Οι επιθέσεις άρνησης υπηρεσίας που μπορούν να προσβάλλουν αυτό το επίπεδο, είναι το συγχρονισμένο πλημμύρισμα (Synchronized Flooding) και ο αποσυγχρονισμός (Desynchronization)**.**

- *Συγχρονισμένο Πλημμύρισμα (Synchronized flooding):* Η επίθεση αυτή πραγματοποιείται με την αποστολή επαναλαμβανόμενων πακέτων από τον κακόβουλο κόμβο (initiating node) ή λογισμικό, προς τον κόμβο προορισμού που

πρόκειται να προσβληθεί (destination). Ο κόμβος που προσβάλλεται διαθέτει ενεργειακούς πόρους ώστε να διατηρήσει τη σύνδεση με τον κόμβο που αποστέλλει τα περίσσεια μηνύματα. Ο μεγάλος αριθμός λήψεων που προκαλείται στον κόμβο-θύμα εξαντλεί τα ενεργειακά του αποθέματα και κατά συνέπεια το χρόνο ζωής του και παραμονής του στο δίκτυο.

- *Αποσυγχρονισμός (desynchronization):* Σε αυτού του τύπου την επίθεση, η επικοινωνία μεταξύ δύο γειτονικών κόμβων διακόπτεται από τον εισβολέα, ο οποίος αποστέλλει πακέτα με ψεύτικες σημαίες (flags) ώστε να αποσυγχρονίσει τα δύο από άκρο-σε-άκρο τερματικά (end-to-end terminals).

Στρώμα Εφαρμογής (Application layer)

Το στρώμα εφαρμογής παρέχει στον χρήστη τον τρόπο ώστε να προσπελάσει, μέσω μίας εφαρμογής, τις πληροφορίες ενός ασύρματου δικτύου. Αυτό το επίπεδο είναι η κύρια διασύνδεση του χρήστη με την εφαρμογή και, συνεπώς, με το δίκτυο. Στο επίπεδο αυτό γίνεται η διαχείριση των κατανεμημένων εφαρμογών, η αποστολή του ηλεκτρονικού ταχυδρομείου, των αυτόματων ειδοποιήσεων (push notifications) κλπ. Σε αυτό το επίπεδο οι πιθανές επιθέσεις DoS που θα συναντήσουμε είναι η επίθεση καταπίεσης 9Overwhelm attack) και η επίθεση επαναπρογραμματισμού (reprogram attack).

- *Επίθεση καταπίεσης (overwhelm attack):* Η επίθεση καταπίεσης παρακινεί τους κόμβους του δικτύου να στείλουν μεγάλο όγκο πακέτων προς τον σταθμό βάσης. Με τον τρόπο αυτό δημιουργείται συμφόρηση πακέτων και εξάντληση πόρων του δικτύου, όπως για παράδειγμα το διαθέσιμο εύρος ζώνης.

- *Επίθεση επαναπρογραμματισμού (reprogram attack):* Κατά τη διαδικασία απομακρυσμένου επαναπρογραμματισμού μίας συσκευής στο δίκτυο, είναι δυνατό να παρεισφρήσει κακόβουλα ο επιτιθέμενος, κατέχοντας του κωδικούς πρόσβασης του μηχανικού δικτύου, με στόχο την ανάληψη ελέγχου του προγραμματισμού ή την αλλαγή παραμέτρων για την πρόκληση δολιοφθοράς.

7.2.2 Άλλες Κατηγορίες Επιθέσεων σε WSNs

Άλλοι προβληματισμοί που αφορούν στα WSNs περιλαμβάνουν την προστασία του απορρήτου, μη εξουσιοδοτημένα σημεία πρόσβασης, άγνωστους σταθμούς βάσης, μη καταγεγραμμένους κόμβους και πλαστογραφημένες αναγνωρίσεις. Επιπλέον, η επιτόπια συντήρηση για απομακρυσμένα εγκατεστημένους κόμβους αισθητήρων είναι πολλές φορές ανέφικτη, επομένως πρέπει να υπάρχει μία ενδελεχής εξέταση των λύσεων ασφαλείας και των εργαλείων αντιμετώπισης προβλημάτων. Ορισμένες ενδιαφέρουσες περιπτώσεις επιθέσεων θα δούμε συνοπτικά παρακάτω [213]:

Επίθεση Σύλληψης Κόμβου (Node Capture Attack)

Μία από τις ξεχωριστές επιθέσεις στα WSN είναι η σύλληψη κόμβου. Σε αυτήν την επίθεση, ένας εισβολέας αποκτά τον πλήρη έλεγχο ενός κόμβου αισθητήρα μέσω άμεσης και μη

εξουσιοδοτημένης φυσικής πρόσβασης. Στη συνέχεια, ο εισβολέας μπορεί εύκολα να εξαγάγει κρυπτογραφικά κλειδιά και να αποκτήσει απεριόριστη πρόσβαση στις πληροφορίες που είναι αποθηκευμένες στο τσιπ μνήμης του καταγεγραμμένου κόμβου μέσω μίας διαδικασίας αντίστροφης μηχανικής (reverse engineering) με τη δυνατότητα να προκαλέσει σημαντική ζημιά σε ολόκληρο το δίκτυο. Εάν οι κόμβοι αισθητήρων εντός του WSN μοιράζονται ένα κλειδί – ή κλειδιά με γειτονικούς κόμβους – που χρησιμοποιείται για την κρυπτογράφηση ή αποκρυπτογράφηση δεδομένων, αυτό αποτελεί έναν σημαντικό παράγοντα ευπάθειας και θέτει το δίκτυο τελικά ως ευάλωτο σε επιθέσεις αυτού του είδους. Η επίθεση σύλληψης κόμβων έχει μεγάλο αντίκτυπο στη δομή ή στην τοπολογία ενός WSN.

Επίθεση Πλευρικών Καναλιών (Side Channel Attack)

Η επίθεση πλευρικού καναλιού (side channel attack) αναφέρεται σε κάθε επίθεση που βασίζεται σε πληροφορίες οι οποίες συλλέγονται από τη φυσική εφαρμογή ενός κρυπτοσυστήματος, σε αντίθεση με τα τρωτά σημεία του ίδιου του αλγορίθμου. Για παράδειγμα, ο εισβολέας παρακολουθεί τον αλγόριθμο δρομολόγησης ενός δικτύου και στη συνέχεια αναλύει τα δεδομένα που συλλέγονται, για να εξάγει το σχετικό κλειδί κρυπτογράφησης.

Οι επιθέσεις πλευρικών καναλιών περιλαμβάνουν:

- Την απλή ανάλυση ισχύος (Simple Power Analysis - SPA) η οποία είναι μία τεχνική που περιλαμβάνει την άμεση ερμηνεία των μετρήσεων κατανάλωσης ενέργειας που συλλέγονται κατά τη διάρκεια κρυπτογραφικών λειτουργιών επικοινωνίας του δικτύου,
- Την απλή ηλεκτρομαγνητική ανάλυση (Simple Electro Magnetic Analysis - SEMA) η οποία είναι σε θέση ώστε να εξάγει πληροφορίες από ένα ηλεκτρομαγνητικό δείγμα το οποίο λαμβάνεται κατά την εκπομπή σημάτων από τον έναν κόμβο στον άλλο, εντός του δικτύου,
- Τη διαφορική ανάλυση[106] ισχύος (Differential Power Analysis - DPA) η οποία παρακολουθεί την ισχύ που καταναλώνουν οι συσκευές στο σύνολο, και στη συνέχεια αναλύει στατιστικά τα συλλεγμένα δεδομένα ώστε να εξάγει ένα κλειδί κρυπτογράφησης,
- Στη διαφορική ηλεκτρομαγνητική ανάλυση (Differential Electro Magnetic Analysis - DEMA), στην οποία ο επιτιθέμενος παρακολουθεί τις ηλεκτρομαγνητικές εκπομπές από το σύνολο των συσκευών και στη συνέχεια γίνεται η ίδια στατιστική ανάλυση με αυτήν για τη διαφορική ανάλυση στα συλλεγμένα ηλεκτρομαγνητικά δεδομένα για την εξαγωγή μυστικών κλειδιών.

[106] Στα μαθηματικά, ο διαφορικός λογισμός είναι μία υποκατηγορία του λογισμού με αντικείμενο τη μελέτη των ρυθμών μεταβολής των ποσοτήτων. Εφόσον η σχέση μεταξύ συνεχώς μεταβαλλόμενων ποσοτήτων και του ρυθμού μεταβολής με το χρόνο είναι γνωστή, η διαφορική ανάλυση επιτρέπει την επεξεργασία αυτής της σχέσης προκειμένου να μοντελοποιήσουμε και να περιγράψουμε φυσικά φαινόμενα, τεχνικές ή φυσικές διεργασίες ή δυναμικά συστήματα. Ένα χαρακτηριστικό παράδειγμα προέρχεται από την κλασική μηχανική όπου η κίνηση ενός σώματος περιγράφεται από τη θέση και την ταχύτητά του σε συνάρτηση με το χρόνο. Πηγή: https://el.wikipedia.org/wiki/Διαφορικός_λογισμός

Επιθέσεις Λογισμικού (Software Attacks)

Ένας εισβολέας μπορεί να προσπαθήσει να τροποποιήσει τον κώδικα λογισμικού σε μία μνήμη ή να εκμεταλλευτεί γνωστά τρωτά σημεία. Ένα γνωστό παράδειγμα μίας τέτοιας επίθεσης είναι μία επίθεση υπερχείλισης αποθηκευτικού χώρου (buffer). Σε αυτόν τον τύπο επίθεσης, μία διαδικασία προσπαθεί να αποθηκεύσει δεδομένα πέρα από τα όρια ενός σταθερού μήκους, με αποτέλεσμα τα επιπλέον δεδομένα να αντικαταστήσουν τις παρακείμενες θέσεις μνήμης.

Επιθέσεις Δρομολόγησης (Routing Attacks)

Η επικοινωνία στα WSNs βασίζεται στη θεώρηση κατά την οποία τα δεδομένα κινούνται προς έναν σταθμό βάσης, σε διάφορα μοτίβα. Ένας εισβολέας είναι σε θέση να συλλέξει πολλές πληροφορίες σχετικά με την τοπολογία του δικτύου, καθώς και με τη θέση του σταθμού βάσης και άλλων στρατηγικών κόμβων, παρατηρώντας τον όγκο και το μοτίβο κίνησης.

Υπάρχουν δύο τύποι επιθέσεων ανάλυσης κίνησης στα WSN, ήτοι: μία επίθεση παρακολούθησης ρυθμού και μία επίθεση συσχέτισης χρόνου. Σε μία επίθεση παρακολούθησης ρυθμού (rate monitoring attack), ένας εισβολέας παρακολουθεί τον ρυθμό αποστολής πακέτων των κόμβων κοντά στον επιτιθέμενο και πλησιάζει τους κόμβους που έχουν υψηλότερο ρυθμό αποστολής πακέτων. Σε μία επίθεση συσχέτισης χρόνου (time correlation attack), ένας επιτιθέμενος παρατηρεί τη συσχέτιση στην αποστολή χρόνου μεταξύ ενός κόμβου και του γειτονικού του κόμβου που υποτίθεται ότι προωθεί το ίδιο πακέτο, και εξάγει την διαδρομή ακολουθώντας το σήμα για κάθε λειτουργία προώθησης, καθώς το πακέτο διαδίδεται προς τον σταθμό βάσης.

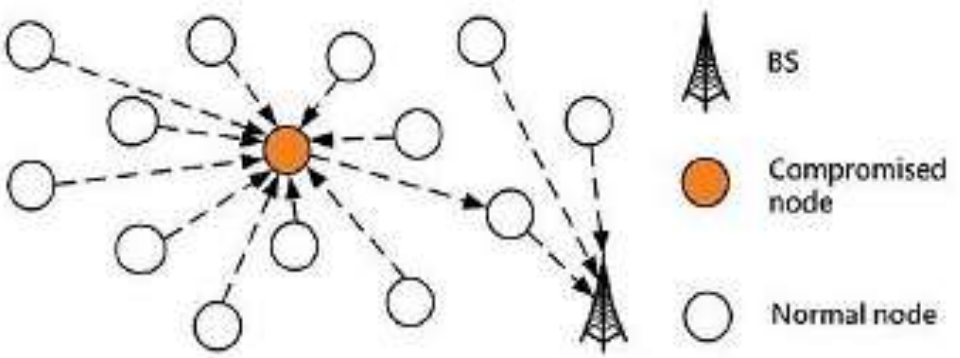
Επιθέσεις Αντιγραφής (Replication Attacks)

Υπάρχουν δύο τρόποι εκκίνησης επιθέσεων αναπαραγωγής σημάτων σε ένα WSN. Πρώτον, ένας εισβολέας μπορεί να παρακολουθεί τις επικοινωνίες και να ξαναστείλει παλιά πακέτα πολλές φορές, για να σπαταλήσει την ενέργεια των γειτονικών κόμβων αισθητήρων. Κατά τον δεύτερο τρόπο, ο εισβολέας μπορεί να εισαγάγει πρόσθετους κλώνους κόμβων αισθητήρων στο WSN αφού έχει πρώτα λάβει κρυπτογραφημένες πληροφορίες από το δίκτυο. Η φυσική επίθεση στοχεύει στη φυσική καταστροφή του κόμβου από τον επιτιθέμενο. Οι κόμβοι που δέχονται φυσική επίθεση είναι δυνατόν να αντικατασταθούν από τον επιτιθέμενο με κόμβους που είναι προγραμματισμένοι από αυτόν και βρίσκονται υπό τον έλεγχό του (επίθεση αναπαραγωγής κόμβου). Με τον τρόπο αυτό, ο επιτιθέμενος μπορεί να θέσει υπό τον έλεγχό του ένα τμήμα του δικτύου και να εξαπολύει μέσω αυτού επιθέσεις προς το υπόλοιπο δίκτυο. Προστασία από τέτοιου είδους φυσικές επιθέσεις μπορεί να πραγματοποιηθεί με φυσική απόκρυψη των κόμβων στον χώρο ανάπτυξης του δικτύου.

Επίθεση Καταβόθρας (Sinkhole)

Στην επίθεση καταβόθρας, ένας κόμβος διαρρηγνύεται με σκοπό να διαχειρίζεται τις πληροφορίες δρομολόγησης που έχει υποκλέψει από το δίκτυο ώστε να γίνει ελκυστικός στους γειτονικούς του κόμβους για λήψη πακέτων από αυτούς. Ως αποτέλεσμα αυτού, οι

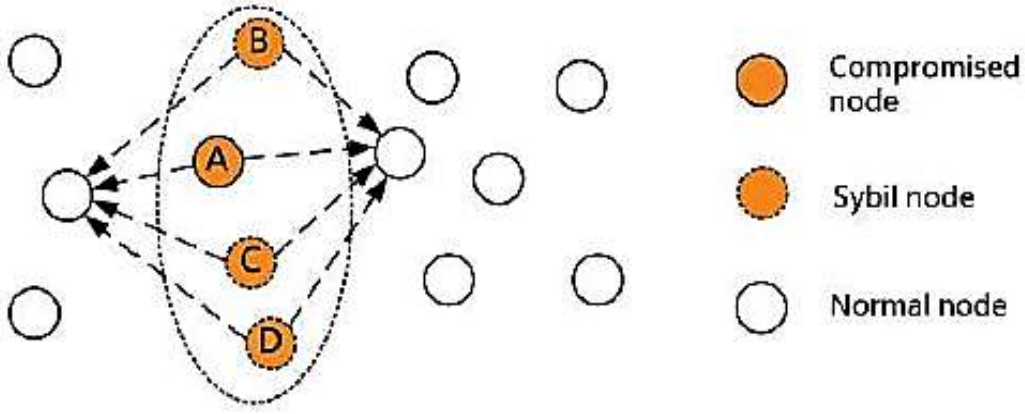
γειτονικοί κόμβοι επιλέγουν τον συγκεκριμένο κόμβο για την προώθηση των μηνυμάτων που λαμβάνουν. Με τον τρόπο αυτό, ο επιτιθέμενος μπορεί να ελέγξει τη ροή πληροφοριών εντός του δικτύου μέσω του προσβεβλημένου κόμβου.



Εικόνα 7-4: Σχηματική αναπαράσταση επίθεσης καταβόθρας (sinkhole attack)

Σιβυλλική Επίθεση (Sybil Attack)

Η σιβυλλική επίθεση σκοπεύει στο να δώσει πολλαπλές ταυτότητες σε έναν κόμβο (στην Εικόνα. 7-5 ο παραβιασμένος κόμβος είναι ο Α). Με τον τρόπο αυτό, ο προσβεβλημένος κόμβος μπορεί να μιμηθεί ταυτότητες άλλων κόμβων ή να αναπαράγει νέες ψεύτικες ταυτότητες. Οι ψεύτικες ταυτότητες υλοποιούν ισάριθμους εικονικούς κόμβους, οι οποίοι καλούνται ως σιβυλλικοί κόμβοι. Οι κόμβοι αυτοί συμμετέχουν κανονικά στις λειτουργίες του δικτύου WSN, αν και αποτελούν στη πραγματικότητα μόνο μία συσκευή. Αποτέλεσμα της επίθεσης είναι η μεγαλύτερη ενεργειακή επιβάρυνση της προσβεβλημένης συσκευής, σε σύγκριση με τις υπόλοιπες συσκευές του δικτύου.



Εικόνα 7-5: Σιβυλλική επίθεση (sybil attack)

Στον Πίνακα 7-1 συγκεντρώνονται συνοπτικά τα είδη επιθέσεων ασφαλείας στα WSN που συναντήσαμε παραπάνω, και ταξινομούνται σύμφωνα με το στρώμα στο οποίο το κάθε είδος επιδρά.

Επίθεση	Στρώμα	Μηχανισμός	Στόχος
Παρεμβολή (jamming)	Φυσικό (Physical)	Πλημμύρισμα τμήματος του δικτύου με θόρυβο	Διαθεσιμότητα/ Ακεραιότητα
Παραβίαση (tampering)		Καταστροφή κόμβων και υποκλοπή δεδομένων	Εμπιστευτικότητα/ Ακεραιότητα/ Αυθεντικότητα
Καταστροφή υλικού		Καταστροφή κόμβου	Διαθεσιμότητα/ Ακεραιότητα
Αναπαραγωγή (replication)		Αντιγραφή κόμβου υπό τον έλεγχο του επιτιθέμενου	Διαθεσιμότητα/ Ακεραιότητα
Σύγκρουση δεδομένων (collision)	Ζεύξης δεδομένων (Data link)	Απώλεια δεδομένων	Διαθεσιμότητα
Εξάντληση (exhaustion)		Εξάντληση ενεργειακών πόρων	Διαθεσιμότητα
Επιλεκτική προώθηση (selective forwarding)	Δικτύου (network)	Απώλεια δεδομένων	Εμπιστευτικότητα/ Διαθεσιμότητα
Καταβόθρας (sinkhole)		Έλεγχος δρομολόγησης	Εμπιστευτικότητα/ Ακεραιότητα/ Αυθεντικότητα
Εξαπάτηση αναγνώρισης (spoofing)		Διακίνηση ψευδών μηνυμάτων	Αυθεντικότητα/ Διαθεσιμότητα
Σκουληκότρυπα (wormhole)		Έλεγχος δρομολόγησης	Εμπιστευτικότητα/ Αυθεντικότητα
Σιβυλλική (sybil)		Δυσλειτουργία στην δρομολόγηση	Αυθεντικότητα/ Διαθεσιμότητα
Ανάλυση κίνησης (traffic analysis)		Ανίχνευση κόμβων κρίσιμης σημασίας	Εμπιστευτικότητα
Πλημμύρα (flooding)	Μεταφοράς (Transport)	Εξάντληση πόρων	Διαθεσιμότητα
Αποσυγχρονισμός (desynchronization)		Δυσλειτουργίες σύνδεσης	Αυθεντικότητα/ Διαθεσιμότητα
Λογισμικό κακόβουλης επίθεσης (malicious sotware)	Εφαρμογής (Application)	Δυσλειτουργία κόμβων - καθυστερήσεις δικτύου	Διαθεσιμότητα
Αποσυγχρονισμός ρολογιού (clock desynchronization)		Λανθασμένες μετρήσεις	Διαθεσιμότητα

Πίνακας 7-1: Επιθέσεις στα ασύρματα δίκτυα αισθητήρων WSNs

7.3 Μηχανισμοί Ασφαλείας WSN

Στο προηγούμενο κεφάλαιο αναφέραμε τις επιθέσεις που θέτουν υπό αμφισβήτηση την ασφάλεια επικοινωνιών σε ένα WSN. Οι στόχοι του επιτιθέμενου, όπως είδαμε αφορούν στη δημιουργία κενών και αμφισβητήσεων όσον αφορά στην ικανοποίηση των

προδιαγραφών ασφάλειας του δικτύου, ώστε με τον τρόπο αυτό η κακόβουλη ενέργεια να θίγει την αξιοπιστία του, την ακεραιότητά του και τη διαθεσιμότητά του.

Ως εκ των παραπάνω, η ασφάλεια των WSNs έχει μεγάλη σημασία, ιδιαίτερα όταν αυτά τα δίκτυα προορίζονται για την προστασία κρίσιμων υποδομών και στρατιωτικών εγκαταστάσεων. Για το λόγο αυτό, είναι απαραίτητη η πρόβλεψη μηχανισμών ασφαλείας οι οποίοι λειτουργούν ως «αντίμετρα» στις πιθανές επιθέσεις εναντίον ενός δικτύου αισθητήρων. Οι περισσότεροι μηχανισμοί ασφαλείας χρησιμοποιούν περισσότερους από έναν αλγορίθμους ή πρωτόκολλα επικοινωνίας, με αποτέλεσμα την αύξηση της πολυπλοκότητας. Επιπρόσθετα, είναι απαραίτητο οι συσκευές του δικτύου να χρησιμοποιούν μυστικά κλειδιά κρυπτογράφησης, γεγονός που περιπλέκει επιπλέον τον σχεδιασμό, ως προς τη διακίνηση και προστασία αυτής της μυστικής πληροφορίας [213].

Ένας μηχανισμός ασφάλειας θα πρέπει να σχεδιάζεται λαμβάνοντας υπόψη τα χαρακτηριστικά επανατακτικότητας, ακεραιότητας και διαθεσιμότητας ενός δικτύου. Για να εξασφαλιστεί η διάθεση των χαρακτηριστικών αυτών, και προκειμένου ένα WSN να μπορεί να αποκρούσει με επιτυχία τυχόν εκδήλωση, θα πρέπει να λαμβάνονται υπόψη τα εξής[107]:

- Ο μηχανισμός ασφαλείας οφείλει να συμμορφώνεται στις απαιτήσεις (προδιαγραφές) ασφαλείας που θέτει ο εκάστοτε κρατικός ή διεθνικός οργανισμός διασφάλισης ποιότητας[108].
- Ο μηχανισμός ασφαλείας οφείλει να μην επηρεάζεται από ενδεχόμενη προσβολή κόμβων και να παρέχει ευρωστία ώστε να είναι σε θέση να συνεχίζει το έργο του.
- Σε ένα WSN, στόχος είναι η μεγιστοποίηση του χρόνου ζωής του, άρα ο μηχανισμός ασφαλείας οφείλει να είναι συμβατός με αυτή την απαίτηση και τη διασφάλιση των ενεργειακών πόρων.
- Η διαχείριση κρυπτογραφικών κλειδιών πρέπει να χαρακτηρίζεται από ευελιξία στη χρήση σε διαφόρους τύπους ανάπτυξης δικτύου.
- Η κλιμακοθετησιμότητα (scalability) θεωρείται απαραίτητο χαρακτηριστικό ενός μηχανισμού ασφαλείας.
- Ο μηχανισμός ασφαλείας οφείλει να μπορεί να παρέχει ασφάλεια στο δίκτυο, ακόμα και με το ενδεχόμενο ύπαρξης σφαλμάτων σε αυτό ή καταστάσεων που τα προκαλούν (π.χ. καταστροφή κόμβων ή παρουσία κακόβουλης ενέργειας).

Ανίχνευση Παρείσφρησης (Intrusion Detection)

Οι μηχανισμοί ασφαλούς δρομολόγησης και συνάθροισης δεδομένων, από μόνοι τους, δεν είναι αρκετοί ώστε να εξασφαλίσουν την πλήρη κάλυψη των απαιτήσεων ασφαλείας ενός δικτύου WSN. Η πιθανότητα εισαγωγής ψευδών δεδομένων από έναν επιτιθέμενο,

[107] Wang, Y., Attebury, G., & Ramamurthy, B. (2006): A Survey of Security Issues in Wireless Sensor Networks. IEEE Communications Surveys and Tutorials, 8(2), pp.2-23.

[108] Στα πλαίσια της Ευρωπαϊκής Ένωσης, η Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 6ης Ιουλίου 2016, καθορίζει τα μέτρα σχετικά το υψηλό κοινό επίπεδο ασφάλειας δικτύων και συστημάτων πληροφοριών σε ολόκληρη την Ένωση.
Πηγή: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

δημιουργεί την ανάγκη ανάπτυξης μηχανισμών ανίχνευσης παρεισφρήσεων. Ένα σύστημα ανίχνευσης παρείσφρησης (Intrusion Detection System – IDS) βασίζεται στην παρακολούθηση του δικτύου και στον εντοπισμό παρατηρήσεων που διαφοροποιούνται από ένα φυσιολογικό πλαίσιο συμπεριφορών[109].

Τα συστήματα ανίχνευσης παρείσφρησης ταξινομούνται σε αυτά τα οποία είναι βασισμένα σε κανόνες (rule – based) και σε εκείνα που βασίζονται στην ανίχνευση στατιστικών ανωμαλιών (anomaly – based)[110]. Τα συστήματα IDS της πρώτης κατηγορίας είναι σχεδιασμένα ώστε να ανιχνεύουν γνωστά πρότυπα παρεισφρήσεων, ενώ τα anomaly-based συστήματα IDS κινούνται προς την κατεύθυνση ανίχνευσης άγνωστης μορφής ανωμαλιών στο δίκτυο. Τα συγκεκριμένα συστήματα ενεργοποιούν έναν συναγερμό στο δίκτυο, με στόχο την ενεργοποίηση των υπευθύνων και την καταπολέμηση της παράβασης. Τα rule-based συστήματα IDS χαρακτηρίζονται από χαμηλότερο ποσοστό ψευδών συναγερμών σε σύγκριση με τα αντίστοιχα anomaly-based, με αντίτιμο όμως το χαμηλότερο ποσοστό ανίχνευσης παρεισφρήσεων (μικρότερη αποτελεσματικότητα ανίχνευσης).

Στα ασύρματα δίκτυα αισθητήρων, εξαιτίας των υπολογιστικών, αποθηκευτικών και ενεργειακών περιορισμών, η ενημέρωση των κόμβων ως προς ένα φυσιολογικό πλαίσιο συμπεριφορών του δικτύου είναι δύσκολη και πολλές φορές ανέφικτη, καθώς κρίνεται μη αποδοτική ενεργειακά. Για το λόγο αυτό αποτελεί πρόκληση η σχεδίαση μηχανισμών ανίχνευσης παρεισφρήσεων σε δίκτυα WSN. Στη βιβλιογραφία αναφέρονται λύσεις όπως οι τεχνικές IHOP[111] και SEF[112].

Η τεχνική IHOP (Interleaved Hop-by-Hop Authentication) εφαρμόζεται σε δίκτυα ιεραρχικής δρομολόγησης ώστε να ο σταθμός βάσης να έχει την ικανότητα να ανιχνεύσει ψευδή δεδομένα που έχουν εισαχθεί στο δίκτυο. Η συγκεκριμένη τεχνική καθορίζει ότι κάθε κόμβος μοιράζεται ένα κρυπτογραφικό κλειδί με τον σταθμό βάσης, και κάθε κόμβος γνωρίζει τους γειτονικούς του κόμβους (απόσταση ενός άλματος) και μοιράζεται με αυτούς κρυπτογραφικά κλειδιά. Επίσης κάθε κόμβος μπορεί να καθορίσει κρυπτογραφικό κλειδί και με μη γειτονικούς κόμβους, εφόσον χρειαστεί.

Ο μηχανισμός SEF (Statistical En-route Filtering) αποσκοπεί στην ανίχνευση και απόρριψη ψευδών δεδομένων μέσω της διαδικασίας προώθησης μηνυμάτων προς τον σταθμό βάσης. Ο μηχανισμός λειτουργεί με την υπόθεση ότι το ψευδές γεγονός γίνεται αντιληπτό από έναν αριθμό αισθητήριων κόμβων, οι οποίοι λειτουργούν συνεργατικά για την ανίχνευση και την αντιμετώπιση της επίθεσης. Είναι δυνατή η απόρριψη περισσότερο από το 70% ψευδών δεδομένων μέσα στα επόμενα πέντε άλματα και με αυτόν τον τρόπο επιτυγχάνεται σημαντική εξοικονόμηση ενέργειας.

---

[109] Jaydip S., (2012). A Survey on Wireless Sensor Network Security. Tata Consultancy Services Limited, Wireless & Multimedia Innovation Lab, Bengal Intelligent Park, Salt Lake Electronics Complex, Kolkata, India, pp.55-78.

[110] Stallings, W., Brown, L., Bauer, M. D., & Bhattacharjee, A. K. (2012). Computer security: principles and practice. Upper Saddle River, NJ, USA. Pearson Education.

[111] S. Zhu, S. Setia, S. Jajodia, and P. Ning (2004): "An interleaved hop by hop authentication scheme for filtering of injected false data in sensor networks". In Proceedings of IEEE Symposium on Security and Privacy, Oakland, CA, May 2004, pp.259-271.

[112] Ye, F., et al., "Statistical En-Route Filtering of Injected False Datasensor Networks". In Proceedings of the IEEE INFOCOM, Hong Kong, 2004.

Αναπαραγωγή Κόμβου

Ένας επιπλέον μηχανισμός άμυνας για την τυχαία αναπαραγωγή κόμβου είναι ο εξοπλισμός των κόμβων με υλισμικό, το οποίο θα τους προστατεύει από τους επιτιθέμενους. Για παράδειγμα, η ύπαρξη υλισμικού με αντίσταση τροποποίησης έχει σκοπό την αποτροπή του επιτιθέμενου στην τροποποίηση ή υποκλοπή δεδομένων που διαχειρίζονται οι κόμβοι. Επίσης, μία ακόμα λύση στην αντιμετώπιση φυσικών επιθέσεων προσφέρει ο αυτο-τερματισμός της συσκευής (self-termination). Σύμφωνα με αυτή, ο κόμβος τερματίζει τη λειτουργία του, καταστρέφοντας δεδομένα και κρυπτογραφικά κλειδιά, όταν ανιχνεύσει μία πιθανή επίθεση. Η τεχνική αυτή είναι αποδοτικότερη σε δίκτυα που υπάρχει πλεονασμός πληροφορίας, ενώ το κλειδί της προσέγγισης αυτής είναι ο εντοπισμός της επίθεσης και η περιοδική αναζήτηση των γειτονικών κόμβων.

Επίθεση καταβόθρας

Το πρωτόκολλο δρομολόγησης Mint-Route[113] παρέχει δυνατότητα ανίχνευσης και καταπολέμησης της συγκεκριμένης επίθεσης. Στο συγκεκριμένο πρωτόκολλο, κάθε κόμβος υπολογίζει την ποιότητα της ζεύξης (link quality) με τους γειτονικούς του κόμβους και σύμφωνα με αυτή, υλοποιείται ένα «δέντρο δρομολόγησης» προς τον σταθμό βάσης. Η ποιότητα της ζεύξης μπορεί να μετρηθεί είτε με το ποσοστό πακέτων που χάνονται είτε με βάση τον λόγο σήματος/θορύβου (Signal to Noise Ratio - SNR) που επιτυγχάνεται.

Σιβυλλική Επίθεση

Στη βιβλιογραφία[114], γνώμονας στις μεθόδους αντιμετώπισης είναι η πιστοποίηση ταυτότητας των κόμβων που συμμετέχουν στο δίκτυο. Η συνηθέστερη λύση είναι η χρήση κρυπτογράφησης δημοσίου κλειδιού[115]. Η προσέγγιση της εμπιστευμένης πιστοποίησης (trusted certification) εξαλείφει εντελώς την επίθεση και εξασφαλίζει ότι κάθε οντότητα του δικτύου έχει μία πιστοποιημένη ταυτότητα. Στη προσέγγιση αυτή, είναι απαραίτητη η ανίχνευση των χαμένων ή κλεμμένων ταυτοτήτων και στη συνέχεια η ανάκλησή τους (απόρριψη από το δίκτυο).

Επίθεση Ανάλυσης Κίνησης

Στη βιβλιογραφία[116] προτείνονται τρεις μέθοδοι για την αντιμετώπιση επίθεσης ανάλυσης κίνησης. Οι μέθοδοι αυτοί στοχεύουν στη δημιουργία κίνησης σε τυχαίες κατευθύνσεις εντός του δικτύου, έτσι ώστε να επιτευχθεί παραπλάνηση του εισβολέα, ως προς τη θέση

---

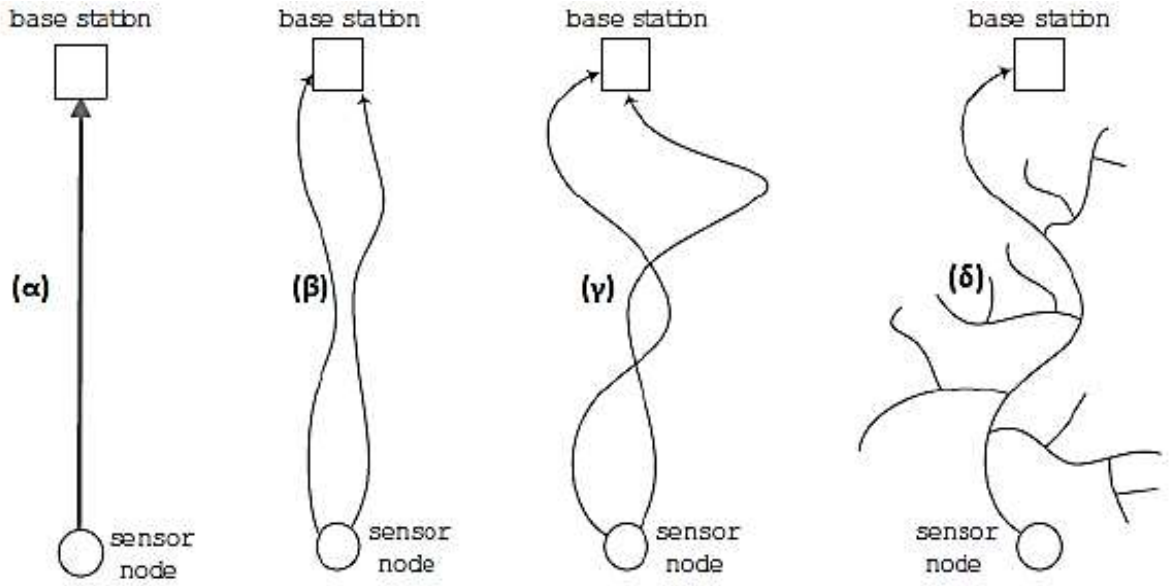
[113] Hegazy, I., Safavi-Naini, R., & Williamson, C. (2010, June). Towards securing mintroute in wireless sensor networks. In Proceedings of the 2010 IEEE International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM) (pp. 1-6). IEEE.

[114] Douceur, J. R. (2016). The Sybil Attack-Microsoft Research. In Proceedings of the 1st International Workshop on Peer-to-Peer Systems.

[115] Βλέπε π.χ.: https://en.wikipedia.org/wiki/Public-key_cryptography

[116] Deng, J., Han, R., and Mishra, S. (2005): Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks. In Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), 2005, pp. 113-126. doi: 10.1109/SECURECOMM.2005.16.

του σταθμού βάσης. Η πρώτη είναι η τεχνική MPR (multiple parent routing), η οποία επιτρέπει τη δρομολόγηση των πακέτων από τον αισθητήριο κόμβο μέχρι τον σταθμό βάσης μέσω εναλλακτικών δρομολογίων (Εικόνα 7-6.(β)) και όχι μέσω του συντομότερου μονοπατιού (Εικόνα 7-6.(α)). Η δεύτερη μέθοδος είναι η τεχνική RW (Random Walk, Εικόνα 7-6.(γ)). Σύμφωνα με αυτή, το μονοπάτι δρομολόγησης καθορίζεται από έναν αλγόριθμο προώθησης που εισάγει τυχαιότητα στον προσδιορισμό του. Κάθε κόμβος που λαμβάνει ένα πακέτο το προωθεί με την ίδια πιθανότητα σε οποιονδήποτε γειτονικό του. Αν και η τεχνική RW εισάγει τυχαιότητα και είναι αποτελεσματικότερη στην παραπλάνηση του εισβολέα, σε σύγκριση με τη τεχνική MPR μπορεί να οδηγήσει σε μεγάλου μήκους μονοπάτια δρομολόγησης. Μεγάλου μήκους μονοπάτια δρομολόγησης όμως οδηγούν σε μεγαλύτερη κατά μέσο όρο κατανάλωση ενέργειας στους κόμβους του δικτύου. Η τρίτη μέθοδος αντιμετώπισης αναφερόμενη ως κλασμομορφική διάδοση (fractal propagation) βασίζεται στη δημιουργία ψευδών πακέτων και στη δημιουργία εικονικής κίνησης στο δίκτυο (Εικόνα 7-6.(δ)). Σύμφωνα με αυτή την τεχνική κάθε κόμβος, λαμβάνοντας ένα πακέτο, δημιουργεί με μία καθορισμένη πιθανότητα ένα ψευδές πακέτο και το προωθεί σε έναν γείτονά του. Ωστόσο, η τεχνική αυτή μειονεκτεί σχετικά με τη δημιουργία μεγάλης κυκλοφορίας κοντά στον σταθμό βάσης, γεγονός το οποίο αυξάνει το ποσοστό συγκρούσεων και την απώλεια πακέτων.



Εικόνα 7-6: Τεχνικές αντιμετώπισης κίνησης: (α) συντομότερο μονοπάτι δρομολόγησης, (β) τεχνική MPR, (γ) τεχνική RW, (δ) τεχνική κλασμομορφικής διάδοσης

7.3.1 Αντιμετώπιση Επιθέσεων DoS

Η αναφορά στις μεθόδους αντιμετώπισης επιθέσεων DoS γίνεται με βάση την πολυεπίπεδη αρχιτεκτονική του δικτύου WSN, όπως παρουσιάζεται παρακάτω σύμφωνα με τη βιβλιογραφία[117],[118]:

Φυσικό στρώμα

Η επίθεση παρεμβολής (Jamming) στο φυσικό στρώμα μπορεί να αντιμετωπιστεί με τις τεχνικές μεταπήδησης συχνότητας FHSS και εξάπλωσης κώδικα (code spreading). Η τεχνική μεταπήδησης συχνότητας μεταβάλλει συνεχώς την κεντρική συχνότητα επικοινωνίας μέσα στο προκαθορισμένο φάσμα, ακολουθώντας μία τυχαία ακολουθία. Το σήμα μεταδίδεται σε μία συχνότητα για σύντομη χρονική διάρκεια και έπειτα μεταπηδά σε μία άλλη συχνότητα. Ο αλγόριθμος μεταπήδησης της συχνότητας γνωστοποιείται από πριν τόσο στον πομπό, όσο και στον δέκτη. Εάν το σήμα ληφθεί από κάποιον μη εξουσιοδοτημένο δέκτη, ερμηνεύεται ως μικρής διάρκειας θόρυβος και αγνοείται. Ο επιτιθέμενος είναι αδύνατο να προβλέψει την ακολουθία μεταπήδησης συχνοτήτων και επομένως δεν μπορεί να δημιουργήσει παρεμβολή, η οποία να συμβαδίζει με αυτή. Ωστόσο, επειδή το διαθέσιμο φάσμα είναι περιορισμένο, ο επιτιθέμενος θα επιτύχει το σκοπό του, εάν παρεμβάλλεται σε όλο το διαθέσιμο εύρος συχνοτήτων.

Η αντιμετώπιση επιθέσεων αλλοίωσης ή υποκλοπής γίνεται με μηχανισμούς προστασίας παραβίασης των συσκευών που απαρτίζουν το δίκτυο. Η επιτυχία εξαρτάται από την ακρίβεια και την πληρότητα που έλαβαν υπόψη οι σχεδιαστές για πιθανές απειλές, τους πόρους που διατίθενται για τον σχεδιασμό, την κατασκευή και τη δοκιμή, καθώς και την ευφυΐα και αποτελεσματικότητα των εισβολέων. Επιπλέον προστασία από τέτοιου είδους επιθέσεις προσφέρει η φυσική απόκρυψη των συσκευών στην περιοχή εφαρμογής τους, καθώς και οι μηχανισμοί απενεργοποίησης της συσκευής σε περίπτωση παραβίασης (self-termination).

Στρώμα Ζεύξης

Η χρήση κωδικών διόρθωσης σφαλμάτων λύνει εν μέρει την επίθεση σύγκρουσης δεδομένων. Αυτοί οι κωδικοί λειτουργούν αποτελεσματικά σε συγκρούσεις μικρής κλίμακας, αν και προσθέτουν πολυπλοκότητα. Σε μία επίθεση δικτύου μεγάλης κλίμακας, αυτοί οι κωδικοί δεν μπορούν να λειτουργήσουν αποτελεσματικά, κάτι που αποτελεί ένα κενό ασφαλείας στο δίκτυο WSN. Είναι πιο αποτελεσματικό το να αποφεύγεται η χρήση πρωτοκόλλων MAC που υποστηρίζουν τη μορφή RTS/CTS[119]. Η αντιμετώπιση της επίθεσης εξάντλησης ενεργειακών πόρων μπορεί να γίνει με χρήση πολλαπλής πρόσβασης διαίρεσης χρόνου (TDMA). Σύμφωνα με αυτή, οι κόμβοι διαχωρίζονται στο πεδίο του χρόνου με

[117] Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks. Communications of the ACM, 47(6), 53-57.
[118] Gavric, Z., Simic, D. (2018). Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks. Ingeniería e Investigación, 38(1), 130-138. DOI: 10.15446/ing.investig.v38n1.65453.
[119] https://en.wikipedia.org/wiki/IEEE_802.11_RTS/CTS

εκχώρηση χρονοθυρίδων (timeslots) σε κάθε έναν εξ' αυτών. Κρίσιμη είναι η επίτευξη συγχρονισμού των κόμβων, η οποία εάν δεν επιτευχθεί, δημιουργείται παρεμβολή μεταξύ τους. Επιπλέον, για την αντιμετώπιση αυτού του είδους της επίθεσης, μόνο αφού πιστοποιηθεί ο αποστολέας και αποκλειστεί το πακέτο δεδομένων ως μεγαλύτερο από το μέγεθος του πακέτου δεδομένων εφαρμογής, μπορεί να παρέχεται δρομολόγηση πακέτων δεδομένων.

Στρώμα Δικτύου

Η αποτελεσματικότερη αντιμετώπιση των επιθέσεων που αφορούν στο στρώμα δικτύου βασίζεται στο εφαρμοζόμενο πρωτόκολλο δρομολόγησης, όπως θα δούμε στο επόμενο κεφάλαιο. Το πρωτόκολλο δρομολόγησης οφείλει να παρακολουθεί τη λειτουργία του δικτύου, εντοπίζοντας μη φυσιολογικές συμπεριφορές και απομονώνοντας τους κόμβους που τις προκαλούν. Η απομόνωση αυτή επιτυγχάνεται με τον καθορισμό εναλλακτικών μονοπατιών δρομολόγησης (πολυδιαδρομική δρομολόγηση). Επιπλέον εξασφάλιση προσφέρεται με τη συμμετοχή στη δρομολόγηση μόνο εξουσιοδοτημένων κόμβων. Τέλος, ο πλεονασμός (redundancy) μεταδιδόμενης πληροφορίας, ο οποίος μπορεί να δημιουργείται είτε λόγω εγγύτητας των κόμβων είτε σκόπιμα με εκπομπή επιπλέον πακέτων, διευκολύνει την αντιμετώπιση κακόβουλων ενεργειών

Στρώμα Μεταφοράς

Στο στρώμα μεταφοράς διακρίναμε τις επιθέσεις πλημμυρίσματος (flooding) και αποσυγχρονισμού (Desynchronization). Για την αντιμετώπιση της επίθεσης πλημμυρίσματος στη βιβλιογραφία[120] συνιστάται η τεχνική «γρίφων πελατών» (client puzzles). Οι γρίφοι διαμοιράζονται από τον σταθμό βάσης στο δίκτυο και η επίλυσή τους από κάθε κόμβο συνεπάγεται ότι η σύνδεση είναι έγκυρη. Ο επιτιθέμενος θα πρέπει να είναι σε θέση να τους επιλύσει, ώστε να ενεργήσει κακόβουλα εναντίον του δικτύου. Επιπλέον αντίμετρα προσφέρουν μέτρα περιορισμού των αριθμού συνδέσεων και μηχανισμούς αυθεντικοποίησης.

Αντίμετρο της επίθεσης αποσυγχρονισμού είναι η πιστοποίηση (αυθεντικοποίηση) όλων των πακέτων που ανταλλάσσονται, συμπεριλαμβανομένων όλων των πεδίων ελέγχου της επικεφαλίδας του πρωτοκόλλου μεταφοράς. Υποθέτοντας ότι ο αντίπαλος δεν μπορεί να παρακάμψει τον μηχανισμό ελέγχου ταυτότητας, οι συμμετέχοντες στην επικοινωνία κόμβοι θα μπορούν να εντοπίσουν και στην συνέχεια να αγνοήσουν τα κακόβουλα πακέτα.

[120] Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks. Communications of the ACM, 47(6), 53-57.

7.3.2 Ασφαλής Δρομολόγηση (Secure Routing) και Ζεύξη

Η εξασφάλιση της αξιόπιστης επικοινωνίας και της ανταλλαγής μηνυμάτων, η οποία συντελείται στο στρώμα δικτύου, μεταξύ των κόμβων ενός ασύρματου δικτύου είναι ιδιαίτερα κρίσιμη, και για το λόγο αυτό είναι θεμιτό το να σταθούμε περισσότερο στη διερεύνηση των μηχανισμών ασφαλείας στο επίπεδο αυτό. Εκτός των μηχανισμών ασφαλείας και των αντιμέτρων που είδαμε στο προηγούμενο κεφάλαιο για τις σημαντικότερες επιθέσεις, ωφέλιμη θα ήταν και η εξέταση ιδιαίτερων – πιο ανθεκτικών – πρωτόκολλων στα WSNs.

Στον παρακάτω πίνακα σημειώνονται συνοπτικά οι επιθέσεις οι οποίες σχετίζονται, έχουν συμβατότητα αλλά και εφαρμογή σε ορισμένα τυπικά πρωτόκολλα δρομολόγησης που συναντούμε στα ασύρματα δίκτυα αισθητήρων [214].

Πρωτόκολλο δρομολόγησης	**Σχετιζόμενη επίθεση**
Κατευθυνόμενη διάδοση (directed diffusion)	Επίθεση μετάδοσης ψευδών μηνυμάτων, επιλεκτική προώθηση, καταβόθρες, σιβυλλική επίθεση, σκουληκότρυπες, HELLO floods
Πρωτόκολλα γεωγραφικής δρομολόγησης (GPSR, GEAR)	Επίθεση μετάδοσης ψευδών μηνυμάτων, επιλεκτική προώθηση, σιβυλλική επίθεση
Ιεραρχικά πρωτόκολλα (LEACH, TEEN, PEGASIS)	Επιλεκτική προώθηση, HELLO floods
Πρωτόκολλα εξοικονόμησης ενέργειας (SPAN, GAF)	Επίθεση μετάδοσης ψευδών μηνυμάτων, σιβυλλική επίθεση, HELLO floods

Πίνακας 7-2: Συμβατές επιθέσεις με πρωτόκολλα δρομολόγησης

Ένας επικεντρωμένος σε ζητήματα ασφάλειας μηχανισμός δρομολόγησης έχει να αντιμετωπίσει τρεις βασικές προκλήσεις, οι οποίες είναι: (α) η πρόληψη, (β) η ανίχνευση της επίθεσης, και (γ) η ανάκτηση λειτουργιών και η επανατακτικότητα σε επιθέσεις (ευρωστία). Για το σκοπό αυτό και για την εξάλειψη των απειλών από ενδεχόμενες επιθέσεις, πρέπει να συμψηφιστούν στο σχεδιασμό του δικτύου τεχνικές αυθεντικοποίησης (πιστοποίηση-επαλήθευση ταυτότητας κόμβων) και κρυπτογράφησης. Επιπλέον, οι τεχνικές πλεονασμού της μεταδιδόμενης πληροφορίας και η πολυδιαδρομική δρομολόγηση κινούνται προς αυτή τη κατεύθυνση.

Με γνώμονα όλες τις παραπάνω προκλήσεις στο στρώμα δικτύου, έχουν σχεδιαστεί πρωτόκολλα τα οποία είναι περισσότερο ανθεκτικά, τα σημαντικότερα των οποίων είναι: το «Πρωτόκολλο Ασφαλείας για Δίκτυα Αισθητήρων» SPINS (Security Protocols for Sensor Networks), το «Πρωτόκολλο δρομολόγησης ανοχής για ασύρματα δίκτυα αισθητήρων» INSENS (Intrusion Tolerant Routing protocol for Wireless Sensor Networks), ο «Μηχανισμός άμυνας κατά επιθέσεων σκουληκότρυπας σε ασύρματα δίκτυα αισθητήρων» με την ονομασία DAWWSEN (Defense Mechanism Against Wormhole attacks in Wireless Sensor Networks), και το πρωτόκολλο Tinysec [220], τα οποία και θα αναλύσουμε συνοπτικά παρακάτω.

Το πρωτόκολλο **SPINS** αποτελείται από δύο δομές, οι οποίες είναι τα πρωτόκολλα SNEP (Sensor Network Encryption Protocol) και μTESLA (micro version of Timed, Efficient, Streaming, Loss – tolerant Authentication Protocol). Το SNEP προσφέρει στην επικοινωνία εμπιστευτικότητα, αυθεντικοποίηση δύο μερών (two-party authentication) και φρεσκάδα δεδομένων, ενώ το μTESLA προσδίδει συμπληρωματικά αυθεντικοποίηση ευρυεκπομπής (broadcast authentication). Επιπρόσθετα, το μTESLA έχει σχεδιασθεί με γνώμονα την εξοικονόμηση πόρων του δικτύου, κάτι που είναι κρίσιμης σημασίας για δίκτυα WSN. Παρόλα αυτά, το SPINS λαμβάνει μέτρα για την πρόληψη και όχι για την ανίχνευση των επιθέσεων ή την ανάκτηση λειτουργιών σε περίπτωση επιθέσεων, οπότε η ασφάλεια που παρέχει το συγκεκριμένο πρωτόκολλο είναι περιορισμένη σε περίπτωση παρουσίας κακόβουλης ενέργειας [216].

Το πρωτόκολλο **INSENS** βασίζεται στην εφαρμογή δρομολόγησης της πληροφορίας μέσω πολλών διαδρομών, προσθέτοντας επανατακτικότητα σε επιθέσεις στο επίπεδο δικτύου. Επιπλέον, το εν λόγω πρωτόκολλο προσδίδει προστασία από επιθέσεις άρνησης εξυπηρέτησης, κακόβουλες ενέργειες κατά την προώθηση δεδομένων και κακόβουλων ενεργειών κατά της εύρεσης μονοπατιού δρομολόγησης. Το INSENS εκμεταλλεύεται τον πλεονασμό της πληροφορίας, και έτσι πετυχαίνει ευρωστία στην περίπτωση που εμφανιστεί μία κακόβουλη ενέργεια. Επιπλέον, αναθέτει αποκλειστικά όλες τις λειτουργίες με μεγάλες απαιτήσεις σε υπολογισμούς, περιορίζοντας τους αισθητήριους κόμβους σε υπολογισμούς που σχετίζονται με την ανεύρεση μονοπατιών δρομολόγησης και επανατακτικότητας παρεισφρήσεων. Με τον τρόπο αυτό, ελαχιστοποιεί τις απαιτήσεις πόρων, όπως μνήμη, εύρος ζώνης κλπ στους κόμβους αισθητήρων. Επίσης, με χρήση κρυπτογράφησης συμμετρικού κλειδιού και μηχανισμών αυθεντικοποίησης, το πρωτόκολλο επιτυγχάνει τον περιορισμό επιπτώσεων παρεισφρήσεων, που ενδεχομένως δεν έχουν ανιχνευθεί. Αν και δεν παρέχει ανίχνευση επιθέσεων, το συγκεκριμένο πρωτόκολλο πλεονεκτεί έναντι των υπολοίπων καθώς λειτουργεί με επάρκεια ακόμα και στην περίπτωση παρείσφρησης σε ένα τμήμα του δικτύου [218].

Το πρωτόκολλο **DAWWSEN** παρέχει προστασία από επιθέσεις σκουληκότρυπας. Πρόκειται για ένα προληπτικό πρωτόκολλο δρομολόγησης, το οποίο βασίζεται στην ιεραρχική δρομολόγηση. Πλεονεκτήματα του συγκεκριμένου πρωτοκόλλου είναι η μη αναγκαιότητα διάθεσης πληροφορίας θέσης από τους κόμβους και η απλότητά του στη μέθοδο ανίχνευσης της επίθεσης, τα οποία κρίνονται σημαντικά σε ένα ασύρματο δίκτυο αισθητήρων όπου οι περιορισμοί των διαθέσιμων πόρων είναι σημαντικοί [219].

Τέλος, το πρωτόκολλο **TinySec** παρέχει εμπιστευτικότητα, αυθεντικοποίηση και ακεραιότητα χρησιμοποιώντας συμμετρικούς αλγόριθμους κρυπτογράφησης όπως οι RC5[121] και Skipjack[122]. Συγκεκριμένα, το εν λόγω πρωτόκολλο παρέχει αυθεντικοποίηση και εμπιστευτικότητα στην επικοινωνία μεταξύ των κόμβων, με χρήση του συμμετρικού αλγορίθμου κρυπτογράφησης AES[123]. Το πρωτόκολλο TinySec σχεδιάστηκε προκειμένου να ισορροπεί ανάμεσα στις απαιτήσεις ασφαλείας και την εξοικονόμηση ενέργειας. Συγκεκριμένα, μπορεί να πετύχει υψηλού επιπέδου αυθεντικοποίηση και μυστικότητα δεδομένων (data secrecy), με έως και 3 φορές μικρότερη κατανάλωση ενέργειας, σε σύγκριση με άλλα πρωτόκολλα [221].

[121] https://en.wikipedia.org/wiki/RC5
[122] https://en.wikipedia.org/wiki/Skipjack_(cipher)
[123] Βλέπε σχετικά: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

8

Περιπτώσεις Χρήσης

Η μελέτη περίπτωσης (case study) είναι μια ερευνητική διαδικασία η οποία διερευνά ένα φαινόμενο στο πλαίσιο της πραγματικής του υπόστασης. Το φαινόμενο αυτό μπορεί να βασιστεί σε θεωρητικά ή σε πειραματικά ή ακόμη και σε εμπειρικά δεδομένα[124]. Στο κεφάλαιο αυτό θα μελετηθούν ορισμένες εφαρμογές των προηγούμενων (θεωρητικών) τμημάτων της εργασίας.

8.1 Περιμετρική Προστασία (Fence Defense) με Ανάλυση Εικόνας Ασύρματων IP Εικονοληπτών (Video Analytics)

Καθώς οι τεχνολογίες εικονοληπτών ασφαλείας συνεχίζουν να εξελίσσονται, οι ασύρματες κάμερες ασφαλείας παρέχουν εξαιρετικά πλεονεκτήματα για όσους χρειάζονται πρόσβαση σε εικόνα χωρίς καλώδια. Αυτή η μελέτη περίπτωσης εισάγει τα πλεονεκτήματα της ασύρματης τεχνολογίας σε ένα δίκτυο συστημάτων παρακολούθησης και καταγραφής εικόνας.

Τα βασικά πλεονεκτήματα που παρέχει ένα ασύρματο τοπικό δίκτυο προέρχονται από την φύση της ασύρματης τεχνολογίας η οποία προσφέρει πολλές ευκολίες. Έτσι, αναφορικά με τα δίκτυα αυτά διακρίνουμε τα εξής πλεονεκτήματα [237]:

- Η εύκολη πρόσβαση, ανεξάρτητα από την τοποθεσία του χρήστη. Επιπλέον, με την υλοποίηση των δικτύων 5ης γενιάς οι υψηλές ταχύτητες επιτρέπουν τη συνύπαρξη πολλών τύπων δεδομένων ταυτόχρονα, όπως π.χ. μετάδοση εικόνας υψηλής ανάλυσης (HD video streaming), μετάδοση φωνητικών σημάτων μέσα από πρωτόκολλο Internet (VoIP – Voice over IP) και απλά δεδομένα δικτύου τα οποία μπορούν να συνυπάρχουν σε διαφορετικές ραδιοσυχνότητες.

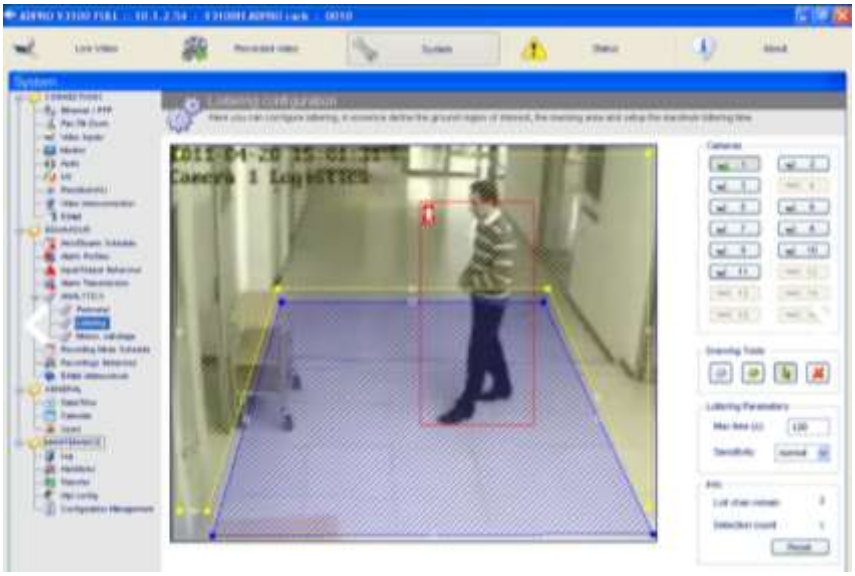
[124] Press Academia (2018). Definition of case study. PressAcademia website. Retrieved August 18, 2021, from https://www.pressacademia.org/definition-of-case-study/

- Η υλοποίηση ενός ασύρματου δικτύου είναι ταχύτερη από την παραδοσιακή υλοποίηση με καλώδια. Ένα ασύρματο δίκτυο μπορεί να χρησιμοποιηθεί ως εργαλείο γρήγορης εγκατάστασης μιας απομακρυσμένης περιοχής. Εάν οι απαιτήσεις σε εύρος ζώνης (bandwidth) δεν είναι ιδιαίτερα υψηλές, μια ασύρματη συσκευή μπορεί να παρέχει δικτυακή διασύνδεση σε αρκετούς χρήστες χωρίς το χρόνο που χρειάζεται η τοποθέτηση καλωδίωσης για την ίδια χρήση. Συνεπώς, με χρήση της ασύρματης τεχνολογίας, η πρόσβαση στο δίκτυο μιας απομακρυσμένης περιοχής μπορεί να υλοποιηθεί σε ώρες αντί για μέρες.

- Η υλοποίηση ενός ασύρματου δικτύου είναι οικονομικότερη από την παραδοσιακή υλοποίηση με καλώδια. Η μείωση του χρόνου εγκατάστασης συνεπάγεται λιγότερες εργατοώρες και κατά συνέπεια χαμηλότερο κόστος. Επίσης, λόγω της απουσίας καλωδίων, τα ασύρματα στοιχεία μπορούν είτε να εγκαθίστανται, είτε να μετακινούνται, είτε να επανατοποθετούνται με μειωμένο κόστος.

Η τεχνολογία εικονικού φράκτη (fence) οριοθετεί μια περιοχή στο πεδίο της παρακολούθησης βίντεο εκ των προτέρων. Η παρακολούθηση βίντεο που βασίζεται σε εικονικό φράκτη μπορεί να αναλύσει έξυπνα τις συμπεριφορές σε πραγματικές σκηνές.

Όπως είδαμε σε προηγούμενο κεφάλαιο, οι τεχνολογίες ανάλυσης βίντεο (VCA – Video Content Analysis) χρησιμοποιούνται παγκοσμίως με αυξανόμενο ρυθμό και τα επόμενα χρόνια αυτός ο ρυθμός θα επιταχυνθεί, καθώς οι καινοτομίες των τεχνολογιών και των ειδικών τεχνικών που χρησιμοποιούνται για την υλοποίησή τους και τις διάφορες εφαρμογές τους, εξελίσσονται διαρκώς[125].



Εικόνα 8-1: Χρήση VCA για εντοπισμό κινούμενου ατόμου εντός καθορισμένης περιοχής

[125] Πηγή: https://protectionplus.gr/video-analytics

Η ενσωμάτωση της ανάλυσης περιεχομένου βίντεο (VCA) στην περιμετρική άμυνα είναι μια από τις πιο δύσκολες περιπτώσεις χρήσης, καθώς πρέπει να αντιμετωπίσει πολλές πηγές θορύβου και να είναι σε θέση ώστε να δημιουργήσει μια ειδοποίηση χωρίς πάρα πολλούς ψευδείς συναγερμούς. Οι τεχνολογικές βελτιώσεις και ο ανταγωνισμός μεταξύ των παρόχων συναφούς εξοπλισμού μείωσαν τις τιμές και αύξησαν περαιτέρω την παρουσία του VCA, όχι μόνο σε εγκαταστάσεις υψηλής ασφάλειας αλλά και σε εμπορικές και οικιστικές εγκαταστάσεις. Η προέλευση της ανάλυσης περιεχομένου βίντεο (VCA) για την περιμετρική άμυνα βρίσκεται στην τεχνολογία ανίχνευσης κίνησης βίντεο (Video Motion Detection - VMD) που είναι παρούσα από τις αρχές της δεκαετίας του 2000. Στην αρχή, το VMD χρησιμοποιήθηκε μόνο για την ανίχνευση κίνησης. Αργότερα, οι εξελίξεις επέτρεψαν στα συστήματα να εκτιμήσουν και να διαφοροποιήσουν το μέγεθος, το χρώμα, την ταχύτητα και την κατεύθυνση. Η χρήση του VCA αφορά σε προειδοποίηση για πιθανά ύποπτα συμβάντα, καθώς η φυσική περίμετρος προτιμάται ως πρώτη μορφή άμυνας και ως ορατή αποτροπή για τους εισβολείς. Το VCA υποστηρίζει την περιμετρική ασφάλεια ως ένα επιπλέον οφθαλμοί-μάτια που υποστηρίζουν το προσωπικό ασφαλείας στο δωμάτιο ελέγχου, ειδοποιώντας το όταν χρειάζεται και βοηθώντας το να ανακτήσει γρήγορα τα σωστά στοιχεία όταν συνέβη κάτι[126].

Στη συγκεκριμένη περίπτωση χρήσης, η ανάλυση βίντεο με την βοήθεια AI (Artificial Intelligence) και βαθιάς εκμάθησης (deep learning) βρίσκει εφαρμογή στην επιτήρηση εικονικού φράκτη για την προστασία υποδομών Παραγωγής Ηλεκτρικής Ενέργειας της Ταϊλάνδης (EGAT - Electricity Generating Authority Thailand). Τα κεντρικά γραφεία της EGAT βρίσκονται στην Μπανγκόκ, κοντά στον ποταμό Chao Phraya. Έχουν γίνει αρκετές διαρρήξεις κατά μήκος της όχθης αυτού του ποταμού, περιοχή όπου πλησιάζουν σκάφη και μπαίνουν στην προστατευόμενη περιοχή. Γι' αυτό ήταν απαραίτητος ο έγκαιρος εντοπισμός όλων των εισβολέων, με στόχο τη βελτίωση του επιπέδου ασφαλείας[127].
Η εταιρεία Point IT Consulting Co., Ltd επέλεξε τους αλγόριθμους VCA της εταιρείας DAVANTIS και αξιοποίησε τη χρήση ανάλυσης εικονοστοιχείων για την προστασία της περιμέτρου της όχθης του ποταμού. Ο πελάτης απαίτησε 24ωρη περιμετρική επιτήρηση για την έγκαιρη ειδοποίηση των φρουρών, με τη χρήση έξυπνου συστήματος αυτόματης παρακολούθησης με περιστρεφόμενες ασύρματες κάμερες. Το σύστημα συνδέθηκε με ένα λογισμικό VMS (Video Management Software), το οποίο χρησιμοποιήθηκε για την ενσωμάτωση των αλγορίθμων VCA και την ενεργοποίηση συναγερμών σε πραγματικό χρόνο.

Ο σχεδιασμός και η υλοποίηση του συστήματος κατέστησε δυνατό τον έγκαιρο εντοπισμό εισβολέων σε απαγορευμένες περιοχές, καθώς και σκάφη τα οποία πλησίαζαν γρήγορα στις περιοχές αυτές. Το τεχνικό προσωπικό του πελάτη εκπαιδεύτηκε στη χρήση του συστήματος, ώστε με την χρήση του VCA να πραγματοποιείται ανάλυση μη εξουσιοδοτημένων συμπεριφορών σε πραγματικό χρόνο, βελτιώνοντας έτσι την ασφάλεια της περιοχής παρακολούθησης, σε μεγάλο βαθμό.

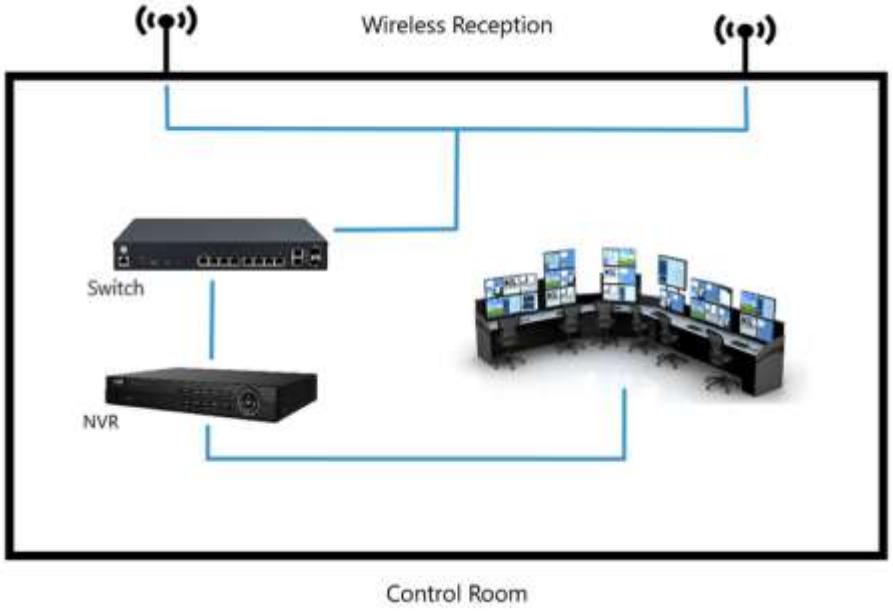
---

[126] Δήλωση του κ. Pieter van de Looveren, Global Marketing Communication Manager σε συνέντευξη σχετικά με συστήματα Βίντεο της Bosch Security Systems, στο περιοδικό A&S International.
Πηγή: https://issuu.com/asmag/docs/a_s_international_dec_2014__trial_v

[127] Περίπτωση χρήσης έργου το οποίο πραγματοποιήθηκε στην Ταϊλάνδη στις 28 Ιανουαρίου 2021 από την εταιρεία Point IT Consulting Co.,Ltd με χρήση των VCA της Ισπανικής εταιρείας Davantis.
Πηγή: https://www.davantis.com/sites/default/files/2021_Egat_Case_Study_EN_.pdf

8.1.1 Αρχιτεκτονική και Λειτουργία του Συστήματος

Στο παραπάνω έργο χρησιμοποιούνται ασύρματοι εικονολήπτες (βλ. κεφ. 6.4.1) τεχνολογίας PTZ , καθένας εκ των οποίων μεταδίδει ροή εικόνας υψηλής ανάλυσης 2,1 Megapixel από όλη την τοποθεσία, σε μέγιστη ταχύτητα μετάδοσης 100Mbps. Η τεχνολογία PTZ, επιτρέπει τη λήψη εικόνων σε προκαθορισμένες θέσεις, οι οποίες εναλλάσσονται σε συγκεκριμένα χρονικά διαστήματα που καθορίζει ο χρήστης, κατά τον προγραμματισμό τους. Όλες οι κάμερες είναι προσβάσιμες γρήγορα και εύκολα από οποιονδήποτε υπολογιστή στο ίδιο δίκτυο, ενώ οθόνες σε έναν κεντρικό σταθμό ελέγχου μπορούν να εμφανίζουν ζωντανές εικόνες σε όλη τη διάρκεια του 24ώρου.

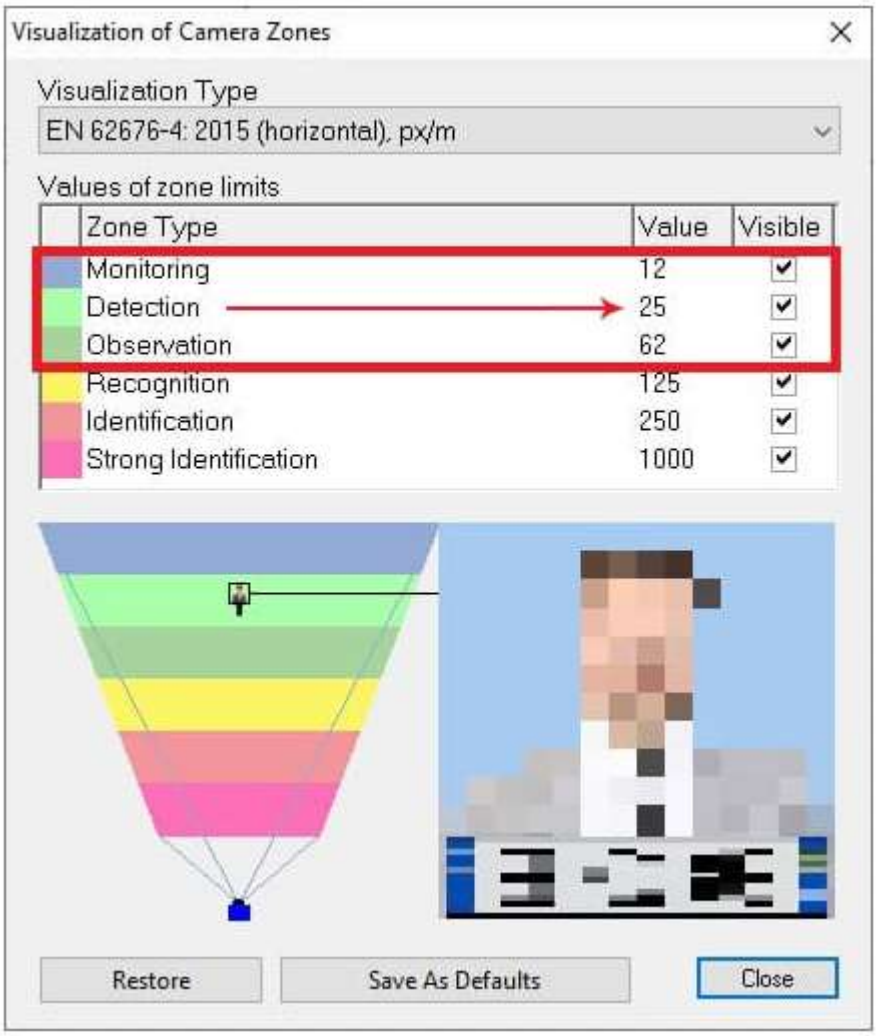


Εικόνα 8-2: Τοπολογία ασύρματου δικτύου μετάδοσης εικόνας[128]

Ο πιο συνηθισμένος τύπος σύνδεσης της IP κάμερας είναι μέσω ενός τυπικού ασύρματου δρομολογητή. Δεν υπάρχουν περιορισμοί στα εξερχόμενα δεδομένα εκτός αν οριστεί διαφορετικά από τον χρήστη στις παραμέτρους του δρομολογητή. Δεν ισχύει όμως το ίδιο και για την αντίθετη κατεύθυνση. Οι δρομολογητές περιλαμβάνουν Τείχος Προστασίας (Firewall) που εμποδίζει οποιονδήποτε χρησιμοποιεί το ευρύτερο δίκτυο (Internet) ώστε να έχει πρόσβαση στο εκάστοτε τοπικό δίκτυο. Έτσι ο Η/Υ και οι τοπικές συσκευές παραμένουν ασφαλείς από εξωτερικές επιθέσεις, αλλά αυτό δημιουργεί αμφίδρομα το πρόβλημα σύνδεσης στην απομακρυσμένη κάμερα. Το άνοιγμα θύρας (Port Forwarding) είναι η διαδικασία με την οποία ο δρομολογητής ενημερώνεται για την πρόσβαση μέσω Internet σε μια συσκευή.

[128] Οι ασύρματοι εικονολήπτες, όπως είδαμε στο κεφ. 6.4.1, τροφοδοτούνται από εξωτερική πηγή ενέργειας όπως για παράδειγμα ένα μικρό φωτοβολταϊκό σύστημα. Στην συνέχεια η ροή εικόνας συμπιέζεται σύμφωνα με τον πρωτόκολλο συμπίεσης εικόνας H264 και αποστέλλεται σε ψηφιακή μορφή προς μετάδοση μέσω ραδιοσημάτων. Η ζεύξη μεταξύ των ασύρματων καμερών και του μηχανήματος λήψης, αποσυμπίεσης και καταγραφής εικόνας (μέσω Network Video Recorder - NVR) γίνεται χωρίς να παρεμβάλλεται το WiFi router της εγκατάστασης.

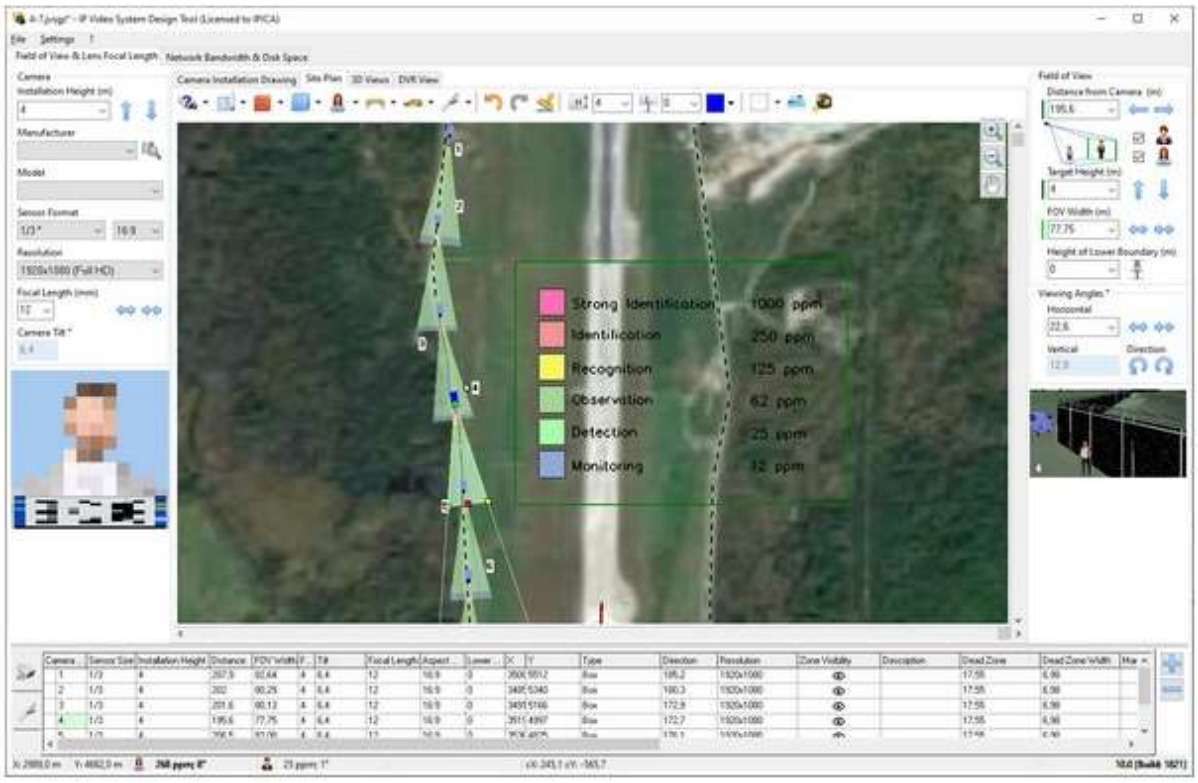
Στην περίπτωση χρήσης που μελετάται εδώ, θεωρήθηκε απαραίτητο να εξασφαλιστεί η συνεχής επιτήρηση της περιμέτρου της κρίσιμης εγκατάστασης, από μήκος 1-2 χιλιομέτρων έως 10-20 χιλιομέτρων χωρίς νεκρές ζώνες. Η τοπογραφική έρευνα καθώς και η δορυφορική εικόνα (από Χάρτη Google) με αναφορά και καταγραφή ενδιάμεσων φυσικών και μηχανολογικών εμποδίων όπως δέντρα, βλάστηση, βράχια, περιμετρικοί φράχτες, πύλες, σημεία ελέγχου ασφαλείας κτλ., κρίθηκε απαραίτητη πριν από τον καθορισμό των σημείων εγκατάστασης των εικονοληπτών ώστε να επιτευχθεί ο κύριος στόχος του συστήματος περιμετρικής επιτήρησης, δηλαδή η έγκαιρη ανίχνευση και ειδοποίηση μη εξουσιοδοτημένης εισόδου στην περιοχή επιτήρησης.



Εικόνα 8-3: Καθορισμός περιοχών και ποιότητας ανίχνευσης[129]

[129] Ο καθορισμός των ζωνών ανίχνευσης καθώς και των εικονοστοιχείων ανά μέτρο τα οποία αντιστοιχούν σε εντοπισμό ή αναγνώριση του ζητούμενου αντικειμένου, καθορίζονται από το Ευρωπαϊκό πρότυπο EN 62676-4:2015. Η σχεδίαση του συστήματος βίντεο IP πραγματοποιήθηκε με τη χρήση του εργαλείο JVSG το οποίο προσφέρει έναν νέο τρόπο σχεδιασμού σύγχρονων συστημάτων παρακολούθησης βίντεο, γρήγορα και εύκολα. Το εργαλείο αυτό διατίθεται δωρεάν σε δοκιμαστική έκδοση στη ιστοσελίδα https://www.jvsg.com/

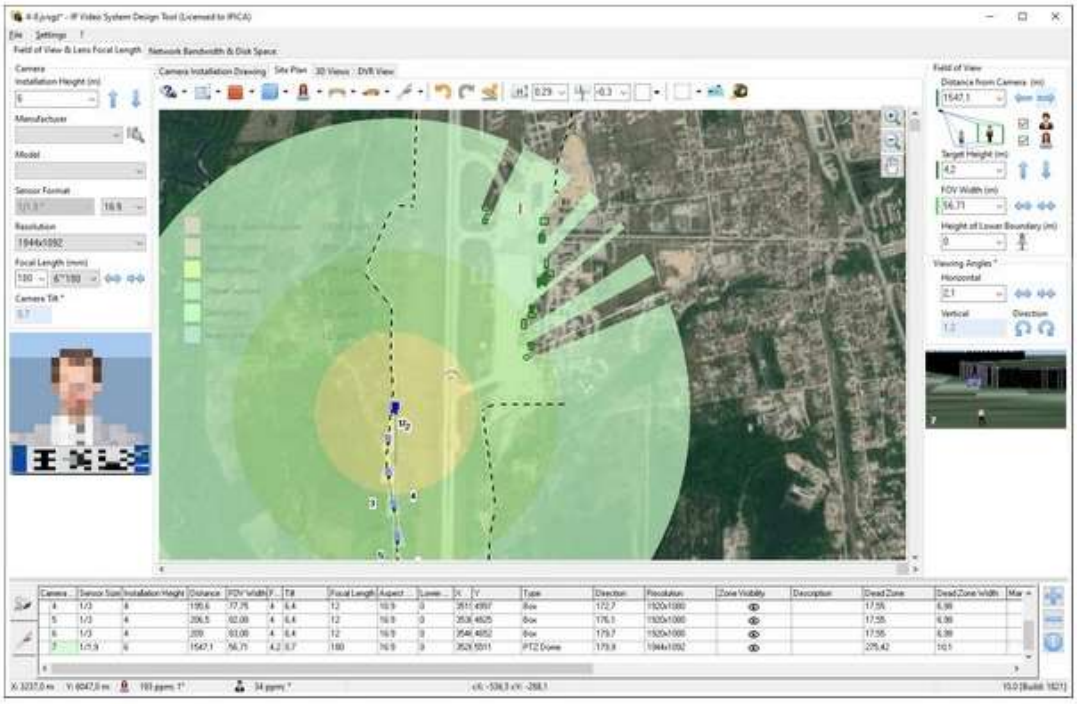
Μια περίμετρος πολλών χιλιομέτρων (ειδικά δεκάδων χιλιομέτρων) προφανώς θα περιλάμβανε μεγάλο αριθμό καμερών. Ταυτόχρονα, οι εικόνες σε αυτές τις κάμερες ήταν επιθυμητό να παρουσίαζαν ποικιλία και να μην επαναλάμβαναν την απεικόνιση ίδιων περιοχών με μονοτονία. Έτσι επιλέχθηκε η κλασική και προτιμότερη μέθοδος τοποθέτησης η οποία συνιστά την τοποθέτηση της μίας κάμερας πίσω από την άλλη (one-after-another) ώστε οι λαμβανόμενες εικόνες να αλληλοκαλύπτονται. Αυτός ο τρόπος τοποθέτησης είναι ο πλέον ενδεικτικός για την επόπτευση μια περιμέτρου μεγάλου μήκους, ενώ ένας σαφής ορισμός των ορίων μεταξύ των εδαφών του χρήστη και μιας «αποστρατικοποιημένης ζώνης» (DMZ - Demilitarized Zone) επιτρέπει την ανίχνευση της δραστηριότητας ενός εισβολέα πριν διεισδύσει στην προστατευόμενη περιοχή. Επίσης, το να είναι όλες οι κάμερες στραμμένες προς την ίδια κατεύθυνση απλοποιεί σημαντικά την ανάλυση της κατάστασης για τους παρατηρητές στο κέντρο παρακολούθησης.



Εικόνα 8-4: Προσδιορισμός τοποθέτησης εικονοληπτών με το εργαλείο JVSG

Το VCA στην περίπτωση των σταθερών καμερών ενισχύει την προστιθέμενη αξία όχι μόνο συμπληρώνοντας τεχνολογικά την απεικόνιση του φυσικού πεδίου, αλλά υποβοηθώντας επίσης τις ικανότητες των χειριστών. Βοηθά στη διατήρηση της επίγνωσης της κατάστασης, ένα σημαντικό χαρακτηριστικό που μπορεί να λείπει σε περίπτωση όπου υπάρχουν χειριστές χαμηλού επιπέδου οι οποίοι φρουρούν τον τόπο. Βοηθά επίσης ώστε να μειωθεί ο χρόνος οπτικής εστίασης των χειριστών σε μια στατική εικόνα, καθώς αυτή καθιστά αδύνατη τη συνεχή παρακολούθηση μιας τοποθεσίας και παράλληλα επιφέρει πολλά λάθη στις περισσότερες περιπτώσεις.

Ωστόσο, το εξωτερικό περιβάλλον θέτει πολλές προκλήσεις στις λύσεις VCA, όπως είναι οι μετεωρολογικές προκλήσεις που αφορούν στα κινούμενα σύννεφα, σε σκιές, στη βροχή, στο χιόνι και σε κεραυνούς, καθώς και οι περιβαλλοντικές προκλήσεις όπως η ανάπτυξη των φυτών. Για την επιπλέον κάλυψη των «νεκρών» οπτικών σημείων που δημιουργούνται, χρησιμοποιήθηκαν επιπλέον κάμερες PTZ.
Οι περιστρεφόμενες κάμερες παίζουν μόνο μικρό ρόλο στη διασφάλιση της περιμετρικής ασφάλειας. Με τον εντοπισμό εισβολής, βοηθούν στη λεπτομέρεια της σκηνής, επαληθεύοντας τους συναγερμούς που δημιουργούνται αυτόματα από τις μονάδες ανάλυσης βίντεο σταθερών καμερών ή μεμονωμένων συστημάτων περιμετρικής ασφάλειας.



Εικόνα 8-5: Προσδιορισμός τοποθέτησης εικονοληπτών PTZ με το εργαλείο JVSG

Στην περίπτωση του έργου που μελετάμε, παρά τον πειρασμό να χρησιμοποιηθούν περιστρεφόμενες κάμερες σε όλες τις τοποθεσίες λόγω της υψηλότερης ισχύος εστίασης (zoom) καθώς και των δυνατοτήτων προβολής 360°, λήφθηκε υπόψη πως αυτές οι κάμερες δεν εξασφαλίζουν ομοιόμορφη περιμετρική αντοχή ούτε και ομαλή λειτουργία των αλγορίθμων VCA. Μια περιστρεφόμενη κάμερα μπορεί να παρατηρήσει μόνο μέρος της εκχωρημένης περιοχής ανά πάσα στιγμή, ενώ η ζώνη που παρατηρείται είναι τυχαία και περιστασιακή, γεγονός που την καθιστά εντελώς ακατάλληλη είτε για ανίχνευση εισβολής είτε για ανάλυση μετά το συμβάν.

Δύο παράγοντες που αυξάνουν σημαντικά την επιτυχία του περιμετρικού VCA και ελήφθησαν σοβαρά υπόψη ήταν ο σωστός φωτισμός καθώς και οι καθαρές περιοχές κοντά στην περίμετρο. Ωστόσο, μέτρα προς αυτή την κατεύθυνση δεν είναι πάντα εύκολο να εκληφθούν και κυρίως να διατηρηθούν. Επιπλέον, για να παρέχεται πλήρης ασφάλεια, έπρεπε να αναπτυχθεί μεγάλος αριθμός καμερών σε σχετικά μικρές αποστάσεις. Επομένως αυτό καθόρισε και τον μεγάλο αποθηκευτικό χώρο για την συνεχή τροφοδοσία βίντεο και

αναλυτικών στοιχείων, καθιστώντας το σύστημα ακριβό και περίπλοκο αναφορικά με τη συντήρησή του.

Επιλογή Κατάλληλων Εικονοληπτών

Η πιθανότητα ανίχνευσης εισβολής επηρεάζεται από διάφορους παράγοντες με σημαντικότερο τη λεπτομέρεια εικόνας (πυκνότητα pixel) αλλά και την ευαισθησία της κάμερας (ικανότητα λήψης εικόνας υψηλής αντίθεσης σε συνθήκες χαμηλού φωτισμού) όπως επίσης και την οπτική πυκνότητα του μέσου (παρουσία βροχόπτωσης, ομίχλη, καπνός ή οτιδήποτε άλλο περιορίζει την ορατότητα). Έτσι η επιλογή των εικονοληπτών ήταν ένας συμβιβασμός μεταξύ των απαιτήσεων εξοικονόμησης πόρων (αύξηση της απόστασης τοποθέτησης της κάμερας, τροφοδοσία, εκπομπή και αναμετάδοση WiFi) και της αξιοπιστίας του συστήματος.

Η επιλογή κατάλληλων καμερών αποδείχθηκε η βέλτιστη, καθώς προσφέρθηκε η ικανότητα εντοπισμού ενός κινούμενου στόχου γρήγορα και με ακρίβεια, ακόμη και από απόσταση, επιτρέποντας στους χρήστες να παρακολουθούν και να ενημερώνονται άμεσα, ανεξάρτητα από την ταχύτητα του αντικειμένου και πολύ πέρα από το οπτικό πεδίο μιας σταθερής κάμερας. Με τη χρήση των καμερών αυτών παρήχθησαν γρήγορα δεδομένα χρήσης, όπως επιβολή κανονισμών κυκλοφορίας, ανίχνευση παραβατικών ενεργειών κλπ. Στην περίπτωση εντοπισμού ενός ατόμου, η λειτουργία έξυπνης παρακολούθησης της κάμερας ενεργοποιείται σύμφωνα με τον προκαθορισμένο κανόνα συναγερμού και εξασφαλίζει αδιάκοπη και αυτόματη παρακολούθηση κινούμενων αντικειμένων, ενώ η βέλτιστη λήψη του κινούμενου αντικειμένου διασφαλίζεται με τη δυναμική προσαρμογή του οπτικού πεδίου.

Εικόνα 8-6: Παράδειγμα σχεδιασμού επιπέδου περίφραξης και ενεργοποίηση του ενσωματωμένου VCA σε μια κάμερα

8.2 Πυρανίχνευση Δασικών Εκτάσεων μέσω Δικτύου Πολλαπλών Αισθητήρων

Η αύξηση των εποχιακών θερμοκρασιών προκάλεσε έκρηξη στον αριθμό των αυτο-αναφλεγόμενων πυρκαγιών σε δασικές περιοχές, οι οποίες πυρκαγιές εξαπλώθηκαν από ανέμους και τροφοδοτήθηκαν από ξηρή βλάστηση και εν τέλει έγιναν καταστροφικές. Οι ακραίες καιρικές συνθήκες, όπως καταιγίδες ή πλημμύρες, αποτελούν επίσης κίνδυνο για αυτούς τους τόπους. Πέρα από τη λήψη προληπτικών μέτρων για την αποφυγή πυρκαγιών στα δάση, η έγκαιρη προειδοποίηση και η άμεση αντίδραση σε πυρκαγιά είναι ο μόνος τρόπος για την αποφυγή ανθρώπινων απωλειών και ζημιών στην περιβαλλοντική και οικολογική κληρονομιά. Αν και έχουν προταθεί αρκετές τεχνολογίες βασισμένες σε διαφορετικούς αισθητήρες για την παρακολούθηση πυρκαγιών σε δασικές εκτάσεις, η πλειονότητα των υπαρχόντων συστημάτων ανίχνευσης δεν εκμεταλλεύεται το πλήρες δυναμικό των τεχνολογιών αιχμής [238].

Ειδικότερα, στο πλαίσιο του έργου FIRESENSE[130], αναπτύχθηκε ένα αυτόματο σύστημα έγκαιρης προειδοποίησης που ενσωματώνει πολλούς αισθητήρες για την απομακρυσμένη παρακολούθηση δασικών περιοχών για την αντιμετώπιση του κινδύνου πυρκαγιάς και ακραίων καιρικών συνθηκών. Το σύστημα ενσωματώνει διάφορους αισθητήρες όπως π.χ. οπτικές κάμερες, κάμερες υπέρυθρων σε διαφορετικές ζώνες κύματος, παθητικούς αισθητήρες υπέρυθρων (PIR), ασύρματα δίκτυα αισθητήρων θερμοκρασίας και υγρασίας και τοπικούς μετεωρολογικούς σταθμούς στις τοποθεσίες ανάπτυξης. Τα σήματα και οι μετρήσεις που συλλέγονται από αυτούς τους αισθητήρες μεταδίδονται στο κέντρο ελέγχου, το οποίο χρησιμοποιεί ευφυείς αλγόριθμους καθώς και τεχνικές σύντηξης δεδομένων για αυτόματη ανάλυση και συνδυασμό πληροφοριών αισθητήρα και ανίχνευση της παρουσίας φωτιάς ή καπνού [239].

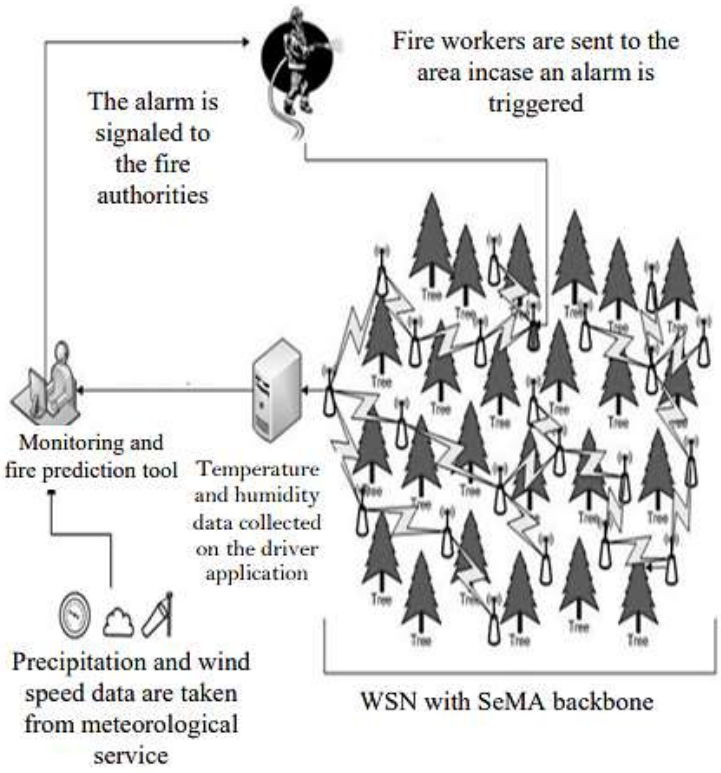
Το κέντρο ελέγχου είναι ικανό ώστε να παράγει αυτόματα προειδοποιητικά σήματα για ανίχνευση καπνού ή φλόγας ή απότομης αύξησης της θερμοκρασίας. Επιπλέον, διαβάζοντας δεδομένα καιρού από επίσημες μετεωρολογικές υπηρεσίες καθώς και από τοπικούς μετεωρολογικούς σταθμούς, μπορεί επίσης να εκδίδει ειδοποιήσεις σε περίπτωση ακραίων καιρικών συνθηκών. Η διεπαφή του κέντρου ελέγχου επιτρέπει την παρακολούθηση του ιστότοπου μέσω των καμερών, την απεικόνιση των χαρτών της περιοχής σε πολλαπλά επίπεδα, τον χειρισμό καμερών PTZ για παροχή βίντεο, καθώς επίσης και τη χρήση δεδομένων αισθητήρων για στατιστικές μελέτες. Επιπλέον, μπορεί να εκτιμήσει, σε πραγματικό χρόνο, την εξέλιξη και διάδοση της πυρκαγιάς βάσει των δεδομένων από το δίκτυο ασύρματων αισθητήρων, του μοντέλου καύσιμης ύλης της περιοχής, τις τοπικές καιρικές συνθήκες και τη μορφολογία του εδάφους. Συμπληρωματικά, είναι σε θέση να υπολογίσει τη κατεύθυνση της πυρκαγιάς με βάση παραμέτρους όπως η ταχύτητα και η διεύθυνση του ανέμου και η μορφολογία του εδάφους. Τέλος, η εκτιμώμενη διάδοση φωτιάς

[130] Το έργο αυτό αναπτύχθηκε ως κοινοπραξία του Ελληνικού Ινστιτούτου Τεχνολογιών Πληροφορικής και Επικοινωνιών, και ορισμένων ξένων ερευνητικών ιδρυμάτων στα πλαίσια του προγράμματος χρηματοδότης Έρευνας και Καινοτομίας Horizon 2020. Το έργο στοχεύει στην ανάπτυξη ενός αυτόματου συστήματος έγκαιρης προειδοποίησης, ώστε να προστατέψει αποτελεσματικότερα χώρους μεγάλης πολιτιστικής και αρχαιολογικής σημασίας από τη φωτιά και ακραία μετεωρολογικά φαινόμενα.
https://www.iti.gr/iti/projects/FIRESENSE.html

απεικονίζεται σε περιβάλλον 3D στο πλαίσιο του Γεωγραφικού Συστήματος Πληροφοριών (GIS). Η εκτιμώμενη κατεύθυνση της πυρκαγιάς απεικονίζεται σε μια διεπαφή 3D που βασίζεται στο σύστημα Google Earth. Αυτές οι πληροφορίες είναι εξαιρετικά πολύτιμες για την αποτελεσματική διαχείριση μιας πυρκαγιάς από τις πυροσβεστικές δυνάμεις [208].

8.2.1 Αρχιτεκτονική και Λειτουργία του Συστήματος FIRESENSE

Το κέντρο ελέγχου FIRESENSE υιοθετεί μια αρθρωτή αρχιτεκτονική, η οποία επιτρέπει την εύκολη ενσωμάτωση διαφορετικών αισθητήρων και μονάδων επεξεργασίας. Υποθέτουμε ότι οι κόμβοι WSNs αναπτύσσονται σε μια δασική περιοχή, με μια τυχαία διάταξη. Όλες οι μετρήσεις των αισθητήρων συλλέγονται σε έναν κόμβο που μεταδίδει τα δεδομένα αυτά για περαιτέρω αξιολόγηση. Επίσης, σε σύνδεση με την Εθνική Μετεωρολογική Υπηρεσία λαμβάνονται πρόσθετα δεδομένα και υπολογισμού τα οποία επηρεάζουν την εξέλιξη της πυρκαγιάς. Οι πυροσβέστες και οι αρμόδιες Αρχές μπορούν να έχουν πρόσβαση στις πιο πρόσφατες πληροφορίες σχετικά με την ένταση και την εξάπλωση της φωτιάς χρησιμοποιώντας τα κινητά τους τηλέφωνα στα οποία είναι εγκατεστημένο το εργαλείο παρακολούθησης και πρόβλεψης.



Εικόνα 8-7: Σχηματική διάταξη αρχιτεκτονικής FIRESENSE[131]

[131] Kucuk, G., et al. (2008): "FireSense: Forest Fire Prediction and Detection System using Wireless Sensor Networks". In Proceedings of the 4th IEEE/ACM International Conference on Distributed Computing in Sensor Systems (DCOSS'08) 2008.

Για τη λειτουργία του FIRESENSE, ένα νέο ασύρματο δίκτυο αισθητήρων σχεδιάστηκε και αναπτύχθηκε από το ΕΚΕΤΑ[132]. Η προσέγγιση σχεδιασμού στοχεύει πρωτίστως σε μια ισχυρή λύση για υπαίθρια ανάπτυξη που να μπορεί να λειτουργήσει με κοινές μπαταρίες διατηρώντας παράλληλα μια καλή απόδοση σε ότι αφορά στο ζητούμενο, δηλαδή στην ανίχνευση της πυρκαγιάς. Επιπλέον, δεδομένου ότι το ασύρματο δίκτυο αισθητήρων αποτελεί μέρος ενός κρίσιμου συστήματος το οποίο βασίζεται σε υπεύθυνο προσωπικό για έγκαιρες προειδοποιήσεις, οποιαδήποτε δυσλειτουργία του θα πρέπει να αναφέρεται άμεσα και αποτελεσματικά μαζί με τη συγκεκριμένη τοποθεσία. Για το λόγο αυτό, σχεδιάστηκε μια ιεραρχία δικτύων με συστοιχίες αισθητήρων που ελέγχονται από έναν επικεφαλής αισθητήρα ο οποίος διαθέτει περισσότερους υπολογιστικούς και ενεργειακούς πόρους από ό,τι οι κοινοί αισθητήρες. Οι επικεφαλής κόμβοι χρησιμοποιούν ασύρματη επικοινωνία χαμηλής εμβέλειας και εξαιρετικά χαμηλής ισχύος για να επικοινωνούν με τους υπόλοιπους αισθητήρες, οι οποίοι μπορούν να τοποθετηθούν σε απόσταση 80 μέτρων το πολύ. Οι ίδιοι οι επικεφαλής κόμβοι συλλέγουν τοπικές μετρήσεις από τους αισθητήρες και τους στέλνουν, μέσω τεχνολογίας WiFi μεγάλης εμβέλειας (μέχρι 200m), στον κεντρικό σταθμό. Επιπλέον, παρακολουθούν παθητικά τους τοπικούς αισθητήρες και τη συμπεριφορά τους και αναφέρουν αμέσως τα όποια προβλήματα προκύψουν.

Η υλοποίηση του συστήματος FIRESENSE αποτελεί μια κοινοπραξία των φορέων ΕΚΕΤΑ - (Ελλάδα), Πανεπιστήμιο Bilkent (Τουρκία), Ecole Supérieure des Communications (Τυνησία), XenICs (Βέλγιο), Stichting Centrum voor Wiskunde en Informatica (Ολλανδία), Marac Electronics S.A (Ελλάδα), Πανεπιστήμιο Bogazici (Τουρκία), Υπουργείο Πολιτισμού (Ελλάδα), Εφορεία Αρχαιοτήτων (Ελλάδα), Industry and Trade Limited Company (Turkey) και Consiglio Nazionale delle Ricerche (Ιταλία).

Το σύστημα FIRESENSE επιδείχθηκε και αξιολογήθηκε σε πέντε μνημεία πολιτιστικής κληρονομιάς στην περιοχή της Μεσογείου, ήτοι: το Ιερό του Κάβειρου στη Θήβα της Ελλάδας, η αρχαία πόλη της Ροδιαπόπολης στην Αττάλεια της Τουρκίας, το κτίριο του Dodge Hall στην Κωνσταντινούπολη, ο ρωμαϊκός Ναό του Νερού στο Πάρκο Djebel Zaghouan στην Τυνησία και το Monteferrato-Galceti στο Prato της Ιταλίας. Πολλές ελεγχόμενες δοκιμές πυρκαγιάς οργανώθηκαν σε αρκετές τοποθεσίες για την αξιολόγηση των λειτουργιών του συστήματος και για την αξιολόγηση της απόδοσης του συστήματος. Το σύστημα πέτυχε υψηλά ποσοστά ανίχνευσης και εντόπισε με επιτυχία δύο πραγματικές πυρκαγιές στη Ροδιαπόπολη τον Σεπτέμβριο και τον Οκτώβριο του 2012.

[132] Το Εθνικό Κέντρο Έρευνας και Τεχνολογικής Ανάπτυξης (ΕΚΕΤΑ), ιδρύθηκε το 2000, είναι ένα από τα κορυφαία ερευνητικά κέντρα της Ελλάδας και βρίσκεται μέσα στη λίστα με τους TOP-20 ερευνητικούς φορείς της Ε.Ε. στην προσέλκυση πόρων από ανταγωνιστικά ευρωπαϊκά προγράμματα. Το ΕΚΕΤΑ έχει να επιδείξει σημαντικά επιστημονικά και τεχνολογικά επιτεύγματα σε ερευνητικές περιοχές με μεγάλο ενδιαφέρον για τον άνθρωπο και την κοινωνία όπως: Ενέργεια, Περιβάλλον, Νέα Λειτουργικά Υλικά, Βιομηχανικές Διεργασίες, Πληροφορική, Τηλεματική, Τηλεπικοινωνίες, Μεταφορές, Αγροβιοτεχνολογία, Επιστήμες Υγείας, Μηχανοτρονική, Αγροτεχνολογία καθώς επίσης και σε διάφορες διαθεματικές επιστημονικές και τεχνολογικές περιοχές που προκύπτουν από τα παραπάνω. Το ΕΚΕΤΑ είναι Νομικό Πρόσωπο Ιδιωτικού Δικαίου (ΝΠΙΔ) μη κερδοσκοπικού χαρακτήρα που εποπτεύεται από τη Γενική Γραμματεία Έρευνας και Καινοτομίας (ΓΓΕΚ) του Υπουργείου Ανάπτυξης και Επενδύσεων.
Πηγή: https://www.certh.gr/root.el.aspx

8.3 Αξιολόγηση Καταστροφής με τη Χρήση Μη Επανδρωμένων Εναέριων Οχημάτων σε Δίκτυο Κινητών Κόμβων

Όπως είδαμε στο κεφ. 5, οι καταστροφές των Κρίσιμων Υποδομών «δοκιμάζουν» την ανθρώπινη αντοχή και επιβίωση, αφού δημιουργούν σοβαρά προβλήματα. Διάφοροι τύποι φυσικών καταστροφών όπως οι γεωφυσικές (σεισμός, τσουνάμι, έκρηξη ηφαιστείου, ολίσθηση εδάφους και χιονοστιβάδα), οι υδρολογικές (μπουρίνι, πλημμύρες), οι κλιματολογικές (υπερβολικές θερμοκρασίες, ξηρασία, και πυρκαγιές) και οι μετεωρολογικές (τροπική καταιγίδα, ανεμοστρόβιλος, καταιγίδα κτλ.) έχουν προκαλέσει μεγάλες απώλειες αγαθών αλλά και ανθρώπινων ζωών. Οι έρευνες έχουν δείξει πως με την πάροδο του χρόνου οι απώλειες γίνονται όλο και μεγαλύτερες, κυρίως διότι βαίνει αυξητικά η ένταση των φαινομένων των φυσικών καταστροφών. Το ερώτημα που καλείται η επιστήμη να απαντήσει είναι αν τελικά μπορεί να γίνει ασφαλής πρόβλεψη μιας επερχόμενης καταστροφής, έτσι ώστε να υπάρξει έγκαιρη πρόληψη και αντιμετώπιση. Στη συνέχεια προτείνεται η αξιοποίηση της τεχνολογίας των δικτύων ασύρματων αισθητήρων και της χρήσης μη επανδρωμένων εναέριων οχημάτων (UAVs - Unmanned Aerial Vehicles) με σκοπό να βελτιωθεί η αξιολόγηση και η ενδεχόμενη αντίδραση σε παρόμοιες καταστάσεις [240].

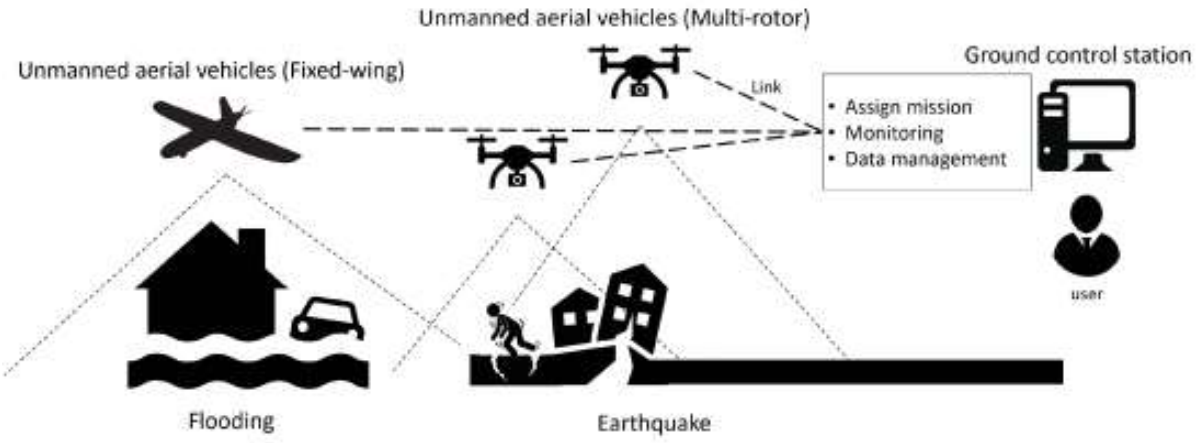
Σε ένα σενάριο πρόληψης και αντιμετώπισης μιας φυσικής καταστροφής, ενδείκνυται η ανάπτυξη μιας υποδομής που θα αποτελείται από μη επανδρωμένα εναέρια οχήματα και τα οποία θα είναι σε θέση να επέμβουν στα διάφορα στάδια του φαινομένου χωρίς την φυσική εμπλοκή/συμμετοχή ανθρώπων. Οι πλέον συνήθεις τύποι είναι αυτοί των οχημάτων που χρησιμοποιούν πτερύγια με κύριό τους χαρακτηριστικό τη μικρή πτητική αυτονομία (25-30 λεπτά) και τον μέσο χρόνο επαναφόρτισης κατά προσέγγιση στα 60 λεπτά. Επίσης, επιλέγονται οχήματα με σταθερά φτερά που προσομοιάζουν μικρά αεροσκάφη και τα οποία έχουν μεγαλύτερη επιχειρησιακή ικανότητα.

Εικόνα 8-8: Μη επανδρωμένο όχημα σταθερών πτερυγίων

Η υποδομή βάσης μπορεί να εδράζεται σε κάποιο σταθερό σημείο ή, ενναλακτικά, σε κάποιο κινητό όχημα που θα βρίσκεται πλησίον της ελεγχόμενης περιοχής και το οποίο πρέπει να είναι εξοπλισμένο με κεραία επικοινωνίας μεγάλων αποστάσεων, γεννήτρια ηλεκτρικής ενέργειας και σύστημα αυτόματης επαναφόρτιση των μπαταριών των οχημάτων.

Η γενική διαχείριση της υποδομής αυτής μπορεί να ανατεθεί σε έναν εξειδικευμένο χειριστή ο οποίος φροντίζει για την ορθή λειτουργία του συστήματος και επίσης όπου χρειάζεται μπορεί να επεμβαίνει και να διορθώνει τις θέσεις αιωρήσεως των οχημάτων μέσω της τεχνολογίας GPS. Σε πιλοτικές εφαρμογές χρησιμοποιούνται, λόγω κόστους, διαθεσιμότητας και ευκολίας χρήσης, οχήματα που μπορούν να βρεθούν εύκολα στην αγορά και στο Διαδίκτυο. Η χρήση ισχυρότερων και ανθεκτικότερων οχημάτων θα οδηγούσε σε περισσότερο αξιόπιστες και εγκυρότερες εφαρμογές, αλλά θα τούτο θα απαιτούσε μια μεγαλύτερη οικονομική επένδυση.

Αναλύοντας τα στάδια μιας φυσικής καταστροφής συμπεραίνουμε πως δεν αρκεί η στατική φύση των δικτύων ασυρμάτων αισθητήρων σε μια γεωγραφική περιοχή. Για να είμαστε πιο ακριβείς, η ύπαρξη των WSNs συμπληρώνεται από τη χρήση μη επανδρωμένων εναέριων οχημάτων ώστε να είναι εφικτή η όσο το δυνατόν καλύτερη αντιμετώπιση των φυσικών καταστροφών.



Εικόνα 8-9: Αποτύπωση της περιοχής καταστροφής από σύστημα πολλαπλών UAVs

Σε αυτόνομες αποστολές, ένα UAV χρησιμοποιεί κυρίως το GPS και τις πυξίδες του για να πλοηγηθεί στα υποδεικνυόμενα σημεία. Οι δέκτες GPS, σε πραγματικό χρόνο μπορούν να βελτιώσουν την ακρίβεια των συστημάτων GPS από μέτρα (στο συμβατικό GPS) μέχρι σε εκατοστά. Άλλοι αισθητήρες που ανιχνεύουν οπτική ροή, υπερήχους και απόσταση (LIDAR – Light Detection and Ranging[133]) εξασφαλίζουν μια σταθερή εμπειρία πτήσης.

[133] Η τεχνική LIDAR (Light Detection And Ranging) βασίζεται στην εκπομπή παλμικής ακτινοβολίας λέιζερ στην ατμόσφαιρα και ακολούθως, στην καταγραφή της οπισθοσκεδαζόμενης ακτινοβολίας λέιζερ. Η ατμόσφαιρα αποτελούμενη από άτομα, μόρια, αιωρούμενα σωματίδια (αερολύματα), κλπ. προκαλεί εξασθένηση της διερχόμενης ακτινοβολίας λέιζερ. Η σκεδαζόμενη ακτινοβολία συλλέγεται από ένα οπτικό τηλεσκόπιο και

Σε ένα σχετικό ερευνητικό έργο, οι P. Razi, και J.T. Sumantyo [241] χρησιμοποίησαν ένα UAV σε μια τεχνική τρισδιάστατης φωτογραμμετρίας[134] που επικυρώνει τη μεθοδολογία παρακολούθησης μιας περιοχής. Μετά τη χαρτογράφηση της παραμόρφωσης της γης και τη διεξαγωγή μιας επίγειας έρευνας, ανέφεραν πιο ακριβή αποτελέσματα παρακολούθησης με τρισδιάστατη φωτογραμμετρία από ό,τι με δορυφόρο προηγμένης παρατήρησης εδάφους. Η μελέτη αυτή επιβεβαίωσε την εξαιρετική απόδοση των UAVs σε δίκτυα αποκατάστασης καταστροφών, ανεξάρτητα από το αν η καταστροφή είναι φυσική ή ανθρωπογενής. Σε αυτή τη μελέτη, τα πολλαπλά UAVs που διανεμήθηκαν στην περιοχή της καταστροφής λειτούργησαν ως αναμεταδότες μεταξύ των «επιζώντων' κινητών σταθμών βάσης. Τα UAVs αύξησαν σημαντικά την ποιότητα των πληροφοριών που παραδόθηκαν στους χρήστες εδάφους και στους επιζώντες σταθμούς βάσης σε περίπτωση καταστροφής και/ή άλλων απρόβλεπτων συμβάντων. Τα UAVs κρίθηκαν κατάλληλα όχι μόνο για αποστολές χαρτογράφησης και τοπογραφίας, αλλά και για παρακολούθηση ανθρώπων μετά από συμβάν καταστροφής.

Πριν την εμφάνιση μιας φυσικής καταστροφής στην ελεγχόμενη γεωγραφική περιοχή αναπτύσσεται δίκτυο ασυρμάτων αισθητήρων που παρέχει αδιάκοπα στοιχεία σχετικά με τα εξεταζόμενα, κάθε φορά, φαινόμενα (π.χ., πλημμύρα, φωτιά, σεισμός). Τα μη επανδρωμένα εναέρια οχήματα σε αυτό το στάδιο χρησιμοποιούνται κατά τις περιπτώσεις που ληφθούν κάποιες ακραίες τιμές-μετρήσεις από τα δίκτυα ασυρμάτων αισθητήρων και καλούνται να εξετάσουν επι τόπου το σημείο του συμβάντος. Ενδεχομένως παράσχουν και οπτικό υλικό στον κέντρο ελέγχου, αφού μπορούν να φέρουν και ειδική κάμερα. Η φάση της προετοιμασίας δεν έχει συγκεκριμένη διάρκεια και θα μπορούσε να αρχίσει αρκετά χρόνια πριν το αναμενόμενο συμβάν, με αποκορύφωση το ίδιο το συμβάν. Αναλόγως του τύπου της καταστροφής, τα δίκτυα ασυρμάτων αισθητήρων διαδραματίζουν πρωταρχικό ρόλο, με τη συμμετοχή/συνδρομή των εναέριων μη επανδρωμένων μέσων να είναι υποστηρικτική [242].

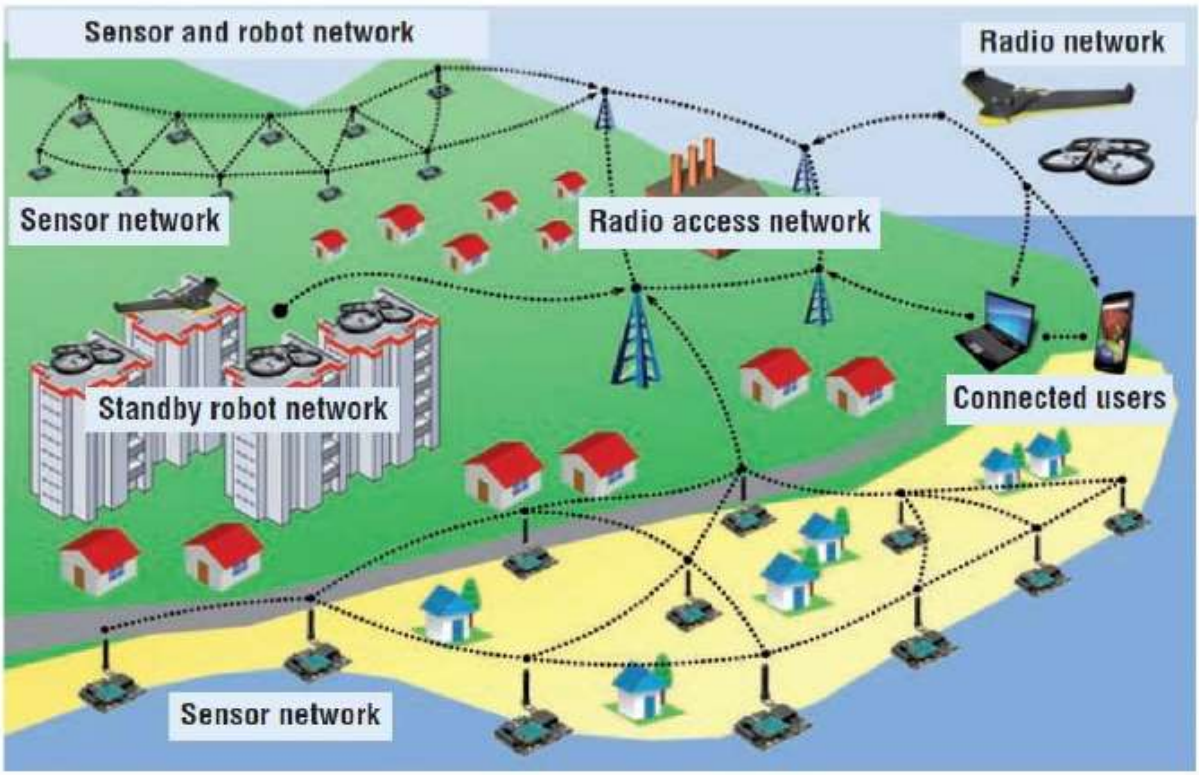
Στην περίπτωση μελέτης για καταγραφή πλημμυρών και κατολισθήσεων σε μια γεωγραφική περιοχή, πολλαπλοί αισθητήρες έχουν συλλέξει πληροφορίες όπως η στάθμη του νερού, η δόνηση ενός σεισμού, η μετατόπιση ενός μέρους γης και τις έχουν προωθήσει ήδη στην περιοχή όπου βρίσκεται το κέντρο ελέγχου όπου έχει γίνει η σχετική καταγραφή. Το δίκτυο που χρησιμοποιείται για την επικοινωνία των αισθητήρων είναι το κυψελοειδές (3G, 4G,

---

οδηγείται στο σύστημα λήψης και καταγραφής των σημάτων LIDAR. Η τεχνική LIDAR, αναλύοντας τα οπισθοσκεδαζόμενα σήματα που προέρχονται από την αλληλεπίδραση των συστατικών της ατμόσφαιρας με την ακτινοβολία λέιζερ, είναι ικανή για να καθορίσει την κατακόρυφη κατανομή των κυριότερων ρύπων και συστατικών της ατμόσφαιρας με μεγάλη χωρική (~3-7 m) και χρονική ακρίβεια (από 10-30 s έως μερικά min).
Πηγή: https://el.wikipedia.org/wiki/LIDAR

[134] Φωτογραμμετρία ονομάζεται μια ιδιαίτερη μέθοδος - τεχνική προσδιορισμού διαστάσεων αντικειμένων με χρήση φωτογραφιών. Στη μέθοδο αυτή ακολουθείται ιδιαίτερος τρόπος φωτογράφησης. Εφευρέτης της μεθόδου αυτής ήταν ο Γάλλος ερευνητής Aimé Laussedat το 1851 και την χρησιμοποίησε ειδικά για τη χαρτογράφηση περιοχών. Ο εξοπλισμός και τα όργανα (φωτογραφικές μηχανές, κ.λπ.) που χρησιμοποιούνται στη μέθοδο αυτή έχουν ήδη εξελιχθεί σε πολύ υψηλό βαθμό μέχρι αυτοματοποίησης. Η δε παράλληλη εξέλιξη των μέσων από τα οποία πραγματοποιείται αυτή, ειδικότερα των διαστημικών μηχανών (τεχνητών δορυφόρων) επιτρέπει πλέον την εφαρμογή σε υψηλό βαθμό ποιότητας, με κάλυψη και των τριών διαστάσεων καλούμενη επί τούτου ως στερεοφωτογραμμετρία.
Πηγή:
https://el.wikipedia.org/wiki/%CE%A6%CF%89%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CE%BC%CE%BC%CE%B5%CF%84%CF%81%CE%AF%CE%B1

4G+) το οποίο είναι ήδη εγκατεστημένο και δεν χρειάζεται κάποια επιπλέον υποδομή. Η εναέρια επιτήρηση μέσω των UAVs είναι περιορισμένη σε τέτοιου τύπου καταστροφές, καθώς απαιτούνται μετρήσεις που έχουν να κάνουν με το έδαφος. Αντί για καταγραφή, τα UAVs θα επιτελέσουν το ρόλο των «μεταφορέων» της πληροφορίας από τους αισθητήρες προς το κέντρο ελέγχου, γεγονός το οποίο θα βοηθήσει στην άμεση ανάλυση ώστε να ληφθεί η εκτίμηση της πιθανότητας πιθανών μελλοντικών καταστροφών.



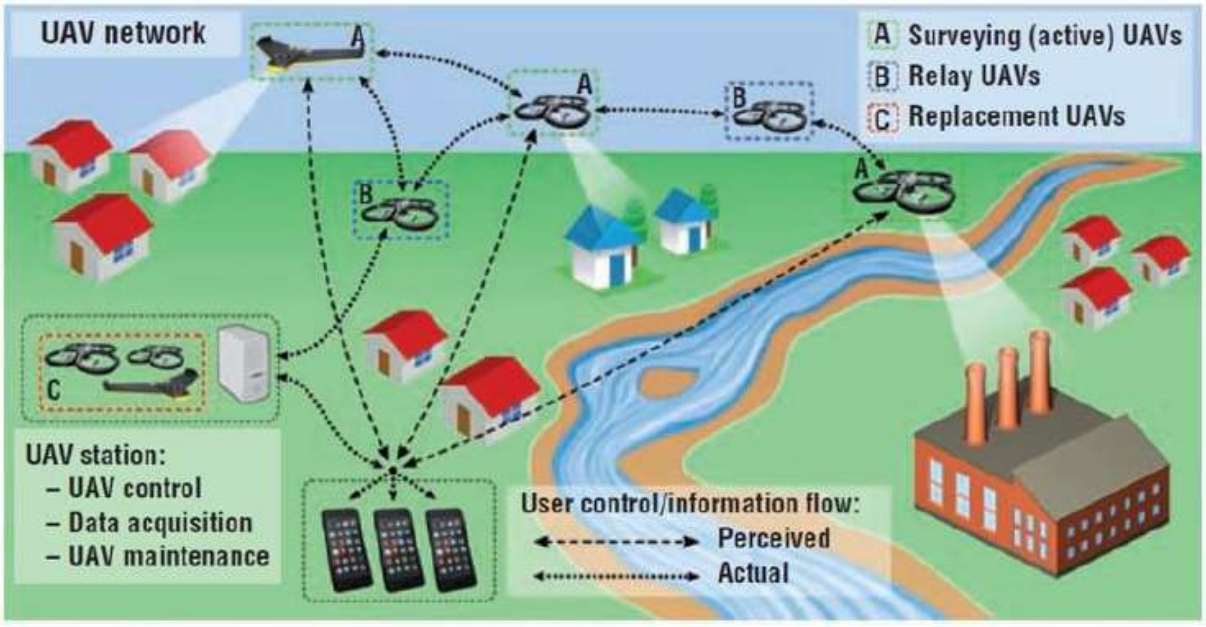
Εικόνα 8-10: Προετοιμασία δικτύου αισθητήρων και UAVs πριν την καταστροφή

Σε δεύτερο στάδιο, αφού έχει εκδηλωθεί κάποιο καταστροφικό φαινόμενο, γίνεται η αξιολόγηση του μεγέθους και της έκτασης της σχετικής καταστροφής. Τα δίκτυα ασυρμάτων αισθητήρων είναι πλέον πιθανό να μην είναι απολύτως λειτουργικά, αφού ενδεχομένως κάποια μέρη τους να έχουν καταστραφεί. Εντούτοις σε περίπτωση, π.χ. μιας πυρκαγιάς, μπορούν να συνεχίσουν να δίνουν δεδομένα από σημεία της ελεγχόμενης περιοχής που δεν έχουν πληγεί ακόμα και το δίκτυο εξακολουθεί να είναι ακόμα λειτουργικό. Τα μη επανδρωμένα εναέρια οχήματα παίζουν σημαντικότερο ρόλο σε αυτό το στάδιο. Παρέχουν πληροφόρηση και δίνουν την εικόνα της κατάστασης σε πραγματικό χρόνο και επίσης παρέχουν στοιχεία που βοηθούν ώστε να μπορέσει να εκπονηθεί σε επερχόμενο στάδιο μια πρώτη μελέτη οικονομικής και υλικής αποκατάστασης της πληγείσας περιοχής. Η λογική λειτουργίας του ασύρματου δικτύου αλλάζει πλέον από λειτουργία καταγραφής σε λειτουργία παροχής ακριβούς αξιολόγησης της κατάστασης.

Πριν την απογείωση των UAVs, σημαντικά στοιχεία προσδιορίζονται και λαμβανονται υπόψη, όπως [243]:

- Τα μοντέλα UAVs και οι προδιαγραφές τους (δηλαδή ταχύτητα εδάφους, μέγιστο ύψος και συμπεριφορά πτήσης).
- Οι προδιαγραφές της κάμερας (εστιακή απόσταση, οπτικό πεδίο (FoV) και απόσταση δειγματοληψίας εδάφους (GSD).
- Το ύψος, το εύρος και ο χρόνος πτήσης.
- Το μέγεθος και η κατάσταση της περιοχής προς εξέταση.
- Το εύρος αλληλοκάλυψης των οχημάτων.

Εφόσον συνεκτιμηθούν οι παράγοντες επιλογής οχημάτων και υλοποιηθεί το σενάριο πτήσης, για τις φυσικές καταστροφές που έχουν ολοκληρωθεί τα μη επανδρωμένα εναέρια οχήματα δημιουργούν ένα ανεξάρτητο δίκτυο χωρίς την υποστήριξη από τους αισθητήρες που είναι ανεπτυγμένοι στο έδαφος. Όπως φαίνεται στην Εικόνα 8-11 δημιουργείται ένα δίκτυο από τα εναέρια εν πτήσει οχήματα που επιτρέπει να συνεχιστεί η ροή των πληροφοριών από την πληγείσα περιοχή προς το κέντρο ελέγχου, ώστε να γίνει η όσο το δυνατόν εγκυρότερη αποτίμησ της τρέχουσας κατάστασης. Επίσης δημιουργείται και ένα προσωρινό δίκτυο που παρέχει κάλυψη στην περιοχή και στους χρήστες που βρίσκονται εκεί, το οποίο είναι βασικός παράγοντας για θέματα χειρισμοών και λήψης αποφάσεων λόγω της έκτακτης κατάστασης που επικρατεί εκείνη τη στιγμή στην υπό θεώρηση περιοχή.



Εικόνα 8-11: Αξιολόγηση καταστροφής από UAVs

Μετά το πέρας της καταστροφής, τα UAVs διαδραματίζουν σημαντικό ρόλο, αφού τα εγκατεστημένα δίκτυα ασυρμάτων αισθητήρων πιθανώς να μην είναι πλέον λειτουργικά. Τα UAVs παρέχουν υποστήριξη, δίνοντας σημαντικές πληροφορίες στις επίγειες ομάδες διάσωσης και οδηγώντας αυτές σε σημεία που ενδεχομένως να κινδυνεύουν ανθρώπινες ζωές. Επίσης παίζουν ρόλο και στην προσωρινή αποκατάσταση των δικτύων επικοινωνίας, όπως για παράδειγμα στα κυψελοειδή δίκτυα, που ενδεχομένως έχουν υποστεί βλάβες ή

έχουν καταστραφεί εντελώς. Τέλος, μπορούν να δώσουν πληροφορίες σχετικά με τις ασφαλείς περιοχές και τις διαδρομές εκκένωσης καθώς και για τη διενέργεια ελέγχων που ζητούνται από τις αρμόδιες Αρχές στην ευρύτερη περιοχή που έχει προκληθεί η καταστροφή.

Το δίκτυο αναμετάδοσης που σχηματίζεται από τα μη επανδρωμένα εναέρια οχήματα απαρτίζεται από εναέριες υποδομές και απαιτείται να διαθέτει υψηλό επίπεδο ανθεκτικότητας ως προς τις διακοπές στις συνδέσεις, λόγω μεταβολών που σχετίζονται με την κίνηση ή την αλλαγή του ενεργειακού επιπέδου των οχημάτων. Η αντιμετώπιση αυτού του ζητήματος απαιτεί τον αρχικό σχεδιασμό πτήσης που θα προσδιορίζει τα βέλτιστα σημεία αναμετάδοσης τα οποία συνδέουν την περιοχή καταστροφής με το πλησιέστερο δίκτυο επικοινωνίας και στη συνέχεια έναν περαιτέρω σχεδιασμό που θα υλοποιείται κατά την διάρκεια της ανάπτυξης και θα καλύπτει τυχόν κενά που εντοπίζονται στην πορεία. Οι πολυμεσικές πληροφορίες (π.χ. βίντεο, φωτογραφίες) που συλλέγονται από τα μη επανδρωμένα εναέρια οχήματα παρουσιάζουν μια γενική εικόνα της κατάστασης. Ωστόσο, πρέπει και οι ίδιοι οι πληγέντες που τυχόν βρίσκονται εκείνη την ώρα στην περιοχή καταστροφής, εάν μπορούν χρησιμοποιώντας τα κοινωνικά μέσα επικοινωνίας, να αναμεταδίδουν ή/και να προωθούν μηνύματα κειμένου ή εικόνες μέσω του Διαδικτύου. Αυτή η δραστηριότητα μπορεί συμπληρωματικά να προσφέρει ακόμα και επί τόπου λεπτομερείς πληροφορίες που μπορούν να φτάσουν στο κέντρο ελέγχου, παράλληλα με τις πληροφορίες που συλλέγονται από τα UAVs [242].

Εικόνα 8-12: Αξιολόγηση καταστροφής του τυφώνα Laura στον κόλπο του Μεξικού, από ερασιτεχνικά UAVs[135]

[135] Πηγή: https://www.cmu.edu/news/stories/archives/2020/august/drones-hurricane-damage.html

9

Συμπεράσματα

Μέσω της συγκεκριμένης εργασίας επιχειρήθηκε μια γενική περιγραφή των δικτύων ασυρμάτων αισθητήρων (WSNs) και του IoT του οποίου η χρήση έχει γίνει σε πολλές περιοχές σχεδόν «καθολική» και συναντάται σε πολλές καθημερινές εφαρμογές, ενώ θεωρείται από τις 21 πιο σημαντικές τεχνολογίες του 21ου αιώνα (Business Week Heralded). Η ανάπτυξη αυτών των δικτύων με την πάροδο του χρόνου είναι αλματώδης τόσο όσον αφορά στην ανάπτυξη ως προς το σχετικό υλισμικό (HW), όσο και ως προς τη βελτίωση των χρησιμοποιούμενων αλγορίθμων δρομολόγησης και επικοινωνίας. Εκτός των άλλων, στην παρούσα εργασία περιγράφεται και η συνεργασία όπως επίσης και η ενσωμάτωση των δικτύων αυτών με μεταγενέστερες τεχνολογίες, γεγονός που έχει ως αποτέλεσμα το να είναι εφικτή η υλοποίηση πολύπλοκων εφαρμογών φυσικής ασφάλειας, μη δυνάμενων διαφορετικά να υλοποιηθούν. Ωστόσο, παρατηρήσαμε πως τα ασύρματα δίκτυα αισθητήρων παρουσιάζουν διάφορες προκλήσεις τις οποίες δεν αντιμετωπίζουν τα συμβατικά ασύρματα δίκτυα. Ως αποτέλεσμα, η συνθήκη αυτή απαιτεί την ανάγκη σχεδιασμού κατάλληλων μεθόδων προστασίας για την αντιμετώπιση των συναφών προκλήσεων.

Από την άλλη μεριά, η διαχείριση της ενεργειακής απόδοσης εξακολουθεί να αποτελεί βασικό μέλημα για τους ερευνητές, ιδίως όσον αφορά στα ασύρματα δίκτυα αισθητήρων, καθώς η πολυπλοκότητα και η αύξηση των εφαρμογών οδηγεί στην ανάγκη εξασφάλισης επαρκούς ενεργειακής αυτονομίας. Η χρήση ανανεώσιμων πηγών ενέργειας και η ενσωμάτωση βοηθητικών μέσων στη λειτουργία των δικτύων, όπως π.χ. των εναέριων μη επανδρωμένων οχημάτων, είναι παράγοντες που διαδραματίζουν σημαντικό ρόλο προς αυτή την κατεύθυνση.

Μια άλλη μεγάλη πρόκληση είναι η προσαρμογή των δικτύων σε περιπτώσεις που οι αντίστοιχες εφαρμογές απαιτούν τη χρήση ετερογενών δικτύων αισθητήρων. Με την αύξηση του αριθμού και της πολυπλοκότητας των εφαρμογών αναμένεται τα παραδοσιακά δίκτυα, τα οποία συνήθως εκτελούσαν μια συγκεκριμένη διεργασία, να πρέπει να υλοποιήσουν ταυτόχρονα πολλαπλές εφαρμογές – συχνά με αποκλίνοντες στόχους η καθεμία – ενώ ένας άλλος κρίσιμος παράγοντας στα δίκτυα ασυρμάτων αισθητήρων είναι η εξασφάλιση της ποιότητας της υπηρεσίας (QoS) υπό συγκεκριμένα και ενίοτε αυστηρά πλαίσια.

Άλλος σημαντικός προβληματισμός που τέθηκε στην εργασία, είναι η διασύνδεση και η συνεργασία των δικτύων ασυρμάτων αισθητήρων με άλλα υφιστάμενα δίκτυα. Σε πολλές εφαρμογές απαιτείται η διασύνδεση των WSNs με άλλους τύπους δικτύων (όπως το Internet, το WiFi ή το κυψελοειδές δίκτυο). Αυτή η «διασυνεργασία» δημιουργεί παράλληλες προκλήσεις που πρέπει τύχουν κατάλληλης διερεύνησης, όπως π.χ. η εξεύρεση αποδοτικότερων τρόπων διασύνδεσης και η δυνατότητα ώστε τα υφιστάμενα πρωτόκολλα ενός WSN να υποστηρίζουν ή τουλάχιστον να μην ανταγωνίζονται με τα πρωτόκολλα των άλλων δικτύων.

Στη συνέχεια της εργασίας και εφόσον οι παραπάνω προβληματισμοί αποδεχτούμε ότι βρίσκονται σε ένα διαρκές στάδιο έρευνας και βελτίωσης, με τα μέσα και τους πόρους που ήδη διατίθενται στην αγορά, διερευνήθηκαν τρόποι εφαρμογής των WSNs για την προστασία Κρίσιμων Υποδομών. Μέσω της προτεινόμενης βιβλιογραφίας και μεθοδολογίας έλαβε χώρα μια προσπάθεια τυποποίησης των παραμέτρων που θεωρούνται ζωτικής σημασίας για μια Κρίσιμη Υποδομή. Επίσης, μέσα από τη μελέτη των ορισμών εξετάστηκαν και άλλες παράμετροι (όπως π.χ. η αλληλοεπίδραση των δομών αυτών, αλλά και ο αντίκτυπος μιας ενδεχόμενης καταστροφής). Στόχος μας αποτέλεσε η αποτίμηση της επικινδυνότητας για τις Κρίσιμες Υποδομές ICT, μέσω της μελέτης βασικών τύπων αποτυχούς λειτουργίας. Με τον τρόπο αυτό μπορεί να είναι εφικτός ο προσδιορισμός των χαρακτηριστικών κάθε τύπου αποτυχίας και συνεπώς μπορεί να προκύπτει ο τρόπος αντιμετώπισης και/ή προφύλαξης.

Εφόσον διακρίνουμε ξεκάθαρα το τρίπτυχο κατά το οποίο διερωτόμαστε «ΤΙ θέλουμε να προστατέψουμε», «από ΠΟΙΟΝ θέλουμε να το προστατέψουμε» και «ΠΩΣ θα το προστατέψουμε», μελετάμε τις πιθανότητες συμβολής των ασύρματων δικτύων αισθητήρων στη φυσική ασφάλεια των Κρίσιμων Υποδομών. Ο λόγος της διερεύνησης αυτής είναι να εκληφθούν τα πλεονεκτήματα που μας προσφέρουν τα WSNs σε σύγκριση με τα συμβατικά συστήματα ασφαλείας τα οποία γνωρίζουμε έως σήμερα. Στα κυριότερα πλεονεκτήματα καταλέγονται η ασύρματη δικτύωση και η ελευθερία κινήσεων σε μια μεγάλη περιοχή, καθώς επίσης και η πληθώρα των τεχνολογιών αλλά και των αισθητήρων που μπορούμε να χρησιμοποιήσουμε ώστε να δημιουργήσουμε αποτελεσματικούς τρόπους προστασίας, τόσο από παραβατικές ενέργειες όσο και από φυσικές καταστροφές σε Κρίσιμες Υποδομές. Σε κάθε περίπτωση, δεν έχουμε παραμελήσει να εξετάσουμε τους τρόπους προστασίας των ίδιων των δικτύων από κακόβουλες ενέργειες και/ή κυβερνοεπιθέσεις, ώστε συνολικά να μπορεί να είναι εφικτή η διασφάλιση άρτιου αποτελέσματος και λειτουργίας όλων των εμπλεκόμενων πόρων και μηχανισμών.

Τα παραπάνω αποδεικνύονται επιτυχώς μέσα από ορισμένες πραγματικές επιλεχθείσες περιπτώσεις χρήσης, οι οποίες έχουν εφαρμοστεί είτε σε πειραματικό είτε σε πραγματικό στάδιο. Μάλιστα, μέσα από τις περιπτώσεις χρήσης διαπιστώνουμε την πολύτιμη συμβολή και άλλων μέσων όπως τα μη-επανδρωμένα οχήματα, αναφορικά με τη διαπίστωση της έκτασης μιας καταστροφής. Εύκολα γίνεται αντιληπτό ότι, ο συνδυασμός των τεχνολογικών μέσων που πλέον διαθέτουμε μας φανερώνει νέους τρόπους και επιλογές στη φυσική προστασία των Κρίσιμων Υποδομών αλλά και του ευρύτερου περιβαλλοντολογικού θησαυρού. Άξιο παρατήρησης είναι επίσης, ότι η πολυπλοκότητα των μεθόδων αυτών απαιτεί εξειδικευμένες και σύγχρονες γνώσεις οι οποίες με την σειρά τους ενδεχομένως θα προδιαγράψουν τις εργασιακές απαιτήσεις του μέλλοντος.

9.1 Παραδοχές και συμβιβασμοί

Γενικά, η παρούσα διατριβή επικεντρώνεται στα μέσα και στις μεθόδους προστασίας πληροφοριακών και επικοινωνιακών κρίσιμων υποδομών, γεγονός που σημαίνει ότι εστιάζει σε υποδομές οι οποίες στοχεύουν στην παροχή πληροφοριών, υπηρεσιών επικοινωνίας ή άλλων ηλεκτρονικών υπηρεσιών. Από την άλλη μεριά, τα μέσα και αυτές οι μέθοδοι εμφανίζουν και αδυναμίες, εκτός των πολλών πλεονεκτημάτων τους. Επίσης, όσον αφορά στις κρίσιμες υποδομές θα πρέπει να σημειώσουμε ότι άλλες σχετικές συνιστώσες δεν ελήφθησαν υπόψη στην προσέγγισή μας, όπως για παράδειγμα οι νομικές που προκύπτουν από τα ισχύοντα θεσμικά πλαίσια ή τυχόν επιχειρηματικές που υπαγορεύονται από συγκεκριμένη στρατηγική και τυχόν αντίστοιχα επενδυτικά σχήματα.

Συνοπτικά, παρακάτω απαριθμούνται οι παραδοχές που υιοθετήθηκαν στα επιμέρους στάδια της διατριβής.

Ζητήματα Ποιότητας των Υπηρεσιών (QoS)

Η φύση των δικτύων WSNs καθιστά δύσκολο εγχείρημα την απαίτηση για διάθεση και εξασφάλιση ακριβούς ποιότητας των αντίστοιχα παρεχόμενων υπηρεσιών. Ενώ τα συμβατικά δίκτυα χρησιμοποιούν παραμέτρους όπως η καθυστέρηση και η απώλεια πακέτων για να καθορίσουν τις απαιτήσεις QoS κάθε εφαρμογής, τα δίκτυα ασυρμάτων αισθητήρων χρησιμοποιούν παραμέτρους όπως η ακρίβεια δεδομένων, η κάλυψη, η ανοχή σφάλματος και η διάρκεια ζωής του δικτύου. Αυτές οι παράμετροι είναι δύσκολο να εκληφθούν απόλυτα υπόψη στα υφιστάμενα πρωτόκολλα ποιότητας υπηρεσίας, λόγω του περιορισμού των πόρων των συναφών κόμβων, του δύσκολου επιχειρησιακού περιβάλλοντος, της μεγάλης κλίμακας και της τυχαίας ανάπτυξης των κόμβων. Έτσι, η περιγραφή και σχεδίαση ενός κατάλληλου μοντέλου QoS για το δίκτυο WSNs συνιστά είναι ένα εξαιρετικά σύνθετο και με πολλές απαιτήσεις πρόβλημα. Ένα κατάλληλο πρωτόκολλο ποιότητας υπηρεσίας θα πρέπει να εξετάζει διάφορες παραμέτρους όπως π.χ.: η ενεργειακή βιωσιμότητα, η αξιοπιστία, η ασφάλεια, η κλιμάκωση, η κινητικότητα και η ετερογένεια.

Τα δομικά στοιχεία ενός δικτύου οφείλουν να καλύπτουν τις απαιτήσεις ποιότητας του τελικού χρήστη, κάτι που αποτελεί βασική μέριμνα του σχεδιαστή του δικτύου. Ειδικότερα σε δίκτυα WSNs, οι απαιτήσεις ποιότητας μπορούν να επικεντρώνονται σε θέματα ακρίβειας δεδομένων, καθυστέρησης μετάδοσης, συνάθροισης δεδομένων, ανοχής σφαλμάτων και κατανάλωσης ενέργειας. Η διαχείριση πολλαπλών σταθμών βάσης συνιστά μείζονα πρόκληση σε θέματα διασφάλισης ποιότητας της υπηρεσίας και το δίκτυο πρέπει να είναι σε θέση ώστε να υποστηρίζει διαφοροποιημένα επίπεδα QoS, ιδίως σε περίπτωση δικτύων με πολλά τερματικά.

Εκτίμηση Κρισιμότητας

Στις ΚΥ απαντώνται περιστατικά τα οποία μπορεί να χαρακτηρίζονται από πολύ χαμηλή πιθανότητα αποτυχίας με ταυτόχρονη, όμως, υψηλή επίπτωση κατά την εκδήλωσή τους. Η αρχική μέθοδος εκτίμησης κρισιμότητας δεν υπολογίζει την πιθανότητα εμφάνισης ενός περιστατικού-απειλής σε κάποια συνιστώσα, ούτε και αν υπάρχουν ευπάθειες οι οποίες διευκολύνουν την εκδήλωσή του εν λόγω περιστατικού ή/και μεγιστοποιούν την πιθανή

επίπτωσή του. Αυτό συμβαίνει λόγω της έλλειψης επαρκών στατιστικών ή ιστορικών δεδομένων αλλά επίσης και εξαιτίας της πολυπλοκότητας των «αλληλεξαρτήσεων» μεταξύ των υποδομών. Έτσι, ο εκάστοτε υπεύθυνος για τη λήψη αποφάσεων θέτει προτεραιότητες για να «σταθμίσει» τους παράγοντες της εμβέλειας, της έντασης και του χρόνου και για να επιλέξει πόσο σημαντικοί είναι αυτοί κατά τον υπολογισμό της αντίστοιχης κρισιμότητας.

Εκτίμηση Επικινδυνότητας

Κάθε υπεύθυνος ασφαλείας υποτίθεται πως έχει εκπονήσει μια βασική μελέτη εκτίμησης της επικινδυνότητας και έχει σχεδιάσει όπως και υιοθετήσει ένα αντίστοιχο πλάνο ασφάλειας. Αυτό μπορεί να είναι εφικτό είτε εφαρμόζοντας κάποια αναγνωρισμένη μέθοδο εκτίμησης επικινδυνότητας είτε υιοθετώντας κάποιο συναφές διεθνές πρότυπο. Η υπόθεση-παραδοχή αυτή συνεπάγεται ότι ο υπεύθυνος ασφαλείας έχει καταγράψει όλα τα σημαντικά του αγαθά, τις ενδεχόμενες απειλές (εκ των «έσω» αλλά και εξωτερικές), τις πιθανές επιπτώσεις και έχει υπολογίσει την επικινδυνότητα. Επίσης, ο υπεύθυνος ασφαλείας έχει εκπονήσει μελέτες ανάλυσης τρωτότητας (vulnerability analysis) για τις τεχνολογικές του συνιστώσες και είναι ενήμερος ή έχει αντιμετωπίσει πιθανά πορίσματα/λύσεις που προκύπτουν από αυτές.

Εφαρμογή Θεωρίας

Μελλοντικό βήμα αποτελεί η εφαρμογή της θεωρίας σε πραγματικό περιβάλλον. Αυτό θα μπορούσε να συμπεριλάβει τον σχεδιασμό περισσότερων μελετών περιπτώσεων χρήσης για τον έλεγχο της εφαρμογής της θεωρίας σε ένα σύνθετο περιβάλλον αλληλεξαρτώμενων κρίσιμων υποδομών. Ένα τέτοιο εγχείρημα είναι εξαιρετικά περίπλοκο και δύσκολο, καθώς απαιτεί τη συνεργασία με διάφορους κοινωνικούς τομείς, όπως επιστημονικούς τομείς, κοινωνιολόγους, ερευνητές κλπ.

9.2 Εκτίμηση της Αγοράς των WSNs

Η αγορά των δικτύων ασύρματων αισθητήρων εκτιμήθηκε στα 29,06 δισεκατομμύρια το 2016 και αναμένεται να φθάσει τα 93,86 δισεκατομμύρια δολάρια έως το 2023, με CAGR 18,55% κατά την περίοδο πρόβλεψης[136]. Τα ασύρματα δίκτυα αισθητήρων αναμένεται να μεταμορφώσουν τον τρόπο που πραγματοποιείται η επικοινωνία στον φυσικό κόσμο. Οι οργανισμοί χρειάζονται ορατότητα και ευφυΐα σε πραγματικό χρόνο για τα οργανωτικά και επιχειρησιακά δεδομένα τους για να φτάσουν σε αυτό το νέο επίπεδο αποτελεσματικότητας, ακρίβειας και εξοικονόμησης κόστους.

Το παγκόσμιο μέγεθος της αγοράς ασύρματων δικτύων βιομηχανικών αισθητήρων αναμένεται να φθάσει τα 8.669,8 εκατομμύρια δολάρια ΗΠΑ έως το 2025, αυξάνοντας με CAGR 15,2% από το 2019 έως το 2025, σύμφωνα με αυτή τη μελέτη. Τα οφέλη που προσφέρει το WSN μέσω ενσύρματων δικτύων, όπως η κινητικότητα, η δυνατότητα αυτο-ανακάλυψης, το συμπαγές μέγεθος, η αποδοτικότητα κόστους και η μειωμένη

[136] Έρευνα της Research and Markets
Πηγή: https://zarifopoulos.com/global-connected-home-security-system-market-2016-2020/

πολυπλοκότητα, αναμένεται να διαδραματίσουν σημαντικό ρόλο στην αύξηση της παγκόσμιας ζήτησης. Η αυξανόμενη υιοθέτηση ασύρματης επικοινωνίας, η ανάγκη για ισχυρή συνδεσιμότητα σε απομακρυσμένες τοποθεσίες και η ζήτηση για υποδομή δικτύου αναμένεται να τροφοδοτήσουν την ανάπτυξη της αγοράς. Οι πρόσφατες εξελίξεις στους τομείς του Internet of Things (IoT) και της Τεχνητής Νοημοσύνης (AI) έχουν αυξήσει περαιτέρω τη ζήτηση για ασύρματα δίκτυα και ισχυρή συνδεσιμότητα. Η ταχεία υιοθέτηση αυτών των τεχνολογιών από το πετρέλαιο και το φυσικό αέριο, τον κατασκευαστικό κλάδο, τις επιχειρήσεις κοινής ωφέλειας και τις βιομηχανίες αυτοκινήτων, αναμένεται να ενισχύσει την ανάπτυξη της βιομηχανικής αγοράς ασύρματων δικτύων αισθητήρων. Επιπλέον, βασικοί παράγοντες και «παίκτες» της αγοράς επενδύουν σε μεγάλο βαθμό για να διερευνήσουν το πεδίο εφαρμογής της τεχνολογίας για καινοτομίες, ολοκλήρωση και νέες εξελίξεις προϊόντων. Για παράδειγμα, η ABB Ltd., η οποία διαθέτει 7 ερευνητικά κέντρα και περισσότερους από 8.000 τεχνολόγους, επένδυσε 1,5 δισεκατομμύρια δολάρια ΗΠΑ σε Ε & Α το 2016.

Παγκόσμιοι παίκτες στην αγορά WSN συνεργάζονται με νεοεισερχόμενους για την παροχή βελτιωμένων προϊόντων και συστημάτων με καλύτερες αποδόσεις. Τον Ιανουάριο του 2017, η Honeywell Process Solutions συνεργάστηκε με την AEREON[137] για την ανάπτυξη λύσεων που βοηθούν τον βιομηχανικό τομέα να βελτιώσει τη λειτουργική αποδοτικότητα, ασφάλεια και αξιοπιστία, φανερώνοντας την πλέον αισιόδοξη μελλοντική τάση όσον αφορά στα ασύρματα δίκτυα αισθητήρων.

9.3 Επίλογος

Η παρούσα διατριβή ασχολήθηκε με την ερευνητική περιοχή των Ασύρματων Δικτύων Αισθητήρων καθώς και με την προστασία Κρίσιμων Υποδομών. Αρχικά η εργασία κινήθηκε στον άξονα της θεωρητικής προσέγγισης των WSNs, ενώ στην συνέχεια επεκτάθηκε στις Κρίσιμες Υποδομές, σε μια προσπάθεια ανάδειξης ορισμών και χαρακτηριστικών. Η χρήση του γνωστικού υποβάθρου αποσκοπούσε στην κατανόηση και στον εντοπισμό γόνιμων ερευνητικών θεμάτων, για την ανάδειξη των τεχνολογιών και των μεθόδων κατά τις οποίες τα ασύρματα δίκτυα αισθητήρων αναδεικνύονται ως μέσα φυσικής προστασίας τόσο των Κρίσιμων Υποδομών όσο και του περιβάλλοντος, ευρύτερα. Στη συνέχεια, η διατριβή εστίασε στη εξέταση μεθόδων και στρατηγικών για την ψηφιακή προστασία των WSNs καθώς παρατηρήθηκε ότι τα δίκτυα αυτά έχουν πλεονεκτήματα αλλά και ορισμένα τεχνολογικά μειονεκτήματα.

Η καθημερινή ζωή βασίζεται σε μεγάλο βαθμό στην αξιόπιστη και ασφαλή λειτουργία και την έξυπνη διαχείριση κρίσιμων υποδομών μεγάλης κλίμακας. Οποιαδήποτε καταστροφή ή διακοπή της ομαλής λειτουργίας αυτών των υποδομών θα προκαλούσε τεράστιες συνέπειες και θα είχε εκτενή αντίκτυπο στην ασφάλεια, την εθνική οικονομία, την εθνική δημόσια υγεία ή σε οποιονδήποτε συνδυασμό αυτών των θεμάτων. Οι κρίσιμες υποδομές νοούνται ως περιουσιακά στοιχεία, συστήματα ή τμήματα αυτών, απαραίτητα για τη διατήρηση

[137] Simley, J. (2017): Honeywell And Aereon To Leverage Industrial Internet of Things (IIoT) For Oil And Gas. Honeywell UOP. Πηγή: https://www.honeywell.com/us/en/press/2017/01/honeywell-and-aereon-to-leverage-industrial-internet-of-things-iiot-for-oil-and-gas

ζωτικών κοινωνικών λειτουργιών, της υγείας, της ασφάλειας, και της οικονομικής ή κοινωνικής ευημερίας. Έτσι, οι πολίτες σήμερα αναμένουν ότι οι υποδομές ζωτικής σημασίας θα είναι πάντα διαθέσιμες και ότι θα υπόκεινται σε αποτελεσματική διαχείριση (με χαμηλό κόστος).

Τα WSNs καθώς και το IoT είναι οι κοινωνικοί μεταρρυθμιστές που μπορούν να μετατρέψουν ολόκληρο τον πλανήτη σε έναν έξυπνο και διασυνδεδεμένο ασφαλή κόσμο. Ωστόσο, η παρουσία περιοριστικών παραγόντων σε ένα ασύρματο δίκτυο αισθητήρων σε συνδυασμό με το ασύρματο μέσο μετάδοσης και την απομακρυσμένη και χωρίς ανθρώπινη επίβλεψη λειτουργία, ενίοτε καθιστούν το δίκτυο αυτό ευαίσθητο/ευάλωτο σε επιθέσεις ή άλλου είδους προσβολές. Οι επιθέσεις αυτές θέτουν υπό αμφισβήτηση τις απαιτήσεις ασφαλείας, στοχεύοντας στις λειτουργίες του ίδιου του δικτύου αλλά και στην κατάρρευση της αρχιτεκτονικής του. Για τον λόγο αυτό, οι μηχανισμοί και τα πρωτόκολλα προστασίας έναντι επιθέσεων τα οποία έχουν αναπτυχθεί και τυγχάνουν εφαρμογής στην ευρύτερη αγορά των τηλεπικοινωνιακών εφαρμογών και υποδομών, έχουν τόσο σημαντικό ρόλο όσο και η φυσική υπόσταση του ίδιου του δικτύου.

Παρά τα χρήσιμα συμπεράσματα που εξάγονται από την παρούσα διατριβή και τη συνεισφορά της στα ερευνητικά αντικείμενα που επισημαίνονται παραπάνω, είναι σαφές ότι απαιτείται περαιτέρω ερευνητική δραστηριότητα προκειμένου η προτεινόμενη προσέγγιση (ή μέρη αυτής) να εφαρμοσθούν σε μεγάλη κλίμακα και σε πραγματικό περιβάλλον. Παρόλα αυτά, η παρούσα διατριβή συνεισφέρει προς αυτή την κατεύθυνση, καθώς θέτει το πλαίσιο για μια πιο ολοκληρωμένη προσέγγιση στην εκτίμηση και την αξιολόγηση των μεθόδων προστασίας υποδομών με την χρήση των WSNs.

Βιβλιογραφία

[1] Agarwal, A., & Unhelkar, B. (2020). The Internet of Things (Chapter 22). In: Warf, B (editor), *Geographies of the Internet, 1st Edition*, Routledge Studies.

[2] Dileep, G. (2020). A survey on smart grid technologies and applications. *Renewable Energy*, *146*, 2589-2625.

[3] Ali, A., Jadoon, Y. K., Changazi, S. A., & Qasim, M. (2020, November). Military Operations: Wireless Sensor Networks based Applications to Reinforce Future Battlefield Command System. In: *2020 IEEE 23rd International Multitopic Conference (INMIC)* (pp. 1-6). IEEE.

[4] Ammar, M., Haleem, A., Javaid, M., Walia, R., & Bahl, S. (2021). Improving material quality management and manufacturing organizations system through Industry 4.0 technologies. In: *Materials Today: Proceedings of the Second International Conference on Aspects of Materials Science and Engineering (ICAMSE 2021*.

[5] Hussein, W., Abdullah, J., & Alduais, N. A. M. (2020). Data Aggregation Algorithms with Multiple Sensors in Clustered-Based WSN/IoT. *International Journal of Computing and Digital Systems*, *9*(03), 535-544.

[6] Faudzi, A. A. M., Sabzehmeidani, Y., & Suzumori, K. (2020). Application of micro-electro-mechanical systems (MEMS) as sensors: A review. *Journal of Robotics and Mechatronics*, *32*(2), 281-288.

[7] Pranata, R., Tondas, A. E., Huang, I., Lim, M. A., Siswanto, B. B., Meyer, M., & Mitrovic, V. (2020). Potential role of telemedicine in solving ST-segment elevation dilemmas in remote areas during the COVID-19 pandemic. *The American Journal of Emergency Medicine, 42*(2), 242-243.

[8] Khalid, M., Wang, K., Aslam, N., Cao, Y., Ahmad, N., & Khan, M. K. (2020). From smart parking towards autonomous valet parking: A survey, challenges and future Works. *Journal of Network and Computer Applications, 175*, Article 102935.

[9] Ortiz, F. M., Sammarco, M., Costa, L. H. M., & Detyniecki, M. (2020). Vehicle Telematics Via Exteroceptive Sensors: A Survey. *arXiv preprint arXiv:2008.12632*.

[10] Ayvaz, S., & Alpay, K. (2021). Predictive maintenance system for production lines in manufacturing: A machine learning approach using IoT data in real-time. *Expert Systems with Applications*, *173*(6), Article 114598.

[11] Pragadeswaran, S., Madhumitha, S., & Gopinath, S. (2021). Certain Investigations on Military Applications of Wireless Sensor Networks. *International Journal of Advanced Research in Science, Communication and Technology, 3*(1), 1-15.

[12] Manisalidis, I., Stavropoulou, E., Stavropoulos, A., & Bezirtzoglou, E. (2020). Environmental and health impacts of air pollution: A review. *Frontiers in Public Health*, *8*.

[13] Al Dakheel, J., Del Pero, C., Aste, N., & Leonforte, F. (2020). Smart buildings features and key performance indicators: A review. *Sustainable Cities and Society, 61*, Article 102328.

[14] Gopalakrishnan, K. (2020). Security vulnerabilities and issues of traditional wireless sensors networks in IoT. In: Peng SL., Pal S., Huang L. (eds), Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm, Intelligent Systems Reference Library, vol.174. (pp. 519-549). Springer, Cham.

[15] Jusak, J., & Mahmoud, S. S. (2018). A novel and low processing time ecg security method suitable for sensor node platforms. *International Journal of Communication Networks and Information Security*, *10*(1), 213-222.

[16] Patil, V. S., Mane, Y. B., & Deshpande, S. (2019). FPGA based power saving technique for sensor node in wireless sensor network (WSN). In: Mishra, B.B., Dehuri, S., et al. (eds) *Computational Intelligence in Sensor Networks,* Studies in Computational Intelligence (SCI), vol.776 (pp. 385-404). Springer, Berlin, Heidelberg.

[17] Ahmed, M. R., Huang, H., Sharma, D., and Cui, H. (2012). Wireless Sensor Network: Characteristics and Architectures. *International Journal of Information and Communication Engineering 6*(12), 1398-1401.
[18] Khelladi, L., Djenouri, D., Rossi, M., & Badache, N. (2017). Efficient on-demand multi-node charging techniques for wireless sensor networks. *Computer Communications*, *101*, 44-56.
[19] Yao, X. W., & Huang, W. (2019). Routing techniques in wireless nanonetworks: A survey. *Nano Communication Networks*, *21*, 100250.
[20] Mayton, B. D. (2020). *Sensor networks for experience and ecology* (Doctoral dissertation, Massachusetts Institute of Technology).
[21] Iqbal, N., Ahmad, S., & Kim, D. H. (2021). Health Monitoring System for Elderly Patients Using Intelligent Task Mapping Mechanism in Closed Loop Healthcare Environment. *Symmetry*, *13*(2), 357.
[22] Hassan, M. M., Alam, M. G. R., Uddin, M. Z., Huda, S., Almogren, A., & Fortino, G. (2019). Human emotion recognition using deep belief network architecture. *Information Fusion*, *51*, 10-18.
[23] Yang, G., Dai, L., & Wei, Z. (2018). Challenges, threats, security issues and new trends of underwater wireless sensor networks. *Sensors*, *18*(11), 3907.
[24] Fanian, F., & Rafsanjani, M. K. (2019). Cluster-based routing protocols in wireless sensor networks: A survey based on methodology. *Journal of Network and Computer Applications*, *142*, 111-142.
[25] Priyadarshi, R., Gupta, B., & Anurag, A. (2020). Deployment techniques in wireless sensor networks: a survey, classification, challenges, and future research issues. *The Journal of Supercomputing*, 1-41.
[26] Djedouboum, A. C., Abba Ari, A. A., Gueroui, A. M., Mohamadou, A., & Aliouat, Z. (2018). Big data collection in large-scale wireless sensor networks. *Sensors, 18*(12), 4474.
[27] Xu, C., Xiong, Z., Zhao, G., & Yu, S. (2019). An energy-efficient region source routing protocol for lifetime maximization in WSN. *IEEE Access*, *7*, 135277-135289.
[28] Hemagowri, J., Baranikumari, C., & Brindha, B. (2013). A study on proactive routing protocol in ad-hoc network. *International Journal of Modern Engineering Research (IJMER)*, 1-4.
[29] Mbarushimana, C., & Shahrabi, A. (2007, May). Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks. In: *Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)* (Vol. 2, pp. 679-684). IEEE.
[30] Kaur, H., Sahni, V., & Bala, M. (2013). A survey of reactive, proactive and hybrid routing protocols in MANET: A review. *Network*, *4*(3), 498-500.
[31] Echoukairi, H., Bourgba, K., & Ouzzif, M. (2015, September). A survey on flat routing protocols in wireless sensor networks. In: *Proceedings of the International Symposium on Ubiquitous Networking (UNet'15)* (pp. 311-324). Springer, Singapore.
[32] Singh, S. P., & Sharma, S. C. (2015). A survey on cluster-based routing protocols in wireless sensor networks. *Procedia computer science*, *45*, 687-695.
[33] El-Basioni, B. M. M., Abd El-kader, S. M., & Eissa, H. S. (2012). Designing a local path repair algorithm for directed diffusion protocol. *Egyptian Informatics Journal*, *13*(3), 155-169.
[35] Huang, L.U. (2013): A Novel Routing Algorithm for Hierarchical Wireless Sensor Networks", figshare. Thesis. https://doi.org/10.6084/m9.figshare.761940.v1 009.
[36] Liu M., Cao J., Chen G., Wang X. (2009) An Energy-Aware Routing Protocol in Wireless Sensor Networks. Sensors 2009, *9*, 445-462.
[37] Tyagi, S., & Kumar, N. (2013). A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor networks. *Journal of Network and Computer Applications*, *36*(2), 623-645.
[38] Jabbar, S., Minhas, A. A., Imran, M., Khalid, S., & Saleem, K. (2015). Energy efficient strategy for throughput improvement in wireless sensor networks. *Sensors*, *15*(2), 2473-2495.
[39] Guleria, K., & Verma, A. K. (2019). Comprehensive review for energy efficient hierarchical routing protocols on wireless sensor networks. *Wireless Networks*, *25*(3), 1159-1183.

[40] https://www.comm.upv.es/en/lines-hierarchical-routing/
[41] Manjeshwar, A., & Agrawal, D. P. (2001, April). TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks. In ipdps (Vol. 1, No. 2001, p. 189).
[42] Wang, J., Gao, Y., Yin, X., Li, F., & Kim, H. J. (2018). An enhanced PEGASIS algorithm with mobile sink support for wireless sensor networks. *Wireless Communications and Mobile Computing*, *Vol.2018, Article ID 9472075.*
[43] Banerjee, S., Ghosh, A., & Mitra, S. K. (2017). A modified mathematical model for life-time enhancement in wireless sensor network. *Mathematical Modelling of Engineer-ing Problems*, *4*(2), 84-90.
[44] Guleria, K., Kumar, S., & Verma, A. K. (2019). Energy Aware Location Based Routing Protocols in Wireless Sensor Networks. *World Scientific News*, *124*(2), 326-333.
[45] Lewandowski, T., Henze, D., Sauer, M., Nickles, J., & Bruegge, B. (2020, April). A Software Architecture to enable Self-Organizing, Collaborative IoT Resource Networks. In: *Proceedings of the 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)* (pp. 70-77). IEEE.
[46] Hawbani, A., Wang, X., Kuhlani, H., Karmoshi, S., Ghoul, R., Sharabi, Y., & Torbosh, E. (2018). Sink-oriented tree-based data dissemination protocol for mobile sinks wireless sensor networks. *Wireless Networks*, *24*(7), 2723-2734.
[47] Aetesam, H., & Snigdh, I. (2017). A comparative analysis of flat, hierarchical and location-based routing in wireless sensor networks. *Wireless Personal Communications*, *97*(4), 5201-5211.
[48] Kuzmin, A., & Fedeka, V. (2017, April). Comparison energy cost wireless sensor networks built on two routing algorithms-Directed Diffusion and Geographic Adaptive Fidelity. In: *Proceedings of the 2017 XIIIth International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH)* (pp. 9-11). IEEE.
[49] Ali, M. F., & Shah, M. A. (2018, September). Adaptive Transmission Power-Geographical and Energy Aware Routing Algorithm for Wireless Sensor Networks. In: *Proceedings of the 2018 24th International Conference on Automation and Computing (ICAC)* (pp. 1-5). IEEE.
[50] Hadi, K. (2017). Analyses of Energy-Aware Geographic Routing Protocols for Wireless Sensor Networks. *Lecture Notes on Information Theory, 5*(1), 44-48.
[51] Chen, B., Jamieson, K., Balakrishnan, H., & Morris, R. (2002). Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks. *Wireless networks, 8*(5), 481-494.
[52] Shabbir, N. and Hassan, S.R. (2017). Routing Protocols for Wireless Sensor Networks (WSNs). In Wireless Sensor Networks - Insights and Innovations. Intech. https://www.intechopen.com/chapters/56541
[53] Gaur, A., and Verma, R. (2020). SPIN protocol in WSN. *International Journal of Engineering Research & Technology (IJERT), 9*(5), 1305-1308.
[54] Shabbir, N., Nawaz, R., Iqbal, M. N., & Zafar, J. (2015, December). Routing protocols for small scale WLAN based Wireless Sensor Networks (WSNs). In: *Proceedings of the 2015 9th International Conference on Sensing Technology (ICST),* (pp. 412-415). IEEE.
[55] Al-Karaki, J. N., & Kamal, A. E. (2004). Routing techniques in wireless sensor networks: a survey. *IEEE Wireless Communications*, *11*(6), 6-28.
[56] Johnson, D. B., & Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. In *Mobile Computing* (pp. 153-181). Springer, Boston, MA.
[57] El-Semary, A. M., & Diab, H. (2019). BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map. *IEEE Access*, *7*, 95197-95211.
[58] Chen, Z., Zhou, W., Wu, S., & Cheng, L. (2020). An adaptive on-demand multipath routing protocol with QoS support for high-speed MANET. *IEEE Access*, *8*, 44760-44773.
[59] Biradar, R.V., Patil, V.C., et al. (2010). Classification and comparison of routing protocols in WSNs. *Special Issue on Ubiquitous Computing Security Systems*, *4*, 704-711.

[60] Sharma, N., & Patterson, P. G. (1999). The impact of communication effectiveness and service quality on relationship commitment in consumer, professional services. *Journal of Services Marketing, 13*(2), 151-170.
[61] Hashish, S., & Tawalbeh, H. (2017). Quality of service requirements and challenges in generic WSN infrastructures. *Procedia Computer Science*, *109*, 1116-1121.
[63] Xu, B., Da Xu, L., Cai, H., Xie, C., Hu, J., & Bu, F. (2014). Ubiquitous data accessing method in IoT-based information system for emergency medical services. *IEEE Transactions on Industrial Informatics*, *10*(2), 1578-1586.
[64] Rault, T., Bouabdallah, A., and Challal, Y. (2014): Energy efficiency in WSNs: a top-down survey. *Computer Networks, Elsevier*, *67*(4), pp. 104-122.
[65] Cui, S., Goldsmith, A. J., & Bahai, A. (2005). Energy-constrained modulation optimization. *IEEE Transactions on Wireless Communications*, *4*(5), 2349-2360.
[66] Costa, F. M., & Ochiai, H. (2010, December). A comparison of modulations for energy optimization in wireless sensor network links. In: *Proceedings of the 2010 IEEE Global Telecommunications Conference GLOBECOM 2010* (pp. 1-5). IEEE.
[67] Fasolo, E., Rossi, M., Widmer, J., & Zorzi, M. (2007). In-network aggregation techniques for wireless sensor networks: a survey. *IEEE Wireless Communications*, *14*(2), 70-87.
[68] Hsu, J., Zahedi, S., Kansal, A., Srivastava, M., & Raghunathan, V. (2006, October). Adaptive duty cycling for energy harvesting systems. In: *Proceedings of the 2006 International Symposium on Low Power Electronics and Design* (pp. 180-185).
[69] Abbasi, A. A., & Younis, M. (2007). A survey on clustering algorithms for wireless sensor networks. *Computer Communications*, *30*(14-15), 2826-2841.
[70] Sudevalayam, S., & Kulkarni, P. (2010). Energy harvesting sensor nodes: Survey and implications. *IEEE Communications Surveys & Tutorials*, *13*(3), 443-461.
[71] Huh, S., Cho, S., & Kim, S. (2017, February). Managing IoT devices using blockchain platform. In: *Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT)* (pp. 464-467). IEEE.
[72] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395-411.
[73] Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431-440.
[74] Mohammadi, M., Al-Fuqaha, A., Sorour, S., & Guizani, M. (2018). Deep learning for IoT big data and streaming analytics: A survey. *IEEE Communications Surveys & Tutorials*, *20*(4), 2923-2960.
[75] Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal*, *5*(2), 1184-1195.
[76] Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2019). A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express*, *5*(1), 1-7.
[77] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*, 173-190.
[78] Xu, G., Shen, W., & Wang, X. (2014). Applications of wireless sensor networks in marine environment monitoring: A survey. *Sensors*, *14*(9), 16932-16954.
[80] Casado-Vara, R., Novais, P., Gil, A. B., Prieto, J., & Corchado, J. M. (2019). Distributed continuous-time fault estimation control for multiple devices in IoT networks. *IEEE Access*, *7*, 11972-11984.
[81] Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I. A. T., Siddiqa, A., & Yaqoob, I. (2017). Big IoT data analytics: architecture, opportunities, and open research challenges. *IEEE Access*, *5*, 5247-5261.
[82] Ahmed, A. A., & AL-Shaboti, M. M. (2017). Implementation of Internet of Things (IoT) Based on IPv6 over Wireless Sensor Networks. *International Journal of Sensors Wireless Communications and Control*, *7*(2), 129-137.
[83] Kim, T. H., Ramos, C., & Mohammed, S. (2017). Smart city and IoT. *Future Generation Computer Systems, 76,* 159-162.

[84] Poslad, S., Ma, A., Wang, Z., & Mei, H. (2015). Using a smart city IoT to incentivise and target shifts in mobility behaviourIs it a piece of pie? *Sensors*, *15*(6), 13069-13096.
[86] Kyriazis, D., Varvarigou, T., White, D., Rossi, A., & Cooper, J. (2013, June). Sustainable smart city IoT applications: Heat and electricity management & Eco-conscious cruise control for public transportation. In: *Proceedings of the 2013 IEEE 14th International Symposium on" A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)* (pp. 1-5). IEEE.
[87] Giang, N. K., Lea, R., Blackstock, M., & Leung, V. C. (2016, December). On building smart city IoT applications: a coordination-based perspective. In: *Proceedings of the 2nd International Workshop on Smart Cities 2016* (pp. 1-6). ACM.
[88] Gaur, A., Scotney, B., Parr, G., & McClean, S. (2015). Smart city architecture and its applications based on IoT. *Procedia Computer Science*, *52*, 1089-1094.
[89] NIST IEEE-P1451 Draft Standard Home Page; http://ieee1451.nist.gov/
[90] Herwig, S., Harvey, K., Hughey, G., Roberts, R., & Levin, D. (2019, January). Measurement and analysis of Hajime, a peer-to-peer IoT botnet. In: *Proceedings of the 2019 Network and Distributed Systems Security (NDSS) Symposium*.
[91] Chen, J. (2017, January). Flowchain: A distributed ledger designed for peer-to-peer iot networks and real-time data transactions. In: *Proceedings of the 2nd International Workshop on Linked Data and Distributed Ledgers (LDDL2)*.
[93] Al-Azez, Z.T., Lawey, A.Q., El-Gorashi, T.E., & Elmirghani, J.M. (2019). Energy efficient IoT virtualization framework with peer to peer networking and processing. *IEEE Access*, *7*, 50697-50709.
[94] H. Hsieh, H. and Lai, C. (2011). Internet of Things Architecture Based on Integrated PLC and 3G Communication Networks. In: *Proceedings of the 2011 IEEE 17th International Conference on Parallel and Distributed Systems*, pp.853-856, doi: 10.1109/ICPADS.2011.73
[95] Conoscenti, M., Vetro, A., & De Martin, J.C. (2017, May). Peer to peer for privacy and decentralization on the internet of things. In: *Proceedings of the 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C)*, (pp. 288-290). IEEE.
[96] Ali, M.S., Dolui, K., & Antonelli, F. (2017, October). IoT data privacy via blockchains and IPFS. In: *Proceedings of the Seventh International Conference on the Internet of Things* (pp. 1-7).
[97] Chen, J. (2018). Devify: Decentralized internet of things software framework for a peer-to-peer and interoperable IoT device. *ACM SIGBED Review*, *15*(2), 31-36.
[98] Farahzadi, A., Shams, P., Rezazadeh, J., & Farahbakhsh, R. (2018). Middleware technologies for cloud of things: a survey. *Digital Communications and Networks*, *4*(3), 176-188.
[99] Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2018, March). Overview of cellular LPWAN technologies for IoT deployment: Sigfox, LoRaWAN, and NB-IoT. In: *Proceedings of the 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)* (pp. 197-202). IEEE.
[100] Triantafyllou, A., Sarigiannidis, P., & Lagkas, T. D. (2018). Network protocols, schemes, and mechanisms for internet of things (IoT): Features, open challenges, and trends. *Wireless communications and mobile computing*, 2018.
[101] Pongle, P., & Chavan, G. (2015, January). A survey: Attacks on RPL and 6LoWPAN in IoT. In: *Proceedings of the 2015 International conference on Pervasive Computing (ICPC)* (pp. 1-6). IEEE.
[102] Rizzi, M., Ferrari, P., Flammini, A., & Sisinni, E. (2017). Evaluation of the IoT LoRaWAN solution for distributed measurement applications. *IEEE Transactions on Instrumentation and Measurement*, *66*(12), 3340-3349.
[103] Molisch, A.F., Balakrishnan, K., Chong, C.C., Emami, S., Fort, A., Karedal, J., et al. (2004). IEEE 802.15. 4a channel model-final report. IEEE P802, 15(04), 0662.
[104] Desai, P., Sheth, A., & Anantharam, P. (2015, June). Semantic gateway as a service architecture for iot interoperability. In: *Proceedings of the 2015 IEEE International Conference on Mobile Services* (pp. 313-319). IEEE.

[105] Dunkels, A. (2007). Programming memory-constrained networked embedded systems (Doctoral dissertation, Institutionen för datavetenskap och elektronik). Available at: http://mdh.diva-portal.org/smash/record.jsf?pid=diva2%3A120604&dswid=-8474
[106] Dameri, R.P. (2013). Searching for smart city definition: a comprehensive proposal. *International Journal of computers & technology*, *11*(5), 2544-2551.
[107] Ramaprasad, A., Sánchez-Ortiz, A., & Syn, T. (2017). A unified definition of a smart city. In: *Proceedings of the 2017 International Conference on Electronic Government* (pp. 13-24). Springer, Cham.
[108] europa.eu, (2019) Final Report Summary - FIRESENSE (Fire Detection and Management through a Multi-Sensor Network for the Protection of Cultural Heritage Areas from the Risk of Fire and Extreme Weather Conditions) https://cordis.europa.eu/project/id/244088/reporting
[109] Al-Falahy, N., & Alani, O. Y. (2017). Technologies for 5G networks: Challenges and opportunities. *IT Professional*, *19*(1), 12-20.
[110] Hu, F. (Ed.). (2016). *Opportunities in 5G networks: A research and development perspective*. CRC press.
[111] Wu, Q., Li, G. Y., Chen, W., Ng, D. W. K., & Schober, R. (2017). An overview of sustainable green 5G networks. *IEEE Wireless Communications*, *24*(4), 72-80.
[112] Cai, Y., Qin, Z., Cui, F., Li, G. Y., & McCann, J. A. (2017). Modulation and multiple access for 5G networks. *IEEE Communications Surveys & Tutorials*, *20*(1), 629-646.
[113] Kekki, S., Featherstone, W., Fang, Y., Kuure, P., Li, A., Ranjan, A., ... & Scarpina, S. (2018). MEC in 5G networks. *ETSI White Paper*, *28*, 1-28.
[114] Buzzi, S., Chih-Lin, I., Klein, T. E., Poor, H. V., Yang, C., & Zappone, A. (2016). A survey of energy-efficient techniques for 5G networks and challenges ahead. *IEEE Journal on Selected Areas in Communications*, *34*(4), 697-709.
[115] T. Barnett, S. Jain, U. Andra, and T. Khurana, (2018). Cisco VNI Global Complete Forecast Update, no. December, pp. 2017–2022.
[116] Ruffini, M. (2016). Multidimensional convergence in future 5G networks. *Journal of Lightwave Technology*, *35*(3), 535-549.
[117] Carugi, M. (2018). Key features and requirements of 5G/IMT-2020 networks, ITU Arab Forum on Emerging Technologies, Algiers – Algeria, 14-15 Feb.2018.
[118] Report ITU-R M.2410-0 (11/2017). "Minimum requirements related to technical performance for IMT-2020 radio interface(s)" (PDF)" ITU. November 2017, Retrieved 28 August 2019.
[119] Zhang, S., Wu, Q., Xu, S., & Li, G. Y. (2016). Fundamental green tradeoffs: Progresses, challenges, and impacts on 5G networks. *IEEE Communications Surveys & Tutorials*, *19*(1), 33-56.
[120] Le, N. T., Hossain, M. A., Islam, A., Kim, D. Y., Choi, Y. J., & Jang, Y. M. (2016). Survey of promising technologies for 5G networks. *Mobile information systems*, *2016*.
[121] Qualcomm, "Designing 5G NR", The 3GPP Release 15 global standard for a unified, more capable 5G air interface, @qualcomm_tech, September 2018
[122] Next Generation Mobile Networks Alliance 5G Initiative, "5G White Paper," A Delivery by NGMN Alliance, p. 124, 2015.
[123] Ding, Z., Liu, Y., Choi, J., Sun, Q., Elkashlan, M., Chih-Lin, I., & Poor, H. V. (2017). Application of non-orthogonal multiple access in LTE and 5G networks. *IEEE Communications Magazine*, *55*(2), 185-191.
[124] Javaid, N., Sher, A., Nasir, H., & Guizani, N. (2018). Intelligence in IoT-based 5G networks: Opportunities and challenges. *IEEE Communications Magazine*, *56*(10), 94-100.
[125] Y. Lin, L. Shao, Z. Zhu, Q. Wang, and R. K. Sabhikhi, (2010). Wireless network cloud: Architecture and system requirements. IBM J. Res. Dev., vol. 54, no. 1.
[126] W. Paper, "Cloud RAN Architecture for 5G Cloud RAN Architecture for 5G A Telefónica White Paper Prepared in collaboration with Ericsson WHITE PAPER Cloud RAN Architecture for 5G," pp. 1–24.

[127] Liu, Y., Shi, X., He, S., & Shi, Z. (2017). Prospective positioning architecture and technologies in 5G networks. *IEEE Network*, *31*(6), 115-121.
[128] Ordonez-Lucena, J., Ameigeiras, P., Lopez, D., Ramos-Munoz, J. J., Lorca, J., & Folgueira, J. (2017). Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges. *IEEE Communications Magazine, 55*(5), 80-87.
[129] Hakiri, A., & Berthou, P. (2015). Leveraging SDN for the 5G networks: Trends, prospects and challenges. *arXiv preprint arXiv:1506.02876*.
[130] Harutyunyan, D., & Riggio, R. (2018). Flex5G: Flexible functional split in 5G networks. *IEEE Transactions on Network and Service Management*, *15*(3), 961-975.
[131] Arfaoui, G., Bisson, P., Blom, R., Borgaonkar, R., Englund, H., Félix, E. & Zahariev, A. (2018). A security architecture for 5G networks. *IEEE Access*, *6*, 22466-22479.
[132] P. Popovski, K. F. Trillingsgaard, O. Simeone, and G. Durisi, (2018). 5G wireless network slicing for eMBB, URLLC, and mMTC: A communication-theoretic view. *IEEE Access*, *6*, 55765–55779.
[133] Li, Z., Uusitalo, M. A., Shariatmadari, H., & Singh, B. (2018). 5G URLLC: Design challenges and system concepts. In 2018 15th International Symposium on Wireless Communication Systems (ISWCS) (pp. 1-6). IEEE.
[134] Chen, Y., Liu, W., Niu, Z., Feng, Z., Hu, Q., & Jiang, T. (2020). Pervasive intelligent endogenous 6G wireless systems: Prospects, theories and key technologies. *Digital Communications and Networks, 6*(3), 312-320.
[135] Yousaf, F. Z., Bredel, M., Schaller, S., & Schneider, F. (2017). NFV and SDN—Key technology enablers for 5G networks. *IEEE Journal on Selected Areas in Communications*, *35*(11), 2468-2478.
[136] Wang, D., Chen, D., Song, B., Guizani, N., Yu, X., & Du, X. (2018). From IoT to 5G I-IoT: The next generation IoT-based intelligent algorithms and 5G technologies. *IEEE Communications Magazine, 56*(10), 114-120.
[137] Karjalainen, J., Nekovee, M., Benn, H., Kim, W., Park, J., & Sungsoo, H. (2014, June). Challenges and opportunities of mm-wave communication in 5G networks. In *2014 9th international conference on cognitive radio oriented wireless networks and communications (CROWNCOM)* (pp. 372-376). IEEE.
[138] Giust, F., Cominardi, L., & Bernardos, C. J. (2015). Distributed mobility management for future 5G networks: overview and analysis of existing approaches. *IEEE Communications Magazine*, *53*(1), 142-149.
[139] Guerzoni, R., Trivisonno, R., & Soldani, D. (2014, November). SDN-based architecture and procedures for 5G networks. In *1st International Conference on 5G for Ubiquitous Connectivity* (pp. 209-214). IEEE.
[140] Prasad, K. S. V., Hossain, E., & Bhargava, V. K. (2017). Energy efficiency in massive MIMO-based 5G networks: Opportunities and challenges. *IEEE Wireless Communications*, *24*(3), 86-94.
[141] Rinaldi, S., Peerenboom, J., Kelly, T. (2001) Identifying, Understanding and analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, *21*(6), 11–25.
[142] Adar E. and Wuchner A., (2005). Risk management for critical infrastructure protection challenges: Best practices and tools", in Proc. of the First IEEE International Workshop on Critical Infrastructure Protection.
[143] Lukas L., Hromada, M., (2011). "Resilience as main part of protection of critical infrastructure", *International Journal of Mathematical Models and Methods in Applied Sciences, 5*(6), 1135-1142.
[144] Elky S., (2006). An Introduction to Information System Risk Management. SANS Institute InfoSec Reading Room, May 31, 2006.
[145] Emergency Management Australia, "Critical Infrastructure Emergency Risk Management and Assurance Handbook", Mount Macedon, Australia, 2003.
[146] International Standard ISO/IEC 27005 (2008). Information technology - Security techniques - Information security risk management. First edition 2008-06-15.

[147] Jose M. Yusta, Gabriel J. Correa, Roberto Lacal-Arántegui. (2011). Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy Policy*, *39*(10), 6100-6119.
[148] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection – Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM(2009)149 final, Brussels, 2009.
[149] Arnason, S. T., & Willett, K. D. (2007). How to achieve 27001 certifications: An example of applied compliance management. CRC Press.
[150] Sokovic, M., Pavletic, D., & Pipan, K. K. (2010). Quality improvement methodologies–PDCA cycle, RADAR matrix, DMAIC and DFSS. *Journal of achievements in materials and manufacturing engineering, 43*(1), 476-483.
[151] Niedermeier, M., He, X., De Meer, H., Buschmann, C., Hartmann, K., Langmann, B., ... & Pfisterer, D. (2015). Critical Infrastructure Surveillance Using Secure Wireless Sensor Networks. *Journal of sensor and actuator networks*, *4*(4), 336-370.
[152] Verdone, R., Dardari, D., Mazzini, G., & Conti, A. (2010). *Wireless sensor and actuator networks: technologies, analysis and design*. Academic Press.
[153] Gomez, L., & Ulmer, C. (2010, July). Secure sensor networks for critical infrastructure protection. In: *2010 Fourth International Conference on Sensor Technologies and Applications* (pp. 144-150). IEEE.
[154] Rehak D., and Hromada. M. (2017). Failures in a Critical Infrastructure System, System of System Failures, Takafumi Nakamura, IntechOpen, DOI: 10.5772/intechopen.70446.
[155] Jonkeren, O., & Giannopoulos, G. (2014). Analysing critical infrastructure failure with a resilience inoperability input–output model. *Economic Systems Research, 26*(1), 39-59.
[156] Little, R. (2002). Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructures. *Journal of Urban Technology*, 109-123.
[157] O'Reilly, G., Jrad, A., Nagarajan, R., Brown, T., and Conrad, S. (2006). Critical Infrastructure Analysis of Telecom for Natural Disasters. In: 12th International Telecommunications Network Strategy and Planning Symposium, 2006, pp. 1-6
[158] Oh, E. H., Deshmukh, A., & Hastak, M. (2010). Disaster impact analysis based on inter-relationship of critical infrastructure and associated industries. *International Journal of Disaster Resilience in the Built Environment, 1*(1), 25-49.
[159] Lukas L., Hromada, M., (2011). Resilience as main part of protection of critical infrastructure. *Internatio,nal Journal of Mathematical Models and Methods in Applied Sciences, 5*(6), 1135-1142.
[160] Little, R.G. (2003). Toward more robust infrastructure: observations on improving the resilience and reliability of critical systems. International Conference on System Sciences (HICSS-2003), IEEE Computer Society, pp. 58-66
[161] Cookea, D. L., and Rohledera, T. R. (2006). Learning from incidents: from normal accidents to high reliability. *Journal of the System Dynamics Society, System Dynamics Review, 22*(3), 213–239.
[162] National Infrastructure Advisory Council (US) (2009). Critical infrastructure resilience: Final report and recommendations. National Infrastructure Advisory Council.
[163] Theoharidou, M., Kotzanikolaou, P., and Gritzalis, D. (2009). Risk-based criticality analysis. In Palmer C., Shenoi S. (Eds.), in Proc. of the third IFIP international conference on critical infrastructure protection (CIP-2009), USA. Springer.
[164] Flammini, F., Gaglione, A., Mazzocca, N., and Pragliola, C. (2009). Quantitative Security Risk Assessment and Management for Railway Transportation Infrastructures. in Critical Information Infrastructure Security, Series: Lecture Notes in Computer, Science, Setola R., Geretshuber S. (Eds.),Vol.5508, pp. 180-189, Springer Berlin / Heidelberg.

[165] Center for Security Studies (2014). Training for the protection of vital infrastructure. European Union, Internal Security Fund "Equality, Solidarity, Protection", p. 30
[166] Police Officer Athanasios Kokkalakis (2008). European Critical Infrastructure Protection Program. Department of Information Analysis and Threat Assessment Crisis Management Directorate, Greek police headquarters. Posted on 18 Nov 2008 at Security Manager magazine.
[167] Katsikas, S., Gritzalis, D., Gritzalis S. (2004). Information Systems Security. Athens: New Technologies, Papasotiriou Publications.
[168] Wenger, A., Mauer, V., Dunn Cavelty M. (2008). An inventory of 25 National and 7 International Critical Infrastructure Protection Policies. Center of Security Studies, ETH Zurich.
[169] Pangalou, G., Mavridi, I. (2002). Security of Information Systems and Networks. Thessaloniki: Anikoula Publications.
[170] Bailey, D., & Wright, E. (2003). Practical SCADA for industry. Elsevier.
[171] Rivelo, M. (2021). CYBER EDU, what is SCADA Security SCADA Network Security Defined and Explored, https://www.forcepoint.com/cyber-edu/scada-security [Accessed June 2021].
[172] Arora, A., Dutta, P., Bapat, S., Kulathumani, V., Zhang, H., Naik, V., et al. (2004). A line in the sand: A wireless sensor network for target detection, classification, and tracking. *Computer Networks, 46*(5), 605-634.
[173] Composition Consortium, (2017). Viability of WSN as ICT overlay for physical security detection. Date: 2017-05-22. Version 1.0
[174] Boulos, M. N. K. & Berry, G. (2012). Real-time locating systems (RTLS) in healthcare: a condensed primer. *International journal of health geographics, 11*, 25.
[175] Jisha, R. C., Ramesh, M. V., & Lekshmi, G. S. (2010, December). Intruder tracking using wireless sensor network. In 2010 IEEE International Conference on Computational Intelligence and Computing Research (pp. 1-5). IEEE.
[176] Arvanitakis, I. (December 2018). Passive Infrared Sensors. [online] Ioarvanit.gr. Available at: https://ioarvanit.gr/archives/3058 [Accessed 26 June 2021].
[177] Matthews, V. O., Noma-Osaghae, E., & Uzairue, S. I. (2018). An Analytics enabled wireless anti-intruder monitoring and alarm system. *International Journal of Scientific Research in Science, Engineering and Technology, 4*(9), 5-11.
[178] Kanellos, L., (2020). Cloud & Security. [online] digittallife. Available at: https://www.digitallife.gr/cloud-asfaleia-30780 [Accessed 20 June 2021].
[179] Z TEAM. (2019, December 18). Access Control Systems . Zarifopoulos S.A. https://zarifopoulos.com/access-control-systems/. [Accessed 26 June 2021]
[180] S. E. H. Jensen and R. H. Jacobsen, (2013). Access Control with RFID on the Internet of Things. 27th International Conference on Advanced Information Networking and Applications Workshops, 2013, pp. 554-559, doi: 10.1109/WAINA.2013.199.
[181] Rida, A., Yang, L., Vyas, R., & Tentzeris, M. M. (2009). Conductive inkjet-printed antennas on flexible low-cost paper-based substrates for RFID and WSN applications. *IEEE Antennas and Propagation Magazine, 51*(3), 13-23.
[182] Verman, Romesh (2005). Distance Education in Technological Age, Anmol Publications Pvt. Ltd., 2005, pp.166, ISBN 81-261-2210-2, ISBN 978-81-261-2210
[183] Nash J. (January 2020). "Global sales of video surveillance equipment projected to surpass $20 billion this year". Biometric Update. Retrieved 26 October 2020.
[184] Gren, M. (September 2017). ONVIF: A guide to the open security platform - IFSEC GLOBAL: Security and fire news and resources. IFSEC Global | Security and Fire News and Resources. https://www.ifsecglobal.com/onvif/
[185] Cho, J. R., Kim, H. S., Chae, D. K., & Lim, S. J. (2017). Smart CCTV security service in IoT environment. Journal of digital contents society, 18(6), 1135-1142.
[186] Zafeiriou, S., Zhang, C., & Zhang, Z. (2015). A survey on face detection in the wild: past, present and future. Computer Vision and Image Understanding, 138, 1-24.
[187] Tsakanikas, V., & Dagiuklas, T. (2018). Video surveillance systems-current status and future trends. Computers & Electrical Engineering, 70, 736-753.

[188] Hossain, M., Mehedi, H.M., Al Qurishi, M., Alghamdi, A. (2012). Resource allocation for service composition in cloud-based video surveillance platform. IEEE international conference on multimedia and expo workshops Melbourne, Australia. 2012
[189] Rodriguez-Silva, D, A, Adkinson-Orellana, L., et al. (2012). Video surveillance based on cloud Storage. IEEE fifth international conference on cloud computing Honolulu, HI, USA.
[190] Kleihorst, R., Schueler, B., Danilin, A., & Heijligers, M. (2006, October). Smart camera mote with high performance vision system. In ACM SenSys 2006 Workshop on Distributed Smart Cameras (DSC 2006) (pp. 22-23).
[191] Hu, J. (2020, July). 5G security cameras set to change the way you secure your property - REOLINK Blog. Reolink. https://reolink.com/5g-security-cameras-buying-guide/
[192] Chowdhury, M. Z., Hossan, M. T., Shahjalal, M., Hasan, M. K., & Jang, Y. M. (2020). A new 5g ehealth architecture based on optical camera communication: An overview, prospects, and applications. IEEE Consumer Electronics Magazine, 9(6), 23-33.
[193] Robinson, D., (2006, Feb.). Predicting Earthquakes. Predicting earthquakes. http://www.geography-site.co.uk/pages/physical/earth/pred.html
[194] Kong, Q., Allen, R. M., Schreier, L., & Kwon, Y. W. (2016). MyShake: A smartphone seismic network for earthquake early warning and beyond. Science advances, 2(2), e1501055.
[195] Cochran, E. S., Lawrence, J. F., Christensen, C., & Jakka, R. S. (2009). The quake-catcher network: Citizen science expanding seismic horizons. Seismological Research Letters, 80(1), 26-30.
[196] Neander, J., Nolin, M., Björkman, M., (2007). Wireless vibration monitoring (Wivib)—an industrial case study. In: Proceedings of 12th IEEE Conference on Emerging Technologies and Factory Automation, IEEE, Patras, Greece, 2007.
[197] Vogl, A., Wang, D. T., Storås, P., Bakke, T., Taklo, M. M., Thomson, A., & Balgård, L. (2009). Design, process and characterisation of a high-performance vibration sensor for wireless condition monitoring. Sensors and actuators a: physical, 153(2), 155-161.
[198] Pasi, A. A., & Bhave, U. (2015). Flood detection system using wireless sensor network. International Journal of Advanced Research in Computer Science and Software Engineering, 5(2), 108-113.
[199] Teixidó, P., Gómez-Galán, J. A., Gómez-Bravo, F., Sánchez-Rodríguez, T., Alcina, J., & Aponte, J. (2018). Low-power low-cost wireless flood sensor for smart home systems. Sensors, 18(11), 3817.
[200] Deve, K. B., Hancke, G. P., & Silva, B. J. (2016, October). Design of a smart fire detection system. In IECON 2016-42nd Annual Conference of the IEEE Industrial Electronics Society (pp. 6205-6210).
[201] Kapatos, G. (2020). New trends in fire detection systems. Electrologos magazine, 47, 44-47.
[202] Aslan, Y. E., Korpeoglu, I., & Ulusoy, Ö. (2012). A framework for use of wireless sensor networks in forest fire detection and monitoring. Computers. Environment and Urban Systems, 36(6), 614-625.
[203] Hartung, C., Han, R. (2006). FireWxNet: A multi-tiered portable wireless system for monitoring weather conditions in wildland fire environments. In: Proc. of 4th international conference on mobile systems, applications and services (pp. 28–41).
[204] Space Hellas. (2017). Security systems management platform. https://www.space.gr/el/digital-integration/security-systems-management-platform [Accessed 16 July 2021]
[205] Zarifopoulos, T. (2018, March 26). Integrating Security Systems https://zarifopoulos.com/upgrade-and-integration-of-security-systems/ [Accessed 16 July 2021]
[206] Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. Future Generation Computer Systems, 78, 964-975.
[207] Vouros, I. A. (2015). WSN Security for territory watching and guarding applications. Technology, Department of Electrical and Computer Engineering, National Metsoveian University, Athens.

[208] Luong, N. C., Hoang, D. T., Wang, P., Niyato, D., & Han, Z. (2017). Applications of economic and pricing models for wireless network security: A survey. IEEE Communications Surveys & Tutorials, 19(4), 2735-2767.
[209] Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. Proceedings of the IEEE, 104(9), 1727-1765.
[210] He, D., Li, X., Chan, S., Gao, J., & Guizani, M. (2019). Security analysis of a space-based wireless network. IEEE Network, 33(1), 36-43.
[211] Ünsal, E., & Çebi, Y. (2013). Denial of service attacks in WSN. In International Symposium on Computing in Science & Engineering. Proceedings (p. 24). GEDIZ University, Engineering and Architecture Faculty.
[212] Mainanwal, V., Gupta, M., & Upadhayay, S. K. (2015, March). A survey on wireless body area network: Security technology and its design methodology issue. In 2015 International conference on innovations in information, embedded and communication systems (ICIIECS) (pp. 1-5). IEEE.
[213] Kaushal, K., & Kaur, T. (2015). A Survey on Attacks of WSN and their Security Mechanisms. International Journal of Computer Applications, 118(18).
[214] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Ad hoc networks, 1(2-3), 293-315.
[215] Sadeghi, M., Khosravi, F., Atefi, K., & Barati, M. (2012). Security analysis of routing protocols in wireless sensor networks. International Journal of Computer science Issues (IJCSI), 9(1), 465-472.
[216] Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: Security protocols for sensor networks. Wireless networks, 8(5), 521-534.
[217] Wood, A. D., Fang, L., Stankovic, J. A., & He, T. (2006, October). SIGF: a family of configurable, secure routing protocols for wireless sensor networks. In Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks (pp. 35-48).
[218] Han, R., Mishra, S., & Deng, J. (2002). INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks; CU-CS-939-02.
[219] El Kaissi, R. Z., Kayssi, A., Chehab, A., & Dawy, Z. (2005). DAWWSEN: A defense mechanism against wormhole attacks in wireless sensor networks (Doctoral dissertation, American University of Beirut, Department of Electrical and Computer Engineering).
[220] Parno, B., Luk, M., Gaustad, E., & Perrig, A. (2006, December). Secure sensor network routing: A clean-slate approach. In: Proceedings of the 2006 ACM CoNEXT conference (pp. 1-13).
[221] Karlof, C., Sastry, N., & Wagner, D. (2004, November). TinySec: a link layer security architecture for wireless sensor networks. In: Proceedings of the 2nd international conference on Embedded networked sensor systems (pp. 162-175).
[222] Luk, M., Mezzour, G., Perrig, A., & Gligor, V. (2007, April). MiniSec: a secure sensor network communication architecture. In: 2007 6th International Symposium on Information Processing in Sensor Networks (pp. 479-488). IEEE.
[223] Stallings, W., Brown, L., Bauer, M. D., & Bhattacharjee, A. K. (2012). Computer security: principles and practice. Upper Saddle River, NJ, USA: Pearson Education.
[224] Kuorilehto, M., Kohvakka, M., Suhonen, J., Hämäläinen, P., Hännikäinen, M., & Hamalainen, T. D. (2008). Ultra-low energy wireless sensor networks in practice: Theory, realization and deployment. John Wiley & Sons.
[225] Sable, A. (2014). Comparative Study on IEEE Standard of WPAN 802.15. 1/3/4. International Journal for research in emerging science and technology, 1(1), 25-28.
[226] Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? IEEE Signal Processing Magazine, 35(5), 41-49.
[227] Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. Computer networks, 148, 283-294.

[228] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access, 7, 82721-82743.
[229] Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015, December). Internet of things (IoT) security: Current status, challenges and prospective measures. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 336-341). IEEE.
[230] Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. IEEE Communications Surveys & Tutorials, 21(3), 2702-2733.
[231] Hwang, Y. H. (2015, April). Iot security & privacy: threats and challenges. In: Proceedings of the 1st ACM workshop on IoT privacy, trust, and security (pp. 1-1).
[232] Román-Castro, R., López, J., & Gritzalis, S. (2018). Evolution and trends in IoT security. Computer, 51(7), 16-25.
[233] Minoli, D., & Occhiogrosso, B. (2018). Blockchain mechanisms for IoT security. Internet of Things, 1, 1-13.
[234] Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. IEEE Communications Surveys & Tutorials, 22(3), 1646-1685.
[235] Alladi, T., Chamola, V., Sikdar, B., & Choo, K. K. R. (2020). Consumer IoT: Security vulnerability case studies and solutions. IEEE Consumer Electronics Magazine, 9(2), 17-25.
[236] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395-411.
[237] Li, Xiaomin, et al. (2017), "A review of industrial wireless networks in the context of industry 4.0." Wireless networks 23.1: 23-41.
[238] Salah, Albert Ali, (2011), "Multimodal monitoring of cultural heritage sites and the FIRESENSE project." Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies.
[239] Kucuk, Gurhan, (2008), "FireSense: Forest Fire Prediction and Detection System using Wireless Sensor Networks." the 4th IEEE/ACM International Conference on Distributed Computing in Sensor Systems (DCOSS'08).
[240] Aljehani, Maher, and Masahiro Inoue, (2019), "Performance evaluation of multi-UAV system in post-disaster application: Validated by HITL simulator." IEEE Access 7 64386-64400.
[241] P. Razi, J. T. S. Sumantyo, D. Perissin, H. Kuze, M. Y. Chua and G. F. Panggabean, (2018), "3D land mapping and land deformation monitoring using persistent scatterer interferometry (PSI) ALOS PALSAR: Validated by geodetic GPS and UAV", IEEE Access, vol. 6, pp. 12395-12404.
[242] Christodoulakis, D. (2019). “Study of Wireless Sensor Networks, integration and interaction with new technologies”, Aegean University.
[243] Michał Okulski, Maciej Ławryńczuk, (2021), "A Novel Neural Network Model Applied to Modeling of a Tandem-Wing Quadplane Drone", Access IEEE, vol. 9, pp. 14159-14178.