ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών
Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών

Ειδίκευση Δικτύων Επικοινωνιών και Κατανεμημένων Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ασφάλεια στο φυσικό επίπεδο για συστήματα διαδικτύου των αντικειμένων

Μουζέλης Νεκτάριος

A.M. mcse19018

Εισηγητής: Αντώνιος Μπόγρης, Καθηγητής

Διπλωματική Εργασία

Ασφάλεια στο φυσικό επίπεδο για συστήματα διαδικτύου των αντικειμένων

Μουζέλης Νεκτάριος

A.M. mcse19018

Εισηγητής:

Αντώνιος Μπόγρης, Καθηγητής

Antonios Bogris
Digitally signed by Antonios Bogris
Date: 2024.09.05 13:25:46 +03'00'

Εξεταστική Επιτροπή:

Αναπλ. καθηγητής Μυριδάκης Νικόλαος

Nikolaos Myridakis
Digitally signed by Nikolaos Myridakis
Date: 2024.09.05 14:46:52 +03'00'

Αναπλ. καθηγήτρια Καντζάβελου Ιωάννα

IOANNA KANTZAVELOU
Digitally signed by IOANNA KANTZAVELOU
Date: 2024.09.05 12:42:24 +02'00'

Ημερομηνία εξέτασης: 04-09-2024

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο/η κάτωθι υπογεγραμμένος Νεκτάριος Μουζέλης του Γεωργίου, με αριθμό μητρώου mcse19018 φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών «Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών» του Τμήματος «Μηχανικών Πληροφορικής και Υπολογιστών» της Σχολής «Μηχανικών» του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Είμαι συγγραφέας αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα 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, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Επιθυμώ την απαγόρευση πρόσβασης στο πλήρες κείμενο της εργασίας μου μέχρι …… και έπειτα από αίτηση μου στη Βιβλιοθήκη και έγκριση του επιβλέποντα καθηγητή.

Ο Δηλών

Μουζέλης Νεκτάριος

ΕΥΧΑΡΙΣΤΙΕΣ

Με το τέλος του παρόντος πονήματος , θα ήθελα να εκφράσω τις ειλικρινείς μου ευχαριστίες στον επιβλέποντα καθηγητή μου κ. Αντώνιο Μπόγρη για την απρόσκοπτη και καθοριστική συμβολή του στην επιλογή του θέματος και στην συγγραφή της παρούσης διπλωματικής εργασίας. Η υπομονή και η κατανόηση του ήταν ζωτικής σημασίας για να μπορέσω να ολοκληρώσω την παρούσα εργασία.

Τέλος ευχαριστώ, την σύζυγο μου και τα έξι παιδιά μου για την στήριξη και συμπαράσταση τους.

ΠΕΡΙΛΗΨΗ

Η μαζική ανάπτυξη του Internet of Things, καθιστά την ασφάλεια των πληροφοριών άνευ προηγουμένου σημαντική. Οι τεχνικές ασφάλειας δικτύου είναι ζωτικής σημασίας όχι μόνο για τη διατήρηση της καλής και αποδοτικής λειτουργίας των δικτύων αλλά και για την πραγματοποίηση ασφαλούς παράδοσης των υπηρεσιών στον χρήστη μέσω των δικτύων αυτών. Μεταξύ των τεχνικών παροχής ασφάλειας επικοινωνιών που εφαρμόζονται, η ασφάλεια φυσικού επιπέδου (PLS), πρέπει να αναπτυχθεί ώστε να είναι ισχυρή, αποδεδειγμένη και μετρήσιμη.

Συγκεκριμένα, το IoT έχει τέσσερα μοναδικά χαρακτηριστικά που πρέπει να προβλεφθούν: χαμηλό κόστος, κάλυψη ευρείας εμβέλειας, τεράστιος αριθμός συνδέσεων και επικοινωνία μεταξύ διαφορετικών υπηρεσιών. Το πώς θα σχεδιαστούν στρατηγικές σε Physical Layer Security που ταιριάζουν καλά με αυτές τις τέσσερις δυνατότητες παραμένει ένα ανοιχτό πρόβλημα, όπου έχει κεντρίσει το ενδιαφέρον τόσο από τον ακαδημαϊκό κόσμο όσο και από τις βιομηχανίες.

Σε αυτό το άρθρο, θα θέλαμε να παρουσιάσουμε μια ολοκληρωμένη ανασκόπηση των τεχνικών ασφάλειας φυσικού επιπέδου για το Internet of Things. Συγκεκριμένα το άρθρο περιλαμβάνει κυρίως την εισαγωγή της βασικής αρχής της ασφάλειας φυσικού επιπέδου, τις αντιπροσωπευτικές τεχνικές PLS, τις μοναδικές προκλήσεις που αντιμετωπίζει ο σχεδιασμός του πρωτοκόλλου PLS και τις αναδυόμενες λύσεις PLS προσανατολισμένες στο IoT.

ABSTRACT

The massive growth of the Internet of Things makes information security unprecedentedly important. Network security techniques are vital not only for maintaining good and efficient operation of networks but also for realizing secure delivery of services to the user over these networks. Among the communication security delivery techniques that are implemented, physical layer security (PLS), must be deployed to be robust, proven and measurable.

In particular, IoT has four unique characteristics that must be provided: low cost, wide-area coverage, huge number of connections and communication between different services. How to design strategies in Physical Layer Security that fit well with these four capabilities remains an open problem, where it has sparked interest from both academia and industry.

In this article, we would like to present a comprehensive review of physical layer security techniques for the Internet of Things. In particular, the article mainly includes the introduction of the basic principle of physical layer security, representative PLS techniques, unique challenges faced in PLS protocol design, and emerging IoT-oriented PLS solutions.

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ: Δικτύων Επικοινωνιών και Κατανεμημένων Συστημάτων
ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ, ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΔΙΑΣΤΡΩΜΑΤΩΣΗ, ΕΠΙΠΕΔΑ OSI, ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΑΝΤΙΚΕΙΜΕΝΩΝ, ΚΙΝΔΥΝΟΙ ΣΤΟ IOT, ΕΙΔΗ ΕΠΙΘΕΣΕΩΝ ΣΤΟ IoT, ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ IoT, ΑΣΦΑΛΕΙΑ ΣΤΟ ΦΥΣΙΚΟ ΕΠΙΠΕΔΟ, PLS, ΣΧΗΜΑΤΑ PLS για το IoT, ΥΠΟΣΧΟΜΕΝΕΣ ΛΥΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΦΥΣΙΚΟΥ ΕΠΙΠΕΔΟΥ ΣΤΟ IoT, NOISE AGGREGATION AND SELF-ENCRYPTION, CONSTELLATION ROTATION, FOUNTAIN-CODING BASED SECURE TRANSMISSION, MACHINE LEARNING, RECONIGURABLE INTELLIGENT SURFACES.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1: ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ – ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ 17

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ 17

Διαθεσιμότητα (Availability) 17

Εμπιστευτικότητα (Confidentiality) 17

Ακεραιότητα (Integrity) 18

ΜΕΘΟΔΟΙ ΕΠΙΘΕΣΗΣ 18

ΜΕΘΟΔΟΙ ΑΠΟΦΥΓΗΣ ΕΠΙΘΕΣΕΩΝ: 19

ΤΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ Η ΔΙΑΣΤΡΩΜΑΤΩΣΗ 19

Η Αναγκαιότητα των επιπέδων 19

Πλεονεκτήματα της Διαστρωμάτωσης 20

ΤΑ ΕΠΙΠΕΔΑ OSI 20

Το μοντέλο αναφοράς OSI 22

Το Επίπεδο Εφαρμογής 23

Το Επίπεδο Παρουσίασης 23

Το Επίπεδο Συνόδου 23

Το Επίπεδο Μεταφοράς 24

Το Επίπεδο Δικτύου 25

Εικόνα: Το μοντέλο αναφοράς OSI κατά την επικοινωνία δυο χρηστών .. 26

Το Επίπεδο Σύνδεσης Δεδομένων 26

Φυσικό Επίπεδο 27

ΜΕΘΟΔΟΙ ΕΠΙΘΕΣΕΩΝ 28

Φυσικό Επίπεδο (Physical layer): 28

Επίπεδο σύνδεσης δεδομένων (Data link layer):.....28
Επίπεδο δικτύου (Network layer):.....28
Επίπεδο μεταφοράς (Transport layer): 28
Επίπεδο συνεδρίας (Session layer:):.....28
Επίπεδο παρουσίασης (Presentation layer): 28
Επίπεδο εφαρμογής (Application layer):.....28
ΜΕΘΟΔΟΙ ΑΜΥΝΑΣ 28
Φυσικό επίπεδο: 28
Επίπεδο σύνδεσης δεδομένων:.....28
Επίπεδο δικτύου: 29
Επίπεδο μεταφοράς:.....29
Επίπεδο περιόδου λειτουργίας: 29
Επίπεδο παρουσίασης:.....29
Επίπεδο εφαρμογής: 29
ΚΕΦΑΛΑΙΟ 2: ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΑΝΤΙΚΕΙΜΕΝΩΝ – ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ.....30
ΚΙΝΔΥΝΟΙ ΣΤΟ IOT – ΕΙΔΗ ΕΠΙΘΕΣΕΩΝ.....32
Έλλειψη συμμόρφωσης εκ μέρους των κατασκευαστών IoT. 33
Έλλειψη γνώσης και ευαισθητοποίησης των χρηστών 33
Προβλήματα ασφάλειας μη ενημερωμένων λογισμικών συσκευών IoT...34
Έλλειψη φυσικής προστασίας της συσκευής.....34
Επιθέσεις botnet 35
Βιομηχανική κατασκοπεία & υποκλοπή 36
Πειρατεία στις συσκευές IoT 36
Κίνδυνοι ακεραιότητας δεδομένων σε συσκευές IoT με εφαρμογή στην υγεία.....37
Παραβιασμένες - Παράνομες συσκευές IoT.....38
Cryptomining with IoT Bots.....39
ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ IoT.....39
RFID.....**Error! Bookmark not defined.**
Service Oriented Application.....41
Wireless Sensor Network.....41
Supply Chain Management 42
Healthcare.....42
Smart Society.....42

Cloud-based Services 42
Security 43
ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΕ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ 43
ΚΕΦΑΛΑΙΟ 3: ΑΣΦΑΛΕΙΑ ΣΤΟ ΦΥΣΙΚΟ ΕΠΙΠΕΔΟ 55
Βιβλιογραφική ανασκόπηση των τεχνικών PLS για το IoT 57
Σχήματα PLS για το IoT: 59
Έγχυση τεχνητού θορύβου (Artificial Noise Injection) 61
Compressive Sensing 61
Bit Flipping 62
Cooperative Secrecy - Jamming 63
Physical Layer Encryption 64
ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΩΝ ΥΦΙΣΤΑΜΕΝΩΝ ΤΕΧΝΙΚΩΝ PLS 66
ΠΡΟΚΛΗΣΕΙΣ ΣΤΗΝ ΣΧΕΔΙΑΣΗ ΤΟΥ PLS ΠΡΩΤΟΚΟΛΛΟΥ ΓΙΑ ΤΟ Internet of Things 67
ΚΕΦΑΛΑΙΟ 4: ΥΠΟΣΧΟΜΕΝΕΣ ΛΥΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΦΥΣΙΚΟΥ ΕΠΙΠΕΔΟΥ ΣΤΟ IoT 69
ΣΥΝΑΘΡΟΙΣΗ ΘΟΡΥΒΟΥ ΚΑΙ ΑΥΤΟΚΡΥΠΤΟΓΡΑΦΗΣΗ (NOISE AGGREGATION AND SELF-ENCRYPTION) 69
ΣΧΕΔΙΑΣΜΟΣ ΣΗΜΑΤΟΣ ΚΑΤΑ ΤΩΝ ΥΠΟΚΛΟΠΩΝ ΜΕΣΩ CONSTELLATION ROTATION 72
ΑΣΦΑΛΗΣ ΜΕΤΑΔΟΣΗ ΜΕ ΒΑΣΗ ΤΗΝ ΚΩΔΙΚΟΠΟΙΗΣΗ ΠΗΓΗΣ (FOUNTAIN-CODING BASED SECURE TRANSMISSION) 74
MACHINE LEARNING 78
RECONIGURABLE INTELLIGENT SURFACES (RSIS) 79
ΣΥΝΟΨΗ ΤΩΝ ΛΥΣΕΩΝ PLS ΜΕ ΠΡΟΣΑΝΑΤΟΛΙΣΜΟ ΣΤΟ IoT 81
ΚΕΦΑΛΑΙΟ 5: ΣΥΜΠΕΡΑΣΜΑΤΑ 83
ΠΑΡΑΡΤΗΜΑ Ι – ΕΥΡΕΤΗΡΙΟ ΟΡΩΝ 85
ΒΙΒΛΙΟΓΡΑΦΙΑ 88

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

Σχήμα 1: Δίκτυο υπολογιστών 17
Σχήμα 2: Επικοινωνία δυο κόμβων δικτύου 22
Σχήμα 3: Το μοντέλο αναφοράς OSI κατά την επικοινωνία δυο χρηστών 26
Σχήμα 4: Ταξινόμηση απαιτήσεων ασφαλείας βασισμένη στα επίπεδα που συμμετέχουν. 32
Σχήμα 5: Αρχιτεκτονική μιας επίθεσης DDos..... 35
Σχήμα 6: Ο υπολογιστής είναι θύμα επιθέσεως και είναι κλειδωμένος..... 37
Σχήμα 7: Ταξινόμηση Εφαρμ. IoT βασισμένες στον τομέα εφαρμογή τους. ... 40
Σχήμα 8: Μεθοδολογίες ασύρματης ασφάλειας και παράγοντες που επηρεάζουν τον σχεδιασμό τους. 45
Σχήμα 9: Διαδικασία ελέγχου ταυτότητας WEP. 47
Σχήμα 10: Διαδικασία ελέγχου ταυτότητας μέσω RSA 50
Σχήμα 11: Διαδικασία ελέγχου ταυτότητας μέσω EAP 50
Σχήμα 12: Αρχιτεκτονική δικτύου LTE. 52
Σχήμα 13: Γενική αρχιτεκτονική ασύρματου πρωτοκόλλου OSI. 54
Σχήμα 14: Τεχνική PLS που βασίζεται σε Beamforming..... 60
Σχήμα 15: Τεχνική PLS που βασίζεται σε Cooperative Jamming 64
Σχήμα 16: Απεικόνιση της μεθόδου συγκέντρωσης θορύβου. 70
Σχήμα 17: Απεικόνιση της μεθόδου συγκέντρωσης θορύβου. 71
Σχήμα 18: Αναπαράσταση της μέθοδου constellation-rotation για την ασφάλεια των αμφίδρομων μη αξιόπιστων συστημάτων αναμετάδοσης. 74
Σχήμα 19: Σύστημα ασφαλούς μετάδοσης με βάση την κωδικοπ. πηγής. 78
Σχήμα 20: Reconfigurable intelligent surfaces in IoT networks 80

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

AES Advanced Encryption Standard

AF Amplify-and-Forward

AN Artificial Noise

CJ Cooperative Jamming

CS Compressive Sensing

CSI-Channel State information

DDoS Distributed Denial of Service

DF Decode-and-Forward

EAP Extensible Authentication Protocol

ECC Elliptic Curve Cryptography

EFC- Eavesdropping Fusion Center

EPC Evolved Packet Core

E-UTRAN Evolved Universal Terrestrial Radio Access Network

FSK Frequency Shift Keying

GSM Global System for Mobile communications

HSS Home Subscriber Server

HVAC Heating Ventilation Air Conditioning

IEEE Institute of Electrical and Electronics Engineers

IoT Internet of Things

IP Internet Protocol

LFC Legitimate Fusion Center

LFC- Legitimate Fusion Center

LT Lube Transform

LTE Long-Term Evolution

MAC Media Access Control

MME Mobility Management Entity

NA Noise Aggregation

NAS Network attached storage

OSI Open Systems Interconnection

PDN-GW Gateway packet data network gateway

PKM Preshared Key Management

PLC Programmable Logic Controller

PLS Physical Layer Security

PSK Phase Shift Keying

PSK PreShared Sey

QKD Quantum Key Distribution

QoS Quality of Service

RFID Radio Frequency Identification oriented application

RSIS Reconfigurable Intelligent Surfaces

RS Reed-Solomon

SCM Supply Chain Management

S-GW Serving Gateway

SNR Signal-to-Noise Ratio

SoA Service-oriented Application

TCP Transmission Control Protocol

TKIP Temporal Key Integrity Protocol

UDP User Datagram Protocol

VPN Virtual Private Network

WEP Wired Equivalent Privacy

WiMAX Worldwide Interoperability for Microwave Access

WPA Wi-Fi Protected Access

WSN Wireless Sensor Network

ML Machine Learning

DNN Deep Neural Network

CNN Convolutional Neural Network

RNN Recurrent Neural Network

MIMO Multiple Input, Multiple Output

ΚΕΦΑΛΑΙΟ 1: ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ – ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Η έννοια της ασφάλειας Δικτύου Υπολογιστών σχετίζεται με την ικανότητα μιας επιχείρησης ή ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Εκτός αυτού, θεωρείται ως η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί, σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί καθώς και τις συναφείς υπηρεσίες που παρέχονται είτε είναι προσβάσιμες μέσω των δικτύων και συστημάτων αυτών.

Σχήμα 1: Δίκτυο υπολογιστών

Η έννοια της ασφάλειας των δικτύων υπολογιστών συνδέεται στενά με τρεις **βασικές έννοιες.**

Διαθεσιμότητα (Availability)

Διαθεσιμότητα ονομάζεται η ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός δικτύου υπολογιστών όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα. Για τους σκοπούς της ασφάλειας, μας απασχολεί βασικά η παρεμπόδιση κακόβουλων επιθέσεων που αποσκοπούν στο να παρακωλύσουν την πρόσβαση των νόμιμων χρηστών σε ένα πληροφοριακό σύστημα. Αυτές οι επιθέσεις ονομάζονται επιθέσεις «άρνησης παροχής υπηρεσιών (denial of service)».

Εμπιστευτικότητα (Confidentiality)

Εμπιστευτικότητα σημαίνει πρόληψη μη εξουσιοδοτημένης αποκάλυψης πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη ανάγνωση.

Επομένως, τα δεδομένα που διακινούνται μεταξύ των υπολογιστών ενός δικτύου, αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα. Άλλες εκφάνσεις της εμπιστευτικότητας είναι:

Η **ιδιωτικότητα**, προστασία των δεδομένων προσωπικού χαρακτήρα, δηλαδή αυτών που αφορούν συγκεκριμένα πρόσωπα και η **μυστικότητα**, προστασία των δεδομένων που ανήκουν σε έναν οργανισμό ή μια επιχείρηση.

Ακεραιότητα (Integrity)

Η ακεραιότητα μπορεί να οριστεί γενικότερα ως η απαίτηση να είναι τα πράγματα όπως πρέπει να είναι. Στην πληροφορική, ακεραιότητα σημαίνει πρόληψη μη εξουσιοδοτημένης μεταβολής πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη εγγραφή ή διαγραφή, συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων.

ΜΕΘΟΔΟΙ ΕΠΙΘΕΣΗΣ

Άρνηση παροχής υπηρεσιών - Denial-of-Service (DoS).

Αποστολή περισσοτέρων αιτήσεων σύνδεσης από όσες μπορεί να επεξεργαστεί ένας server με αποτέλεσμα να μην μπορεί ο server να παρέχει τις υπηρεσίες που θεωρητικά παρέχει.

Μη εξουσιοδοτημένη πρόσβαση (Unauthorized access attacks).

Διάφοροι τρόποι επίθεσης που εμπεριέχουν την ανάκτηση του δικαιώματος εισόδου, εκτέλεσης εντολών, ή ανάκτησης πληροφορίας σε ένα μηχάνημα που δεν παρέχει τέτοιες υπηρεσίες στους επιτιθέμενους αλλά μόνο στους εξουσιοδοτημένους χρήστες.

Επιθέσεις στους κωδικούς - Password attacks.

Αποτελεί την μέθοδο εύρεσης ενός password, είτε με επαναληπτικό τρόπο δοκιμάζοντας όλους τους δυνατούς συνδυασμούς, είτε με αποκρυπτογράφηση του κωδικού πρρόσβασης (password) δοκιμάζοντας όλους τους δυνατούς συνδυασμούς των πιθανών κλειδιών κρυπτογράφησης.

Δούρειοι Ίπποι - Trojan Horses

Είναι ένα πρόγραμμα που περιέχει η εγκαθιστά μία «κακόβουλη» (malicious) εφαρμογή.

Ανιχνευτές πακέτων δικτύου - Network packet sniffers

Είναι προγράμματα ή μηχανές τα οποία μπορούν να υποκλέψουν την κίνηση που μεταφέρεται σε ένα δίκτυο.

ΜΕΘΟΔΟΙ ΑΠΟΦΥΓΗΣ ΕΠΙΘΕΣΕΩΝ:

Έλεγχος γνησιότητας της ταυτότητας (identification and authentication)

Των χρηστών , των προγραμμάτων ή των μηχανημάτων καθώς και των εξουσιοδοτήσεων που αυτά διαθέτουν για την προσπέλαση των προστατευμένων πόρων του συστήματος με συνδυασμένη χρήση συνθηματικών και ψηφιακών πιστοποιητικών.

Προστασία της εμπιστευτικότητας των δεδομένων (data confidentiality)

Δηλαδή προστασία ενάντια σε μη εξουσιοδοτημένες αποκαλύψεις πληροφοριών.

Τοίχος Προστασίας (Firewall)

Το οποίο είναι ένα πρόγραμμα ή ένα μηχάνημα που μπορεί να χρησιμοποιηθεί σαν διαχωριστικό μεταξύ των χρηστών και των προγραμμάτων.

Κωδικοποίηση / Κρυπτογράφηση - Πρωτόκολλα Ασφαλείας

Τα πρωτόκολλα αυτά εφαρμόζονται στα επίπεδα Πρόσβασης Δικτύου, Internet, Μεταφοράς και Εφαρμογής.

Ενημέρωση Λογισμικού

Του λειτουργικού συστήματος operating systems και των εφαρμογών που τρέχουν στο σύστημα.

ΤΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ Η ΔΙΑΣΤΡΩΜΑΤΩΣΗ

Ένα δίκτυο υπολογιστών αποτελείται από υπολογιστές, οι οποίοι συνδέονται μεταξύ τους, ασύρματα ή ενσύρματα. Η αρχιτεκτονική δικτύου αναφέρεται στις λεπτομέρειες υλοποίησης της διασύνδεσης, και στην τοπολογία δικτύου, δηλαδή τον τρόπο αυτό διασύνδεσης ώστε να πραγματοποιείται η ανταλλαγή δεδομένων και η επικοινωνία των υπολογιστών.

Ένα δίκτυο υπολογιστών θα πρέπει να έχει σχεδιαστεί και αναπτυχθεί έτσι ώστε να αποτελεί ένα αξιόπιστο, αποδοτικό, ασφαλές και οικονομικό μέσο ανταλλαγής ή μεταβίβασης πληροφοριών μεταξύ των χρηστών. Επίσης, κατά τη σχεδίαση και ανάπτυξη ενός δικτύου Η/Υ θα πρέπει να λαμβάνεται υπόψη ότι είναι ένα περιβάλλον δυναμικά εξελισσόμενο, καθώς προσπαθεί να ικανοποιήσει τόσο τις συνεχώς αυξανόμενες και μεταβαλλόμενες απαιτήσεις των χρηστών όσο και να ενσωματώσει τις ραγδαίες τεχνολογικές εξελίξεις.

Η Αναγκαιότητα των επιπέδων

Όλες οι παραπάνω απαιτήσεις καθιστούν τη σχεδίαση ενός δικτύου υπολογιστών ένα πολύπλοκο πρόβλημα. Για να μπορέσουν να χειριστούν αυτή την πολυπλοκότητα, οι σχεδιαστές οργανώνουν τις λειτουργίες των δικτύων

υπολογιστών σε σειρές από στρώματα ή επίπεδα. Αυτή η διαστρωμάτωση είναι η βασική ιδέα, αλλά και η κοινή πρακτική, σε όλες τις αρχιτεκτονικές δικτύων.

Το Διαδίκτυο, όπως όλα τα δίκτυα, βασίζει τη λειτουργία του στην ύπαρξη ενός συνόλου πρωτοκόλλων που είναι δομημένα σε μια ιεραρχία διακριτών επιπέδων. Ο λόγος που συμβαίνει κάτι τέτοιο, είναι επειδή τα δίκτυα υπολογιστών είναι περίπλοκα συστήματα και η οργάνωσή τους σε διακριτά επίπεδα κάνει εφικτή την ενασχόληση με ένα μόνο επίπεδο. Το πλεονέκτημα αυτής της μεθόδου είναι ότι επιτρέπει τη μελέτη και ανάπτυξη κάθε επιπέδου του συστήματος ανεξάρτητα από τα υπόλοιπα. Ακόμα κάνει πιο εύκολη την αλλαγή της υλοποίησης ενός επιπέδου χωρίς να επηρεάζονται τα υπόλοιπα. Κάθε δικτυακό επίπεδο παρέχει στα ανώτερα επίπεδα κάποιες υπηρεσίες. Οι παρεχόμενες υπηρεσίες κάθε επιπέδου είτε υλοποιούνται μέσα στο ίδιο το επίπεδο εκτελώντας κάποιες ενέργειες ή κάνουν χρήση του αμέσως προηγούμενου επιπέδου.

Στα συστήματα επικοινωνιών, η αφαιρετική τους θεώρηση συνήθως οδηγεί στην ιεράρχηση υπηρεσιών και στη διαστρωμάτωση. Για την παροχή μιας σύνθετης τηλεπικοινωνιακής υπηρεσίας η βασική ιδέα είναι απλή στη σύλληψη: ξεκινάμε με τις υπηρεσίες που παρέχει το χρησιμοποιούμενο υλικό και πάνω τους «χτίζουμε» μια σειρά από επίπεδα, το καθένα από τα οποία προσφέρει υπηρεσίες με υψηλότερο βαθμό αφαίρεσης. Οι υπηρεσίες των υψηλότερων επιπέδων σχεδιάζονται και υλοποιούνται έτσι ώστε να χρησιμοποιούν τις υπηρεσίες των χαμηλότερων επιπέδων.

Πλεονεκτήματα της Διαστρωμάτωσης

Ο σχεδιασμός δικτύων σε επίπεδα απλοποιεί την υλοποίησή τους. Αντί να αναπτυχθεί ο απαραίτητος κώδικας ως ένα μονολιθικό κομμάτι το οποίο θα επιλύει όλα τα ενδεχόμενα προβλήματα διασύνδεσης, είναι απλούστερο να αναπτυχθούν ξεχωριστά κομμάτια κώδικα για καθένα διαφορετικό πρόβλημα, τα οποία θα αλληλοεπιδρούν με σαφή και προκαθορισμένο τρόπο.

Επιπλέον, η διαστρωμάτωση μας παρέχει τις δυνατότητες της δομημένης σχεδίασης και της επαναχρησιμοποίησης λογισμικού. Για παράδειγμα, εάν στο σύστημα ο τερματικός σταθμός Α επικοινωνήσει απευθείας με το δορυφόρο (δηλαδή εάν οι σύνδεσμοι α και β αντικατασταθούν με ένα νέο δορυφορικό σύνδεσμο), τότε η εφαρμογή του ηλεκτρονικού ταχυδρομείου δε χρειάζεται να υποστεί καμία τροποποίηση, καθώς αλληλοεπιδρά μόνο με την υπηρεσία της από άκρο σε άκρο επικοινωνίας. Όλες οι απαραίτητες τροποποιήσεις απορροφούνται στα χαμηλότερα επίπεδα επικοινωνίας.

ΤΑ ΕΠΙΠΕΔΑ OSI

Το μοντέλο OSI βασίζεται σε μια πρόταση, που ανέπτυξε ο Οργανισμός Διεθνών Προτύπων ISO, ως ένα πρώτο βήμα προς την κατεύθυνση της διεθνούς προτυποποίησης των πρωτοκόλλων που χρησιμοποιούνται στα

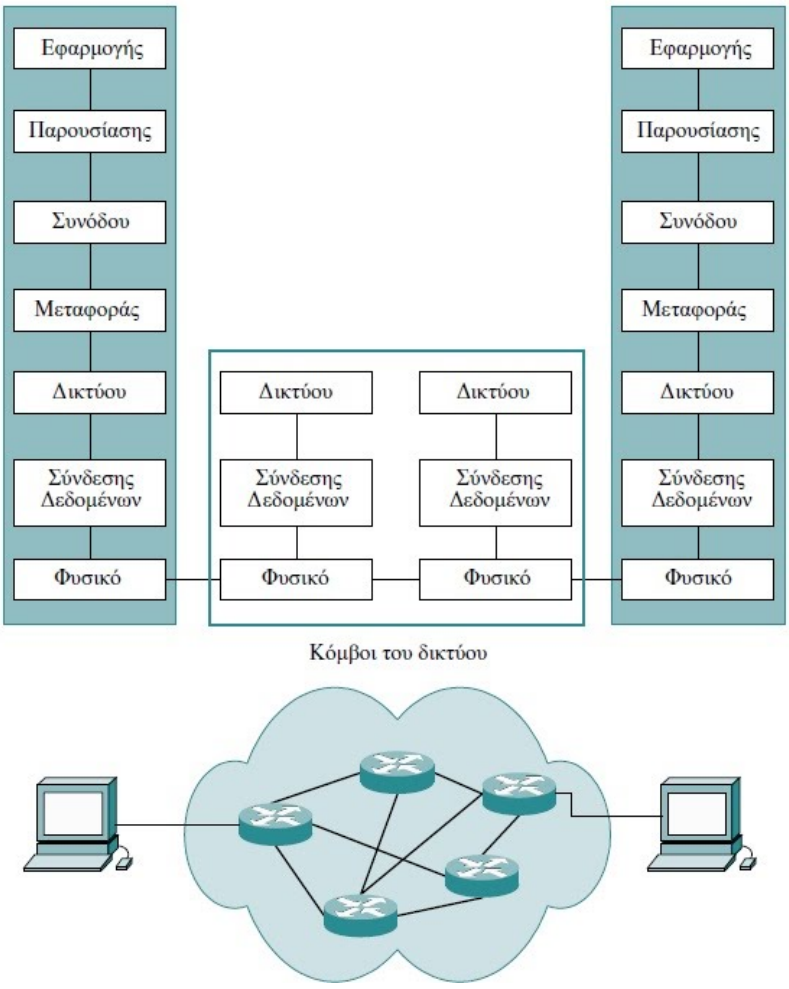
διάφορα στρώματα. Το μοντέλο αποκαλείται μοντέλο αναφοράς OSI (Open Systems Interconnection) του ISO, επειδή αφορά ανοικτά συστήματα, δηλαδή συστήματα ανοικτά στην επικοινωνία με άλλα συστήματα.

Το μοντέλο αυτό έχει επτά στρώματα καθένα από τα οποία εκτελεί συγκεκριμένες λειτουργίες και επικοινωνεί με τα επίπεδα που είναι ακριβώς από πάνω και από κάτω του. Τα ανώτερα επίπεδα ασχολούνται κυρίως με τις υπηρεσίες, εφαρμογές και δραστηριότητες χρηστών και τα κατώτερα στρώματα ασχολούνται κυρίως με την καθαυτού μετάδοση δεδομένων.

Το μοντέλο αναφοράς Ανοικτής Διασύνδεσης Συστημάτων, ή μοντέλο αναφοράς OSI (αγγλ. OSI reference model) είναι μια διαστρωματωμένη, αφηρημένη περιγραφή για τη σχεδίαση τηλεπικοινωνιακών και δικτυακών πρωτοκόλλων η οποία καθορίστηκε από την πρωτοβουλία Ανοικτή Διασύνδεση Συστημάτων – OSI. Είναι γνωστό και ως μοντέλο των επτά επιπέδων.

Στα τέλη της δεκαετίας του 1970, ο Διεθνής Οργανισμός Τυποποίησης (International Organization for Standardization, ISO) διατύπωσε μια σειρά από οδηγίες για την αρχιτεκτονική δικτύου. Αυτές οι οδηγίες συνέθεσαν το μοντέλο αναφοράς για τη Διασύνδεση Ανοικτών Συστημάτων (Open Systems Interconnection, OSI), το οποίο συνοπτικά θα αναφέρεται ως μοντέλο αναφοράς OSI.

Αξίζει να παρατηρήσουμε ότι το μοντέλο αναφοράς OSI δεν αποτελεί μια αρχιτεκτονική δικτύου, καθώς δεν καθορίζει τα αναγκαία πρωτόκολλα και τα σημεία επαφής τους. Ο οργανισμός ISO, σε συνδυασμό με τη Διεθνή Ένωση Τηλεπικοινωνιών(International Telecommunication Union, ITU), καθόρισε μια σειρά από πρωτόκολλα βασισμένα στο μοντέλο αναφοράς OSI, τα οποία συχνά καλούνται ως η σειρά πρωτοκόλλων «X.» (π.χ. X.25, X.400, X.500 κ.ά.). Τα πρωτόκολλα ISO δεν έτυχαν όμως ευρείας αποδοχής και χαρακτηρίστηκαν έτσι από την εμπορική αποτυχία τους.



Σχήμα 2: Επικοινωνία δυο κόμβων δικτύου

Το μοντέλο αναφοράς OSI

Το μοντέλο αναφοράς OSI οργανώνεται σε επτά επίπεδα. Οι λειτουργίες των τριών χαμηλότερων επιπέδων (Φυσικό, Σύνδεσης Δεδομένων και Δικτύου) διενεργούν τον έλεγχο της μετάδοσης μηνυμάτων μέσα στο δίκτυο, ενώ οι λειτουργίες των υπόλοιπων ανώτερων επιπέδων (Μεταφοράς, Συνόδου, Παρουσίασης και Εφαρμογής) παρέχουν την αξιόπιστη μεταβίβαση της πληροφορίας από άκρο σε άκρο.

Το μοντέλο αναφοράς OSI επηρέασε όχι τόσο τον τρόπο με τον οποίο σχεδιάζουμε, αλλά πολύ περισσότερο τον τρόπο με τον οποίο κατανοούμε τα δίκτυα υπολογιστών. Το μοντέλο αναφοράς OSI έχει επτά επίπεδα (βλέπε Σχήμα). Τα τρία χαμηλότερα επίπεδα ασχολούνται με τον έλεγχο της μετάδοσης των μηνυμάτων μέσα στο δίκτυο, ενώ τα τέσσερα ανώτερα επίπεδα παρέχουν την αξιόπιστη μεταβίβαση των δεδομένων μεταξύ των τελικών χρηστών. Έτσι, και τα επτά επίπεδα υλοποιούνται μόνο στους υπολογιστές που λειτουργούν ως τερματικοί σταθμοί.

Το Επίπεδο Εφαρμογής

Το Επίπεδο Εφαρμογής παρέχει ένα σύνολο δικτυακών υπηρεσιών στις τελικές εφαρμογές των χρηστών (όπως, π.χ. το ηλεκτρονικό ταχυδρομείο, η μεταφορά αρχείων, η εξομοίωση τερματικών, η σύνδεση σε απομακρυσμένους σταθμούς εργασίας κ.ά.).

Ο αναγνώστης δε θα πρέπει να συγχέει την τελική εφαρμογή με την αντίστοιχη στοιχειώδη υπηρεσία του Επιπέδου Εφαρμογής. Για παράδειγμα, ένα πρόγραμμα μεταφοράς αρχείου είναι μια τελική εφαρμογή χρήστη που βασίζεται στο πρωτόκολλο

μεταφοράς αρχείου του Επιπέδου Εφαρμογής. Το πρόγραμμα και το πρωτόκολλο είναι δύο τελείως διαφορετικές οντότητες και δεν πρέπει να τις συγχέουμε ως έννοιες, παρ' όλο που έχουν το ίδιο ακρωνύμιο (FTP).

Το Επίπεδο Παρουσίασης

Το Επίπεδο Παρουσίασης ασχολείται με την αναπαράσταση των δεδομένων και έχει ως κύρια λειτουργία την εξασφάλιση της αναγνωσιμότητάς τους, ακόμα και μεταξύ κόμβων που χρησιμοποιούν διαφορετικές μορφές αναπαράστασης της πληροφορίας.

Για παράδειγμα, έστω ότι ο αποστολέας κόμβος χρησιμοποιεί την κωδικοσειρά ASCII για την αναπαράσταση χαρακτήρων και ότι οι ακέραιοι αριθμοί εκφράζονται σαν συμπλήρωμα ως προς ένα. Επίσης, έστω ότι ο παραλήπτης κόμβος χρησιμοποιεί την κωδικοσειρά EBCDIC και οι ακέραιοι αριθμοί του εκφράζονται σαν συμπλήρωμα ως προς δύο. Για να μπορέσουν να επικοινωνήσουν οι δύο κόμβοι, θα πρέπει τα δεδομένα του αποστολέα να μετατραπούν στη μορφή δεδομένων που αναγνωρίζει ο παραλήπτης. Αυτή η μετατροπή διενεργείται στο Επίπεδο Παρουσίασης.

Τέλος, στο Επίπεδο Παρουσίασης συμφωνείται η τεχνική συμπίεσης δεδομένων και το σχήμα κρυπτογράφησης της πληροφορίας που θα ακολουθούν ο αποστολέας και ο παραλήπτης κόμβος για την εξοικονόμηση των πόρων του δικτύου και την εξασφάλιση της μυστικότητας και της γνησιότητας της πληροφορίας, αντίστοιχα.

Το Επίπεδο Συνόδου

Σε αυτό το επίπεδο διενεργούνται όλες οι απαραίτητες λειτουργίες για την εγκαθίδρυση, την επίβλεψη και τον τερματισμό των συνόδων (sessions) μεταξύ των τελικών εφαρμογών.

Για παράδειγμα, πριν από την έναρξη της μετάδοσης δεδομένων οι τελικές εφαρμογές θα πρέπει να συμφωνήσουν εάν η επικοινωνία θα είναι αμφίδρομη (full duplex), εναλλακτικά αμφίδρομη (half duplex) ή μονόδρομη (simplex). Στην πρώτη περίπτωση τα δεδομένα μπορούν να μεταδίδονται και προς τις δύο κατευθύνσεις ταυτόχρονα, στη δεύτερη περίπτωση μπορούν να μεταδίδονται

και προς τις δύο κατευθύνσεις αλλά όχι ταυτόχρονα, ενώ στην τρίτη περίπτωση τα δεδομένα μεταδίδονται μόνο προς μία κατεύθυνση. Αυτή η διαπραγμάτευση διενεργείται μεταξύ των ομότιμων οντοτήτων του Επιπέδου Συνόδου.

Επίσης, από το Επίπεδο Συνόδου προσφέρεται και η υπηρεσία συγχρονισμού, η οποία χαρακτηρίζεται εξαιρετικά χρήσιμη για την αποτελεσματική αντιμετώπιση καταστάσεων κατάρρευσης της σύνδεσης. Η βασική ιδέα είναι πολύ απλή. Στην ακολουθία δεδομένων εισάγονται κάποια προσυμφωνημένα σημεία συγχρονισμού πριν από τη μετάδοσή τους. Εάν η σύνδεση καταρρεύσει, τότε θα επαναμεταδοθούν μόνο τα δεδομένα που εστάλησαν από το τελευταίο σημείο συγχρονισμού και μετά και όχι το σύνολό τους, κάτι που θα αποφέρει σημαντική εξοικονόμηση των πόρων του δικτύου.

Το Επίπεδο Μεταφοράς

Στο Επίπεδο Μεταφοράς υλοποιείται το κανάλι επικοινωνίας μεταξύ των τερματικών κόμβων, μέσω του οποίου θα μεταβιβάζονται αξιόπιστα τα μηνύματά τους.

Στον αποστολέα κόμβο τα μηνύματα που εισέρχονται από το ανώτερο Επίπεδο Συνόδου συνήθως διασπώνται σε πακέτα, τα οποία αριθμούνται και προωθούνται για μετάδοση στο χαμηλότερο Επίπεδο Δικτύου. Αντίστοιχα, στον παραλήπτη κόμβο τα αρχικά μηνύματα επανασυνθέτονται από τα εισερχόμενα πακέτα και προωθούνται προς επεξεργασία στο Επίπεδο Συνόδου. Σε αυτό το επίπεδο συνήθως συμπεριλαμβάνεται και ένα σχήμα επιβεβαίωσης, το οποίο χρησιμοποιείται για την επαλήθευση της ορθής παράδοσης των πακέτων στον προορισμό τους.

Επίσης, το Επίπεδο Μεταφοράς είναι υπεύθυνο για την εγκαθίδρυση, τη συντήρηση και τον τερματισμό των καναλιών επικοινωνίας μεταξύ των τερματικών κόμβων. Αυτά μπορεί να είναι είτε ιδεατά κυκλώματα είτε να υλοποιούνται με αυτοδύναμα πακέτα, επιτυγχάνοντας αντίστοιχα επικοινωνία με σύνδεση (connection oriented) ή χωρίς σύνδεση (connectionless).

Σε αρκετές περιπτώσεις περισσότερα από ένα διαφορετικά μηνύματα χρησιμοποιούν το ίδιο κανάλι επικοινωνίας μεταξύ των τερματικών κόμβων. Σε άλλες περιπτώσεις ένα μήνυμα μπορεί να χρησιμοποιήσει περισσότερα από ένα κανάλια επικοινωνίας μεταξύ του αποστολέα και του προορισμού για να βελτιώσει το ρυθμό εξυπηρέτησής του. Η πολύπλεξη των μηνυμάτων πραγματοποιείται στο Επίπεδο Μεταφοράς και διενεργείται με τρόπο διάφανο στο Επίπεδο Συνόδου.

Τέλος, στο Επίπεδο Μεταφοράς διενεργείται και ο έλεγχος της ροής των δεδομένων μεταξύ των τερματικών κόμβων, έτσι ώστε να μη λαμβάνει ο παραλήπτης κόμβος περισσότερα δεδομένα από όσα μπορεί απρόσκοπτα να εξυπηρετήσει. Ο έλεγχος ροής σε αυτό το επίπεδο είναι ξεχωριστός και ανεξάρτητος από τον έλεγχο ροής που διενεργείται στο Επίπεδο Σύνδεσης Δεδομένων.

Επειδή σε αυτό το επίπεδο ελέγχεται η από άκρο σε άκρο επικοινωνία, το Επίπεδο Μεταφοράς (και όλα τα ανώτερα από αυτό επίπεδα) υλοποιείται μόνο στους τερματικούς και όχι στους ενδιάμεσους κόμβους.

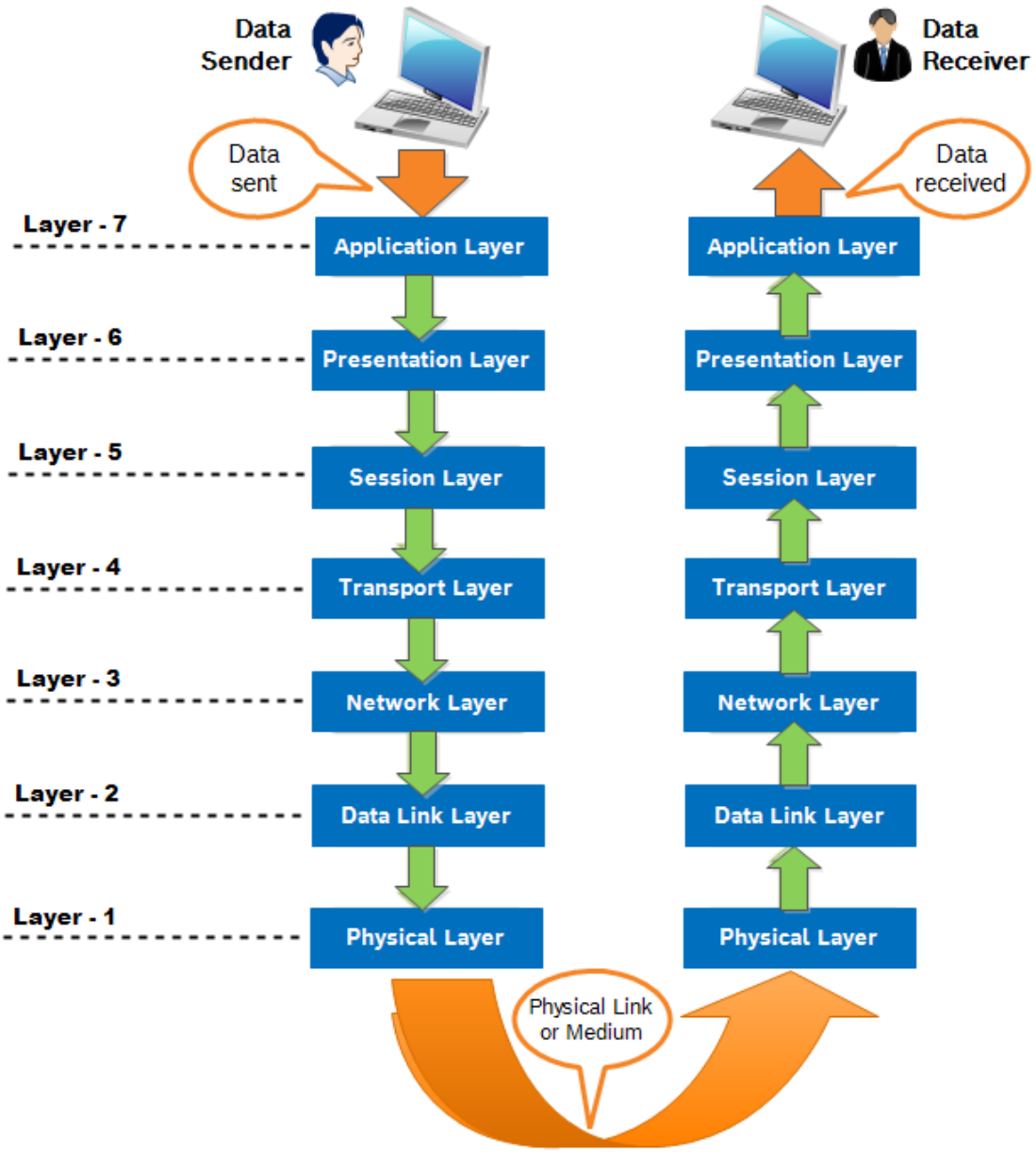
Το Επίπεδο Δικτύου

Οι μονάδες δεδομένων που ανταλλάσσουν οι ομότιμες διεργασίες στο Επίπεδο Δικτύου καλούνται πακέτα. Στο Επίπεδο Δικτύου καθορίζεται ο τρόπος δρομολόγησης των πακέτων από τον αποστολέα στον παραλήπτη και ο έλεγχος συμφόρησης του δικτύου. Ως συμφόρηση ορίζεται εκείνη η κατάσταση του δικτύου όπου η εισερχόμενη κυκλοφορία είναι μεγαλύτερη από αυτή που μπορεί να εξυπηρετήσει απρόσκοπτα το δίκτυο.

Ο αλγόριθμος δρομολόγησης των πακέτων μπορεί να είναι είτε στατικός είτε δυναμικός. Στη δεύτερη περίπτωση, κατά την επιλογή της διαδρομής διοχέτευσης της κυκλοφορίας μιας κλήσης λαμβάνεται υπόψη και ο φόρτος του δικτύου.

Οι σημερινοί δυναμικοί αλγόριθμοι δρομολόγησης έχουν ως κύριο στόχο τη γρήγορη εξάλειψη των περιστατικών συμφόρησης στο δίκτυο. Στα μελλοντικά δίκτυα υψηλής απόδοσης, όπου θα προσφέρονται υπηρεσίες πραγματικού χρόνου που θα απαιτούν εγγυημένη ποιότητα εξυπηρέτησης από το δίκτυο, οι αλγόριθμοι δρομολόγησης θα επιδιώκουν την αποφυγή των περιστατικών συμφόρησης.

Τέλος, σε αυτό το επίπεδο υλοποιείται το σχήμα διευθυνσιοδότησης του δικτύου. Κάθε κόμβος που ανήκει σε ένα δίκτυο χαρακτηρίζεται μοναδικά από τη διεύθυνση δικτύου. Η διεύθυνση δικτύου είναι μια παράμετρος του κόμβου, ορίζεται στο λογισμικό μέρος του και δεν πρέπει να συγχέεται με τη φυσική διεύθυνσή του. Η δρομολόγηση των πακέτων γίνεται με βάση τη διεύθυνση δικτύου του παραλήπτη κόμβου.



Σχήμα 3: Το μοντέλο αναφοράς OSI κατά την επικοινωνία δυο χρηστών

Το Επίπεδο Σύνδεσης Δεδομένων

Το Επίπεδο Σύνδεσης Δεδομένων μας παρέχει την αξιόπιστη μεταφορά των δεδομένων πάνω από τα φυσικά μέσα. Έτσι, στο Επίπεδο Δικτύου το φυσικό μέσο μετάδοσης εμφανίζεται ως ένας σύνδεσμος απαλλαγμένος από σφάλματα μεταφοράς,

κάτι που στην πραγματικότητα δεν ισχύει.

Τα δεδομένα που εισέρχονται στο Επίπεδο Σύνδεσης Δεδομένων από το υψηλότερο Επίπεδο Δικτύου οργανώνονται σε πλαίσια (frames). Στα πλαίσια ενσωματώνονται οι πληροφορίες ελέγχου αυτού του επιπέδου, με τη μορφή

επικεφαλίδας και «ουράς». Εκτός από τον έλεγχο σφαλμάτων, οι πληροφορίες που περιέχονται στις επικεφαλίδες και στις «ουρές» των πλαισίων συνήθως χρησιμοποιούνται για τον έλεγχο ροής (flow control) και για τον προσδιορισμό της διεύθυνσης του φυσικού μέσου.

Στον παραλήπτη, όταν διαπιστωθεί σφάλμα μεταφοράς κατά τον έλεγχο ενός πλαισίου, τότε, συνήθως, είτε ζητείται η επανεκπομπή του λανθασμένου πλαισίου είτε απλώς ενημερώνεται το αμέσως ανώτερο επίπεδο με την αποστολή ενός σχετικού μηνύματος ειδοποίησης.

Ένα άλλο θέμα με το οποίο ασχολείται το Επίπεδο Σύνδεσης Δεδομένων είναι ο έλεγχος της ροής δεδομένων μεταξύ δύο κόμβων, έτσι ώστε να μη στέλνονται περισσότερα δεδομένα από αυτά που μπορεί να δεχτεί ο κόμβος προορισμού.

Εδώ αξίζει να παρατηρήσουμε ότι, με βάση τους διαφορετικούς τρόπους χειρισμού των σφαλμάτων μεταφοράς και της ροής δεδομένων, το Επίπεδο Σύνδεσης Δεδομένων μπορεί να προσφέρει περισσότερες από μία υπηρεσίες στο Επίπεδο Δικτύου, η καθεμία με διαφορετική ποιότητα και τιμή.

Τέλος, εάν το φυσικό μέσο μετάδοσης υποστηρίζει κάποιο σχήμα διευθυνσιοδότησης, τότε αυτό υλοποιείται στο Επίπεδο Σύνδεσης Δεδομένων. Έτσι, στην επικεφαλίδα του πλαισίου δεδομένων θα πρέπει να καθορίζεται η «φυσική» διεύθυνση του κόμβου προορισμού του. Με τον όρο «φυσική» διεύθυνση ενός κόμβου εννοούμε τη διεύθυνση της αντίστοιχης μονάδας προσπέλασης του φυσικού μέσου μετάδοσης πάνω από το οποίο υλοποιείται το δίκτυο. Η φυσική διεύθυνση είναι αποτυπωμένη στο υλικό μέρος αυτής της συσκευής προσπέλασης («hardwired») και είναι μοναδική για κάθε συσκευή προσπέλασης του φυσικού μέσου που κατασκευάζεται.

Φυσικό Επίπεδο

Στο Φυσικό Επίπεδο καθορίζονται οι ηλεκτρικές, μηχανικές και λειτουργικές προδιαγραφές για τη μετάδοση των δεδομένων πάνω από ένα φυσικό μέσο, όπως, π.χ. η οπτική ίνα, το ομοαξονικό καλώδιο, η μικροκυματική ζεύξη κ.ά.

Για παράδειγμα, οι ερωτήσεις που θα πρέπει να απαντηθούν από τις προδιαγραφές του Φυσικού Επιπέδου είναι της μορφής:

— Ποια στάθμη τάσης αντιστοιχεί στο bit 1 και ποια στο bit 0;

— Ποια είναι η χρονική διάρκεια του παλμού ενός bit;

— Ποια είναι η διαδικασία εγκαθίδρυσης της σύνδεσης με το δίκτυο πριν από τη μετάδοση των δεδομένων και ποια η διαδικασία τερματισμού αυτής;

— Πώς καθορίζεται ο ρυθμός μετάδοσης των δεδομένων;

— Σε τι σήμα αντιστοιχεί ο κάθε ακροδέκτης του συνδετήρα του δικτύου;

Σε αυτό το σημείο θα πρέπει να τονίσουμε ότι στο Φυσικό Επίπεδο τα δεδομένα γίνονται αντιληπτά ως μια «ακατέργαστη» ακολουθία bits και μόνο.

ΑΣΦΑΛΕΙΑ ΣΤΑ ΔΙΑΦΟΡΑ ΕΠΙΠΕΔΑ OSI

Το μοντέλο OSI είναι σημαντικό για την ασφάλεια στον κυβερνοχώρο, διότι βοηθά στον εντοπισμό και την αποτροπή πιθανών επιθέσεων σε κάθε επίπεδο του (Imperva Application Security, 2023), (Mullins, 2020). Ορισμένα παραδείγματα επιθέσεων σε διάφορα επίπεδα είναι τα εξής:

ΜΕΘΟΔΟΙ ΕΠΙΘΕΣΕΩΝ

Φυσικό Επίπεδο (Physical layer): Κοπή ενός καλωδίου ή μπλοκάρισμα ενός ασύρματου σήματος για να προκαλέσει επίθεση τύπου άρνησης της υπηρεσίας (denial-of-service) (Mullins, 2020).

Επίπεδο σύνδεσης δεδομένων (Data link layer): Παραπλάνηση ή υποκλοπή διευθύνσεων MAC για απόκτηση μη εξουσιοδοτημένης πρόσβασης σε ένα δίκτυο (Mullins, 2020).

Επίπεδο δικτύου (Network layer): Αποστολή πακέτων IP με κακή μορφή ή πλαστές διευθύνσεις IP για να προκαλέσει επίθεση DoS ή να παραβιάσει μια περίοδο λειτουργίας. του (Imperva Application Security, 2023), (Mullins, 2020).

Επίπεδο μεταφοράς (Transport layer): Εκμετάλλευση τρωτών σημείων σε πρωτόκολλα TCP ή UDP για να προκαλέσει επίθεση DoS ή να εισαγάγει κακόβουλα δεδομένα (Imperva Application Security, 2023) (Mullins, 2020).

Επίπεδο συνεδρίας (Session layer:): Τερματισμός ή παραβίαση μιας συνεδρίας για διακοπή της επικοινωνίας ή κλοπή πληροφοριών. (Imperva Application Security, 2023) (Mullins, 2020)

Επίπεδο παρουσίασης (Presentation layer): Αποκρυπτογράφηση ή τροποποίηση κρυπτογραφημένων δεδομένων για να τεθεί σε κίνδυνο η εμπιστευτικότητα ή η ακεραιότητά τους (Mullins, 2020).

Επίπεδο εφαρμογής (Application layer): Τακτικές ηλεκτρονικού ψαρέματος (phishing), κακόβουλου λογισμικού (maware), SQL injection, δέσμης ενεργειών (scripting) μεταξύ τοποθεσιών web ή άλλων επιθέσεων που στοχεύουν συγκεκριμένες εφαρμογές ή χρήστες (Imperva Application Security, 2023) (Mullins, 2020).

ΜΕΘΟΔΟΙ ΑΜΥΝΑΣ

Για την προστασία από αυτές τις επιθέσεις, διάφορες υπηρεσίες και μηχανισμοί ασφαλείας μπορούν να εφαρμοστούν σε κάθε επίπεδο του μοντέλου OSI (riarawal99, 2023). Για παράδειγμα:

Φυσικό επίπεδο: Χρήση κλειδαριών ασφαλείας, συναγερμών, καμερών ή προσωπικού ασφαλείας για την εξασφάλιση φυσικής πρόσβασης σε συσκευές δικτύου (riarawal99, 2023).

Επίπεδο σύνδεσης δεδομένων: Χρήση κρυπτογράφησης, ελέγχου ταυτότητας ή φιλτραρίσματος MAC για την ασφάλεια πλαισίων δεδομένων στο δίκτυο (riarawal99, 2023).

Επίπεδο δικτύου: Χρήση τείχους προστασίας, VPN ή IPSec για την ασφάλεια των πακέτων δεδομένων στο δίκτυο (riarawal99, 2023).

Επίπεδο μεταφοράς: Χρήση SSL/TLS ή SSH για την ασφάλεια τμημάτων δεδομένων στο δίκτυο (riarawal99, 2023).

Επίπεδο περιόδου λειτουργίας: Χρήση cookies, tokens ή πιστοποιητικών για την ασφάλεια των περιόδων σύνδεσης στο δίκτυο (riarawal99, 2023).

Επίπεδο παρουσίασης: Χρήση κρυπτογράφησης, συμπίεσης ή κατακερματισμού για την ασφάλεια των δεδομένων στο δίκτυο (riarawal99, 2023).

Επίπεδο εφαρμογής: Χρήση προστασίας από ιούς, antispam, φίλτρα στον ιστό ή τείχη προστασίας για την ασφάλεια εφαρμογών στο δίκτυο (riarawal99, 2023).

Στην παρούσα εργασία θα ασχοληθούμε μόνο με την ασφάλεια στο φυσικό επίπεδο και συγκεκριμένα για συσκευές στο Internet of Things (Διαδίκτυο των αντικειμένων). Είναι σημαντικό να αναφερθούμε στο σχετικά πρόσφατο αυτό δίκτυο με την ραγδαία εξέλιξη καθώς και τις ιδιαιτερότητες του.

ΚΕΦΑΛΑΙΟ 2: ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΑΝΤΙΚΕΙΜΕΝΩΝ – ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

Το Διαδίκτυο των πραγμάτων (IoT) αναφέρεται στο δίκτυο συνδεδεμένων συσκευών και αισθητήρων που μπορούν να επικοινωνούν και να ανταλλάσσουν δεδομένα μεταξύ τους μέσω του Διαδικτύου. Αυτές οι συσκευές, συχνά ενσωματωμένες με αισθητήρες και ενεργοποιητές, μπορούν να συλλέγουν και να μεταδίδουν δεδομένα, να λαμβάνουν εντολές και να αλληλεπιδρούν με το περιβάλλον τους.

Η ιδέα πίσω από το IoT είναι να επιτρέψει στα καθημερινά αντικείμενα και συσκευές να γίνουν "έξυπνα", συνδέοντάς τα στο Διαδίκτυο, επιτρέποντάς τους να συλλέγουν και να μοιράζονται δεδομένα και να εκτελούν έξυπνες ενέργειες. Αυτή η συνδεσιμότητα και η ανταλλαγή δεδομένων ανοίγουν ένα ευρύ φάσμα δυνατοτήτων και εφαρμογών σε διάφορους τομείς, όπως έξυπνα σπίτια, υγειονομική περίθαλψη, μεταφορές, γεωργία, βιομηχανικός αυτοματισμός και πολλά άλλα.

Οι συσκευές IoT μπορεί να ποικίλουν από απλά αντικείμενα, όπως οικιακές συσκευές, wearables και περιβαλλοντικούς αισθητήρες, μέχρι σύνθετα συστήματα, όπως αυτόνομα οχήματα και έξυπνες πόλεις. Συνήθως χρησιμοποιούν τεχνολογίες ασύρματης επικοινωνίας, όπως Wi-Fi, Bluetooth ή κυψελοειδή δίκτυα, για να συνδεθούν στο Διαδίκτυο και να επικοινωνήσουν με άλλες συσκευές ή κεντρικές πλατφόρμες.

Τα δεδομένα που συλλέγονται από τις συσκευές IoT μπορούν να αναλυθούν και να υποβληθούν σε επεξεργασία για την απόκτηση πολύτιμων πληροφοριών, τη βελτιστοποίηση των διαδικασιών, τη βελτίωση της αποδοτικότητας, τη βελτίωση της λήψης αποφάσεων και την ενεργοποίηση νέων υπηρεσιών και εμπειριών. Ωστόσο, είναι σημαντικό να εξεταστούν και να αντιμετωπιστούν οι ανησυχίες για την ασφάλεια και την προστασία της ιδιωτικής ζωής που σχετίζονται με τις τεράστιες ποσότητες δεδομένων που παράγονται και μοιράζονται στο οικοσύστημα IoT.

Συνολικά, το Διαδίκτυο των πραγμάτων έχει τη δυνατότητα να φέρει επανάσταση στον τρόπο με τον οποίο αλληλεπιδρούμε με τον φυσικό κόσμο, να δημιουργήσει πιο συνδεδεμένα και αποδοτικά συστήματα και να μεταμορφώσει διάφορους κλάδους και πτυχές της καθημερινής μας ζωής.

Το Διαδίκτυο των Πραγμάτων (IoT), το οποίο ορίζεται ως το "παγκόσμιο δίκτυο διασυνδεδεμένων αντικειμένων" (C. Perera, 2014) επεκτείνει τη συνδεσιμότητα από την επικοινωνία ανθρώπου-μηχανής στην επικοινωνία μηχανής-μηχανής. Το IoT προσφέρει μεγάλης κλίμακας ενσωμάτωση ετερογενών δικτύων και συσκευών, η οποία εκτός από τις προφανείς ευκαιρίες, εισάγει και μεγάλες προκλήσεις για την ασφάλεια και την προστασία της ιδιωτικής ζωής. Οι προκλήσεις αυτές δεν είναι καινούργιες, καθώς έχουν μελετηθεί καλά στη σχετική βιβλιογραφία σε διάφορους τομείς του IoT (όπως η ηλεκτρονική υγεία, Smart City, Smart Grid) (Wei Zhou, 2018). Μεταξύ των διαφόρων προκλήσεων

ασφάλειας στο IoT, η πρόσβαση είναι μια κρίσιμη και ανοικτή πρόκληση (Green, 2015).

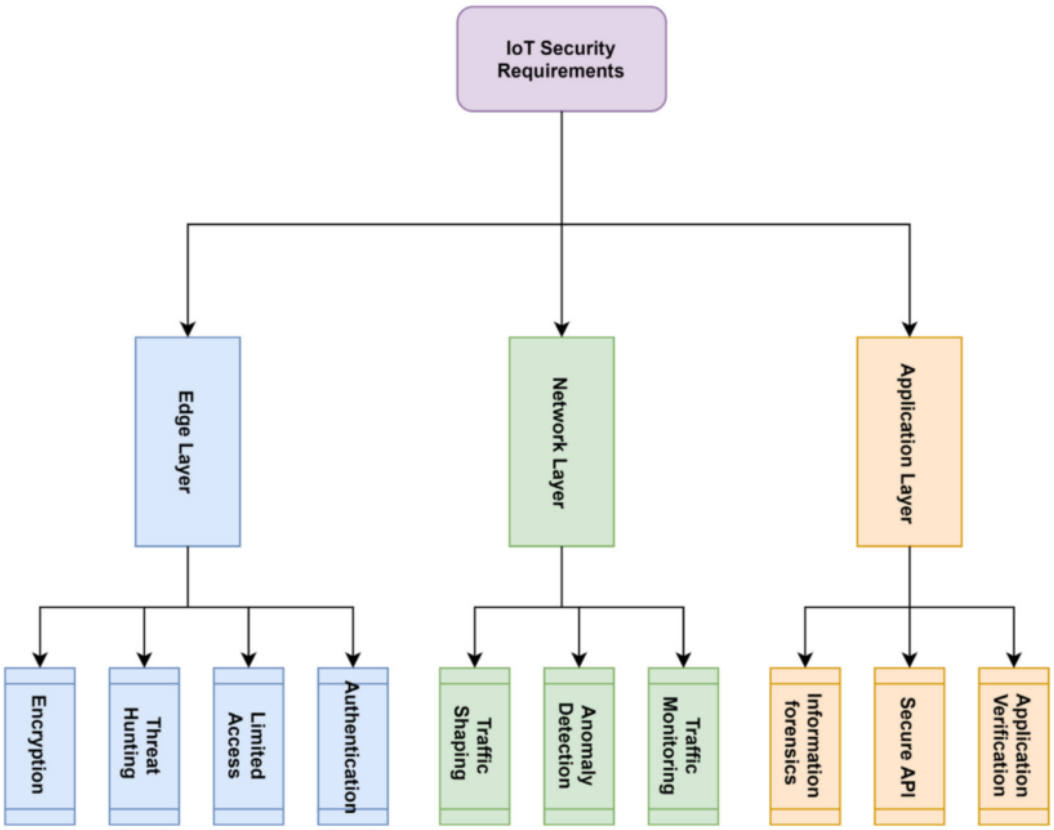
Εξ' αιτίας των μοναδικών χαρακτηριστικών του IoT, όπως η **επεκτασιμότητα**, η **ετερογένεια**, η **διαλειτουργικότητα**, ο **δυναμισμός** και η **κοινή χρήση πόρων** πολλαπλασιάζονται οι προκλήσεις ασφαλείας σχετικά με την πρόσβαση στον έλεγχο και την διαχείριση τέτοιων δικτύων. Αυτό ισχύει ως εξής:

Η **επεκτασιμότητα** πηγάζει από την εκθετική ανάπτυξη του IoT που έχει επίσης ως αποτέλεσμα χιλιάδες συσκευές να συνδέονται συνεχώς στο δίκτυο. Σύμφωνα με την Gartner, ο αριθμός των συσκευών που συνδέονται στο Διαδίκτυο θα φτάσουν τα 20–50 δισεκατομμύρια συσκευές μέχρι το 2020 (Nordrum, 2016). Ως αποτέλεσμα, αυτό μεγιστοποιεί τις προκλήσεις ασφάλειας στο IoT απαιτώντας περισσότερη προσπάθεια και πόρους που απαιτούνται για τους ελέγχους ασφαλείας (όπως ο μηχανισμός ελέγχου πρόσβασης) για την αντιμετώπισή τους (Yuankun Xue, 2017)

Η **ετερογένεια** και η **διαλειτουργικότητα** στο IoT προέρχονται από τις διαφορετικές τεχνολογίες και δίκτυα (όπως RFID, WSN, GSM) που υπάρχουν στο IoT. Συνεπώς, η δυνατότητα απρόσκοπτης λειτουργίας και ασφαλή ενσωμάτωση αυτών των διαφορετικών πλατφορμών αποτελεί πρόκληση, καθώς ο βαθμός πολυπλοκότητας αυξάνεται δραματικά όταν διαφορετικές τεχνολογίες συγχωνεύονται για να σχηματίζουν ένα πολύπλοκο ενιαίο δίκτυο. Ομοίως, η **διαλειτουργικότητα** φέρνει νέες προκλήσεις στον τομέα του ελέγχου πρόσβασης στα δεδομένα (Giaffreda, Capra, & Antonelli, 2016). Για παράδειγμα στην επικοινωνία οχημάτων που κινούνται από έναν γεωγραφικό τομέα (π.χ. Ηνωμένο Βασίλειο) σε έναν άλλο (π.χ. Γαλλία) μπορεί να προκληθεί πρόβλημα πρόσβασης στα δεδομένα, λόγω των προβλημάτων διαλειτουργικότητας μεταξύ υποδομών δημόσιου κλειδιού μεταξύ των διαφορετικών περιοχών αυτών. (Li, Qi, & Lu, 2017)

Ο **δυναμισμός** στο IoT πηγάζει από το γεγονός ότι τα διασυνδεδεμένες συσκευές πρέπει να αλληλεπιδρούν μεταξύ τους σε πραγματικό χρόνο. Ως εκ τούτου, η ανάγκη για μια κατάλληλη ανταπόκριση στις ταχείες αλλαγές του φυσικού κόσμου που προκαλούνται από αυτές τις αλληλεπιδράσεις θέτουν νέες τεχνολογικές προκλήσεις όχι μόνο για τον έλεγχο της πρόσβασης, αλλά επίσης για την ανάγκη οι παρεχόμενες υπηρεσίες να είναι σχετικές με τον χρήστη. (Bo Cheng, 2017)

Η **κοινή χρήση πόρων** σε διαφορετικές εφαρμογές του IoT (π.χ. έξυπνα δίκτυα, έξυπνη πόλη) είναι αναπόφευκτη [13, 14]. Για παράδειγμα, η κοινή χρήση πόρων σε διαφορετικά δικτυακά περιβάλλοντα δίνουν μεγαλύτερη αξία σε αυτές τις υλοποιήσεις , βελτιώνοντας την απόδοση των εμπλεκόμενων, με λιγότερους πόρους. Εκτός από τα πλεονεκτήματα τίθενται όμως και θέματα ασφαλείας και από εσωτερικές απειλές. (Sadegh Dorri, 2016). Οι ίδιες απειλές μπορούν να επεκταθούν στην έξυπνη πόλη, όπου για παράδειγμα μοιράζονται πληροφορίες για την κυκλοφορία δύο ή περισσότερων οχημάτων (π.χ. πληροφορίες σχετικά με τις θέσεις τους). (Jiawen Kang).



Σχήμα 4: Ταξινόμηση απαιτήσεων ασφαλείας βασισμένη στα επίπεδα που συμμετέχουν.

ΚΙΝΔΥΝΟΙ ΣΤΟ IOT – ΕΙΔΗ ΕΠΙΘΕΣΕΩΝ

Όπως είδαμε στην προηγούμενη ενότητα στο διαδίκτυο των πραγμάτων τα ιδιαίτερα χαρακτηριστικά του IOT, όπως η ετερογένεια, ο δυναμισμός και η κοινή χρήση πόρων αυξάνουν την πολυπλοκότητα του δικτύου και το κάνουν ποιο ευάλωτο σε επιθέσεις. Το IOT εμφανίζει μερικά σημαντικά ζητήματα ασφάλειας. Οι βασικοί κίνδυνοι του IoT περιλαμβάνουν ευπάθειες του δικτύου και ξεπερασμένο λογισμικό (software) και υλικολογισμικό (firmware) (Shea, 2022). Συχνά υπάρχουν ευπάθειες γύρω από την ασφάλεια των νέων υποδομών του IoT και κενά στην προστασία των παλαιών συστημάτων που μπορεί να συνδέονται σε νεότερα ανοικτά περιβάλλοντα. Στην περίπτωση αυτή, η παραβίαση μιας συσκευής IoT μπορεί να οδηγήσει ακόμη και σε μη εξουσιοδοτημένη πρόσβαση στα παλαιά συστήματα. (THELES, 2022).

Ενώ οι περισσότεροι από τους κινδύνους των ζητημάτων ασφάλειας του IoT εξακολουθούν να απασχολούν τους κατασκευαστές των υποδομών και των έξυπνων συσκευών, οι χρήστες και οι επιχειρήσεις μπορούν να δημιουργήσουν μεγαλύτερες απειλές. Ένας από τους μεγαλύτερους κινδύνους και προκλήσεις για την ασφάλεια του IoT είναι η άγνοια και η έλλειψη ευαισθητοποίησης των

χρηστών σχετικά με τη λειτουργικότητα και τους κινδύνους του IoT, ως αποτέλεσμα, όλοι τίθενται σε κίνδυνο (intellectsoft, 2020).

Τον Οκτώβριο του 2016, ένας χάκερ βρήκε μια ευπάθεια σε ένα συγκεκριμένο μοντέλο καμερών ασφαλείας. Σχεδόν 300.000 βιντεοκάμερες του Διαδικτύου των Πραγμάτων (IoT) ενεργοποιήθηκαν και κατέγραφαν σε πολλούς ιστότοπους κοινωνικής δικτύωσης και τελικά έριξαν το Twitter και άλλες πλατφόρμες υψηλού προφίλ για σχεδόν δύο ώρες. Αυτή η επίθεση είναι μόνο ένα παράδειγμα του τι μπορεί να συμβεί σε συσκευές IoT με ανεπαρκή ασφάλεια. Η έλλειψη συμμόρφωσης εκ μέρους των κατασκευαστών IoT οδήγησε σε αδύναμους και μη προστατευμένους κωδικούς πρόσβασης σε ορισμένες βιντεοκάμερες IoT, οι οποίοι, με τη σειρά τους, οδήγησαν σε μία από τις πιο επιζήμιες επιθέσεις botnet, το κακόβουλο λογισμικό Mirai.

Για να προστατευτούν οι συσκευές IoT, πρέπει να ακολουθηθούν οι παρακάτω οδηγίες:

- Αλλαγή των προεπιλεγμένων κωδικών πρόσβασης
- Να διατηρείτε το λογισμικό ενημερωμένο
- Χρήση ισχυρής κρυπτογράφησης
- Να χρησιμοποιείτε έλεγχος ταυτότητας δύο παραγόντων
- Να απενεργοποιηθούν οι περιττές λειτουργίες
- Χρήση VPN4

Υπάρχουν πολλές απειλές για την ασφάλεια του IoT, αλλά θα επισημάνουμε τις πιο σημαντικές:

Έλλειψη συμμόρφωσης εκ μέρους των κατασκευαστών IoT.

Νέες συσκευές IoT κυκλοφορούν σχεδόν καθημερινά, όλες με τρωτά σημεία που δεν έχουν διερευνηθεί. Η κύρια πηγή των περισσότερων προβλημάτων ασφάλειας του IoT είναι ότι οι κατασκευαστές δεν αφιερώνουν αρκετό χρόνο και πόρους στην ασφάλεια. Όσο δεν υπάρχουν καθολικά πρότυπα ασφαλείας IoT, οι κατασκευαστές θα συνεχίσουν να δημιουργούν συσκευές με ανεπαρκή ασφάλεια. Οι κατασκευαστές που πρόσθεσαν την ικανότητα σύνδεσης στο Διαδίκτυο στις συσκευές τους δεν έχουν πάντα την έννοια της "ασφάλειας" ως το κρίσιμο στοιχείο στη διαδικασία σχεδιασμού των προϊόντων τους αλλά την συνδεσιμότητα.

Έλλειψη γνώσης και ευαισθητοποίησης των χρηστών

Με την πάροδο των ετών, οι χρήστες του Διαδικτύου έχουν μάθει πώς να αποφεύγουν τα μηνύματα spam ή phishing, να πραγματοποιούν σαρώσεις για ιούς στους υπολογιστές τους και να ασφαλίζουν τα δίκτυα WiFi με ισχυρούς κωδικούς πρόσβασης. Αλλά το IoT είναι μια νέα τεχνολογία και οι άνθρωποι δεν γνωρίζουν ακόμη πολλά γι' αυτό. Ενώ οι περισσότεροι κίνδυνοι από τα ζητήματα ασφάλειας του IoT εξακολουθούν να αφορούν την πλευρά του κατασκευαστή, οι απλοί χρήστες και οι επιχειρήσεις μπορούν να

δημιουργήσουν ακόμη μεγαλύτερες απειλές. Ένας από τους μεγαλύτερους κινδύνους και προκλήσεις για την ασφάλεια του IoT είναι η άγνοια και η έλλειψη ενημέρωσης των χρηστών σχετικά με τη λειτουργικότητα του IoT. Ως αποτέλεσμα, όλοι τίθενται σε κίνδυνο.

Η εξαπάτηση ενός ανθρώπου είναι, τις περισσότερες φορές, ο ευκολότερος τρόπος για να αποκτήσει κάποιος πρόσβαση σε ένα δίκτυο. Ένας τύπος κινδύνου ασφαλείας του IoT που συχνά παραβλέπεται είναι οι επιθέσεις εναντίον των χειριστών των μηχανών. Αντί να στοχεύει συσκευές, ένας χάκερ στοχεύει έναν άνθρωπο, χρησιμοποιώντας το IoT. Η προσέγγιση αυτή χρησιμοποιήθηκε στην επίθεση Stuxnet του 2010 εναντίον μιας πυρηνικής εγκατάστασης στο Ιράν. Η επίθεση απευθυνόταν σε βιομηχανικούς προγραμματιζόμενους λογικούς ελεγκτές (PLC), οι οποίοι επίσης εμπίπτουν στην κατηγορία συσκευών IoT. Η επίθεση κατέστρεψε 1.000 φυγοκεντρικές μηχανές και έκανε το εργοστάσιο να είναι έτοιμο να εκραγεί. Παρόλο που πίστευαν ότι είναι ασφαλείς, διότι το εσωτερικό δίκτυο ήταν απομονωμένο από το δημόσιο δίκτυο για την αποφυγή επιθέσεων, αλλά το μόνο που χρειάστηκε ήταν ένας εργαζόμενος να συνδέσει ένα μολυσμένο USB flash drive σε έναν από τους εσωτερικούς υπολογιστές.

Προβλήματα ασφάλειας μη ενημερωμένων λογισμικών συσκευών IoT

Μια άλλη πηγή κινδύνων για την ασφάλεια του IoT είναι το μη ασφαλές λογισμικό ή υλικολογισμικό. Παρόλο που ένας κατασκευαστής μπορεί να πουλήσει μια συσκευή με την τελευταία ενημέρωση λογισμικού, είναι σχεδόν αναπόφευκτο να εμφανιστούν νέα τρωτά σημεία. Οι ενημερώσεις είναι ζωτικής σημασίας για τη διατήρηση της ασφάλειας στις συσκευές IoT. Θα πρέπει να ενημερώνονται αμέσως μετά την ανακάλυψη νέων ευπαθειών. Παρόλα αυτά, σε σύγκριση με τα smartphones ή τους υπολογιστές που λαμβάνουν αυτόματες ενημερώσεις, ορισμένες συσκευές IoT συνεχίζουν να χρησιμοποιούνται χωρίς τις απαραίτητες ενημερώσεις. Ένας άλλος κίνδυνος είναι ότι κατά τη διάρκεια μιας ενημέρωσης, μια συσκευή θα στείλει το αντίγραφο ασφαλείας της στο σύννεφο και θα υποστεί μια σύντομη διακοπή λειτουργίας. Εάν η σύνδεση δεν είναι κρυπτογραφημένη και τα αρχεία ενημέρωσης είναι απροστάτευτα, ένας χάκερ θα μπορούσε να κλέψει ευαίσθητες πληροφορίες.

Έλλειψη φυσικής προστασίας της συσκευής

Η έλλειψη φυσικής προστασίας μπορεί επίσης να προκαλέσει προβλήματα ασφάλειας του IoT. Παρόλο που ορισμένες συσκευές IoT θα πρέπει να μπορούν να λειτουργούν αυτόνομα χωρίς καμία παρέμβαση από τον χρήστη, πρέπει να είναι φυσικά ασφαλισμένες από εξωτερικές απειλές. Μερικές φορές, οι συσκευές αυτές μπορεί να βρίσκονται σε απομακρυσμένες τοποθεσίες για μεγάλα χρονικά διαστήματα και θα μπορούσαν να υποστούν φυσική παρέμβαση, για παράδειγμα, με τη χρήση μιας μονάδας USB flash με κακόβουλο λογισμικό. Η διασφάλιση της φυσικής ασφάλειας μιας συσκευής IoT ξεκινά από τον κατασκευαστή. Όμως η κατασκευή ασφαλών αισθητήρων και

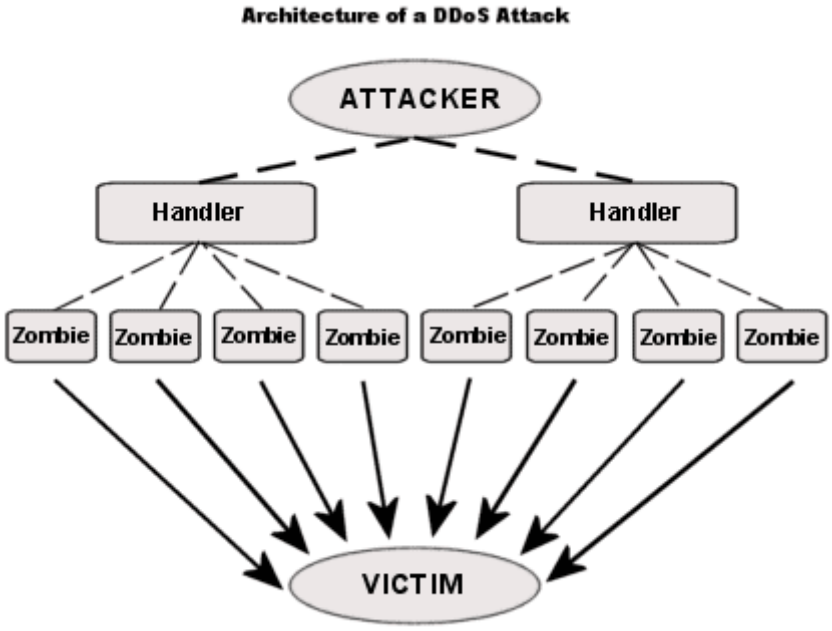
πομπών στις ήδη χαμηλού κόστους συσκευές αποτελεί παρ' όλα αυτά ένα δύσκολο έργο για τους κατασκευαστές. Οι χρήστες είναι επίσης υπεύθυνοι για τη διατήρηση της φυσικής ασφάλειας των συσκευών IoT. Ένας έξυπνος αισθητήρας κίνησης ή μια βιντεοκάμερα που βρίσκεται έξω από ένα σπίτι θα μπορούσε να αλλοιωθεί εάν δεν προστατεύεται επαρκώς.

Επιθέσεις botnet

Μια μεμονωμένη συσκευή IoT που έχει μολυνθεί με κακόβουλο λογισμικό δεν αποτελεί πραγματική απειλή, αλλά ένα υπο-σύνολο από αυτές τις μολυσμένες συσκευές μπορεί να προκαλέσει την κατάρρευση του συνόλου των συσκευών. Για να πραγματοποιήσει μια επίθεση botnet, ένας χάκερ δημιουργεί έναν στρατό από bots μολύνοντάς τα με κακόβουλο λογισμικό και τα κατευθύνει να στέλνουν χιλιάδες αιτήματα ανά δευτερόλεπτο ώστε ο στόχος να μην μπορεί να εξυπηρετήσει τα αιτήματα και τελικά να βγαίνει εκτός λειτουργίας.

Μεγάλο μέρος της αναταραχής σχετικά με την ασφάλεια του IoT ξεκίνησε μετά την επίθεση του bot Mirai το 2016. Πολλαπλές επιθέσεις DDoS (Distributed Denial of Service) με τη χρήση εκατοντάδων χιλιάδων καμερών IP, NAS και οικιακών δρομολογητών μολύνθηκαν και κατευθύνθηκαν για να ρίξουν το DNS που παρείχε υπηρεσίες σε πλατφόρμες όπως το GitHub, το Twitter, το Reddit, το Netflix και το Airbnb.

Το πρόβλημα είναι ότι οι συσκευές IoT είναι ιδιαίτερα ευάλωτες σε επιθέσεις κακόβουλου λογισμικού. Δεν έχουν τις τακτικές ενημερώσεις ασφαλείας λογισμικού που έχει ένας υπολογιστής. Έτσι μετατρέπονται γρήγορα σε μολυσμένες συσκευές «ζόμπι» και χρησιμοποιούνται ως όπλα για την αποστολή απίστευτα μεγάλων ποσοτήτων δεδομένων αυξάνοντας την κυκλοφορία του δικτύου.



Σχήμα 5: Αρχιτεκτονική μιας επίθεσης DDos

Επιπλέον, ένα botnet μπορεί να αποτελέσει απειλή για την ασφάλεια ηλεκτρικών δικτύων, εργοστασίων παραγωγής, συστημάτων μεταφορών και εγκαταστάσεων επεξεργασίας νερού, γεγονός που μπορεί να απειλήσει μεγάλες ομάδες ανθρώπων. Για παράδειγμα, ένας χάκερ θα μπορούσε να ενεργοποιήσει ταυτόχρονα ένα σύστημα ψύξης και θέρμανσης, δημιουργώντας αιχμές στο δίκτυο ηλεκτρικής ενέργειας- σε περίπτωση επίθεσης μεγάλης κλίμακας, οι χάκερ μπορούν να δημιουργήσουν διακοπή ρεύματος σε εθνικό επίπεδο.

Βιομηχανική κατασκοπεία & υποκλοπή

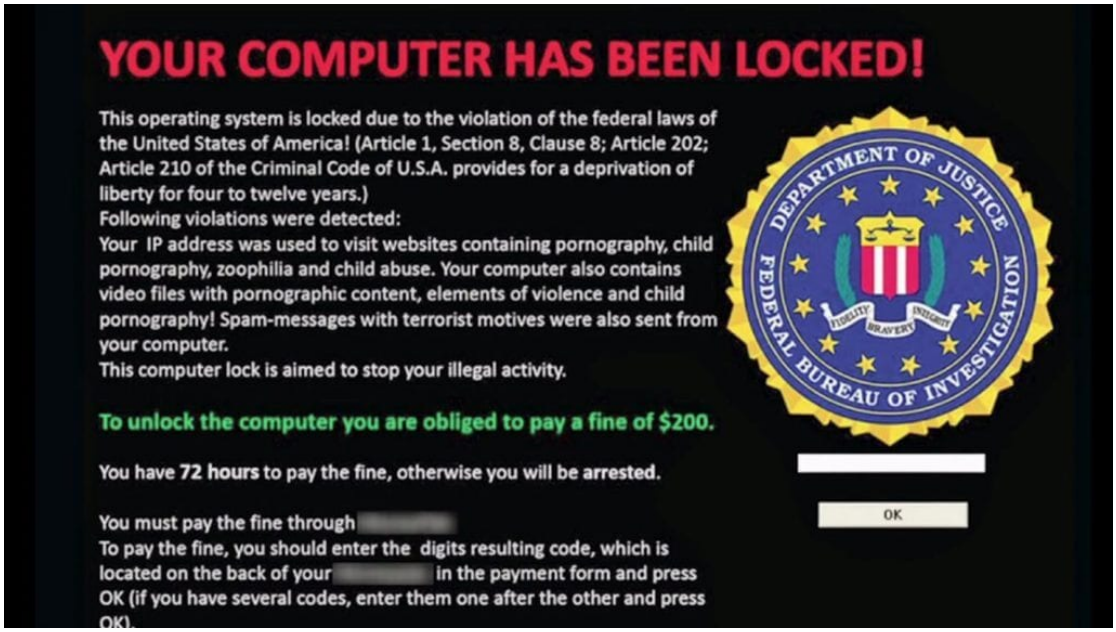
Εάν οι χάκερς διεισδύσουν σε μια υποδομή μολύνοντας συσκευές IoT, η υποκλοπή δεδομένων μπορεί να μην είναι η μόνη επικίνδυνη συνέπεια. Μπορούν επίσης να πραγματοποιήσουν τέτοιου είδους επιθέσεις με απαγωγές για να ζητήσουν λύτρα . Συνεπώς, η παραβίαση της ιδιωτικότητας είναι ένα άλλο εξέχον ζήτημα στην ασφάλεια στο IoT. Η παρακολούθηση και η διείσδυση μέσω συσκευών IoT είναι ένα πραγματικό πρόβλημα, καθώς ποικίλα ευαίσθητα δεδομένα μπορεί να παραβιαστούν και να χρησιμοποιηθούν εναντίον του ιδιοκτήτη τους.

Σε πρώτη φάση, ένας χάκερ μπορεί να θέλει να καταλάβει μια κάμερα και να τη χρησιμοποιήσει για παρακολούθηση. Ακόμα, δεν πρέπει να ξεχνάμε ότι πολλές συσκευές IoT καταγράφουν πληροφορίες του χρήστη, είτε πρόκειται για εξοπλισμό υγείας, έξυπνα παιχνίδια, wearables κ.λπ. Σε βιομηχανικό επίπεδο, τα δεδομένα μιας εταιρείας μπορούν να συλλεχθούν από χάκερ για να εκθέσουν ευαίσθητες επιχειρηματικές πληροφορίες.

Ορισμένες χώρες αρχίζουν να απαγορεύουν συγκεκριμένες συσκευές IoT με προβλήματα ασφαλείας. Για παράδειγμα, η διαδραστική κούκλα IoT με συσκευή Bluetooth, η οποία έδινε πρόσβαση στο μικρόφωνο και το ηχείο του παιχνιδιού σε οποιονδήποτε βρισκόταν σε ακτίνα 25-30 μέτρων. Η κούκλα χαρακτηρίστηκε ως συσκευή που επέτρεπε την παρακολούθηση και απαγορεύτηκε στη Γερμανία.

Πειρατεία στις συσκευές IoT

Το Ransomware έχει χαρακτηρισθεί ως ένας από τους πιο επικίνδυνους τύπους κακόβουλου λογισμικού που υπήρξαν ποτέ. Το Ransomware δεν καταστρέφει τα ευαίσθητα αρχεία σας – αλλά μπλοκάρει την πρόσβαση σε αυτά μέσω κρυπτογράφησης. Στη συνέχεια, ο χάκερ που μόλυνε τη συσκευή απαιτούσε λύτρα για το κλειδί αποκρυπτογράφησης που θα ξεκλειδώσει τα αρχεία. Εάν ο υπολογιστής σας μολυνθεί με ransomware θα εμφανιστεί ένα μήνυμα της ακόλουθης μορφής που θα σας ενημερώνει ότι έχουμε μολυνθεί και οδηγίες πληρωμής για να ξεκλειδωθεί το υπολογιστικό σας σύστημα.



Σχήμα 6: Ο υπολογιστής είναι θύμα επιθέσεως και είναι κλειδωμένος

Οι επιθέσεις Ransomware στοχεύουν και σε συσκευές IoT με ανεπαρκή ασφάλεια οι οποίες μπορούν επίσης να αποτελέσουν στόχους.

Λίγο πριν από την ομιλία για την ορκωμοσία του Τραμπ, περίπου το 70% των καμερών παρακολούθησης της Ουάσινγκτον μολύνθηκαν με ransomware, αφήνοντας την αστυνομία χωρίς τη δυνατότητα καταγραφών για αρκετές ημέρες.

Οι περιπτώσεις συσκευών IoT που μολύνονται με ransomware δεν είναι συνηθισμένες, αλλά υπάρχει μια αυξανόμενη τάση στην κοινότητα των hackers. Ακόμα, τα wearables, τα gadgets υγειονομικής περίθαλψης, τα έξυπνα σπίτια και άλλες έξυπνες συσκευές και οικοσυστήματα ενδέχεται να στοχοποιηθούν και να κινδυνεύσουν στο μέλλον.

Εδώ, υπάρχουν καλά νέα και κακά νέα. Ενώ το συγκεκριμένο κακόβουλο λογισμικό (Ransomware) μπορεί να μην βρίσκει πολύτιμα δεδομένα για να κλειδώσει, επειδή οι περισσότερες πληροφορίες IoT αποθηκεύονται στο cloud και όχι στην συσκευή, μπορεί όμως να κλειδώσει τη λειτουργικότητα ολόκληρης της συσκευής και να την βγάλει εκτός λειτουργίας. Φανταστείτε ότι το όχημά σας δεν θα εκκινείτε όταν το χρειάζεστε αν δεν πληρώσετε λύτρα - ή ότι το σπίτι σας θα είναι κλειδωμένο, με τον θερμοστάτη ή το φούρνο ρυθμισμένο στο μέγιστο.

Κίνδυνοι ακεραιότητας δεδομένων σε συσκευές IoT με εφαρμογή στην υγεία

Με το IoT, τα δεδομένα βρίσκονται πάντα σε κίνηση. Μεταδίδονται, αποθηκεύονται και υποβάλλονται σε επεξεργασία. Οι περισσότερες συσκευές IoT εξάγουν και συλλέγουν πληροφορίες από το εξωτερικό περιβάλλον. Μπορεί να είναι ένας έξυπνος θερμοστάτης, HVAC, τηλεοράσεις, ιατρικές συσκευές.

Αλλά μερικές φορές αυτές οι συσκευές στέλνουν τα δεδομένα που συλλέγονται στο cloud χωρίς καμία κρυπτογράφηση. Ως αποτέλεσμα, ένας χάκερ μπορεί να αποκτήσει πρόσβαση σε μια ιατρική συσκευή IoT, να αποκτήσει τον έλεγχό της και να είναι σε θέση να μεταβάλει τα δεδομένα που συλλέγει. Μια παραβιασμένη ιατρική συσκευή IoT μπορεί να χρησιμοποιηθεί για την αποστολή ψευδούς πληροφορίας, η οποία με την σειρά της μπορεί να προκαλέσει τους επαγγελματίες υγείας να προβούν σε ενέργειες που μπορεί να βλάψουν την υγεία των ασθενών τους.

Για παράδειγμα, μια παραβιασμένη ιατρική συσκευή IoT μπορεί να αναφέρει μια πλήρως φορτισμένη μπαταρία στο σταθμό παρακολούθησης, ενώ στην πραγματικότητα η μπαταρία να είναι έτοιμη να αδειάσει και να μην μπορεί η συσκευή πλέον να υποστηρίξει τον ασθενή. Ακόμα χειρότερα, υπάρχουν κίνδυνοι για την ασφάλεια του IoT σε συσκευές υγειονομικής περίθαλψης, όπως οι βηματοδότες ή αυτές που κάνουν τις ενέσεις ινσουλίνης. Οι ευπάθειες που βρέθηκαν στα εμφυτεύματα καρδιάς της St. Jude Medical έδωσαν πρόσβαση σε χάκερ, επιτρέποντάς τους να επηρεάσουν την λειτουργία του βηματοδότη ή να προκαλέσουν ηλεκτροσόκ ή ακόμη χειρότερα, να εξαντλήσουν την μπαταρία, οπότε και θα σταματούσε η λειτουργία της συσκευής υποστήριξης και θα πέθαινε ο ασθενής.

Παραβιασμένες - Παράνομες συσκευές IoT

Ίσως γνωρίζουμε ήδη, την ταχεία αύξηση του αριθμού των συσκευών IoT, ο οποίος προβλέπεται να φτάσει τα 18 δισεκατομμύρια μέχρι το 2022, σύμφωνα με την Ericsson. Ένας από τους σημαντικότερους κινδύνους και προκλήσεις για την ασφάλεια του IoT είναι να μπορούμε να διαχειριστούμε όλες τις συσκευές και να κλείσουμε την περίμετρο από είσοδο επικίνδυνων συσκευών. Όμως, οι παραβιασμένες συσκευές ή οι κακόβουλες συσκευές IoT αρχίζουν να εγκαθίστανται σε ασφαλή δίκτυα χωρίς εξουσιοδότηση. Μια επιβλαβής συσκευή αντικαθιστά μια άλλη ή ενσωματώνεται, χωρίς εξουσιοδότηση, ως μέλος μιας ομάδας για να συλλέξει ή να αλλοιώσει ευαίσθητες πληροφορίες. Αυτές οι συσκευές παραβιάζουν την ασφάλεια του δικτύου και καθιστούν το δίκτυο επικίνδυνο.

Παράδειγματα τέτοιων συσκευών επικίνδυνων για το IoT μπορεί να είναι το Raspberry Pi ή το WiFi Pineapple. Αυτές μπορούν να μετατραπούν σε ένα AP (Access Point), θερμοστάτη, βιντεοκάμερα κ.α. και να υποκλέψουν τις εισερχόμενες επικοινωνίες δεδομένων εν αγνοία των χρηστών. Στο μέλλον ενδέχεται να εμφανιστούν και άλλες παραλλαγές αυτών των επικίνδυνων συσκευών.

Ενδιαφέρον έχει η παλιά ταινία τρόμου "Child's Play" που είναι εμπνευσμένη από την ιδέα της συσκευής που παραβιάζει ένα ασφαλές δίκτυο. Στην ταινία, ο Chucky είναι μια κακόβουλη συσκευή IoT που έχει πάρει τον έλεγχο από άλλες συσκευές σε ένα έξυπνο οικιακό σύστημα και έχει γίνει μια υψηλού επιπέδου απειλή για τις ζωές των ανθρώπων του σπιτιού.

Cryptomining with IoT Bots

Η εξόρυξη κρυπτονομισμάτων απαιτεί τεράστιους πόρους CPU και GPU, και ένα άλλο ζήτημα ασφάλειας στο IoT έχει προκύψει λόγω αυτής της προϋπόθεσης - Cryptomining με bots IoT συσκευές. Αυτός ο τύπος επίθεσης περιλαμβάνει μολυσμένα botnets που στοχεύουν σε συσκευές IoT, με στόχο όχι να δημιουργήσουν ζημιά, αλλά να εξορύξουν cryptocurrency.

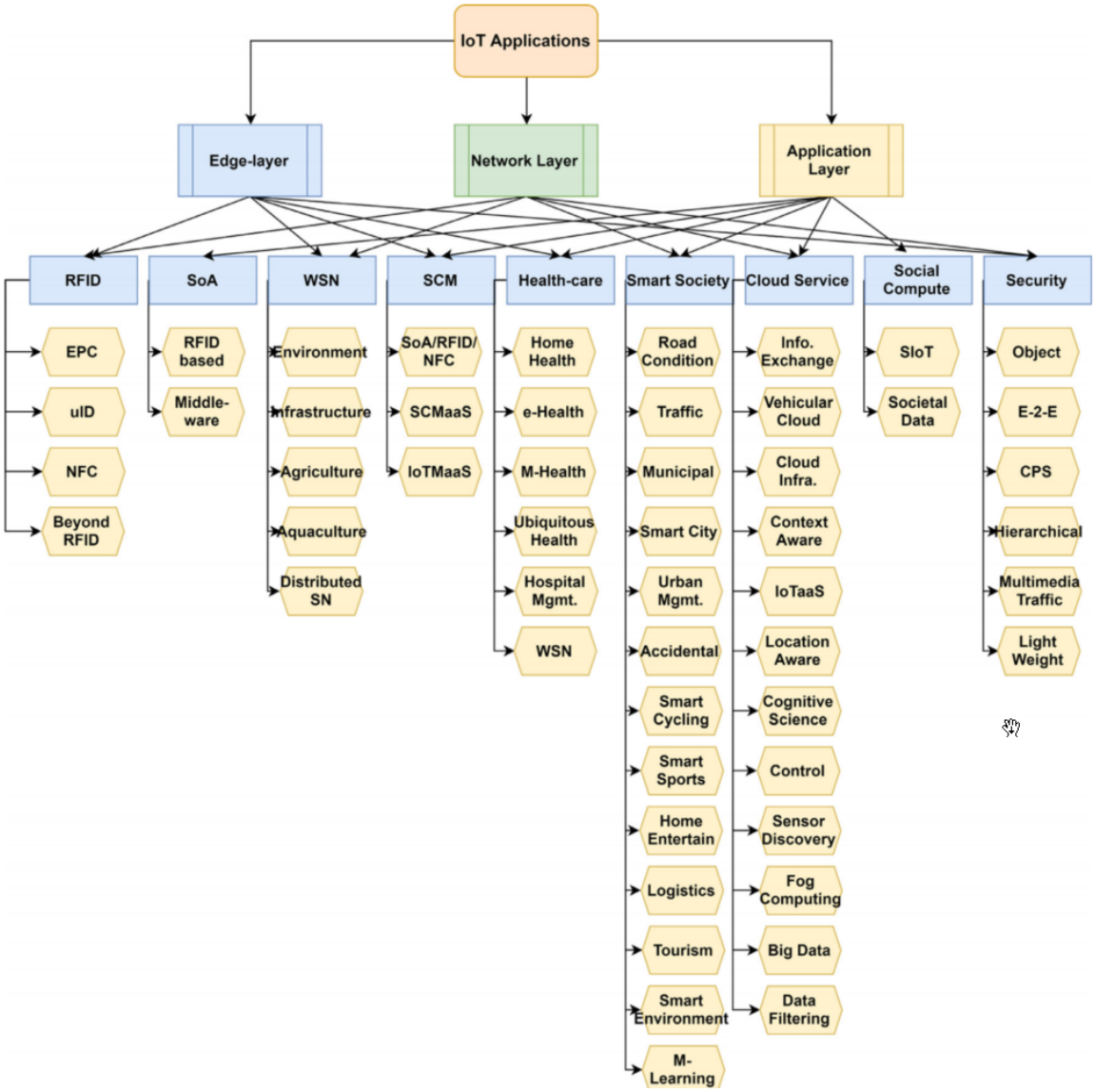
Το κρυπτονόμισμα ανοικτού κώδικα Monero έπεσε θύμα επίθεσης ενός botnets, χρησιμοποιώντας μολυσμένες συσκευές IoT, όπως κάμερες βίντεο. Αν και μια βιντεοκάμερα δεν έχει ισχυρούς πόρους για την εξόρυξη cryptocurrency, ένας στρατός τους επιτυγχάνει τον σκοπό.

Οι κυνηγοί κρυπτο-νομισμάτων botnet IoT αποτελούν μεγάλη απειλή για την αγορά κρυπτο-νομισμάτων , καθώς έχουν τη δυνατότητα να πλημμυρίσουν και να διαταράξουν ολόκληρη την αγορά σε μία μόνο επίθεση.

ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΕ ΚΑΘΕ ΚΑΤΗΓΟΡΙΑ ΥΛΟΠΟΙΗΣΗΣ IOT

Για τον περιορισμό των απειλών στον κυβερνοχώρο σε διάφορες εφαρμογές του IoT, πρέπει να προβλεφθούν κατάλληλα οι απαιτήσεις ασφαλείας. Η παρούσα ενότητα προτείνει αρχικά μια ταξινόμηση των εφαρμογών IoT με βάση τον βαθμό εμπλοκής σε κάθε επίπεδο. Στη συνέχεια, παρέχει τις βασικές απαιτήσεις ασφάλειας από την αρχιτεκτονική που βασίζεται σε επίπεδα.

Δεδομένου ότι κάθε συσκευή του IoT είναι σε θέση να λειτουργεί χωρίς καμία παρέμβαση τρίτων, ο ρόλος και η συμπεριφορά της πρέπει να καθοριστεί σε κάθε ημιαυτόματο ή πλήρως αυτοματοποιημένο περιβάλλον αντίστοιχα. Η υγειονομική περίθαλψη, οι μεταφορές και οι αυτοκινητοβιομηχανίες ήταν οι πρώτοι τομείς που υλοποίησαν εφαρμογές στο IoT με μεγάλο ενδιαφέρον.



Σχήμα 7: Ταξινόμηση Εφαρμ. IoT βασισμένες στον τομέα εφαρμογή τους.

Παράλληλα, υιοθετήθηκε μια κατηγοριοποίηση για την παροχή ταξινόμησης (Ray, 2018) των τριών επιπέδων (Edge-layer, Network Layer, Application Layer) για τις εφαρμογές του IoT. Όπως φαίνεται στο παραπάνω σχήμα, οι περισσότερες εφαρμογές του IoT χωρίζονται σε εννέα κλάσεις, ήτοι: Radio Frequency Identification (RFID) oriented application, Service-oriented Application (SoA), Wireless Sensor Network (WSN), Supply Chain Management(SCM), Healthcare που περιλαμβάνει (m-health and e-health), Smart Society, Cloudbased Services, Social compute and Security. Κάθε μία από αυτές τις κλάσεις ανήκει αποκλειστικά στον τομέα για τον οποίο υλοποιήθηκαν οι εφαρμογές της. Κάθε όμως κλάση μπορεί να εμπλέκεται με ένα ή περισσότερα επίπεδα της αρχιτεκτονικής του IoT (Edge-layer, Network Layer, Application Layer). Αυτές οι κλάσεις περιγράφονται ως εξής:

Radio Frequency Identification

Η σύνδεση των αντικειμένων με την τεχνολογία αναγνώρισης ραδιοσυχνοτήτων είναι γνωστή τεχνολογία από τις αρχές της δεκαετίας του 2000, οι ερευνητές τώρα πιστεύουν ότι αυτή η αρχιτεκτονική σχετίζεται με το περιβάλλον IoT (X. Jia, 2012). Η τεχνολογία RFID έχει μεγάλη σχέση με το επίπεδα Edge Layer για την αλληλεπίδραση με το περιβάλλον και το Network Layer για τη διαχείριση της επικοινωνίας. Για να έχουμε όμως λειτουργικές και ασφαλείς υλοποιήσεις, αυτός ο μηχανισμός ασφαλείας δύο επιπέδων πρέπει να επιβεβαιωθεί.

Service Oriented Application

Μια Service Oriented Application(Εφαρμογή Εστιασμένη στις Υπηρεσίες) (SOA) είναι μια αρχιτεκτονική λογισμικού που σχεδιάζεται για να υποστηρίξει ευέλικτες και ανεξάρτητες υπηρεσίες που συνεργάζονται μεταξύ τους. Σε μια SOA, το σύστημα αποτελείται από διαφορετικές υπηρεσίες που επικοινωνούν μεταξύ τους μέσω πρωτοκόλλων και διεπαφών για να επιτύχουν τις λειτουργικές και επιχειρησιακές απαιτήσεις της εφαρμογής. Στην αρχιτεκτονική SOA, οι υπηρεσίες θεωρούνται πυρήνας του συστήματος, και είναι σχεδιασμένες να είναι ανεξάρτητες και επαναχρησιμοποιήσιμες, παρέχοντας λειτουργικότητα ή ακόμη και δεδομένα στους άλλους πελάτες ή υπηρεσίες που τις καλούν. Κάθε υπηρεσία παρέχει μια συγκεκριμένη λειτουργία και μπορεί να επικοινωνεί με άλλες υπηρεσίες για να εκτελέσει πιο σύνθετες λειτουργίες. Μπορούν να αντιδρούν ευέλικτα σε αλλαγές και αλληλεπιδράσεις με άλλες υπηρεσίες, ενσωματώνοντας νέες λειτουργίες ή προσαρμόζοντας τις υπάρχουσες επαναχρησιμοποιώντας τις. Επιπλέον, μια SOA μπορεί να προσφέρει τη δυνατότητα ολοκλήρωσης διαφορετικών συστημάτων και εφαρμογών, προσθέτοντας ή ανταλλάσσοντας υπηρεσίες ανάμεσα σε αυτά.

Συνολικά, μια εφαρμογή που υιοθετεί την αρχιτεκτονική SOA παρέχει ένα ευέλικτο και επαναχρησιμοποιήσιμο σχήμα ανάπτυξης λογισμικού, διευκολύνοντας την ανάπτυξη, τη συντήρηση και την εξέλιξη της εφαρμογής, καλύπτοντας έτσι σύγχρονες. επιχειρηματικές ανάγκες μέσω ταχείας ανάπτυξης ή επαναχρησιμοποίησης/ενσωμάτωσης υφιστάμενων πόρων (S.A. Al-Qaseemi, 2016).

Wireless Sensor Network

Το Wireless Sensor Network (WSN) είναι ένα δίκτυο ασύρματων αισθητήρων που αποτελείται από μια συλλογή αισθητήρων που επικοινωνούν ασύρματα μεταξύ τους για τη συλλογή και τη μεταφορά δεδομένων. Οι αισθητήρες αυτοί μπορούν να ανιχνεύουν διάφορες φυσικές και περιβαλλοντικές παραμέτρους, όπως θερμοκρασία, ένταση φωτός, πίεση, κίνηση, ήχο και χημικά στοιχεία.

Τα WSN χρησιμοποιούνται σε πολλούς τομείς, όπως η περιβαλλοντική παρακολούθηση, η γεωργία, η ιατρική, η βιομηχανία, οι έξυπνοι οικιακοί αυτοματισμοί και άλλοι. Η αρχιτεκτονική των WSN βασίζεται στη συλλογή δεδομένων από τους αισθητήρες με χαμηλή κατανάλωση ενέργειας και τη μετάδοση των δεδομένων αυτών προς έναν κεντρικό σημείο συλλογής, που μπορεί να είναι ένας υπολογιστής ή μια πύλη (gateway) (Akyildiz, 2002).

Supply Chain Management

Το IoT διαδραματίζει ζωτικό ρόλο στη διαδικασία διαχείρισης της αλυσίδας εφοδιασμού στους περισσότερους τομείς εφαρμογών. Η διαδικασία αυτή περιλαμβάνει ροή αγαθών από τους προμηθευτές στους καταναλωτές με αυτοματοποιημένο τρόπο (A. Whitmore, 2015), (M. Abdel-Basset, 2018).

Healthcare

Η εφαρμογή του IoT στο σύστημα υγειονομικής περίθαλψης έχει αυξηθεί δραματικά τα τελευταία χρόνια. Για παράδειγμα, η τεχνολογία που συνοδεύει τις φορητές συσκευές είναι μία από τις πιο βασικές τεχνολογίες που χρησιμοποιούνται στο σύστημα υγειονομικής περίθαλψης που βασίζεται στο IoT. Δεδομένου ότι οι φορητές συσκευές (αισθητήρες) χρησιμοποιούνται για τη συλλογή ευαίσθητων δεδομένων για να εξυπηρετήσουν μια εφαρμογή, παράλληλα λόγω την διασύνδεσης της συσκευής με το διαδίκτυο ελλοχεύει ο κίνδυνος υποκλοπής ή αλλοίωσης των δεδομένων. Συνεπώς, μια ουσιαστική απαίτηση στην υλοποίηση τέτοιων συστημάτων είναι οι μηχανισμοί ασφαλείας για την αποφυγή κακόβουλης αλληλεπίδρασης με το κεντρικό σύστημα συλλογής – επεξεργασίας πληροφοριών (J. Santos, 2016).

Smart Society

Η ιδέα της έξυπνης κοινότητας είναι να λαμβάνονται ακριβείς πληροφορίες από μια περιοχή τη σωστή στιγμή, προκειμένου να γίνεται επαρκής επεξεργασία των παρεχόμενων πληροφοριών και να λαμβάνεται η βέλτιστη απόφαση σχετικά με ένα συμβάν. Για την συλλογή των πληροφοριών συμμετέχουν ένας τεράστιος αριθμός ενσύρματων και ασύρματων αισθητήρων με τα χαρακτηριστικά του IoT για τη δημιουργία μιας έξυπνης πόλης. Η βασική πρόκληση για να πετύχουμε την οικοδόμηση έξυπνων πόλεων είναι να συνδέσουμε όλα τα δεδομένα της πόλης που παράγονται από διάφορα έξυπνα συστήματα και αισθητήρες σε ένα μέρος (M.M. Rathore, 2018). Επιπλέον, η ανησυχία για την ασφάλεια όσον αφορά την προστασία της ιδιωτικής ζωής μιας τεράστιας συλλογής προσωπικών δεδομένων, θεωρείται ένα δύσκολο και επικίνδυνο ζήτημα.

Cloud-based Services

Οι υπηρεσίες IoT που βασίζονται στο cloud και λειτουργούν ως back-end υποδομές του IoT ταξινομούνται σε σταθερές και κινητές εφαρμογές. Εξαιτίας των περιορισμένων πόρων και της μικρής κάλυψης στην επικοινωνία και η δύσκολη πρόσβαση των συσκευών IoT, έχει ως αποτέλεσμα την περιορισμένη

αυτονομία τους και την υψηλή ζήτηση για προώθηση πακέτων σε υπηρεσίες βασισμένες στο σύννεφο σε περιβάλλοντα IoT.

Security

Οι συσκευές IoT διαδραματίζουν ζωτικό ρόλο στην παρακολούθηση μιας περιοχής και των αντικειμένων μέσα σε αυτή. Η παρακολούθηση περιοχών μέσω συσκευών IoT χρειάζονται έναν αξιόπιστο μηχανισμό ασφαλείας για την πρόληψη της παραβίασης δεδομένων και τη διατήρηση της εμπιστευτικότητας των δεδομένων στις συσκευές.

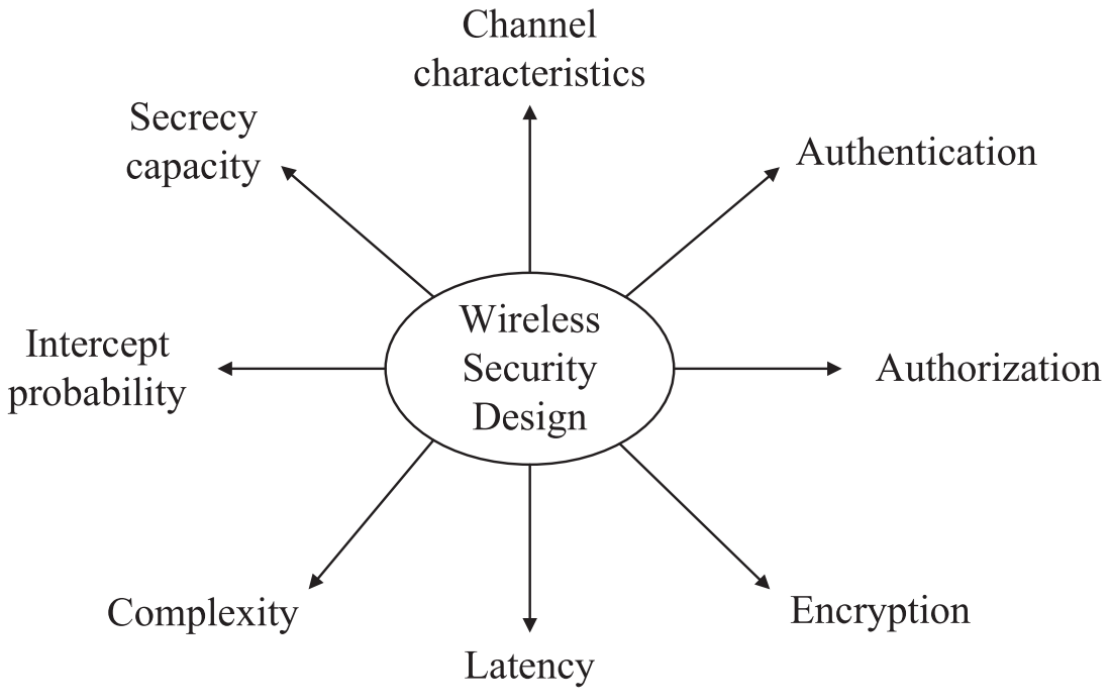
Επιπλέον, για την παρακολούθηση σε πραγματικό χρόνο αυτές οι συσκευές πρέπει να εκτελούν έναν ελαφρύ κρυπτογραφικό αλγόριθμο λόγω της μικρής επεξεργαστικής τους ισχύος.

ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΕ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

Τις τελευταίες δεκαετίες, οι υποδομές και οι υπηρεσίες ασύρματων επικοινωνιών έχουν πολλαπλασιαστεί με στόχο την κάλυψη των ταχέως αυξανόμενων αναγκών (O. Aliu, 2013) (H. ElSawy, 2013). Σύμφωνα με τα τελευταία στατιστικά στοιχεία που δημοσίευσε η Διεθνής Ένωση Τηλεπικοινωνιών το 2013 (ITU, 2013), ο αριθμός των συνδρομητών κινητής τηλεφωνίας έφθασε τα 6,8 δισεκατομμύρια παγκοσμίως και σχεδόν το 40% του παγκόσμιου πληθυσμού χρησιμοποιεί πλέον το Διαδίκτυο. Εν τω μεταξύ, έχει αναφερθεί (Department S. N., 2012) ότι ένας αυξανόμενος αριθμός ασύρματων συσκευών χρησιμοποιούνται για παράνομες ή ακόμη και για εγκληματικές δραστηριότητες στον κυβερνοχώρο, συμπεριλαμβανομένων κακόβουλων επιθέσεων, υποκλοπών από υπολογιστικά συστήματα, πλαστογράφησης δεδομένων, κλοπή οικονομικών - χρηματοοικονομικών πληροφοριών, διαδικτυακός εκφοβισμός/παρακολούθηση κ.ο.κ. Αυτό προκαλεί την άμεση απώλεια περίπου 83 δισεκατομμυρίων ευρώ σε περίπου 556 εκατομμύρια χρήστες παγκοσμίως που πέφτουν θύματα από τα έγκλημα στον κυβερνοχώρο κάθε χρόνο, σύμφωνα με την έκθεση Norton για το έγκλημα στον κυβερνοχώρο του 2012 (Department T. S., 2012). Ως εκ τούτου, είναι υψίστης σημασίας η βελτίωση της ασφάλειας των ασύρματων επικοινωνιών και η καταπολέμηση των εγκληματικών δραστηριοτήτων στον κυβερνοχώρο, ιδίως επειδή όλο και περισσότεροι άνθρωποι χρησιμοποιούν ασύρματα δίκτυα (π.χ. κινητά δίκτυα και Wi-Fi) για ηλεκτρονικές τραπεζικές συναλλαγές και διακινούνται προσωπικές και απόρρητες πληροφορίες σε ηλεκτρονικά μηνύματα, λόγω της ευρείας χρήσης των smartphones.

Τα ασύρματα δίκτυα υιοθετούν γενικά το OSI μοντέλο διαστρωμάτωσης (M. M. Rashid, 2009) που περιλαμβάνει το επίπεδο εφαρμογής, το επίπεδο μεταφοράς, το επίπεδο δικτύου (F. Foukalas, Apr. 2008), το επίπεδο MAC (R. Jurdak, IEEE Commun. Surv. Tut., vol. 6) και το φυσικό επίπεδο (M. Takai, 2001). Οι απειλές ασφαλείας και τα τρωτά σημεία που έχει κάθε επίπεδο αντιμετωπίζονται με διαφορετικές μεθόδους σε κάθε επίπεδο αντίστοιχα. Οι

απαιτήσεις ασφαλείας συμπεριλαμβάνουν την αυθεντικότητα της πληροφορίας, την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα (C. Kolias, 2013). Για παράδειγμα η κρυπτογράφηση χρησιμοποιείτε για να εξασφαλίσει την εμπιστευτικότητα των δεδομένων, αποτρέποντας την αποκάλυψη πληροφοριών σε μη εξουσιοδοτημένους χρήστες (Stamp, 2011). Αν και η κρυπτογραφία εξασφαλίζει εν μέρει την εμπιστευτικότητα των επικοινωνιών, από την άλλη όμως απαιτεί πρόσθετη υπολογιστική ισχύ και επιφέρει μια καθυστέρηση στην μετάδοση της πληροφορίας μιας και απαιτείται επιπλέον χρόνος τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των μεταδιδόμενων δεδομένων (G. Apostolopoulos, 2000). Προκειμένου να εξασφαλιστεί η αυθεντικότητα στην επικοινωνία ενός συστήματος που καλεί και ενός που λαμβάνει, στις υπάρχουσες τεχνολογίες ασύρματων δικτύων, εφαρμόζονται ταυτόχρονα πολλαπλές προσεγγίσεις αυθεντικοποίησης και διαφορετικά πρωτόκολλα σε περισσότερα επίπεδα διαστρωμάτωσης του μοντέλου OSI, συμπεριλαμβανομένης της αυθεντικοποίησης επιπέδου MAC (K. Wong, 2006), της αυθεντικοποίησης επιπέδου δικτύου (A. Aziz and W. Diffie, Aug. 2002) και της αυθεντικοποίησης επιπέδου μεταφοράς (Agrawal, 2000). Στο επίπεδο δικτύου, το WPA και το WPA2 είναι δύο ευρέως χρησιμοποιούμενα πρωτόκολλα ελέγχου ταυτότητας (A. H. Lashkari, 2009). Επιπρόσθετα, η αυθεντικοποίηση στο επίπεδο μεταφοράς περιλαμβάνει το SSL πρωτόκολλο και τους διαδόχους του, δηλαδή τα πρωτόκολλα TLS (5246, 2008). Γίνεται προφανές ότι η εμπλοκή πολλαπλών μηχανισμών ελέγχου ταυτότητας σε διαφορετικά στρώματα του μοντέλου OSI, είναι ικανή να ενισχύσει την ασύρματη ασφάλεια, αλλά με κόστος την υψηλή υπολογιστική πολυπλοκότητα και καθυστέρηση. Όπως φαίνεται και στο ακόλουθο σχήμα, οι κυριότερες μεθοδολογίες ασφαλείας στις ασύρματες επικοινωνίες περιλαμβάνουν την αυθεντικοποίηση, την εξουσιοδότηση και την κρυπτογράφηση. Πρέπει όμως οι κατασκευαστές των προτύπων ασφαλείας να συνυπολογίσουν μαζί με το επίπεδο ασφάλειας που εγγυούνται και άλλους ουσιαστικούς παράγοντες όπως η πολυπλοκότητα υλοποίησης και η καθυστέρηση επικοινωνίας λόγω των πολλαπλών πρωτοκόλλων και ελέγχων που εφαρμόζονται.



Σχήμα 8: Μεθοδολογίες ασύρματης ασφάλειας και παράγοντες που επηρεάζουν τον σχεδιασμό τους.

Στα ασύρματα δίκτυα, οι πληροφορίες ανταλλάσσονται μεταξύ εξουσιοδοτημένων χρηστών, αλλά αυτή η διαδικασία της εκπομπής-λήψης είναι ευάλωτη σε διάφορες κακόβουλες απειλές λόγω της φύσης του ασύρματου μέσου. Οι απαιτήσεις ασφάλειας στα ασύρματα δίκτυα εξασφαλίζουν τα δίκτυα από επιθέσεις και προστατεύουν τις ασύρματες μεταδόσεις ενώ ταυτόχρονα μειώνουν τους κινδύνους από επιθέσεις υποκλοπής, ή επίθεσης DDoS, ή επίθεσης παραποίησης δεδομένων, ή επίθεσης διακύβευσης κόμβων, και άλλων μεθόδων επιθέσεων (Tsudik, 2010), (H. Kumar, 2008). Για παράδειγμα, η διατήρηση εμπιστευτικότητας των δεδομένων είναι μια τυπική απαίτηση ασφάλειας, η οποία αναφέρεται στη δυνατότητα περιορισμού της πρόσβασης στα δεδομένα μόνο σε εξουσιοδοτημένους χρήστες, ενώ παράλληλα αποτρέπονται οι μη εξουσιοδοτημένοι χρήστες να διεισδύσουν και να υποκλέψουν τις πληροφορίες. Γενικά, οι ασφαλείς ασύρματες επικοινωνίες θα πρέπει να ικανοποιούν τις απαιτήσεις αυθεντικότητας, εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας (Y. Shiu et al., 2011).

Τα ποιο διαδεδομένα πρότυπα επικοινωνίας είναι σήμερα τα Bluetooth, Wi-Fi, WiMAX και LTE, στην συνέχεια θα δούμε τα πρωτόκολλα ασφαλείας που χρησιμοποιούνται στα προαναφερθέντα ασύρματα πρότυπα για την προστασία της αυθεντικότητας, της εμπιστευτικότητας, της ακεραιότητας, και της διαθεσιμότητας των μεταδόσεων διαμέσου του εξοπλισμού ασύρματης διάδοσης.

Bluetooth

Το **Bluetooth** είναι ένα μικρής εμβέλειας και χαμηλής ισχύος ασύρματο πρότυπο δικτύωσης, το οποίο έχει εφαρμογή κυρίως σε συσκευές πληροφορικής και επικοινωνιών, καθώς και σε περιφερειακές συσκευές, όπως κινητά τηλέφωνα, πληκτρολόγια, ακουστικά κ.λπ. Ωστόσο, οι συσκευές Bluetooth έχουν γίνει αντικείμενο πολλών επιθέσεων και μπορούν εύκολα να παραβιαστούν. Ως προστασία, το Bluetooth εισάγει διάφορα χαρακτηριστικά και πρωτόκολλα ασφαλείας, για την εξασφάλιση των μεταδόσεών του έναντι δυνητικά σοβαρών επιθέσεων (Muller, 1999). Για λόγους ασφαλείας κάθε συσκευή Bluetooth έχει τέσσερα μοναδικά χαρακτηριστικά, τη διεύθυνση της συσκευής (BD_ADDR), το ιδιωτικό κλειδί ελέγχου ταυτότητας, το ιδιωτικό κλειδί κρυπτογράφησης και έναν τυχαίο αριθμό (RAND). Οι τιμές αυτών των χαρακτηριστικών χρησιμοποιούνται για τον έλεγχο ταυτότητας, την εξουσιοδότηση και την κρυπτογράφηση, αντίστοιχα. Η διαδικασία εξουσιοδότησης χρησιμοποιείται για τη λήψη της απόφασης αν μια συσκευή Bluetooth έχει το δικαίωμα πρόσβασης σε μια συγκεκριμένη υπηρεσία ή όχι. Συνήθως, στις αξιόπιστες συσκευές επιτρέπεται να πρόσβαση σε όλες τις υπηρεσίες, ωστόσο οι μη αξιόπιστες ή άγνωστες συσκευές απαιτούν εξουσιοδότηση, προτού τους επιτραπεί η πρόσβαση στις υπηρεσίες. Εάν η συσκευή Bluetooth είναι αξιόπιστη, η εξουσιοδότηση δεν είναι αναγκαία. Διαφορετικά, η εξουσιοδότηση και η διαδικασία χαρακτηρισμού της συσκευής ως έμπιστης θα εκτελούνται διαδοχικά. Εάν η εξουσιοδότηση αποτύχει, η συσκευή δεν θα έχει πρόσβαση σε ορισμένες υπηρεσίες. Σε αντίθεση, μια επιτυχής εξουσιοδότηση καθιστά τις αντίστοιχες συσκευές Bluetooth αξιόπιστες για πρόσβαση σε όλες τις διαθέσιμες υπηρεσίες. Επιπρόσθετα, χρησιμοποιείται στο Bluetooth η κρυπτογράφηση για να προστατεύσει την εμπιστευτικότητα των δεδομένων μετάδοσης. Στη συνέχεια, θα σταλούν τα κλειδιά κρυπτογράφησης που θα χρησιμοποιήσουν οι συσκευές για την κρυπτογράφηση και την αποκρυπτογράφηση δεδομένων σε όλη τη διάρκεια της συνεδρίας. Η διαχείριση ασφάλειας Bluetooth έχει διάφορα στάδια στα οποία χρησιμοποιούνται διαφορετικοί αλγόριθμοι κλειδιών κρυπτογράφησης για να λειτουργήσουν σωστά. Οι πιο συνηθισμένοι αλγόριθμοι κλειδιών κρυπτογράφησης που χρησιμοποιούνται από την πιο πρόσφατη έκδοση του Bluetooth (4.0 και άνω) μπορεί να είναι οι ακόλουθοι:

Συμμετρικό κλειδί: Αυτός ο τύπος κρυπτογράφησης χρησιμοποιεί ένα μόνο κλειδί για την αποκρυπτογράφηση των κατακερματισμών ή των μηδενικών.

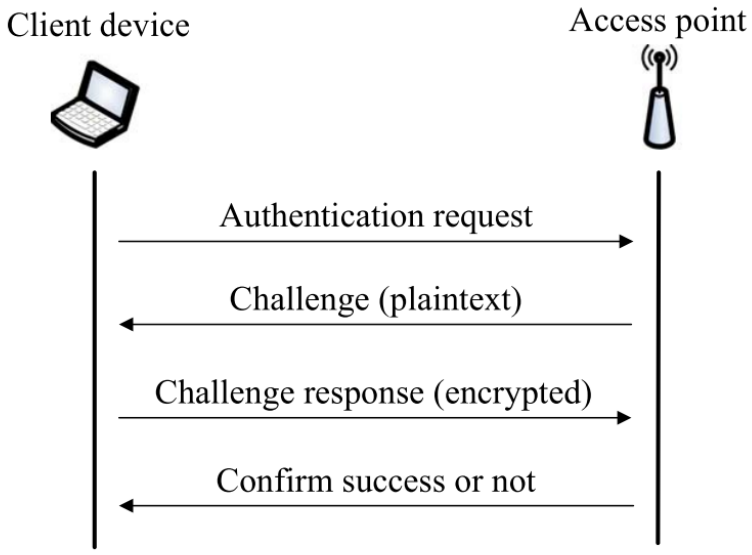
Ασύμμετρο κλειδί: Αυτός ο τύπος κρυπτογράφησης χρησιμοποιεί αυτό που είναι γνωστό ως δημόσιο κλειδί και ιδιωτικό κλειδί. Το δημόσιο κλειδί χρησιμοποιείται για την κρυπτογράφηση των δεδομένων, ενώ το ιδιωτικό κλειδί αποκρυπτογραφεί τα κρυπτογραφημένα δεδομένα.

Κωδικοποίηση ελλειπτικής καμπύλης (ECC): Χρησιμοποιεί μια εξίσωση ελλειπτικής καμπύλης για τη δημιουργία πλήκτρων που είναι πολύ μικρότερα από τα συμμετρικά ή ασύμμετρα κλειδιά, αλλά είναι εξίσου ασφαλή.

Προηγμένο πρότυπο κρυπτογράφησης (AES): είναι ένας συμμετρικός κρυπτογράφησης μπλοκ που εκτείνεται σε 128 bit. (DzTechs, n.d.)

Wi-Fi

Η οικογένεια των δικτύων **Wi-Fi** και βασίζεται κυρίως στα πρότυπα IEEE 802.11 b/g έχει επεκταθεί εκρηκτικά. Τα πιο συνηθισμένα πρωτόκολλα ασφαλείας στο Wi-Fi είναι τα WEP και WPA (A. Lashkari, 2009). Το WEP προτάθηκε το 1999 ως πρότυπο ασφαλείας για δίκτυα Wi-Fi για να καταστήσει τις ασύρματες μεταδόσεις δεδομένων εξίσου ασφαλείς με τα παραδοσιακά ενσύρματα δίκτυα. Ωστόσο, το WEP αποδείχτηκε ότι είναι ένα σχετικά αδύναμο πρωτόκολλο ασφαλείας, με πολλές αδυναμίες. Ως εκ τούτου, μπορεί να "παραβιαστεί" μέσα σε λίγα λεπτά χρησιμοποιώντας έναν απλό φορητό υπολογιστή. Εναλλακτικά, προτάθηκε το 2003 το πρότυπο WPA για την αντικατάσταση του WEP, ενώ το βελτιωμένο WPA2 αποτελεί μια αναβαθμισμένη έκδοση του προτύπου WPA. Συνήθως, τα WPA και WPA2 είναι πιο ασφαλή από το WEP και έτσι χρησιμοποιούνται ευρέως στα σύγχρονα δίκτυα Wi-Fi. Παρακάτω, περιγράφουμε τον έλεγχο ταυτότητας και τις διαδικασίες κρυπτογράφησης των πρωτοκόλλων WEP, WPA και WPA2. Το πρωτόκολλο WEP αποτελείται από δύο διαδικασίες, συγκεκριμένα τη διαδικασία ελέγχου ταυτότητας και τη διαδικασία κρυπτογράφησης. Με την εγκαθίδρυση ελέγχου πρόσβασης επιτυγχάνεται η αποτροπή πρόσβασης μη εξουσιοδοτημένων χρηστών χωρίς το κατάλληλο κλειδί WEP και με την κρυπτογράφηση επιτυγχάνεται η ιδιωτικότητα των δεδομένων κρυπτογραφώντας τις ροές δεδομένων με τη βοήθεια του κλειδιού WEP. Όπως φαίνεται στο ακόλουθο σχήμα, ο έλεγχος ταυτότητας WEP χρησιμοποιεί μια χειραψία τεσσάρων βημάτων "πρόκληση-απάντηση" μεταξύ ενός πελάτη Wi-Fi και ενός σημείου πρόσβασης, που λειτουργεί με τη βοήθεια ενός κοινού κλειδιού WEP.



Σχήμα 9: Διαδικασία ελέγχου ταυτότητας WEP.

Παρόλο που το WEP εκτελεί τόσο τις λειτουργίες ελέγχου ταυτότητας όσο και τις λειτουργίες κρυπτογράφησης, εξακολουθεί να παραμένει αδύναμο σε απειλές ασφαλείας. Για παράδειγμα, το WEP πρότυπο, αποτυγχάνει να προστατεύσει τις πληροφορίες από την πλαστογραφία και τις επιθέσεις αναπαραγωγής, επομένως ένας επιτιθέμενος μπορεί να είναι σε θέση να τροποποιήσει είτε να αναπαραγάγει τα πακέτα δεδομένων χωρίς οι νόμιμοι χρήστες να αντιληφθούν ότι έχει γίνει παραποίηση ή/και αναπαραγωγή των δεδομένων. Επιπρόσθετα, είναι εύκολο για έναν εισβολέα να πλαστογραφήσει ένα μήνυμα ελέγχου ταυτότητας στο WEP, γεγονός που καθιστά εύκολη την πρόσβαση μη εξουσιοδοτημένων χρηστών ώστε να προσποιούνται ότι είναι νόμιμοι χρήστες και να μπορούν να κλέψουν εμπιστευτικές πληροφορίες (E. Tews, 2007).

Ως μέτρο αντιμετώπισης των προαναφερθέντων προβλημάτων ασφαλείας του προτύπου WEP, προτάθηκε η λύση του προτύπου WPA. Το WPA χρησιμοποιεί διάφορες τεχνικές για την προστασία των ασύρματων δικτύων, συμπεριλαμβανομένης της κρυπτογράφησης TKIP (Temporal Key Integrity Protocol) για την ασφάλεια των δεδομένων και το πρωτόκολλο ελέγχου πρόσβασης 802.1X για την ταυτοποίηση χρηστών. Το πρότυπο WPA έχει δύο κύριους τύπους:

1. το προσωπικό WPA χρησιμοποιείται κυρίως σε οικιακά δίκτυα χωρίς την παρέμβαση ενός διακομιστή ελέγχου ταυτότητας, όπου ένα μυστικό κλειδί μοιράζεται εκ των προτέρων μεταξύ του πελάτη και του σημείου πρόσβασης, το οποίο ονομάζεται WPA-PSK (preshared key - προσυμφωνημένο κλειδί).
2. το εταιρικό WPA που χρησιμοποιείται για εταιρικά δίκτυα, το οποίο απαιτεί έναν διακομιστή ελέγχου ταυτότητας 802.1x για την εκτέλεση του ελέγχου ασφαλείας για την αποτελεσματική προστασία από κακόβουλες επιθέσεις.

Το κύριο πλεονέκτημα του WPA έναντι του WEP είναι ότι το WPA χρησιμοποιεί πιο ισχυρή κρυπτογράφηση δεδομένων (TKIP- Temporal Key Integrity Protocol), η οποία υποβοηθείται από ένα MIC key (Message Integrity Code key) που χρησιμοποιείτε για την προστασία της ακεραιότητας και της εμπιστευτικότητας των δεδομένων των δικτύων Wi-Fi (J. Lin, Apr. 2006). Η TKIP (Temporal Key Integrity Protocol) κρυπτογράφηση λειτουργεί με την ακόλουθη διαδικασία:
Δημιουργία Προσωρινών Κλειδιών (Temporal Keys): Κάθε φορά που συνδέεται μια συσκευή στο ασύρματο δίκτυο, δημιουργούνται προσωρινά κλειδιά για την κρυπτογράφηση και την αυθεντικοποίηση των δεδομένων.

Κρυπτογράφηση με Ροή Κλειδιών (Key Mixing): Η TKIP χρησιμοποιεί ένα συνδυασμό του σταθερού κλειδιού (που κοινοποιείται σε όλες τις συσκευές του δικτύου) και ενός προσωρινού κλειδιού για κάθε πακέτο δεδομένων. Αυτός ο συνδυασμός δημιουργεί μια μορφή δυναμικής κρυπτογράφησης που είναι πιο ασφαλής από το στατικό κλειδί που χρησιμοποιείτο στο WEP.

Αλλαγή των Κλειδιών (Key Rotation): Η TKIP υποστηρίζει την αλλαγή των προσωρινών κλειδιών σε τακτά χρονικά διαστήματα, καθιστώντας δυσκολότερη την αποκάλυψη των κλειδιών από επιτιθέμενους.

Αν και η TKIP βελτιώνει την ασφάλεια σε σχέση με το WEP, έχει αντικατασταθεί κατά κύριο λόγο από το πιο ασφαλές πρότυπο κρυπτογράφησης AES (Advanced Encryption Standard) που χρησιμοποιείται στο πρωτόκολλο WPA2 και WPA3. Το AES παρέχει ακόμα υψηλότερο επίπεδο ασφάλειας σε σύγκριση με την TKIP. Επομένως, συνιστάται να χρησιμοποιείτε WPA2 ή WPA3 αν είναι δυνατόν για την ασφάλεια του ασύρματου δικτύου σας.

WiMax

WiMAX είναι μια τεχνολογία ασύρματης επικοινωνίας που αναπτύχθηκε για να παρέχει υψηλές ταχύτητες μεταφοράς δεδομένων σε μεγάλες ασύρματες αποστάσεις. Το WiMAX σημαίνει "Παγκόσμια Πρότυπα για τις Επικοινωνίες με Μεταβαλλόμενο Εύρος Ζώνης" (Worldwide Interoperability for Microwave Access).

Η τεχνολογία WiMAX χρησιμοποιεί ασύρματες συχνότητες για τη μετάδοση δεδομένων, και μπορεί να χρησιμοποιηθεί για πολλούς σκοπούς, συμπεριλαμβανομένης της παροχής υπηρεσιών Internet σε αστικές και αγροτικές περιοχές, καθώς και για επιχειρηματικές εφαρμογές και υπηρεσίες φορητής επικοινωνίας.

Οι κύριες χαρακτηριστικές του WiMAX περιλαμβάνουν:

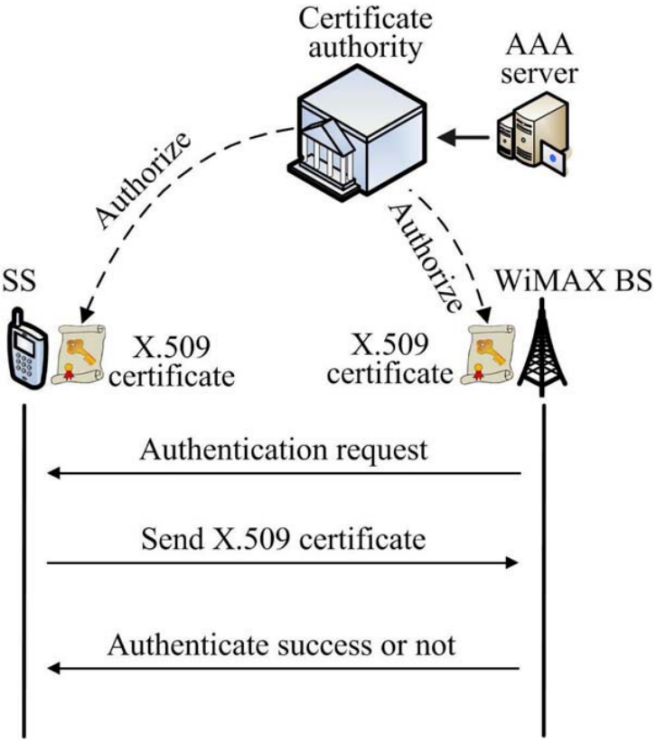
1. **Υψηλή Ταχύτητα Δεδομένων**: Η τεχνολογία WiMAX μπορεί να παρέχει υψηλές ταχύτητες μεταφοράς δεδομένων, παρόμοιες με αυτές που προσφέρονται από τις συμβατικές επικοινωνίες ευρείας ζώνης (broadband).

2. **Μεγάλη Κάλυψη**: Λόγω της φύσης της ασύρματης τεχνολογίας, το WiMAX μπορεί να καλύψει μεγάλες γεωγραφικές περιοχές με μια βάση σταθμού.

3. **Ευελιξία**: Το WiMAX μπορεί να χρησιμοποιηθεί για διάφορους σκοπούς, όπως η παροχή υπηρεσιών Internet, η επικοινωνία μεταξύ συσκευών (M2M), η επέκταση των επιχειρηματικών δικτύων κ.λπ.

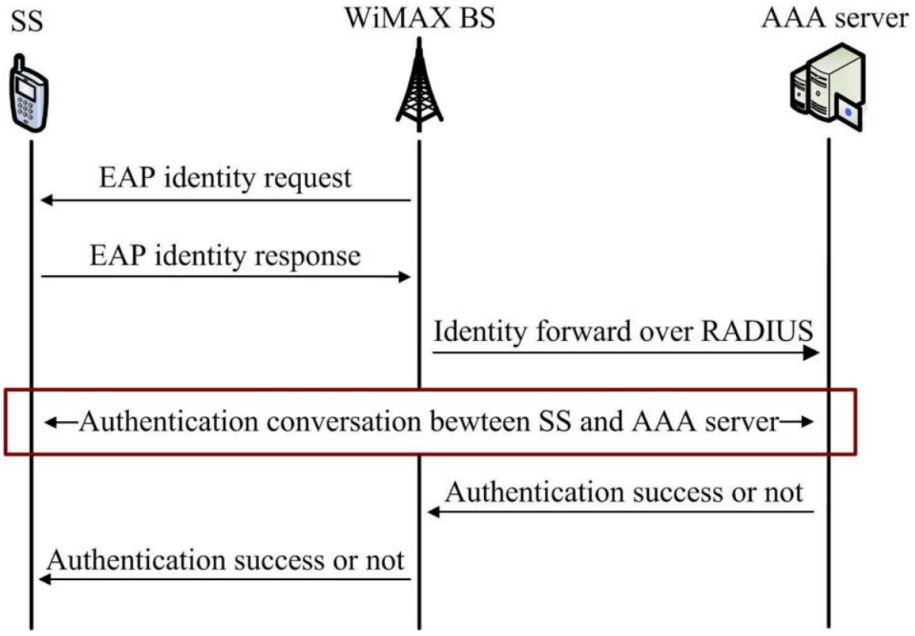
Η πιστοποίηση ταυτότητας στο WiMAX επιτυγχάνεται με το PKM πρωτόκολλο, το οποίο υποστηρίζει δύο βασικές προσεγγίσεις ελέγχου ταυτότητας, δηλαδή τον έλεγχο ταυτότητας με βάση το RSA και την αυθεντικοποίηση με βάση τον EAP (Extensible Authentication Protocol) (Walker, Jun. 2004).

Στο ακόλουθο σχήμα παρουσιάζεται η διαδικασία ελέγχου ταυτότητας με βάση το RSA, όπου μια έμπιστη αρχή πιστοποιητικών είναι υπεύθυνη για την έκδοση ενός ψηφιακού πιστοποιητικού X.509 σε καθέναν από τους κόμβους του δικτύου, συμπεριλαμβανομένου του SS και το WiMAX BS



Σχήμα 10: Διαδικασία ελέγχου ταυτότητας μέσω RSA

Η διαδικασία ελέγχου ταυτότητας με βάση το EAP απεικονίζεται στο ακόλουθο σχήμα, όπου ένας WiMAX BS στέλνει πρώτα ένα αίτημα ταυτότητας σε έναν SS, ο οποίος απαντά με τις πληροφορίες ταυτότητάς του.



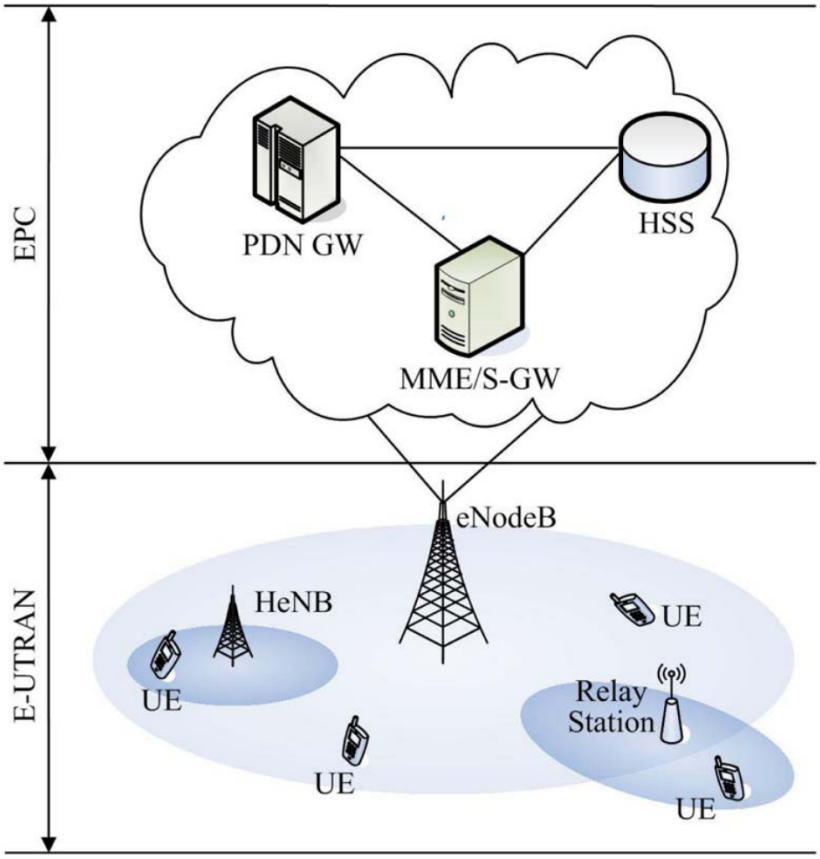
Σχήμα 11: Διαδικασία ελέγχου ταυτότητας μέσω EAP

Στη συνέχεια, ο WiMAX BS διαβιβάζει την ταυτότητα του SS σε έναν διακομιστή AAA μέσω ενός ασφαλούς πρωτοκόλλου δικτύωσης που αναφέρεται ως RADIUS. Στη συνέχεια, ο SS και ο AAA διακομιστής ξεκινούν τη διαδικασία ελέγχου ταυτότητας, όπου είναι διαθέσιμες τρεις διαφορετικές επιλογές EAP ανάλογα με τον SS και τη δυνατότητα του διακομιστή AAA, συμπεριλαμβανομένης της EAP-AKA, EAP-TLS και EAP-TTLS. Τέλος, ο διακομιστής AAA θα αποφασίσει για την επιτυχία (ή την αποτυχία) του ελέγχου ταυτότητας και θα ενημερώσει τον SS.

Παρόλα αυτά, η διάδοση του WiMAX ως τεχνολογίας έχει περιοριστεί κάπως λόγω της εμφάνισης πιο αποδοτικών τεχνολογιών όπως το LTE (Long-Term Evolution) και το 5G, τα οποία προσφέρουν ακόμη μεγαλύτερες ταχύτητες και λειτουργικότητες. Ωστόσο, το WiMAX εξακολουθεί να χρησιμοποιείται σε ορισμένες περιοχές και εφαρμογές όπου οι εναλλακτικές επιλογές είναι περιορισμένες ή ανύπαρκτες.

LTE - Long-Term Evolution

Το LTE είναι το πιο πρόσφατο πρότυπο που αναπτύχθηκε από την εταιρική σύμπραξη 3G για δίκτυα κινητής τηλεφωνίας επόμενης γενιάς σχεδιασμένο για την παροχή απρόσκοπτης κάλυψης, υψηλού ρυθμού δεδομένων και χαμηλή καθυστέρηση (al, 2009). Ένα δίκτυο LTE αποτελείται συνήθως από ένα EPC (Evolved Packet Core) και ένα E-UTRAN (Evolved Universal Terrestrial Radio Access Network), όπως φαίνεται στο παρακάτω σχήμα. ((3GPP), 2012) .Το EPC αποτελεί τον κύριο πυρήνα δικτύου για ένα LTE δίκτυο. Είναι υπεύθυνο για τη διαχείριση της κίνησης δεδομένων, τη δρομολόγηση της κλήσης, την αυθεντικοποίηση των χρηστών και άλλες λειτουργίες που σχετίζονται με τη μετάδοση δεδομένων σε ένα LTE δίκτυο. Το E-UTRAN αποτελεί το ασύρματο τμήμα του LTE δικτύου. Αποτελείται από τους LTE κεραίες βάσης και τον εξοπλισμό σταθμού βάσης που παρέχει τη σύνδεση με τα κινητά τηλέφωνα και άλλες συσκευές LTE. Κατά τη λειτουργία του, τα δεδομένα που μεταδίδονται μέσω του E-UTRAN από τα κινητά τηλέφωνα ή άλλες συσκευές LTE προωθούνται μέσω του EPC, το οποίο είναι υπεύθυνο για την αποθήκευση, τη δρομολόγηση και τη μετάδοση αυτών των δεδομένων προς τον προορισμό τους.



Σχήμα 12: Αρχιτεκτονική δικτύου LTE.

Αν και η εισαγωγή αυτών των ιδιαίτερων χαρακτηριστικών στο LTE έχουν ως αποτέλεσμα την βελτίωση της κάλυψης του δικτύου και της ποιότητα της επικοινωνίας, η πολυπλοκότητα όμως που εισήχθη έχει ως αντίκτυπο νέα τρωτά σημεία ασφαλείας που αποτελούν στόχους από αυτούς που προσπαθούν να παραβιάσουν το δίκτυο. Ακολουθούν ορισμένα από αυτά τα σημεία ασφαλείας και απειλές:

Ευπάθειες στην Αυθεντικοποίηση και Εξουσιοδότηση (Authentication and Authorization): Το LTE περιλαμβάνει μηχανισμούς αυθεντικοποίησης και εξουσιοδότησης για τη σύνδεση των χρηστών στο δίκτυο. Οι επιθέσεις που στοχεύουν στην αυθεντικοποίηση και την εξουσιοδότηση μπορούν να αποτελέσουν σοβαρή απειλή (3GPP, n.d.).

Επιθέσεις στην Κρυπτογράφηση Δεδομένων: Η κρυπτογράφηση των δεδομένων είναι κρίσιμη για την προστασία της ιδιωτικότητας και της ασφάλειας των επικοινωνιών. Επιθέσεις ενάντια στους μηχανισμούς κρυπτογράφησης μπορούν να αποκαλύψουν ευαίσθητες πληροφορίες (Anastasios Bikos, 2012).

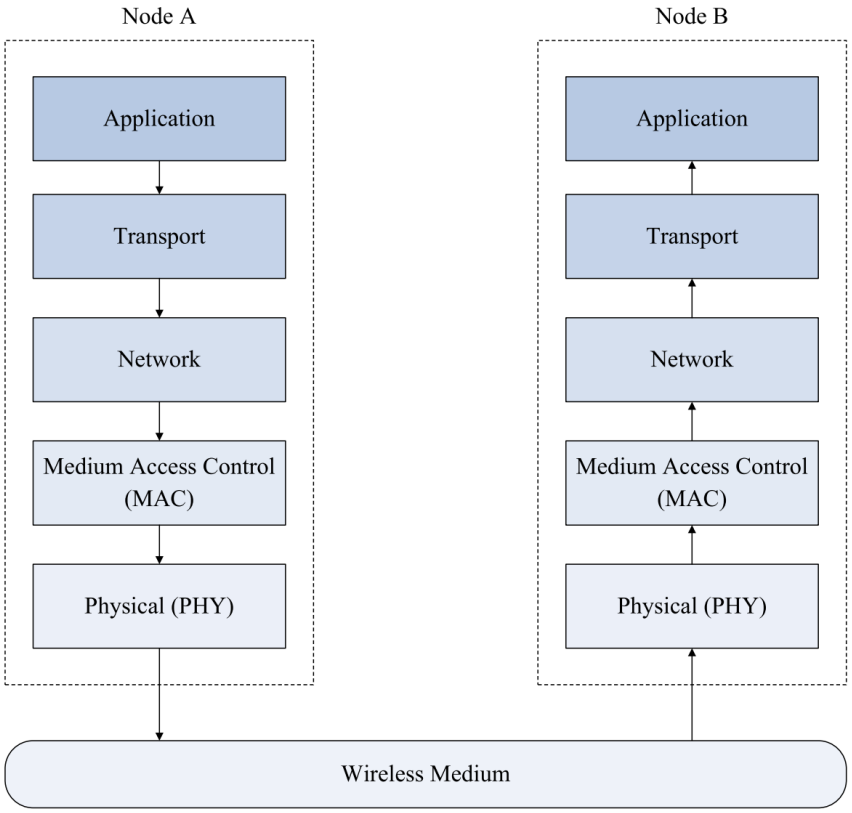
Κίνδυνοι από κακόβουλες Συσκευές και Διαχείριση Ταυτότητας Κινητής Συσκευής: Οι επιθέσεις που στοχεύουν στη διαχείριση της ταυτότητας των κινητών συσκευών μπορούν να οδηγήσουν σε παραβιάσεις της ασφάλειας και της ιδιωτικότητας (Ma, 2012).

Επιθέσεις με Χρήση Κακόβουλου Λογισμικού στην Διαχείριση Κινητής Δικτύωσης: Οι επιθέσεις που στοχεύουν στη διαχείριση της κινητής δικτύωσης μπορούν να προκαλέσουν προβλήματα στη λειτουργία του δικτύου και να απειλήσουν την αξιοπιστία του (Jin Cao, n.d.).

Επιθέσεις στην Διαχείριση Πόρων Δικτύου: Οι επιθέσεις που στοχεύουν στη διαχείριση των πόρων του δικτύου μπορούν να προκαλέσουν προβλήματα απόρριψης υπηρεσιών (DoS) ή να προβληματίσουν την απόδοση του δικτύου του (Jin Cao, n.d.).

Αυτά τα σημεία ασφαλείας και οι απειλές μπορούν να αντιμετωπιστούν με την υιοθέτηση κατάλληλων μέτρων ασφαλείας, συμπεριλαμβανομένων των μηχανισμών αυθεντικοποίησης, της κρυπτογράφησης δεδομένων, των μηχανισμών προστασίας της ταυτότητας και της διαχείρισης πόρων.

Συνοψίζοντας, την παρούσα ενότητα, συζητήσαμε τα πρωτόκολλα ασφαλείας των Bluetooth, Wi-Fi, WiMAX καθώς και του LTE και παρατηρήσαμε ότι τα υπάρχοντα ασύρματα δίκτυα τείνουν να βασίζονται σε μηχανισμούς ασφαλείας που αναπτύσσονται σε στα ανώτερα στρώματα OSI του παρακάτω σχήματος (π.χ. επίπεδο MAC, επίπεδο δικτύου, επίπεδο μεταφοράς, τόσο για τον έλεγχο ταυτότητας των χρηστών όσο και για την κρυπτογράφηση δεδομένων.



Σχήμα 13: Γενική αρχιτεκτονική ασύρματου πρωτοκόλλου OSI.

Για παράδειγμα, τα WEP και WPA αποτελούν ένα ζεύγος πρωτοκόλλων ασφαλείας που χρησιμοποιούνται συνήθως σε δίκτυα Wi-Fi για την εξασφάλιση της εμπιστευτικότητας των δεδομένων και ακεραιότητας, ενώ τα δίκτυα WiMAX υιοθετούν το πρωτόκολλο PKM για την επίτευξη ασφαλών μεταδόσεων έναντι κακόβουλων επιθέσεων.

Στα παραπάνω η ασφάλεια των επικοινωνιών στο φυσικό επίπεδο έχει σε μεγάλο βαθμό αγνοηθεί στα υπάρχοντα ασύρματα πρωτόκολλα ασφαλείας. Ωστόσο, λόγω της ραδιοφωνικής διάδοσης, το φυσικό επίπεδο της ασύρματης μετάδοσης είναι εξαιρετικά ευάλωτο τόσο σε επιθέσεις υποκλοπής όσο και σε επιθέσεις παρεμβολής. Αυτό καθιστά αναγκαία την ανάπτυξη της ασφάλειας φυσικού επιπέδου ως συμπλήρωμα των συμβατικών πρωτοκόλλων ασφαλείας των ανωτέρων επιπέδων OSI. Στην επόμενη ενότητα θα παρουσιαστεί η ασφάλεια στο φυσικό επίπεδο που σχεδιάστηκε για την ενίσχυση της ασφαλούς μετάδοσης πληροφοριών, διαμέσου ασύρματων επικοινωνιών.

.

ΚΕΦΑΛΑΙΟ 3: ΑΣΦΑΛΕΙΑ ΣΤΟ ΦΥΣΙΚΟ ΕΠΙΠΕΔΟ

Το φυσικό στρώμα περιγράφει τι συμβαίνει όταν ένα ηλεκτρομαγνητικό κύμα φεύγει από τη συσκευή μας. Η απόκτηση ασφάλειας φυσικού επιπέδου (PLS) είναι να εκμεταλλευόμαστε τις φυσικές ιδιότητες του καναλιού για να προστατεύσουμε τις πληροφορίες μας από τις υποκλοπές.

Η ασφάλεια στο φυσικό επίπεδο δεν προορίζεται σε καμία περίπτωση να αντικαταστήσει την κρυπτογραφική ασφάλεια, αλλά μάλλον παρέχει ένα πρόσθετο επίπεδο προστασίας.

Μεταξύ των ήδη παρεχόμενων τεχνικών ασφάλειας στις επικοινωνίες, η ασφάλεια στο φυσικό μέσο (PLS) υπόσχεται ότι μπορεί να παρέχει μια αδιάσπαστη, αποδεδειγμένη και μετρήσιμη ασφάλεια στο απόρρητο των επικοινωνιών, προκαλώντας το ενδιαφέρον τόσο της ακαδημαϊκής όσο και της βιομηχανικής κοινότητας.

Ωστόσο, τα μοναδικά χαρακτηριστικά του IoT, όπως ότι είναι υλοποίηση χαμηλού κόστους, κάλυψη μεγάλης περιοχής, ο μεγάλος αριθμός συνδέσεων και οι ποικίλες παρεχόμενες υπηρεσίες, θέτουν μεγάλες προκλήσεις για το σχεδιασμό του αναμενόμενου πρωτοκόλλου PLS (Physical Layer Security) στο IoT.

Αρχικά θα δούμε τις τεχνικές PLS που εφαρμόστηκαν προς υλοποίηση IOT δικτύων. Αρχικά παρουσιάζεται συνοπτικά η βασική αρχή του PLS και στην συνέχεια μια επισκόπηση των υφιστάμενων τεχνικών PLS.

Στην συνέχεια παρουσιάζονται τα χαρακτηριστικά του IOT που σχετίζονται με τις προκλήσεις που αντιμετώπισε η σχεδίαση του πρωτοκόλλου PLS. Παρακάτω, επισημαίνονται τρεις πρόσφατα προτεινόμενες λύσεις PLS, οι οποίες ταιριάζουν καλά με τα χαρακτηριστικά του IoT και αναμένεται να εφαρμοστούν στο εγγύς μέλλον. Τέλος, ολοκληρώνουμε την εργασία και επισημαίνουμε ορισμένες περαιτέρω ερευνητικές κατευθύνσεις.

Οι τεχνικές ασφάλειας φυσικού επιπέδου (PLS) χρησιμοποιούνται όλο και περισσότερο στο (IoT) λόγω της ικανότητάς τους να παρέχουν ασφάλεια χωρίς να απαιτούν σημαντικούς πόρους (IEEE, 2021). Αυτές οι τεχνικές είναι ιδιαίτερα χρήσιμες για συσκευές IoT με περιορισμένους πόρους (IEEE, 2021). Επιπρόσθετα η εμφάνιση ασύρματων δικτύων πέμπτης γενιάς (5G) με βελτιωμένο ρυθμό δεδομένων, εγκαινιάζει μια νέα εποχή για το IOT, δημιουργώντας νέες ανάγκες, νέες εφαρμογές και νέες αγορές εξειδικευμένων υπηρεσιών. Η μαζική ανάπτυξη του IoT καθιστά την ασφάλεια των πληροφοριών πρωταρχικώς σημαντική. Οι τεχνικές ασφάλειας δικτύων είναι ζωτικής σημασίας όχι μόνο για τη διατήρηση της απρόσκοπτης λειτουργίας των δικτύων αλλά και για την υλοποίηση της ασφαλούς παροχής υπηρεσιών μέσω των δικτύων αυτών. Επιπλέον η **εξασφάλιση** της ασφάλειας στις διακινούμενες πληροφορίες, θα είναι ένας νέος τύπος παρεχόμενης υπηρεσίας όπως η φωνή ή τα δεδομένα στο παρελθόν. Για παράδειγμα οι χρήστες θα μπορούν να αγοράσουν το επίπεδο ασφαλείας που επιθυμούν, με βάση τις απαιτήσεις τους

αλλά και το κόστος αγοράς της παρεχόμενων υπηρεσιών. Αυτό θα παρέχει μια πληρέστερη και ποιοτικότερη υπηρεσία QoS (Quality-of-Service), σε ετερογενείς χρήστες, καθιστώντας την ασφάλεια των δεδομένων ένα νέο επικερδές πεδίο για τους διαχειριστές των ασύρματων δικτύων επικοινωνίας.

Οι παραδοσιακές λύσεις βασίζοντας κυρίως στις τεχνολογίες που αναπτύχθηκαν γύρω από την κρυπτογράφηση αλλά αυτές εφαρμόζονται σε υψηλότερα επίπεδα στο μοντέλο OSI. Παρόλο που η κρυπτογράφηση είναι μια δημοφιλής μέθοδος που χρησιμοποιείται ευρέως για ενσύρματα δίκτυα (π.χ. δίκτυα υπολογιστών) και υποδομές ασύρματων δικτύων (π.χ., δίκτυα κινητής τηλεφωνίας), δεν είναι πλήρως κατάλληλη για το σημερινό-μελλοντικό IoT, όπως αναλύεται στη συνέχεια.

Πρώτον, το IoT αποτελείται από μεγάλο αριθμό συσκευών χαμηλού κόστους. Οι συσκευές IoT είναι συνήθως εξοπλισμένες με περιορισμένη μνήμη αποθήκευσης και τροφοδοτούνται με μπαταρίες, οι οποίες με τη σειρά τους περιορίζουν τις εφαρμογές στην πληροφορική και στις επικοινωνίες. Ως αποτέλεσμα, περίπλοκες κρυπτογραφικές μέθοδοι και πρωτόκολλα που εφαρμόζονται, καθώς και εξελιγμένοι αλγόριθμοι κρυπτογράφησης - αποκρυπτογράφησης δεν μπορούν να προσαρμοστούν ώστε να χρησιμοποιηθούν στις νέες ανάγκες.

Δεύτερον, το IoT είναι ένα δίκτυο μεγάλης κλίμακας που υποστηρίζει μαζικές συνδέσεις. Όπως αναφέρεται από το 3GPP TR 45.820 Technical Specification, οι μελλοντικές υλοποιήσεις IoT πρέπει να μπορούν να εξυπηρετήσουν εκατομμύρια συσκευές IoT συνδεδεμένες εντός μιας κυψέλης κινητής τηλεφωνίας. Επιπλέον αν και η δυνατότητα για επεξεργασία των δεδομένων, που δέχονται αυτές οι συσκευές, είναι περιορισμένη όπως και η περιοχή που μπορούν να καλύψουν μεμονωμένες συσκευές (πχ αισθητήρες) επικοινωνώντας μεταξύ τους, είναι αρκετά μικρή, θα πρέπει το δίκτυο στο σύνολο του να ικανοποιεί την απαίτηση κάλυψης ευρείας εμβέλειας, έτσι ώστε τα τοπικά δεδομένα που ανιχνεύονται να μπορούν να παραδοθούν στα απομακρυσμένα κέντρα ελέγχου για περαιτέρω επεξεργασία. Για να ικανοποιηθεί η παραπάνω απαίτηση, τα πρωτόκολλα μετάδοσης έχουν να ενσωματώσουν πολλά νέα χαρακτηριστικά, όπως δρομολόγηση πολλαπλών βημάτων, ώστε να μπορέσουν να καλύψουν περιοχή μεγαλύτερη από αυτή που μπορεί να καλύψει μια μεμονωμένη συσκευή, συνεργατική αναμετάδοση (cooperative relaying) του μεταδιδόμενου σήματος, δυναμική πρόσβαση κ.λπ. Αυτό καθιστά το IoT εξαιρετικά ετερογενές και δυναμικό. Σε ένα τέτοιο περιβάλλον δικτύου, είναι εξαιρετικά δύσκολη η διαχείριση και η διανομή των μυστικών κλειδιών.

Τρίτον, λόγω των πολλαπλών διαφορετικών υλοποιήσεων που καλείτε το IOT να εξυπηρετήσει, είναι αναμενόμενο να αναπτυχθούν και πολλές υπηρεσίες που θα ικανοποιούν την ποικιλομορφία των απαιτήσεων. Διαφορετικές υπηρεσίες θέτουν τελείως διαφορετικό επίπεδο QoS καθώς και επίπεδο ασφαλείας. Για παράδειγμα, οι ηλεκτρονικές πληρωμές απαιτούν πολύ υψηλότερο επίπεδο ασφάλειας από ό,τι η συνηθισμένη υπηρεσία περιήγησης

στο διαδίκτυο. Ωστόσο, οι μέθοδοι που βασίζονται στην κρυπτογράφηση παρέχουν μόνο "δυαδική" (binary) επίπεδο ασφάλειας. Οι μεταδιδόμενες πληροφορίες είναι απόλυτα ασφαλείς εάν το κλειδί κρυπτογράφησης μπορεί να περάσει με ασφάλεια από όλες τις ενδιάμεσες συσκευές, διαφορετικά υπάρχει σοβαρός κίνδυνος υποκλοπής της μεταδιδόμενης πληροφορίας.

Σε αντίθεση με τις παραδοσιακές κρυπτογραφικές προσεγγίσεις, η ασφάλεια φυσικού επιπέδου (PLS) εκμεταλλεύεται τα εγγενή χαρακτηριστικά των ασύρματων καναλιών, όπως ο θόρυβος, η εξασθένιση και οι παρεμβολές, ώστε να ενισχύσει το σήμα προς τον εξουσιοδοτημένο αποδέκτη και να υποβαθμίσει την ποιότητα του σήματος προς τους επίδοξους υποκλοπείς. Αυτό επιτυγχάνετε κατά το σχεδιασμό του μεταδιδόμενου σήματος καθώς επίσης και κατά την επεξεργασία του.

Πρώτον , τα συστήματα PLS δεν βασίζονται σε λειτουργίες κρυπτογράφησης/ αποκρυπτογράφησης, ξεπερνώντας έτσι το δύσκολο έργο της διανομής και διαχείρισης των μυστικών κλειδιών σε ετερογενής περιβάλλοντα σε IOT εφαρμογές μεγάλης κλίμακας.

Δεύτερον, οι τεχνικές PLS μπορούν να αξιοποιήσουν πλήρως τα χαρακτηριστικά των ασύρματων καναλιών προχωρώντας σε κατάλληλο σχεδιασμό σήματος και κατανομή των διαθέσιμο πόρων, παρέχοντας έτσι ευέλικτες λύσεις και υλοποιήσεις με ποικίλα επίπεδα ασφαλείας, εξασφαλίζοντας παράλληλα ικανοποιητικά επίπεδα παρεχόμενων υπηρεσιών.

Τρίτον, οι τεχνικές PLS εκτελούν μόνο τους σχετικά απλούς αλγορίθμους επεξεργασίας σήματος, χωρίς την ανάγκη μεγάλης υπολογιστικής ισχύς, σε σύγκριση με την εκτέλεση των πολύπλοκων αλγόριθμων κρυπτογράφησης που εκτελούνται σε άλλα δίκτυα.

Παρόλο που η έρευνα και η ανάπτυξη τεχνικών PLS έχει επιφέρει καρπούς, εξακολουθεί να αποτελεί πρόκληση η ανάπτυξη λύσεων PLS για εφαρμογές IoT. Ειδικότερα, το IoT έχει τέσσερα μοναδικά χαρακτηριστικά: χαμηλό κόστος, ευρεία κάλυψη, μαζικές συνδέσεις και διαφοροποιημένες υπηρεσίες. Πώς να σχεδιαστούν στρατηγικές PLS που ικανοποιούν καλά με αυτά τα τέσσερα χαρακτηριστικά παραμένει ένα ανοιχτό πρόβλημα.

Βιβλιογραφική ανασκόπηση των τεχνικών PLS για το IoT

Η ασφάλεια στο φυσικό επίπεδο αναφέρθηκε στο μακρινό παρελθόν από τον Shannon στην έρευνα του με τίτλο «Communication theory of secrecy systems» (Shannon, 1949). Σύμφωνα με τη θεωρία του Shannon, το σύστημα θεωρείται ότι βρίσκεται σε τέλεια μυστικότητα εάν ικανοποιείται η ακόλουθη συνθήκη: H(M|X) = H(M), (1) όπου H(M) και H(M|X) είναι η εντροπία του μηνύματος M και η υπό συνθήκη εντροπία του M και X η παρακολούθηση του υποκλοπέα. Για την επίτευξη τέλειας μυστικότητας, ο κώδικας που χρησιμοποιείται για την κωδικοποίηση του μηνύματος πρέπει να είναι

ανεξάρτητος από το ίδιο το μήνυμα. Μια εφικτή προσέγγιση για την υλοποίηση αυτού του στόχου είναι η κρυπτογράφηση "one-time pad", είναι μία μέθοδος κρυπτογράφησης που χρησιμοποιεί ένα κλειδί μίας χρήσης για να κρυπτογραφήσει τα δεδομένα. Αυτό το κλειδί έχει την ιδιότητα ότι πρέπει να είναι τυχαίο, ακαταμάχητο και να μην επαναχρησιμοποιείται. Κάθε φορά που κρυπτογραφούμε ή αποκρυπτογραφούμε δεδομένα, χρησιμοποιούμε ένα νέο κλειδί της ιδίου μήκους με τα δεδομένα. Αυτό καθιστά τη μέθοδο ασφαλή, καθώς δυσκολεύει την αποκάλυψη των πληροφοριών ακόμα και αν ένα κρυπτογραφημένο κείμενο πέσει σε λάθος χέρια. Ωστόσο, η μέθοδος απαιτεί ασφαλή και απόλυτα τυχαία κλειδιά, κάτι που την καθιστά απαιτητική στην πράξη. Σε αντίθεση με το έργο του Shannon, ο Aaron Wyner πρότεινε «ένα κανάλι υποκλοπής με θόρυβο» μοντέλο το 1975. Σύμφωνα με αυτό το μοντέλο, το θορυβώδες κανάλι υποκλοπής αποτελείται από έναν νόμιμο πομπό (Alice), έναν νόμιμο δέκτη (Bob) και έναν υποκλοπέα (Eve). Στο μοντέλο του ο Wyner διατύπωσε τη συνθήκη για ασφαλή μετάδοση τονίζοντας ότι: η μετάδοση είναι θεωρητικά ασφαλής εάν η πιθανότητα σφάλματος αποκωδικοποίησης στο νόμιμο δέκτη μπορεί να είναι αυθαίρετα μικρή, ενώ καμία πληροφορία της πηγής δεν μπορεί να αποκτηθεί από τον υποκλοπέα. Ο μέγιστος ρυθμός με τον οποίο μπορεί να ικανοποιηθεί η παραπάνω συνθήκη ονομάζεται **ικανότητα απορρήτου**, η οποία χαρακτηρίζει τα όρια απόδοσης για ασφαλείς μεταδόσεις σε θορυβώδη κανάλια.

Ωστόσο, παρόλη τη μακρά περίοδο από τη δημοσίευση του έργου του Wyner, η τεχνική PLS δεν έχει προσελκύσει μεγάλη προσοχή. Αυτό αποδίδεται στους ακόλουθους λόγους: **πρώτον**, είναι εξαιρετικά δύσκολο να κατασκευαστούν πρακτικοί στοχαστικοί κώδικες με μικρή πολυπλοκότητα ώστε να επιτευχθεί η επιθυμητή ικανότητα απορρήτου. **Δεύτερον**, προκειμένου να επιτευχθεί η επιθυμητή ικανότητα απορρήτου SC (Secrecy Capacity), το λαμβανόμενο SNR (Signal-to-Noise Ratio) στον νόμιμο χρήστη πρέπει να είναι αυστηρά υψηλότερο από εκείνο στον υποκλοπέα, πράγμα που είναι δύσκολο να εξασφαλιστεί σε ασύρματα περιβάλλοντα. Η "secrecy capacity" αναφέρεται στη μέγιστη ποσότητα πληροφορίας που μπορεί να μεταδοθεί με απόλυτη μυστικότητα από έναν αποστολέα σε έναν παραλήπτη. Αυτή η ικανότητα καθορίζεται από την ασφάλεια του καναλιού επικοινωνίας και τη μορφή της κρυπτογράφησης που χρησιμοποιείται.

Συγκεκριμένα, η "secrecy capacity" μπορεί να οριστεί ως η διαφορά μεταξύ της κανονικής χωρητικότητας του καναλιού (η οποία μετρά την ποσότητα πληροφορίας που μπορεί να μεταδοθεί χωρίς κρυπτογράφηση) και της χωρητικότητας του καναλιού υπό την προϋπόθεση πλήρους μυστικότητας των μηνυμάτων.

Σκοπός της secrecy capacity είναι να παράσχει μία μέτρηση για την ασφάλεια μιας κρυπτογραφημένης επικοινωνίας και να βοηθήσει στον σχεδιασμό ασφαλών συστημάτων κρυπτογράφησης. **Τελευταίο** αλλά όχι λιγότερο σημαντικό, λίγο μετά την παρουσίαση της έννοιας της ικανότητας απορρήτου CS, οι Diffie και Hellman επινόησαν το δημόσιο κλειδί στην κρυπτογραφία. Το

"public-key" αναφέρεται σε ένα συστήματα κρυπτογράφησης που χρησιμοποιεί ένα ζεύγος κλειδιών για την κρυπτογράφηση και αποκρυπτογράφηση των μηνυμάτων.

Στο σύστημα κρυπτογράφησης με δημόσιο κλειδί, το ζεύγος κλειδιών αποτελείται από ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί. Το δημόσιο κλειδί είναι γνωστό σε όλους και χρησιμοποιείται για την κρυπτογράφηση των μηνυμάτων από τον αποστολέα. Αντίθετα, το ιδιωτικό κλειδί είναι μυστικό και γνωρίζεται μόνο από τον παραλήπτη, ο οποίος το χρησιμοποιεί για την αποκρυπτογράφηση των μηνυμάτων που έχουν κρυπτογραφηθεί με το δημόσιο κλειδί.

Το σύστημα δημόσιου κλειδιού επιτρέπει την ασφαλή επικοινωνία και την αποστολή μυστικών πληροφοριών μεταξύ δύο ή περισσότερων μερών, χωρίς την ανάγκη κοινής γνώσης του ιδιωτικού κλειδιού. Μπορεί να χρησιμοποιηθεί για ασφαλή ανταλλαγή πληροφοριών, διαδικτυακές συναλλαγές, αυθεντικοποίηση χρηστών κ.ά. Η ιδέα βασίζεται σε μαθηματικές συναρτήσεις που πιστεύεται ότι είναι δύσκολο να υπολογιστούν και έχει κυριαρχήσει στην έρευνα για την ασφάλεια, από τότε που παρουσιάστηκε. Λόγω των παραπάνω λόγων, η έρευνα της θεωρητικής ασφάλειας υποβαθμίστηκε στη δεκαετία 1970-1980.

Από τη δεκαετία του 1990, με την ευρεία διάδοση των τεχνικών ασύρματων επικοινωνιών καθώς και την αυξανόμενη δημοτικότητα των ασύρματων υπηρεσιών, το ζήτημα της ασφάλειας των ασύρματων δικτύων γίνεται όλο και πιο σημαντικό, γεγονός που αναζωπυρώνει το ερευνητικό ενδιαφέρον για τη θεωρητική ασφάλεια της πληροφορίας. Στο πλαίσιο αυτό, έχουν επιτευχθεί σημαντικές πρόοδοι στις μελέτες θεωρητικής ασφάλειας, κυρίως όσον αφορά την ανάλυση της secrecy capacity για διάφορα μοντέλα δικτύων.

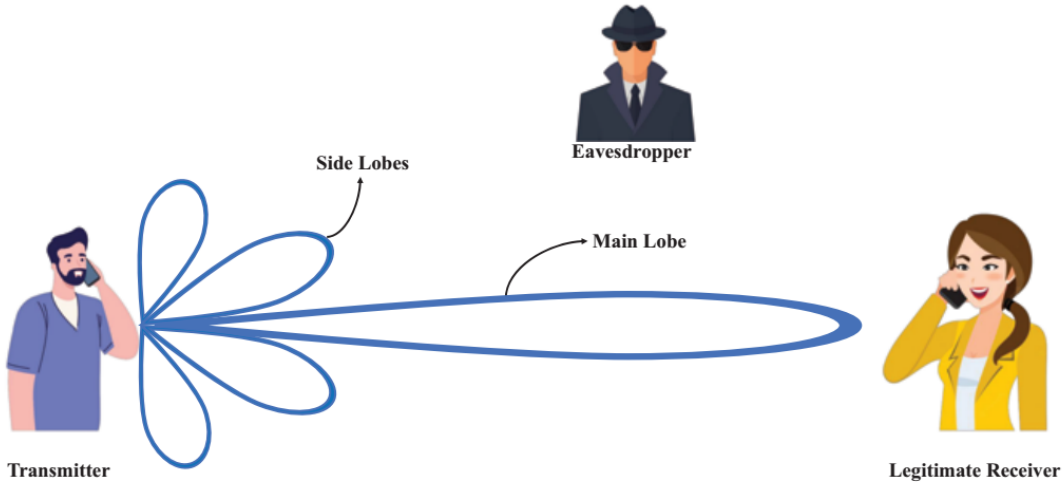
Με την ανάπτυξη της θεωρίας της πληροφορίας πολλαπλών χρηστών, το επίκεντρο της θεωρητικής ασφάλειας της πληροφορίας μετατοπίζεται επίσης από τα συστήματα σημείο-προς-σημείο στα συστήματα πολλαπλών χρηστών. Στα συστήματα πολλαπλών χρηστών, υπάρχει συνεργασία και παρεμβολές μεταξύ διαφορετικών χρηστών, γεγονός που δημιουργεί μεγάλες προκλήσεις στην ανάλυση της secrecy capacity του συστήματος και στο σχεδιασμό στρατηγικών PLS, και παρέχει σημαντικές ευκαιρίες έρευνας στο πεδίο αυτό.

Τα προαναφερθέντα ερευνητικά αποτελέσματα στις πληροφοριο-θεωρητικές μελέτες θέτουν τα θεμέλια για το σχεδιασμό πρακτικών στρατηγικών κωδικοποίησης και μετάδοσης της πληροφορίας, με άμυνα κατά των υποκλοπών και παρέχουν τα αναλυτικά εργαλεία για την αξιολόγηση των επιδόσεων των τεχνικών που εφαρμόστηκαν στο PLS.

Σχήματα PLS για το IoT:

Μέχρι στιγμής, έχουν αναπτυχθεί στη βιβλιογραφία πολλά σχήματα PLS, όπως (α) «την τεχνητή έγχυση θορύβου - artificial noise injection», (β) «τον ασφαλή σχηματισμό δέσμης/προκωδικοποίηση secure beamforming/precoding». Είναι

μια τεχνική που χρησιμοποιείται για να κατευθύνει την εκπομπή των ραδιοσημάτων από έναν πομπό προς έναν συγκεκριμένο παραλήπτη. Αυτός ο παραλήπτης λαμβάνει σήματα με μεγαλύτερη ισχύ συγκριτικά με τις παρεμβολές και τον θόρυβο, γεγονός που βελτιώνει την ποιότητα και την αξιοπιστία της επικοινωνίας.



Σχήμα 14: Τεχνική PLS που βασίζεται σε Beamforming

Η σχεδίαση του σχήματος συμπεριλαμβάνει την κρυπτογράφηση των δεδομένων που μεταδίδονται, την ανίχνευση και εξάλειψη των παρεμβολών, και την προστασία από επιθέσεις κατασκοπείας ή απάτης.

Η secure beamforming/precoding μπορεί να εφαρμοστεί σε διάφορους τύπους ασύρματων δικτύων, όπως ασύρματα δίκτυα αισθητήρων, ασύρματες επικοινωνίες δεδομένων ή ακόμη και σε κινητά δίκτυα. (γ) «το σχεδιασμό σήματος κατά της υποκλοπής - anti-eavesdropping signal design». Το αντι-παρακολούθησης (anti-eavesdropping) signal design αναφέρεται σε μια τεχνική που σχεδιάζει τα σήματα επικοινωνίας με σκοπό την αντιμετώπιση της παρακολούθησης ή της παρακολούθησης από έναν άγνωστο ή κακόβουλο τρίτο. Ο σχεδιασμός αυτός λαμβάνει υπόψη διάφορους μηχανισμούς προστασίας της απόρρητης επικοινωνίας, με στόχο την πρόληψη της παρακολούθησης των δεδομένων ή των μηνυμάτων από μη εξουσιοδοτημένους παρατηρητές. Αυτό μπορεί να περιλαμβάνει τη χρήση κρυπτογράφησης για να μετατρέψει τα δεδομένα σε ακαταλαβίστικη μορφή για τον επιτιθέμενο, καθώς και μηχανισμούς για την ανίχνευση και αποτροπή παραβιάσεων. Κατά τον σχεδιασμό των σημάτων αντι-παρακολούθησης (anti-eavesdropping), μπορούν να χρησιμοποιηθούν διάφορες τεχνικές. Αυτές μπορεί να περιλαμβάνουν τη χρήση ειδικών αλγορίθμων κρυπτογράφησης που προσφέρουν υψηλή ασφάλεια, τη χρήση αντι-παρακολούθησης των καναλιών επικοινωνίας για την ανίχνευση παρεμβολών ή παραπλανητικών σημάτων, και τη χρήση τεχνικών όπως η συντονισμένη διαμόρφωση σημάτων που αποσκοπεί στην αποτροπή ή την αποτροπή της παραβίασης της απόρρητης επικοινωνίας και αποτελεί σημαντικό μέτρο ασφαλείας στα ασύρματα δίκτυα

επικοινωνίας. (δ) «τις τεχνικές ασφαλούς μετάδοσης με βάση τη συνεργασία - cooperation-based secure transmission», (ε) «την κατανομή ισχύος και την κατανομή πόρων - power allocation and resource allocation» κ.λπ. Σε αυτό το υποκεφάλαιο, θα θέλαμε να παρουσιάσουμε μια βιβλιογραφική ανασκόπηση των σχημάτων PLS που είναι εφαρμόσιμα στο IoT.

Έγχυση τεχνητού θορύβου (Artificial Noise Injection)
Η “Έγχυση Τεχνητού Θορύβου” (Artificial Noise Injection) είναι μια τεχνική που χρησιμοποιείται σε διάφορους τομείς, όπως η ασφαλής ασύρματη επικοινωνία και η εκπαίδευση νευρωνικών δικτύων. Στο πλαίσιο της ασφαλούς ασύρματης επικοινωνίας, η Έγχυση Τεχνητού Θορύβου χρησιμοποιείται για τη βελτίωση του ρυθμού μυστικότητας των συστημάτων. Για παράδειγμα, σε ένα σύστημα προτείνεται μια μέθοδος έγχυσης τεχνητού θορύβου για να αποτρέψει έναν παράνομο δέκτη από το να κατασκοπεύει τις πληροφορίες που παρέχονται από τον πομπό στον δέκτη. Με αυτόν τον τρόπο, το AN υποβαθμίζει μόνο τον υποκλοπέα, αλλά έχει ελάχιστες επιπτώσεις στον νόμιμο δέκτη.

Η έκχυση AN έχει ως στόχο να δημιουργήσει ένα ποιοτικό κανάλι επικοινωνίας για τους εξουσιοδοτημένους χρήστες από τον πομπό μέχρι τον δέκτη. Ωστόσο, τα περισσότερα από τα σχήματα PLS με βάση το AN βασίζονται στην ανάπτυξη πολλαπλών κεραιών στον πομπό (Zhang, McKay, Zhou, & Heath, 2015) (Wang, Meng, Heng, & Chen, 2018), το οποίο παραβιάζει την απαίτηση χαμηλού κόστους υλοποιήσεις και μικρού μεγέθους των συσκευών IoT. Για την αντιμετώπιση αυτού του ζητήματος, η συνεργατική έγχυση AN γίνεται μια πολλά υποσχόμενη λύση για τη διασφάλιση της ασφαλούς μετάδοσης σε IoT περιβάλλοντα. (Hu L. Wen, 2018). Για να αποκαλυφθεί η απόδοση ασφάλειας που επιτυγχάνεται από αυτές τις στρατηγικές, αναλύθηκε η πιθανότητα απώλειας μυστικότητας του συστήματος με πολλαπλούς συνεργαζόμενους παρεμβολείς και πολλαπλούς υποκλοπείς. Ο συνδυασμός της έγχυσης AN με άλλες τεχνικές ασφαλούς μετάδοσης μπορεί να βελτιώσει περαιτέρω τις επιδόσεις ασφάλειας του συστήματος. (Sun, Ren, Du, & Wang, Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks., 2016). Συνδιάζοντας την τεχνική συμπιεστικής ανίχνευσης με την τεχνική έγχυσης AN, βελτιώνεται η ασφάλεια του συστήματος ενώ παράλληλα μειώνεται η επιβάρυνση ανατροφοδότησης.

Compressive Sensing
Η συμπιεστική ανίχνευση (CS) μπορεί να συμπιέσει σήματα με πολύ χαμηλότερο ρυθμό σε σύγκριση με τον ρυθμό δειγματοληψίας Nyquist. Ο ρυθμός δειγματοληψίας Nyquist είναι σημαντική έννοια στον τομέα της σήματος και της επεξεργασίας σήματος. Ο Νόμος του Nyquist, που διατυπώθηκε από τον επιστήμονα Claude Shannon, καθορίζει τον ελάχιστο ρυθμό δειγματοληψίας που απαιτείται για να ανακατασκευαστεί μια συχνότητα σε ένα ψηφιακό σύστημα. Η ακριβής δήλωση του νόμου είναι ότι η συχνότητα δειγματοληψίας πρέπει να είναι τουλάχιστον διπλάσια από τη μέγιστη συχνότητα του σήματος που καταγράφεται. Αν δεν τηρηθεί ο νόμος του Nyquist, μπορεί να προκύψει φαινόμενο που ονομάζεται "αλληλουχία". Αυτό συμβαίνει

όταν η συχνότητα ενός σήματος υπερβαίνει το μισό του ρυθμού δειγματοληψίας, και το αποτέλεσμα είναι η παραποίηση του σήματος κατά τη δειγματοληψία. Πρόσφατα, η τεχνική CS χρησιμοποιήθηκε για την υλοποίηση της ασφάλειας φυσικού επιπέδου (Mukherjee, 2015). Στο CS, ένας γραμμικός μετασχηματισμός εφαρμόζεται στο σήμα που φέρει πληροφορίες πολλαπλασιάζοντάς το με έναν πίνακα μέτρησης. Το απόρρητο μετάδοσης μπορεί να διασφαλιστεί εάν ο πίνακας μέτρησης είναι άγνωστος στον υποκλοπέα. Για την επίτευξη αυτού του στόχου, (Dautov & Tsouri, 2016) προτάθηκε ένα σχήμα που χρησιμοποιεί μια ακολουθία m για την κατασκευή του πίνακα μέτρησης. Στην συνέχεια (Choi, 2016) αναπτύχθηκε ένα σύστημα κρυπτογράφησης με βάση το CS για συστήματα πολλαπλών φορέων. Προκειμένου να μειωθεί η πιθανότητα ορθής ανάκτησης του πίνακα μέτρησης από τον επιτιθέμενο, οι συγγραφείς πρότειναν τη μετάδοση τεχνητού θορύβου μαζί με το μήνυμα. Επιπλέον, η κατάσταση του καναλιού (CSI-Channel State information) αξιοποιήθηκε για την επιλεκτική μετάδοση ενός τεχνητού θορύβου, έτσι ώστε η αρνητική επίδραση στον νόμιμο δέκτη μπορεί να ελαχιστοποιηθεί.

Ακολούθως, μελετήθηκε η απόδοση ασφαλείας κρυπτοσυστήματος με βάση το CS (Yu, 2017). Η ανάλυση εκεί δείχνει ότι το κρυπτοσύστημα με βάση το CS με κυκλικούς πίνακες πάνω από ασύρματα κανάλια μπορεί να είναι υπολογιστικά ασφαλές όσον αφορά την δυνατότητα διάκρισης, εφόσον τα κέρδη του καναλιού και ο λόγος καθαρού κειμένου προς θόρυβο του επιτιθέμενου διατηρούνται σε χαμηλά επίπεδα για μια μεγάλη ροή κλειδιών και σύντομο κρυπτογραφημένο κείμενο. Η τεχνική CS χρησιμοποιείται επίσης για την επίτευξη ασφάλειας φυσικού επιπέδου σε συνεργατικά συστήματα πολλαπλών κόμβων, όπου ο πίνακας καναλιού μεταξύ πολλαπλών πηγών και πολλαπλών αναμεταδοτών θεωρείται ως πίνακας μέτρησης CS (Barcelo-Llado, Morell, & Seco-Granados, Amplify-and-forward compressed sensing as an energy-efficient solution in wireless sensor networks., 2014).

Όπως φαίνεται από την έρευνα των (Barcelo-Llado, Morell, & Seco-Granados, G. Amplify-and-forward compressed sensing as a physical-layer secrecy solution in wireless sensor networks. , 2014), με την υιοθέτηση αυτής της μεθόδου, η πιθανότητα ανάκτησης σήματος από τον υποκλοπέα είναι μηδενική. Πρέπει να σημειωθεί ότι η έρευνα επικεντρώθηκε μόνο σχετικά με τη ασφαλεία μετάδοσης σε dual-hop συστήματα με CS. Σε αντίθεση η έρευνα των (Q, Han, & Fu, 2018) χρησιμοποίησε το multi-hops για να την υλοποιήση του CS, επιτυγχάνοντας έτσι ασφάλεια στην επικοινωνία χωρίς κλειδί, για δίκτυα πολλαπλών βημάτων (multi-hop).

Bit Flipping

Η τεχνική αντιστροφής bit εφαρμόζεται κυρίως για να εξασφαλιστεί η ασφάλεια των επικοινωνιών μεταξύ των πολλαπλών κόμβων και του νόμιμου κέντρου σύντηξης (LFC- legitimate fusion center). Τα κέντρα συγχώνευσης πληροφοριών συγκεντρώνουν, αναλύουν και μοιράζονται πληροφορίες από διάφορες πηγές για να ενισχύσουν την κατανόηση και την αντιμετώπιση απειλών ασφαλείας. Σε αυτή την προσέγγιση, οι κόμβοι αισθητήρων χωρίζονται

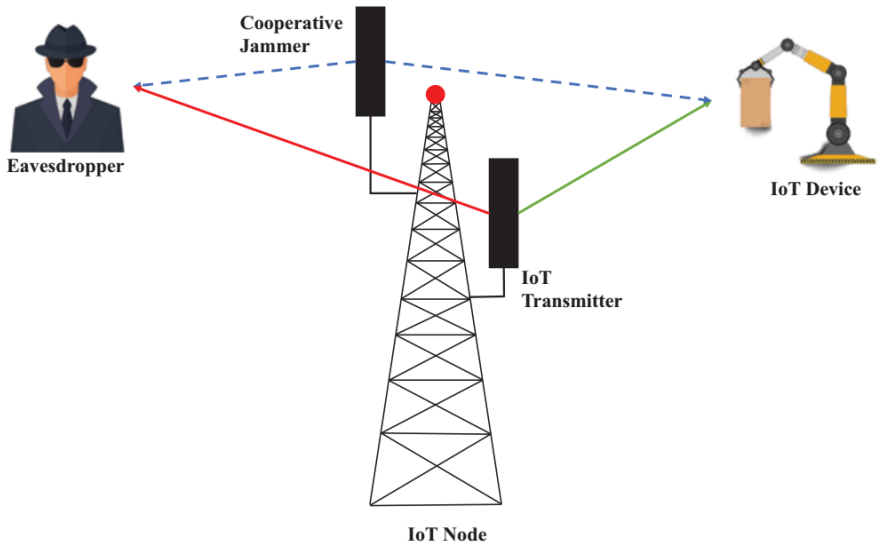
σε δύο ομάδες (μια ισχυρή ομάδα και μια αδύναμη ομάδα) με βάση τη δύναμη του καναλιού τους στο LFC. Οι αισθητήρες με χειρότερες ιδιότητες καναλιού, οι οποίοι κατηγοριοποιούνται στην αδύναμη ομάδα, απαιτείται να στέλνουν τα bit-flipped δεδομένα, δηλαδή ψευδή δεδομένα, για να παρεμποδίσουν την υποκλοπή από το κέντρο του υποκλοπέα (EFC- eavesdropping fusion center), ενώ οι αισθητήρες με καλύτερες ιδιότητες καναλιού (δηλαδή αυτοί που ανήκουν στην ισχυρή ομάδα) χρησιμοποιούνται για την αποστολή των δεδομένων που φέρουν πληροφορίες.

Λόγω της στατιστικής ανεξαρτησίας μεταξύ του νόμιμου καναλιού και του καναλιού υποκλοπής, υπάρχει μεγάλη πιθανότητα, το λαμβανόμενο SNR (Signal-to-noise ratio) στο EFC(eavesdropping fusion center) είναι πολύ χαμηλότερο από εκείνο στο LFC(legitimate fusion center), αποδίδοντας έτσι σημαντική υποβάθμιση της απόδοσης στο EFC.

Κατά τη διάρκεια μετάδοσης των πραγματικών δεδομένων, οι αισθητήρες που ανήκουν στην ισχυρή ομάδα μεταδίδουν τα πραγματικά δεδομένα, ενώ οι αισθητήρες που ανήκουν στην αδύναμη ομάδα στέλνουν τα ψεύτικα δεδομένα με αντιστροφή του bit για να προκαλέσουν σύγχυση στο EFC (eavesdropping fusion center). Ακολουθεί μια εργασία των (Jeon, Hwang, Choi, Lee, & Ha, 2011) και (Jeon, Choi, McLaughlin, & Ha, 2013), με μια μετάδοση τριών κατωφλίων όπου όλοι οι αισθητήρες χωρίζονται σε τρεις ομάδες. Εκτός από τους αισθητήρες που μεταδίδουν τα πραγματικά δεδομένα και τα ψευδή δεδομένα, υπάρχουν και κάποιοι άλλοι αισθητήρες που παραμένουν σιωπηλοί κατά τη διάρκεια της μετάδοσης.

Cooperative Secrecy - Jamming

Το IoT αποτελείται συνήθως από μαζικά φυσικά αντικείμενα, όπως αισθητήρες (sensors), ελεγκτές (controllers) και ενεργοποιητές (actuators). Αν και η ικανότητα επεξεργασίας κάθε μιας συσκευής είναι περιορισμένη, οι απαιτήσεις απορρήτου των χρηστών μπορούν να ικανοποιηθούν με την αξιοποίηση της συνεργασίας μεταξύ αυτών των συσκευών χαμηλής ισχύος. Η βασική ιδέα της συνεργατικής μυστικότητας (Cooperative Secrecy) είναι να επιτρέπουμε στους φιλικούς κόμβους να λειτουργούν ως παρεμβολείς για να στέλνουν τεχνητές παρεμβολές για να υποβαθμίσουν τη λήψη σήματος στον υποκλοπέα.



Σχήμα 15: Τεχνική PLS που βασίζεται σε Cooperative Jamming

Η έρευνα των (Dong, Han, Petropulu, & Poor, 2010) ανέπτυξε τη στρατηγική «συνεργατικό μπλοκάρισμα» (CJ-cooperative jamming) για συστήματα ενίσχυσης και προώθησης (AF-amplify-and-forward) και αποκωδικοποίησης και προώθησης (DF-decode-and-forward), αντίστοιχα, όπου οι κόμβοι αναμετάδοσης μεταδίδουν ανεξάρτητα τους σταθμισμένους τεχνητούς θορύβους για να επιδεινώσουν το κανάλι του υποκλοπέα.

Η έρευνα των (Hu, και συν., 2018) συνδύασε τον ασφαλή σχηματισμό δέσμης με τη συνεργατική παρεμβολή για την ενίσχυση της ασφάλειας του φυσικού στρώματος. Εκτός από τη συνεργατική παρεμβολή, μια άλλη δημοφιλής προσέγγιση συνεργατικής μυστικότητας είναι η τεχνική «ασφαλούς επιλογής αναμεταδότη». Η έρευνα των (Krikidis, Thompson, & McLaughlin, 2009) ανέπτυξε μια πολιτική επιλογής, για την επιλογή των πληροφοριών και τον φιλικό παρεμβολέα, και εισήγαγε έναν προσαρμοστικό μηχανισμό για την επιλογή του τρόπου συνεργασίας έτσι ώστε να ελαχιστοποιείται η πιθανότητα διακοπής της μυστικότητας.

Physical Layer Encryption

Αντί να κοινοποιηθεί άμεσα ένα μυστικό μήνυμα χρησιμοποιώντας τις προαναφερθέντες PLS τεχνικές, η Alice και ο Bob μπορούν επίσης να εκμεταλλευτούν το θορυβώδες κανάλι για να δημιουργήσουν ένα μυστικό κλειδί και να χρησιμοποιήσουν αυτό το κλειδί ως one-time pad για να εξασφαλίσουν πληροφοριοθεωρητική ασφάλεια. Από πρακτική άποψη, ο σχεδιασμός συστημάτων με κρυπτογράφηση φυσικού στρώματος από παρατηρήσεις του καναλιού μετάδοσης, αποδεικνύεται ότι είναι ένα απλούστερο πρόβλημα από την κατασκευή κωδικών από το παγιδευμένο κανάλι. Η **διαδικασία παραγωγής κλειδιού** στο φυσικό επίπεδο περιλαμβάνει κυρίως τέσσερα βήματα: **(1) Διερεύνηση καναλιού**: Η διερεύνηση καναλιού (channel probing) αναφέρεται στη διαδικασία όπου ένα ασύρματο σύστημα ελέγχει τη διαθεσιμότητα και τις συνθήκες επικοινωνίας σε διάφορα κανάλια

ραδιοσυχνοτήτων προτού επιλέξει το κατάλληλο κανάλι για τη μετάδοση δεδομένων. **(2) Κβάντιση παραμέτρων (Parameter quantization)**: Η παραμετρική κβαντοποίηση (parameter quantization) αναφέρεται στη διαδικασία μείωσης του αριθμού των bits που χρησιμοποιούνται για να αναπαρασταθούν οι παράμετροι ενός μοντέλου ή ενός συστήματος. Κατά τη διάρκεια της κβαντοποίησης, οι πραγματικές τιμές των παραμέτρων αντικαθίστανται από κβαντισμένες (περιορισμένους) αριθμούς bits. Η κβαντοποίηση εισόδου και εξόδου μπορεί να γίνει επίσης για τη μείωση των απαιτήσεων σε μνήμη ή τον υπολογιστικό φόρτο. Οι προκλήσεις της παραμετρικής κβαντοποίησης περιλαμβάνουν την εύρεση της ισορροπίας μεταξύ μείωσης της πολυπλοκότητας του μοντέλου και διατηρησιμότητας της ακρίβειας της πρόβλεψης. Παρά τα προβλήματα, η παραμετρική κβαντοποίηση είναι μια τεχνική που χρησιμοποιείται για την εφαρμογή μοντέλων μηχανικής μάθησης σε περιορισμένους πόρους, όπως κινητές συσκευές ή συστήματα με περιορισμένη ενέργεια. **(3) Συμφιλίωση πληροφοριών (Information reconciliation)**: Η "συμφιλίωση πληροφοριών" (information reconciliation) είναι μια διαδικασία που εφαρμόζεται σε κρυπτογραφικά πρωτόκολλα, κυρίως σε πρωτόκολλα κβαντικής κρυπτογραφίας. Στο πλαίσιο της κβαντικής κρυπτογραφίας, τα συστήματα συχνά χρησιμοποιούνται για την ασφαλή μεταφορά και ανταλλαγή κρυπτογραφημένων πληροφοριών μεταξύ δύο ή περισσότερων συνεργαζόμενων σταθμών. Η συμφιλίωση πληροφοριών συμβαίνει μετά από μια φάση της διαδικασίας που ονομάζεται "κβαντική διανομή κλειδιών" (quantum key distribution - QKD). Κατά τη διάρκεια της QKD, δύο μέρη χρησιμοποιούν τα κβαντικά χαρακτηριστικά των φωτόνων για να δημιουργήσουν ένα ασφαλές κοινό κλειδί που χρησιμοποιείται για την κρυπτογράφηση των μηνυμάτων τους.

Η συμφιλίωση πληροφοριών αναφέρεται στη διαδικασία επαλήθευσης και ευθυγράμμισης των κλειδιών που δημιουργήθηκαν από τα δύο μέρη κατά τη διάρκεια της QKD. Κατά τη συμφιλίωση, ελέγχεται αν τα κλειδιά που έχουν δημιουργηθεί είναι συμβατά μεταξύ των δύο μερών. Αν υπάρχουν ασυμφωνίες, η διαδικασία επαναλαμβάνεται για να διασφαλιστεί η ασφάλεια των κρυπτογραφημένων επικοινωνιών. Η συμφιλίωση πληροφοριών είναι κρίσιμη για την εξασφάλιση ότι οι χρήστες έχουν ένα κοινό κλειδί που μπορεί να χρησιμοποιηθεί ασφαλώς για την κρυπτογράφηση και αποκρυπτογράφηση των μηνυμάτων τους. **(4) Ενίσχυση της ιδιωτικότητας (Privacy amplification)**: Η "ενίσχυση απορρήτου" (Privacy amplification) αναφέρεται σε μια διαδικασία που χρησιμοποιείται στο πλαίσιο της κβαντικής κρυπτογραφίας, συγκεκριμένα στη φάση της κβαντικής διανομής κλειδιών (Quantum Key Distribution - QKD).

Κατά την διάρκεια της QKD, μπορεί να υπάρχουν πιθανοί κίνδυνοι ή απειλές που μπορεί να αποκαλύψουν μέρος του κοινού κλειδιού. Η διαδικασία της ενίσχυσης του απορρήτου χρησιμοποιείται για να μειώσει τον κίνδυνο αποκάλυψης πληροφοριών, εξασφαλίζοντας ένα ασφαλές και ανθεκτικό κοινό κλειδί. Η διαδικασία της ενίσχυσης του απορρήτου περιλαμβάνει συνήθως τη χρήση ενός κρυπτογραφικού αλγορίθμου (όπως το Universal Hash Function) για να επεξεργαστεί το αρχικό κοινό κλειδί και να παράγει ένα νέο κλειδί, το

οποίο είναι ασφαλές από τις πιθανές απειλές που μπορεί να υπάρχουν. Αυτό το νέο κλειδί θα χρησιμοποιηθεί για την πραγματοποίηση ασφαλών κρυπτογραφημένων επικοινωνιών μεταξύ των συσκευών. Η ενίσχυση του απορρήτου είναι σημαντική για τη διατήρηση της ασφάλειας των κρυπτογραφημένων κλειδιών ακόμα και αν υπάρχουν απειλές ή επιθέσεις κατά τη διάρκεια της QKD.

Η έρευνα του (Zeng, 2015) παρουσίασε μια ολοκληρωμένη ανασκόπηση των τεχνικών κρυπτογράφησης του φυσικού επιπέδου, επισημαίνοντας τις σημαντικότερες τεχνικές αλλά και τις προκλήσεις και λύσεις. Η έρευνα του (Wilson, Tse, & Scholtz, 2007) διερεύνησε το ζήτημα της δημιουργίας μυστικού κλειδιού για τα κανάλια υπερ-ευρείας ζώνης (UWB), όπου η απόκριση παλμού του νόμιμου καναλιού χρησιμοποιείται ως τυχαία πηγή για την εξαγωγή των κλειδιών. Η έρευνα των (Premnath, και συν., 2013) χρησιμοποίησε την ισχύ του λαμβανόμενου σήματος όπως την κοινή τυχαιότητα για τους νόμιμους χρήστες, η οποία έχει χαμηλή πολυπλοκότητα υλοποίησης.

Εκτός από τις παραπάνω "ντετερμινιστικές" τεχνικές κρυπτογράφησης όπου η αντιστοίχιση ένα προς ένα είναι μεταξύ του απλού κειμένου και του κρυπτογραφημένου κειμένου, υπάρχει και μια άλλη μέθοδος κρυπτογράφησης που ονομάζεται πιθανολογική κρυπτογράφηση.

ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΩΝ ΥΦΙΣΤΑΜΕΝΩΝ ΤΕΧΝΙΚΩΝ PLS

Κάθε μία από τις προαναφερθείσες τεχνικές PLS έχει τα πλεονεκτήματα και τα μειονεκτήματά της. Η έγχυση AN είναι εύκολο να εφαρμοστεί, επειδή οι τεχνητοί θόρυβοι μπορούν να παραχθούν με τη χρήση ενός ψευδοτυχαίου αριθμού με μια γεννήτρια τυχαίων αριθμών, για την οποία μπορούν να χρησιμοποιηθούν άμεσα πολλοί υπάρχοντες αλγόριθμοι. Ωστόσο, το κέρδος μυστικότητας που προσφέρει η προσέγγιση έγχυσης AN έχει ως κόστος την πρόσθετη κατανάλωση ενέργειας, η οποία χρησιμοποιείται για την αποστολή του σήματος τεχνητού θορύβου. Σε σύγκριση με την τεχνική έγχυσης AN, η μέθοδος Compressive Sensing ως τεχνική ασφαλούς μετάδοσης δεν βασίζεται στη δαπάνη πρόσθετης ισχύος και συνεπώς είναι πιο ενεργειακά αποδοτική. Ωστόσο, ένας πίνακας μέτρησης πρέπει να μοιράζεται μεταξύ των νόμιμων πομποδεκτών, ενώ πρέπει να διατηρηθεί μυστικός από τους υποκλοπείς, γεγονός που απαιτεί προσυμφωνημένη γνώση σχετικά με το CS σε διαφορετικούς αποδέκτες. Αυτό προκαλεί μη αμελητέα επιβάρυνση στο σχεδιασμό του πρωτοκόλλου. Η τεχνική αντιστροφής bit μπορεί να μειώσει σημαντικά την πολυπλοκότητα της υλοποίησης και να ξεπεράσει τις αδυναμίες της CS-based (Compressive Sensing) προσέγγισης. Ωστόσο, στη μέθοδο εναλλαγής bit (Bit Flipping), οι αισθητήρες εντός της αδύναμης ομάδας πρέπει να μεταδώσουν τα ψευδή δεδομένα για να μπερδέψουν τον υποκλοπέα, με αποτέλεσμα τη σπατάλη ισχύος και εύρους ζώνης. Το συνεργατικό απόρρητο (Cooperative Secrecy) μπορεί να είναι η πιο ευρέως υιοθετημένη προσέγγιση PLS. Η εισαγωγή του μηχανισμού συνεργασίας προσφέρει στις συσκευές

χαμηλής ισχύος τη δυνατότητα καταπολέμησης των ισχυρών υποκλοπέων με κατανάλωση σε λιγότερους πόρους. Ωστόσο, το σημαντικότερο μειονέκτημα της τεχνικής του συνεργατικού απορρήτου είναι ότι απαιτείται πρόσθετη σηματοδοσία για το συντονισμό των διαφόρων συσκευών εντός του δικτύου, γεγονός που περιπλέκει το σχεδιασμό του πρωτοκόλλου. Η κρυπτογράφηση φυσικού επιπέδου είναι ουσιαστικά μια προσέγγιση πολλαπλών επιπέδων,

η οποία συνδυάζει τη δημιουργία μυστικού κλειδιού στο φυσικό επίπεδο και την κρυπτογράφηση στο επίπεδο εφαρμογής. Το μεγαλύτερο πλεονέκτημα αυτής της προσέγγισης είναι ότι μπορεί εύκολα να ενσωματωθεί με τα υπάρχοντα πρωτόκολλα ασφαλείας δικτύου, η οποία βασίζεται σε τεχνικές κρυπτογράφησης στο επίπεδο εφαρμογής. Από την άλλη πλευρά, η αποτελεσματικότητα της κρυπτογράφησης φυσικού επιπέδου εξαρτάται σε μεγάλο βαθμό από το γεγονός ότι τα επικοινωνούντα μέρη πρέπει να καταλήξουν σε συμφωνία σχετικά με τα παραγόμενα κλειδιά, πράγμα που είναι μάλλον δύσκολο σε ασύρματα περιβάλλοντα.

ΠΡΟΚΛΗΣΕΙΣ ΣΤΗΝ ΣΧΕΔΙΑΣΗ ΤΟΥ PLS ΠΡΩΤΟΚΟΛΛΟΥ ΓΙΑ ΤΟ Internet of Things

Όπως αναφέρθηκε προηγουμένως, η έρευνα των τεχνικών PLS έχει δημιουργήσει ένα μεγάλο όγκο βιβλιογραφίας, που κυμαίνεται από θεμελιώδεις πληροφοριοθεωρητικές μελέτες έως τον πρακτικό σχεδιασμό πρωτοκόλλων PLS. Ωστόσο για να σχεδιαστούν στρατηγικές PLS που να ταιριάζουν καλά με τα μοναδικά χαρακτηριστικά του IoT εξακολουθεί να είναι μια ανοιχτή πρόκληση. Η πλειονότητα των γνωστών τεχνικών PLS έχουν τα ακόλουθα μειονεκτήματα που απαγορεύουν την άμεση εφαρμογή τους στο IoT.

Πρώτον, οι συσκευές IoT χαρακτηρίζονται από "χαμηλό κόστος", πράγμα που σημαίνει ότι αυτές οι συσκευές έχουν συνήθως πολύ περιορισμένες δυνατότητες μνήμης αποθήκευσης και επεξεργασίας. Επιπρόσθετα, οι συσκευές IoT τροφοδοτούνται κυρίως με μπαταρίες, γεγονός που επιβάλλει σημαντικούς ενεργειακούς περιορισμούς. Τα χαρακτηριστικά, χαμηλό κόστος και η χαμηλή κατανάλωση ενέργειας επιβάλουν οι στρατηγικές PLS να είναι ιδιαίτερα ενεργειακά αποδοτικές και να μπορούν να υλοποιηθούν με πολύ χαμηλή πολυπλοκότητα. Για παράδειγμα μια στρατηγική που βασίζεται σε έγχυση τεχνητών σημάτων θορύβου (Artificial Noise Injection), αυτό συνεπάγεται πρόσθετη κατανάλωση ενέργειας. Ομοίως μια στρατηγική που βασίζεται σε μεθόδους διαμόρφωσης δέσμης/ προκωδικοποίησης (beamforming/precoding) αυτό συνεπάγεται τη χρήση πολλαπλών κεραιών από την πλευρά του πομπού, η οποία είναι ανέφικτη λαμβάνοντας υπόψη το μέγεθος και το κόστος των συσκευών IoT. Ενισχύοντας τα παραπάνω η στρατηγική της συνεργασίας (Cooperative Secrecy) απαιτούν την ύπαρξη φιλικών παρεμβολών που στέλνουν σήματα παρεμβολής, τα οποία επίσης περιπλέκουν το σχεδιασμό του πρωτοκόλλου και αυξάνουν την κατανάλωση ισχύος. Από πρακτική άποψη, τα πρωτόκολλα PLS με προσανατολισμό στο IoT πρέπει να λαμβάνουν υπόψη τους περιορισμούς πόρων των συσκευών IoT, και

να κάνουν συμβιβασμό μεταξύ της ασφάλειας, της πολυπλοκότητας και της κατανάλωσης ενέργειας.

Δεύτερον, από την οπτική της δικτύωσης, το IoT αναμένεται να υποστηρίξει μετάδοση ευρείας εμβέλειας. Για παράδειγμα, στα ασύρματα δίκτυα αισθητήρων, τα οποία είναι μια υλοποίηση του IoT, τα τοπικά δεδομένα που συλλέγονται από αισθητήρες πρέπει να παραδίδονται στο απομακρυσμένο κέντρο ελέγχου για περαιτέρω επεξεργασία. Ωστόσο, η απόσταση μετάδοσης ενός βήματος (single-hop) στο IoT είναι μάλλον περιορισμένη λόγω της χαμηλής ισχύος των συσκευών IoT. Επομένως, για να αντιμετωπιστεί η απαίτηση κάλυψης ευρείας εμβέλειας, τα πρωτόκολλα μετάδοσης δικτύου πρέπει να ενσωματώσουν πολλά νέα χαρακτηριστικά, όπως δρομολόγηση πολλαπλών βημάτων, συνεργατική αναμετάδοση, γνωστική μετάδοση, κ.λπ. Αυτό με τη σειρά του απαιτεί οι στρατηγικές PLS να είναι αρκετά "έξυπνες" ώστε να προσαρμόζονται σε περίπλοκα περιβάλλοντα δικτύων. Για παράδειγμα, οι συσκευές IoT πρέπει να συνεργάζονται με πολλούς αναξιόπιστους γειτονικούς κόμβους. Αν και αυτοί οι μη αξιόπιστοι κόμβοι μπορεί να μην είναι απαραίτητα κακόβουλες οντότητες, είναι πιθανό να είναι μη πιστοποιημένοι και με χαμηλότερο επίπεδο ασφαλείας από τις συσκευές IoT. Πώς μπορούμε να εκμεταλλευτούμε τους αναξιόπιστους κόμβους για να βοηθήσουν την παράδοση πληροφοριών, διατηρώντας παράλληλα το περιεχόμενο των δεδομένων απόρρητο σε αυτούς; Πόσο μπορεί να επηρεάσει ο αριθμός των μη αξιόπιστων αναμεταδοτών την απόδοση της ασφάλειας του δικτύου; Αυτά τα ζητήματα δεν έχουν γίνει ακόμη πλήρως κατανοητά και απαιτείται μια πιο εμπεριστατωμένη έρευνα.

Τρίτον, το IoT στοχεύει στην ικανότητα παροχής μαζικών συνδέσεων που μπορεί να φιλοξενήσει εκατομμύρια συσκευές ανά τετραγωνικό χιλιόμετρο για την ανταλλαγή πληροφοριών. Επιπλέον, οι συσκευές του IoT, που παράγονται από διαφορετικές εταιρείες, είναι ετερογενείς κόμβοι με εντελώς διαφορετικούς τύπους υπηρεσιών, μοτίβα κυκλοφορίας και τρόπους μετάδοσης. Αυτά τα χαρακτηριστικά καθιστούν το IoT ένα ετερογενές δίκτυο μεγάλης κλίμακας, για το οποίο το ζήτημα της επεκτασιμότητας αποτελεί πρωταρχικό μέλημα. Ωστόσο, τα υπάρχοντα συστήματα PLS έχουν κυρίως αναπτυχθεί για δίκτυα μικρής κλίμακας, για τα οποία έχουν γίνει μετρήσεις απόδοσης μόνο σε επίπεδο σύνδεσης, π.χ. ποσοστό μυστικότητας, πιθανότητα υποκλοπής πληροφοριών κ.λπ. Αρκετά θεμελιώδη προβλήματα για την ασφαλή μετάδοση σε δίκτυα μεγάλης κλίμακας δεν αντιμετωπίζονται όπως πρέπει. Για παράδειγμα, πώς διασφαλίζεται η μυστικότητα του συστήματος με τον μεγάλο αριθμό κόμβων στο δίκτυο; Πώς μπορούμε να μετατρέψουμε την ικανότητα του δικτύου για μαζικές συνδέσεις σε έναν ισχυρό εργαλείο κατά των υποκλοπών; Για να απαντήσουμε σε αυτά τα ερωτήματα, πρέπει να αναπτυχθούν νέα μαθηματικά εργαλεία και καινοτόμα πρωτόκολλα μετάδοσης δικτύου πρέπει να επινοηθούν.

Τέταρτον, το μελλοντικό IoT αναμένεται να υποστηρίζει διάφορα σενάρια ασύρματων λύσεων με διαφορετικές υπηρεσίες. Διαφορετικοί τύποι υπηρεσιών έχουν εντελώς διαφορετικές απαιτήσεις όσον αφορά την ασφάλεια, την

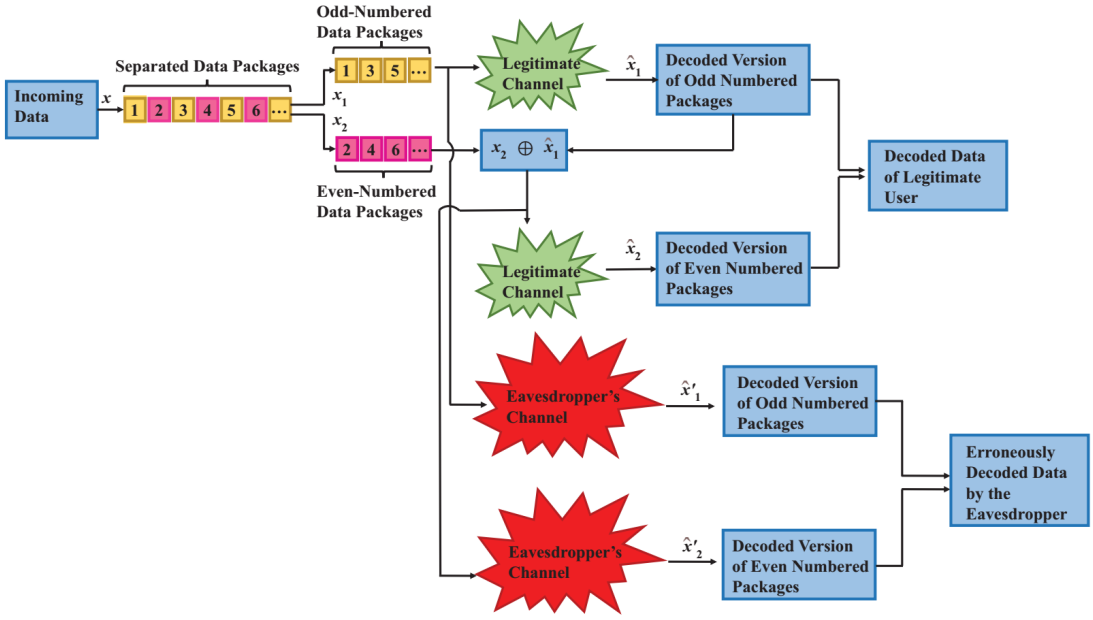
καθυστέρηση, την απόδοση, και την αξιοπιστία μετάδοσης. Ωστόσο, η πλειονότητα των υφιστάμενων πρωτοκόλλων PLS στοχεύει απλώς στην βελτιστοποίηση του ρυθμού μυστικότητας ή της πιθανότητας διακοπής μυστικότητας από υποκλοπές. Έτσι, είναι αδύνατο να παρέχουν ολοκληρωμένη διασφάλιση του QoS (Quality of Service) για εφαρμογές IoT. Για να ξεπεραστεί αυτή η δυσκολία, ο σχεδιασμός του πρωτοκόλλου PLS θα πρέπει να εξετάζει από κοινού διάφορες πτυχές των απαιτήσεων των χρηστών, συμπεριλαμβανομένων της καθυστέρησης, της αξιοπιστίας και της απόδοσης, παράλληλα με την μυστικότητα.

ΚΕΦΑΛΑΙΟ 4: ΥΠΟΣΧΟΜΕΝΕΣ ΛΥΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΦΥΣΙΚΟΥ ΕΠΙΠΕΔΟΥ ΣΤΟ IoT

Όπως περιεγράφηκε στην προηγούμενη ενότητα, το IoT έχει τέσσερα rnημοναδικά χαρακτηριστικά σε σύγκριση με τα παραδοσιακά ασύρματα δίκτυα: χαμηλό κόστος, ευρεία κάλυψη, μαζικές συνδέσεις και διαφοροποιημένες υπηρεσίες. Στην συνέχεια, θα θέλαμε να επισημάνουμε τρεις αναδυόμενες τεχνικές PLS που ταιριάζουν καλά με αυτά τα χαρακτηριστικά του IOT και είναι πολλά υποσχόμενες σε μελλοντικές εφαρμογές.

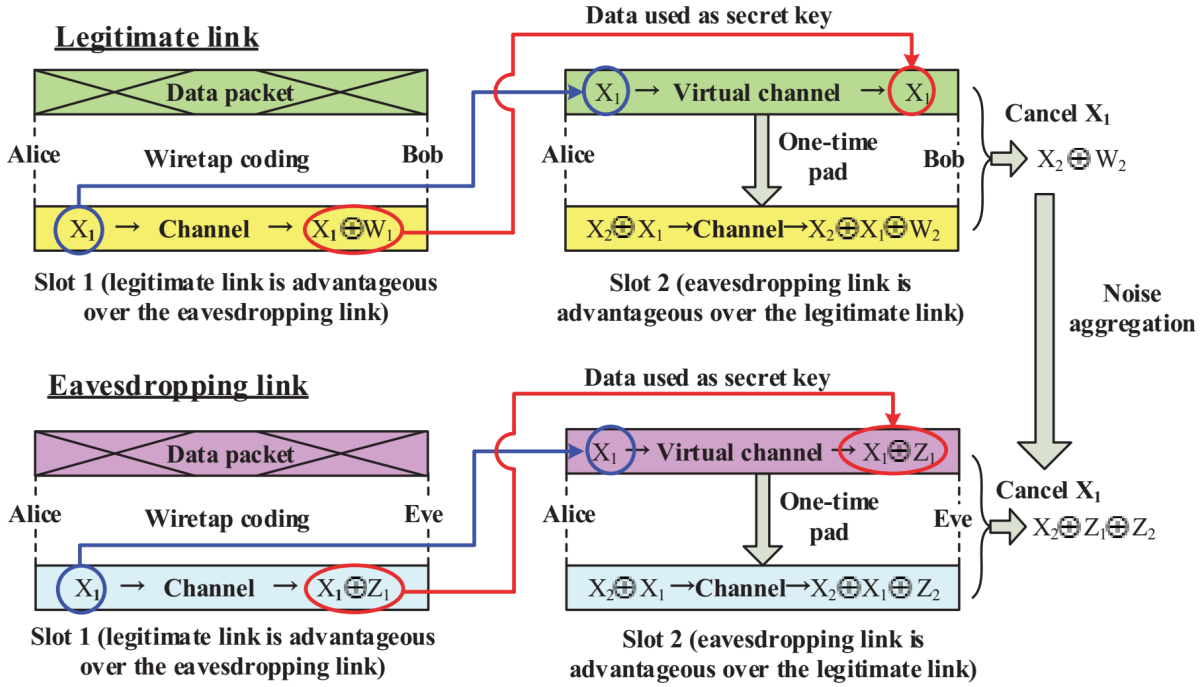
ΣΥΝΑΘΡΟΙΣΗ ΘΟΡΥΒΟΥ ΚΑΙ ΑΥΤΟΚΡΥΠΤΟΓΡΑΦΗΣΗ (NOISE AGGREGATION AND SELF-ENCRYPTION)

Η βασική ιδέα της ασφάλειας του φυσικού στρώματος (PLS) στα ασύρματα δίκτυα, είναι η εκμετάλλευση της τυχαιότητας των καναλιών για να υποβαθμίσει την ποιότητα του λαμβανόμενου σήματος στον υποκλοπέα. Μια δημοφιλής μέθοδος για την επίτευξη αυτού του στόχου είναι η έγχυση του AN (Artificial Noise) στον χώρο του νόμιμου καναλιού. Ωστόσο, η χρήση του AN έχει ως αποτέλεσμα μια πρόσθετη κατανάλωση ενέργειας, η οποία δεν είναι αποδεκτή για συσκευές IoT που λειτουργούν με μπαταρία. Για την αντιμετώπιση αυτού του ζητήματος, προτείνεται μια νέα μέθοδο που ονομάζεται συνάθροιση θορύβου (Noise Aggregation) (Hussain, Du, Sun, & Ren, Security enhancement for video transmission via noise aggregation in immersive systems., 2016), η οποία λειτουργεί ως εξής: πριν από τη μετάδοση των πακέτων δεδομένων, σε κάθε πακέτο προς αποστολή αποδίδεται ένας θετικός αριθμός που αντιστοιχεί στο δείκτη πακέτου. Τα πακέτα με μονό αριθμό και τα πακέτα με ζυγό αριθμό μεταδίδονται εντός του αντίστοιχου μονού ή ζυγού slot. Κατά τη διάρκεια της μετάδοσης δεδομένων, τα πακέτα με μονό αριθμό αποστέλλονται απευθείας προς τον δέκτη ενώ τα ζυγά πακέτα αποκωδικοποιούνται με XOR με τις αποκωδικοποιημένες εκδόσεις των περιττών πακέτων, που έχουν αποκωδικοποιηθεί επιτυχώς από τον νόμιμο δέκτη.



Σχήμα 16: Απεικόνιση της μεθόδου συγκέντρωσης θορύβου.

Λόγω της ανεξαρτησίας μεταξύ της νόμιμης ζεύξης και της ζεύξης υποκλοπής, η αποκωδικοποίηση των πακέτων δεδομένων με μονό αριθμό στον υποκλοπέα μπορεί να είναι εσφαλμένη. Ως αποτέλεσμα, ο "θόρυβος αποκωδικοποίησης" από τα slot με περιττά πακέτα θα διαδοθεί στα slot με τα ζυγά πακέτα, και αθροιστικά με το θόρυβο του καναλιού θα επιδεινώσει την απόδοση ανίχνευσης των ζυγών αριθμών πακέτων στον υποκλοπέα. Αυτό είναι το λεγόμενο φαινόμενο συνάθροισης θορύβου, το οποίο χρησιμοποιεί τους φυσικούς θορύβους αντί για τεχνητούς θορύβους για την υλοποίηση της ασφάλειας στη μετάδοση. Η αρχή της μεθόδου συνάθροισης θορύβου μπορεί να απεικονιστεί λεπτομερέστερα με τη χρήση του ακόλουθου σχήματος. Για την ευκολία της παρουσίασης, υποθέτουμε ότι οι μεταδόσεις από την Alice στον Bob είναι slotted, και κάθε slot έχει το ίδιο μήκος. Το ασύρματο κανάλι της ζεύξης Alice-Bob καθώς και εκείνο της ζεύξης Alice-Eve μοντελοποιείται ως δυαδικό συμμετρικό κανάλι (BSC). Υποτίθεται περαιτέρω ότι η κατάσταση εξασθένισης του καναλιού παραμένει αμετάβλητη σε κάθε slot και μεταβάλλεται ανεξάρτητα από slot σε slot.



Σχήμα 17: Απεικόνιση της μεθόδου συγκέντρωσης θορύβου.

Όπως απεικονίζεται στο παραπάνω σχήμα, θεωρούμε δύο διαδοχικές χρονοθυρίδες μετάδοσης. Χωρίς απώλεια στη γενικότητα, υποθέτουμε ότι η ποιότητα του καναλιού της νόμιμης ζεύξης (Alice-Bob) είναι καλύτερη από εκείνη της ζεύξης υποκλοπής (Alice-Eve) στο slot 1, ενώ στο slot 2, η ποιότητα του καναλιού της νόμιμης ζεύξης (Alice-Bob) είναι χειρότερη από εκείνη της ζεύξης υποκλοπής (Alice-Eve). Η λεπτομερής μετάδοση διαδικασία περιγράφεται ως εξής.

(α) Στο πρώτο slot, το νόμιμο κανάλι πλεονεκτεί έναντι του καναλιού υποκλοπής. Ως εκ τούτου, δεν υπάρχει ανάγκη να εκτελεστεί η κρυπτογράφηση one time pad. Αντ' αυτού, το απόρρητο της μετάδοσης του μηνύματος από την πηγή, διασφαλίζεται με τη χρήση κάποιου αλγορίθμου κωδικοποίησης και κρυπτογράφησης. Ας υποθέσουμε ότι η κωδικοποιημένη λέξη που μεταδίδεται από την Alice είναι X1. Τότε, οι λαμβανόμενες κωδικοποιημένες λέξεις στον Bob και την Eve θα είναι X1 ⊕ W1 (το πάνω αριστερό τμήμα του Σχήματος) και X1 ⊕ Z1 (το κάτω αριστερό τμήμα του Σχήματος), αντίστοιχα, όπου W1 και Z1 είναι οι αντίστοιχοι θόρυβοι του καναλιού, αντίστοιχα.

(β) Εκμεταλλευόμενη την ανατροφοδότηση του καναλιού από τον Bob προς την Alice, η Alice μπορεί να κατασκευάσει κώδικα ικανό ώστε να διασφαλίσει ότι ο X1 μπορεί να αποκωδικοποιηθεί επιτυχώς από τον Bob. Σημειώστε ότι το κανάλι υποκλοπής είναι υποβαθμισμένο σε σύγκριση με το νόμιμο κανάλι κατά τη διάρκεια του 1ου slot. Επομένως, η αποκωδικοποίηση του X1 στην Eve είναι αποτυχημένη. Αυτό μας παρακινεί να χρησιμοποιήσουμε το X1 ως κλειδί για την κρυπτογράφηση του μεταδιδόμενου σήματος στο slot 2. Ας υποθέσουμε ότι τα δεδομένα πηγής που πρέπει να μεταδοθούν εντός του slot 2 είναι το X2.

Τότε, τα κρυπτογραφημένα δεδομένα είναι X2 ⊕ X1. Στο τέλος αυτού του slot, οι λαμβανόμενες κωδικοποιημένες λέξεις στον Bob και την Eve εκφράζονται ως εξής X2 ⊕ X1 ⊕ W2 (το πάνω δεξί τμήμα του Σχήματος) και X2 ⊕ X1 ⊕ Z2 (το κάτω δεξί τμήμα του Σχήματος), αντίστοιχα.

(γ) Μετά τη λήψη του σήματος X2 ⊕ X1 ⊕ W2, ο Bob εκτελεί αποκωδικοποίηση καναλιού για να ανακτήσει το X2. Δεδομένου ότι το "μυστικό κλειδί" X1 έχει ήδη ληφθεί στο slot 1, ο Bob μπορεί να κάνει XOR X1 με X2 ⊕ X1 ⊕ W2 για να παράγει το X2 ⊕ W2, το οποίο είναι επαρκές για την ανίχνευση του X2. Στη συνέχεια, το σήμα που ανιχνεύεται στον Bob επηρεάζεται μόνο από το θόρυβο στο slot 2. Αντίθετα, τα σήματα που λαμβάνονται στην Eve στο slot 1 και στο slot 2 είναι X1 ⊕ Z1 και X2 ⊕ X1 ⊕ Z2, αντίστοιχα. Μετά την εφαρμογή της XOR η οποία ακυρώνει την παρεμβολή X1, το επαρκές για την ανίχνευση του X2 θα είναι X2 ⊕ Z1 ⊕ Z2. Σημείωση, ότι επειδή οι X1 και X2 είναι ανεξάρτητες μεταβλητές που είναι και οι δύο άγνωστες στην Eve, η παρατήρηση X1 ⊕ Z1 είναι στατιστικά ανεξάρτητη από την X2 ⊕ Z1 ⊕ Z2, η οποία δεν προσφέρει πληροφορία για την ανάκτηση του X2. Προφανώς, οι θόρυβοι εντός τόσο του slot 1 όσο και του slot 2 αθροίζονται στην Eve, υποβαθμίζοντας έτσι την δυνατότητα ανίχνευσης σήματος του υποκλοπέα.

Σε σύγκριση με τις προσεγγίσεις με βάση το AN (Artificial Noise), η μέθοδος συγκέντρωσης θορύβου δεν εξαρτάται από τη χρήση τεχνητών σημάτων θορύβου. Ως εκ τούτου, είναι πιο ενεργειακά αποδοτική και συνεπώς είναι ελκυστική για εφαρμογές IoT. Από την άλλη πλευρά, σε αντίθεση με την παραδοσιακή μέθοδο κρυπτογράφησης η οποία βασίζεται στην ανταλλαγή αποκλειστικών μυστικών κλειδιών, η προσέγγιση συνάθροισης θορύβου είναι ουσιαστικά μια τεχνική αυτο-κρυπτογράφησης η οποία χρησιμοποιεί τα μηνύματα που έχουν μεταδοθεί προηγουμένως για την κρυπτογράφηση νέων μηνυμάτων. Για την υλοποίηση της αυτοκρυπτογράφησης, ο πομπός χρειάζεται μόνο να εκτελέσει τη λειτουργία XOR, η οποία είναι επίσης ικανοποιητική από την άποψη της πολυπλοκότητα υλοποίησης. Η προσέγγιση αυτοκρυπτογράφησης με βάση τη συγκέντρωση θορύβου έχει ήδη εφαρμοστεί σε διάφορα σενάρια εφαρμογών. Για παράδειγμα (Hussain, Du, Sun, & Ren, Security enhancement for video transmission via noise aggregation in immersive systems., 2016), αναπτύχθηκε ένα σχήμα ενίσχυσης της ασφάλειας για τη μετάδοση βίντεο, όπου η υιοθέτηση της συνάθροισης θορύβου επιφέρει περίπου 1 dB SNR για τον Bob σε σύγκριση με την Eve στο ίδιο επίπεδο ρυθμού σφάλματος (Frame Error Rate).

ΣΧΕΔΙΑΣΜΟΣ ΣΗΜΑΤΟΣ ΚΑΤΑ ΤΩΝ ΥΠΟΚΛΟΠΩΝ ΜΕΣΩ CONSTELLATION ROTATION

Σύμφωνα με τους (Xu, Sun, Ren, & Du, 2015) αναπτύχθηκε ένα σύστημα ενάντια στην υποκλοπή βασισμένο στην μέθοδο constellation-rotation για την ασφάλεια των αμφίδρομων μη αξιόπιστων συστημάτων αναμετάδοσης, όπου δύο χρήστες ανταλλάσσουν πληροφορίες αμφίδρομα με έναν αναξιόπιστο

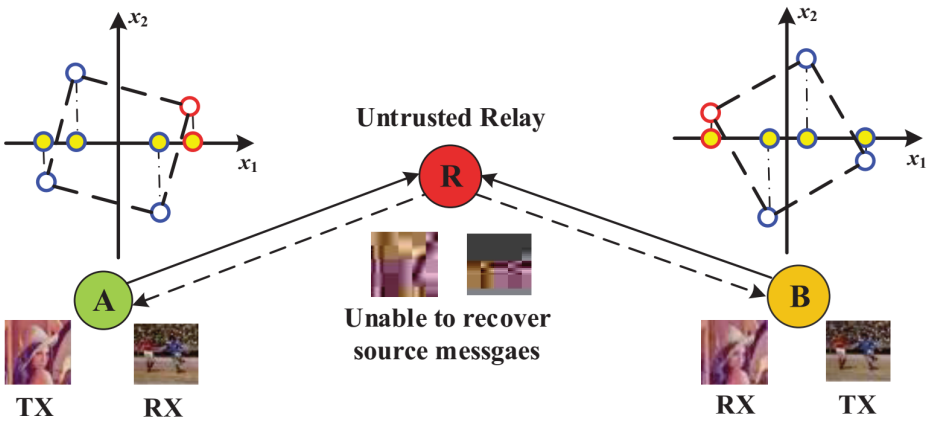
κόμβο αναμετάδοσης. Το βασικό ζήτημα στη σχεδίαση συστημάτων PLS για αυτό το σύστημα είναι να διασφαλιστεί η μη διαρροή πληροφοριών στον αναξιόπιστο αναμεταδότη, ενώ παράλληλα να αξιοποιηθεί η ικανότητα του αναμεταδότη για τη διευκόλυνση της αμφίδρομης παράδοσης πληροφοριών.

Η βασική ιδέα είναι η περιστροφή των constellations των σημάτων.

Στο πλαίσιο των επικοινωνιών και των τηλεπικοινωνιών, ο όρος "constellation rotation" (περιστροφή στοιχείων) μπορεί να αναφέρεται σε μια τεχνική που χρησιμοποιείται σε συστήματα επικοινωνίας με πολυπλεξία διαμόρφωσης όπως π.χ. στα συστήματα διαμόρφωσης πλήθους συχνοτήτων (Frequency Shift Keying - FSK) ή στα συστήματα διαμόρφωσης πλήθους φάσεων (Phase Shift Keying - PSK) στο πεδίο των ψηφιακών επικοινωνιών. Η περιστροφή των στοιχείων στο πλαίσιο της συστηματικής διαμόρφωσης σημαίνει ότι οι συμβολοσειρές που αποστέλλονται δεν παραμένουν σταθερές, αλλά υπόκεινται σε μια περιστροφή ή μετατόπιση στον χώρο των συμβόλων (constellation). Αυτό μπορεί να βοηθήσει στην αντιμετώπιση προβλημάτων όπως η παραμόρφωση του σήματος λόγω διάφορων παραμέτρων καναλιού, όπως η αλλαγή στο περιβάλλον επικοινωνίας. Ανάλογα με το συγκεκριμένο πλαίσιο της εφαρμογής, η περιστροφή των στοιχείων μπορεί να χρησιμοποιείται για τη βελτιστοποίηση της απόδοσης του συστήματος επικοινωνιών.

Όπως φαίνεται στο σχήμα, οι constellations που χρησιμοποιούνται και στους δύο τερματικούς χρήστες περιστρέφονται πρώτα έτσι ώστε να υπάρχει μια αντιστοίχιση ένα προς ένα μεταξύ του περιστρεφόμενου constellation σήματος και της πραγματικής ή φανταστικής συνιστώσας του. Στη συνέχεια, μόνο μία διάσταση complex-valued σήματος χρησιμοποιείται για να μεταφέρει τις πληροφορίες του χρήστη και η άλλη διάσταση χρησιμοποιείται για την αποστολή του τεχνητού θορύβου. Με προσεκτικό σχεδιασμό όπως φαίνεται παρακάτω, το AN (Artificial Noise) από έναν χρήστη ευθυγραμμίζεται

με το σήμα που μεταφέρει πληροφορίες από τον άλλο χρήστη στον αναξιόπιστο αναμεταδότη, γεγονός που μειώνει την απόδοση ανίχνευσης του αναξιόπιστου αναμεταδότη δραματικά και διατηρεί τα δεδομένα των χρηστών απόρρητα από τον αναξιόπιστο αναμεταδότη.



Σχήμα 18: Αναπαράσταση της μέθοδου constellation-rotation για την ασφάλεια των αμφίδρομων μη αξιόπιστων συστημάτων αναμετάδοσης.

Από την πλευρά της υλοποίησης, τα κύρια πλεονεκτήματα του προτεινόμενου συστήματος συνοψίζονται στα ακόλουθα: **Πρώτον**, μέσω της περιστροφής των constellations σήματος, ο βαθμός ελευθερίας του χώρου σήματος μπορεί να αξιοποιηθεί πλήρως για την ενίσχυση της εμπιστευτικότητας των δεδομένων, αποφεύγοντας έτσι την υπερβολική κατανάλωση ισχύος για τη μετάδοση τεχνητού θορύβου. **Δεύτερον**, οι γωνίες περιστροφής εξαρτώνται μόνο από την υιοθετημένη μορφή διαμόρφωσης και δεν απαιτούνται υπολογισμοί σε πραγματικό χρόνο για την εύρεση ή την ενημέρωση των τιμών των γωνιών περιστροφής, γεγονός που συνεπάγεται χαμηλή πολυπλοκότητα υλοποίησης. **Τρίτον**, σε σύγκριση με τις μεθόδους κρυπτογράφησης φυσικού επιπέδου που βασίζονται σε μυστικά κλειδιά, το προτεινόμενο σύστημα δεν χρειάζεται εξαγωγή κλειδιών που εξαρτώνται από το CSI (Channel State Information) ή διαμοιρασμό μεταξύ των νόμιμων χρηστών, μειώνοντας έτσι την επιβάρυνση του συστήματος σημαντικά.

ΑΣΦΑΛΗΣ ΜΕΤΑΔΟΣΗ ΜΕ ΒΑΣΗ ΤΗΝ ΚΩΔΙΚΟΠΟΙΗΣΗ ΠΗΓΗΣ (FOUNTAIN-CODING BASED SECURE TRANSMISSION)

Το fountain coding, ή αλλιώς γνωστό και ως κώδικας fontana, είναι μια τεχνική κώδικα που χρησιμοποιείται για την αποτελεσματική μετάδοση και ανάκτηση δεδομένων σε ασύρματα και ασταθή δίκτυα. Το fountain coding είναι βασισμένο σε ένα μαθηματικό μοντέλο που ονομάζεται "γεννήτορας κώδικας fountain". Σε αντίθεση με παραδοσιακές τεχνικές κωδικοποίησης, όπου για την ανάκτηση των δεδομένων απαιτείται η λήψη ολόκληρου του κώδικα, ο κώδικας fountain επιτρέπει την ανάκτηση των αρχικών δεδομένων από οποιοδήποτε μέρος του κώδικα, σε οποιαδήποτε σειρά και με αυθαίρετο ποσοστό αποτυχίας. Ο γεννήτορας κώδικας fountain δημιουργεί ένα τεράστιο αριθμό κωδικών συμβόλων από ένα αρχικό μήνυμα. Αυτός ο αριθμός είναι μεγαλύτερος από το μέγεθος του αρχικού μηνύματος και είναι απροσδιόριστος. Κάθε σύμβολο κωδικοποίησης είναι ανεξάρτητο και προέρχεται από μια πιθανότητα κατανομής. Κατά τη μετάδοση, το fountain coding επιτρέπει την αποστολή διάφορων κωδικών συμβόλων στον παραλήπτη. Ο παραλήπτης δεν χρειάζεται να λάβει τον ίδιο ακέραιο αριθμό κωδικών συμβόλων για να ανακτήσει τα αρχικά δεδομένα - αρκεί να λάβει μια συγκεκριμένη ποσότητα για την ανάκτηση ακριβώς των αρχικών δεδομένων.

Οι τεχνικές κωδικοποίησης fountain είναι πολύ χρήσιμες σε ασύρματες επικοινωνίες, ιδίως όταν υπάρχουν προβλήματα με τον ασύρματο κανάλι, όπως απώλεια πακέτων, θόρυβος και παρεμβολές. Επιτρέπουν περισσότερη ευελιξία, αξιοποιώντας την επαναληπτική μετάδοση και την ανάκτηση σε περιβάλλοντα με υποβαθμισμένη ποιότητα σήματος.

Σύμφωνα με αυτή τη μέθοδο μετάδοσης, το προς μετάδοση αρχείο πηγής χωρίζεται πρώτα σε πακέτα ίσου μήκους, τα οποία ονομάζονται πακέτα πληροφοριών. Στη συνέχεια, ο πομπός κωδικοποιεί τα πακέτα πληροφοριών

για να παράγει τα κωδικοποιημένα πακέτα, και εκτοξεύει επίμονα τα κωδικοποιημένα πακέτα προς τον δέκτη. Εδώ, σε κάθε κωδικοποιημένο πακέτο έχει εφαρμοστεί bit-by-bit XOR πολλών διαφορετικών πακέτων πηγής. Κατά τη λήψη ενός κωδικοποιημένου πακέτου, ο δέκτης προσπαθεί να αποκωδικοποιήσει χρησιμοποιώντας κάποιους επαναληπτικούς αλγορίθμους αποκωδικοποίησης. Καθώς η επαναληπτική αποκωδικοποίηση προχωρά, ανακτώνται όλο και περισσότερα πακέτα πληροφοριών. Μόλις ολόκληρο το αρχείο ανακατασκευαστεί, ο δέκτης θα στείλει ένα σήμα ανατροφοδότησης για να ενημερώσει τον πομπό να σταματήσει να παράγει νέα κωδικοποιημένα πακέτα. Ορισμένοι γνωστοί κώδικες, που εφαρμόζονται στην πηγή και έχουν προταθεί μέχρι σήμερα περιλαμβάνουν τον κώδικα LT (Luby transform) (Luby, 2002), τον κώδικα Raptor (Shokrollahi, 2006), και ο κώδικας Reed-Solomon (RS) (Nonenmacher, Biersack, & Towsley, 1998).

Το ουσιαστικό σημείο της μεθόδου για την κωδικοποίηση της πηγής, για την ενίσχυση της ασφάλειας είναι η επιτάχυνση της αποκωδικοποίησης στον νόμιμο δέκτη, έτσι ώστε ο υποκλοπέας να μην μπορεί να συγκεντρώσει αρκετά πακέτα για την ανακατασκευή ολόκληρου του αρχικού αρχείου. Ποιο συγκεκριμένα, αν υποθέσουμε ότι ο αριθμός των πακέτων πληροφορίας που συνθέτουν το μπλοκ δεδομένων της πηγής είναι K, μόλις ο δέκτης λάβει επιτυχώς, τουλάχιστον K ανεξάρτητα κωδικοποιημένα πακέτα, ολόκληρο το αρχείο μπορεί να ανακτηθεί (MacKay, 2005). Η κωδικοποίηση των δεδομένων στην πηγή συνεπάγεται ότι, η παράδοση δεδομένων από την πηγή στον προορισμό είναι ασφαλής εάν ο προορισμός μπορεί να συγκεντρώσει τα K ανεξάρτητα κωδικοποιημένα πακέτα πριν από τον υποκλοπέα. Για να επιτευχθεί αυτός ο στόχος, θα πρέπει να αξιοποιηθούν πλήρως τα μοναδικά χαρακτηριστικά της νόμιμης μετάδοσης, όπως το πρότυπο σφάλματος (error pattern) και το CSI (Channel State Information). Εν τω μεταξύ, θα πρέπει επίσης να διασφαλίσουμε ότι, οι πληροφορίες αυτές, ακόμη και αν είναι γνωστές από την υποκλοπέα, δεν μπορούν να του προσφέρουν κανένα όφελος. Με αυτήν την μέθοδο, υπάρχει μεγάλη πιθανότητα, ο νόμιμος δέκτης να μπορεί να συγκεντρώσει αρκετά κωδικοποιημένα πακέτα πριν ο υποκλοπέας να το κάνει, επιτυγχάνοντας έτσι μυστικότητα μετάδοσης. Η πιθανότητα υποκλοπής όταν έχει εφαρμοστεί η κωδικοποίηση της πηγής και με την υποβοήθηση ενός σχεδίου ασφαλούς μετάδοσης αναλύθηκε στην έρευνα των (Khan, Tassi, & Chatzigeorgiou, 2015), όπου αναπτύχθηκε ένα μοντέλο βελτιστοποίησης για την ελαχιστοποίηση της πιθανότητας υποκλοπής από καθυστέρηση και περιορισμούς αξιοπιστίας. Στην εργασία των (Karim, Esmaeilzadeh, & Sadeghi, 2017) εφαρμόστηκε τυχαία γραμμική κωδικοποίηση δικτύου για την υλοποίηση ασφαλούς παράδοσης βίντεο και παρουσιάστηκε ένα πλαίσιο για να αποτρέψει τον υποκλοπέα από το να υποκλέψει τα δεδομένα του βίντεο. Ενώ οι παραπάνω εργασίες επικεντρώθηκαν σε ένα απλό μοντέλο υποκλοπής με μόνο τρεις κόμβους, υπάρχουν επίσης αρκετές εργασίες που μελετούν την ασφαλή μετάδοση με κωδικοποίηση πηγής σε δίκτυα με συνεργατική αναμετάδοση της πληροφορίας. Στην εργασία των (Sun, Ren, Du, & Wang, Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks., 2016)

συνδυάζεται η κωδικοποίηση της πηγής με τη συνεργατική παρεμβολή (cooperative jamming) για να αποτραπεί η διαρροή της πληροφορίας σε συστήματα αναμετάδοσης διπλού άλματος (dual-hop), αποκωδικοποίησης και προώθησης (DF- decode-and-forward), όπου η τεχνική CR - Constellation Rotation αξιοποιήθηκε για να αλλοιωθεί σημαντικά η ποιότητα του λαμβανόμενου σήματος στον υποκλοπέα. Κοινό χαρακτηριστικό των υφιστάμενων εργασιών που αναφέρθηκαν είναι ότι όλες τους επικεντρώνονται στον τρόπο εκμετάλλευσης της εξασθένισης του καναλιού και των τεχνικών φυσικού επιπέδου για την επίτευξη υψηλότερου ρυθμού απολαβής στο νόμιμο δέκτη. Ωστόσο, καμία από αυτές τις εργασίες δεν διερευνά τον τρόπο κατασκευής της fountain κωδικοποίησης από την πλευρά της μυστικότητας.

Σε σχετικά πρόσφατη εργασία των (Sun & Xu, Fountain-coding based secure communications exploiting outage prediction and limited feedback., 2018) παρουσιάστηκε μια fountain-coding προσέγγιση υποβοηθούμενη από ένα σύστημα μετάδοσης που εκμεταλλεύεται την πρόβλεψη διακοπών και την περιορισμένη ανατροφοδότηση, η οποία έχει πολύ χαμηλή πολυπλοκότητα υλοποίησης και συνεπώς είναι εφαρμόσιμο στο IoT. Στην συνέχεια, παρουσιάζεται μια σύντομη εισαγωγή αυτού του συστήματος μετάδοσης.

Όπως απεικονίζεται στο ακόλουθο σχήμα, θεωρούμε ένα ασύρματο δίκτυο αισθητήρων που αποτελείται από πολλούς κόμβους αισθητήρων, μια κεντρική μονάδα ελέγχου Bob, και έναν παθητικό υποκλοπέα Eve. Ο αισθητήρας κόμβος Alice θέλει να παραδώσει με ασφάλεια ένα απόρρητο αρχείο στον Bob. Για την επίτευξη αυτού του στόχου, η Alice χωρίζει πρώτα το αρχείο της πηγής σε K πακέτα που συμβολίζονται με (u1, u2, . . . , uK). Στη συνέχεια, χρησιμοποιείται fountain coding για την κωδικοποίηση αυτών των πακέτων, σε έναν δυνητικά άπειρο αριθμό fountain πακέτων (v1, v2, . . .). Τέλος, αυτά τα fountain πακέτα

περαιτέρω κωδικοποιούνται με κώδικα capacity-achieving στο φυσικό επίπεδο για την παραγωγή των μεταδιδόμενων πακέτων (p1, p2, ...). Για να καταδειχθεί καλύτερα η προσέγγιση αυτή, εστιάζουμε σε δύο διαδοχικά slots μετάδοσης, έστω τα slot t - 1 και slot t. Εντός του slot t - 1, μετά την λήψη του μεταδιδόμενου πακέτου pt-1, ο Bob προβλέπει την υπό συνθήκη πιθανότητα διακοπής (COP-Conditional Outage Probability) του slot t βασιζόμενος στην τρέχουσα κατάσταση του καναλιού και το συγκεκριμένο μοντέλο καναλιού. Εάν η προβλεπόμενη COP (Conditional Outage Probability) είναι χαμηλότερη από ένα προκαθορισμένο κατώφλι διακοπής λειτουργίας, η στρατηγική fountain coding στο slot t θα δίνεται από τη σχέση:

$$\mathbf{v}_t = \mathbf{u}_{d,1} \oplus \mathbf{u}_{d,2} \oplus \ldots \oplus \mathbf{u}_{d,k} \oplus \mathbf{u}_{n,p},$$

όπου $u_{d,1}$, ... , $u_{d,k}$ αντιπροσωπεύουν όλα τα πακέτα πηγής που έχουν ανακτηθεί από τον Bob μέχρι το slot t – 1 και το $u_{n,p}$ είναι ένα τυχαία επιλεγμένο πακέτο πηγής που δεν έχει ανακτηθεί ακόμη από τον Bob. Η λογική πίσω από αυτή την πολιτική είναι η εξής. Εάν το προβλεπόμενο COP είναι χαμηλότερο από το κατώφλι, τότε ένα καλής ποιότητας κανάλι αναμένεται για τη νόμιμη σύνδεση στο επόμενο slot. Η παραπάνω στρατηγική κωδικοποίησης

εξασφαλίζει την άμεση ανάκτηση ενός νέου πακέτου πηγής μόλις η μετάδοση του επόμενου slot είναι επιτυχής. Αντιθέτως,

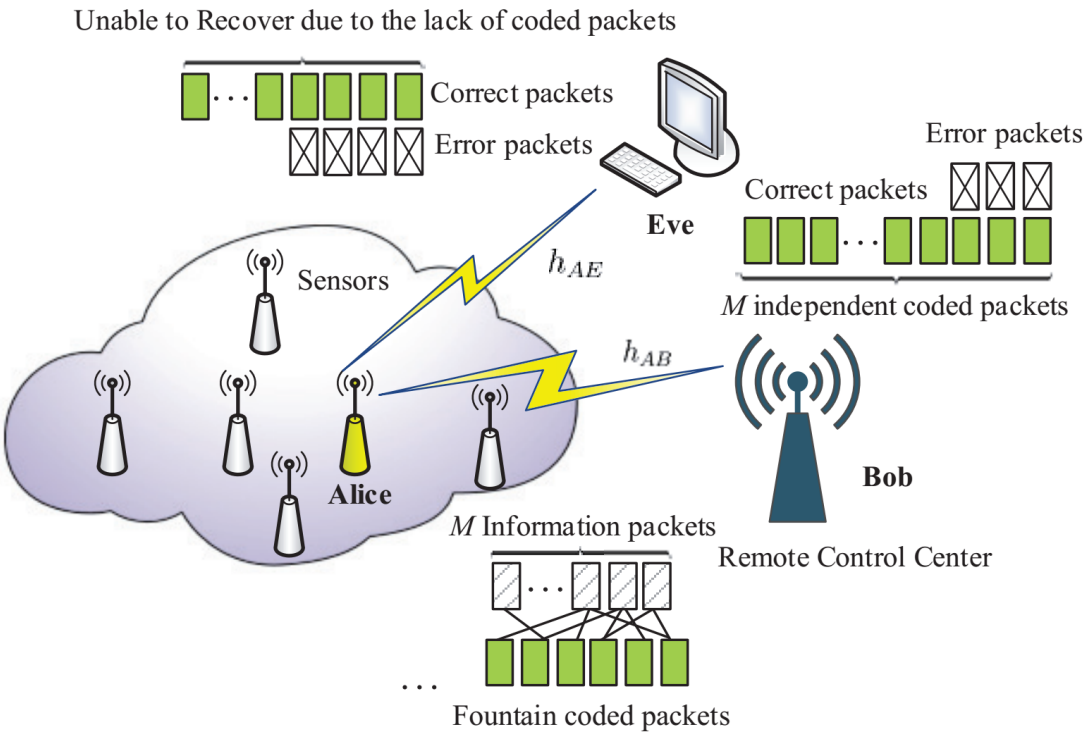
εάν το προβλεπόμενο COP είναι υψηλότερο από το κατώφλι, γεγονός που σημαίνει ότι η μετάδοση μέσω της νόμιμης ζεύξης είναι πιθανότατα σε αποτυχία, η στρατηγική κωδικοποίησης της πηγής στη σχισμή t θα πρέπει να είναι:

$$\mathbf{v}_t = \mathbf{u}_1 \oplus \mathbf{u}_2 \oplus ... \oplus \mathbf{u}_K,$$

το οποίο είναι το XOR όλων των πακέτων πηγής. Με αυτόν τον τρόπο, ο υποκλοπέας εμποδίζεται από το να εξάγει ένα νέο πακέτο πηγής από το λαμβανόμενο σήμα.

Με την προτεινόμενη στρατηγική, ο fountain κωδικοποιητής ταιριάζει με τις χρονικά μεταβαλλόμενες συνθήκες του καναλιού της νόμιμης σύνδεσης, έτσι ώστε ο δέκτης να μπορεί να επιτύχει πολύ υψηλότερο ρυθμό αποκωδικοποίησης για τα πακέτων πηγής σε σύγκριση με τον υποκλοπέα, εξασφαλίζοντας έτσι το απόρρητο της μετάδοσης. Η πολυπλοκότητα του σχήματος ασφαλούς μετάδοσης με fountain κωδικοποίηση, περιλαμβάνει κυρίως δύο μέρη:

Πρώτον, η fountain κωδικοποίηση/αποκωδικοποίηση απαιτείται στο επίπεδο εφαρμογής. **Δεύτερον**, απαιτείται ανατροφοδότηση καναλιού από τον Bob στην Alice για τη δυναμική προσαρμογή της δομής του κωδικοποιητή fountain. Ωστόσο, η fountain κωδικοποίηση/αποκωδικοποίηση μπορεί να πραγματοποιηθεί με τη χρήση διαφόρων κοινών αλγορίθμων με γραμμική χρονική πολυπλοκότητα. Εκτός αυτού, μόνο δύο bits απαιτούνται για ανατροφοδότηση. Το ένα bit χρησιμοποιείται για την ενημέρωση της Alice σχετικά με το αποτέλεσμα της πρόβλεψης διακοπής, και το άλλο bit χρησιμοποιείται για να υποδείξει την κατάσταση αποκωδικοποίησης (επιτυχία ή αποτυχία) του τρέχοντα λαμβανόμενου κωδικοποιημένου πακέτου. Επομένως, η πρόσθετη επιβάρυνση του προτεινόμενου συστήματος είναι ασήμαντη και μπορεί να είναι αποδεκτό για τις περισσότερες εφαρμογές IoT.



Σχήμα 19: Σύστημα ασφαλούς μετάδοσης με βάση την κωδικοπ. πηγής.

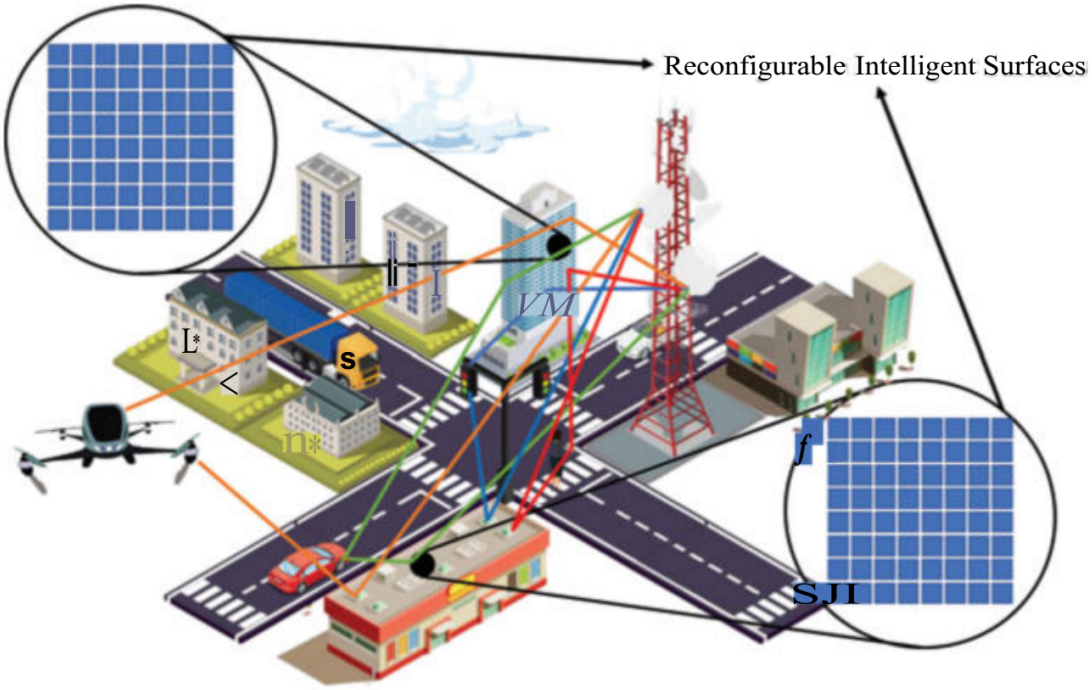
MACHINE LEARNING

Η ραγδαία αύξηση του αριθμού των συσκευών IoT που είναι συνδεδεμένες σε δίκτυα, οδηγεί σε τεράστια κυκλοφορία δεδομένων. Λόγω του μεγάλου όγκου δεδομένων που παράγονται σε πραγματικό χρόνο, η επεξεργασία και η ασφάλειά τους καθιστούν δύσκολο το έργο της διαχείρισης των σε στα περιβάλλοντα IoT. Από αυτή την άποψη, η μηχανική μάθηση (ML) είναι μια αναδυόμενη τεχνολογία για τη μείωση της επιβάρυνσης της επικοινωνίας και της πολυπλοκότητας της επεξεργασίας σήματος και υπόσχεται να ενισχύσει την ασφάλεια των επικοινωνιών. Τα εργαλεία ML αξιοποιούνται για την ενίσχυση της ακρίβειας του δακτυλικού αποτυπώματος RF αναγνώρισης για συσκευές IoT και για τη βελτίωση της αποτελεσματικότητας του PLS έναντι διαφόρων επιθέσεων. Με βάση αυτήν την προοπτική προτάθηκαν δυο προσεγγίσεις (Moon T, 2022), ώστε σε ένα πραγματικό ασύρματο δίκτυο αισθητήρων, να λειτουργεί ένα σύστημα συνεχούς ελέγχου ταυτότητας φυσικού επιπέδου και ανίχνευσης πλαστοπροσωπίας με βάση το δακτυλικό αποτύπωμα RF. Οι έρευνες και τα αποτελέσματα δείχνουν ότι ο προτεινόμενος αλγόριθμος μπορεί να επιτύχει υψηλό επίπεδο ακρίβειας στην ταξινόμηση που αντιστοιχεί στην ορθή ταυτοποίηση του νόμιμου χρήστη. Μια άλλη έρευνα εξετάζει ένα Βαθύ Νευρωνικό Δίκτυο (DNN - Deep Neural Network), ένα Συνελικτικό Νευρωνικό Δίκτυο (CNN - Convolutional Neural Network) και το επαναλαμβανόμενο νευρωνικό δίκτυο (RNN - Recurrent Neural Network) για τον αναγνώριση RF δακτυλικών αποτυπωμάτων για συσκευές IoT και τη διάκριση μεταξύ RF δακτυλικών αποτυπωμάτων άλλων συσκευών IoT της ίδιας κατασκευάστριας εταιρείας, για τη βελτίωση της ασφάλειας συσκευών σε IoT δίκτυο (Space,

2014). Στην έρευνα των (Wang Y, 2015) παρουσιάστηκε μια νέα μέθοδος αναγνώρισης δακτυλικών αποτυπωμάτων RF που συνδύαζε τη μέθοδο DCTF (Differential Constellation Trace Figure) και τη CNN-based ταξινόμηση χωρίς να απαιτείται επιπρόσθετα συγχρονισμός και αντιστάθμιση. Στην έρευνα των (Washington R, 2021) παρουσιάστηκαν τα αποτελέσματα της εφαρμογής ενός συστήματος ML σε ένα «έξυπνο σπίτι» ως χαρακτηριστικό δείγμα IoT. Όσον αφορά το προτεινόμενο σχήμα, εφαρμόζονται αλγόριθμοι ML στα δεδομένα που είναι αποθηκευμένα στο δίκτυο blockchain ώστε να εντοπιστούν παράνομες συσκευές που διεισδύουν στο δίκτυο συμβάλλοντας έτσι στην ενίσχυση της ασφάλειας του δικτύου IoT. Για να ενισχυθεί η ασφάλεια των ασύρματων δικτύων σε επίπεδο βιομηχανίας από επιθέσεις πλαστογράφησης, προτάθηκε μια μέθοδος (Elliott C, 2003), συνδυάζοντας τρεις ήδη γνωστούς αλγόριθμους ελέγχου ταυτότητας των κόμβων αισθητήρων, συμπεριλαμβανομένης της μεθόδου ελέγχου ταυτότητας των κόμβων αισθητήρων με βάση το DNN, το CNN και το CPNN. Παρόλο που οι τεχνικές ML έχουν χρησιμοποιηθεί για την ενίσχυση της ακρίβειας των δακτυλικών αποτυπωμάτων RF για συσκευές IoT, όπως συζητήθηκε προηγουμένως, περαιτέρω έρευνες για την αξιοποίηση των ML για την για την απόκτηση ενός θεωρητικά τέλειου CSI (Channel State information) απαιτούνται σήμερα. Τα υπάρχοντα σχήματα εκτίμησης κατάστασης καναλιού είναι ανεπαρκή για να μας διασφαλίσουν αποτελεσματικά την επικοινωνία. Η χρήση τεχνικών ML στην εκτίμηση καναλιού έχει προταθεί ως λύση. Ως εκ τούτου, η απόδοση των υφιστάμενων τεχνικών εκτίμησης καναλιού μπορούν να βελτιωθεί, με χαμηλή πολυπλοκότητα σε πρακτικές εφαρμογές.

RECONIGURABLE INTELLIGENT SURFACES (RSIS)

Όπως αναφέρθηκε προηγουμένως, λόγω του μικρού μεγέθους των συσκευών IoT, δεν είναι ρεαλιστικό να προτείνουμε την τοποθέτηση πολλαπλών κεραιών στην πλευρά του χρήστη για την εκμετάλλευση των πλεονεκτημάτων της MIMO. Ως εκ τούτου, προτείνεται η έννοια της επανα-διαμορφώσιμης ευφυούς επιφάνειας (RIS) ως λύση για την λόγω της ακαταλληλότητας της χρήσης MIMO στο IoT. Η RIS μπορεί να οριστεί ως μια συστοιχία μεγάλης κλίμακας που αποτελείται από μεγάλο αριθμό παθητικών στοιχείων χαμηλού κόστους, τα οποία μπορούν να ανακλούν ή να μεταδίδουν τα προσπίπτοντα ηλεκτρομαγνητικά κύματα προς τις επιθυμητές κατευθύνσεις ρυθμίζοντας κατάλληλα τις μετατοπίσεις φάσης τους (Poppe A, 2008).



Σχήμα 20: Reconfigurable intelligent surfaces in IoT networks

Παρόλο που η RIS τεχνολογία έχει μεγάλη εφαρμογή στα ασύρματα δίκτυα με αξιοσημείωτα πλεονεκτήματα, η παρούσα ενότητα εστιάζει και εξετάζει μόνο τα πλεονεκτήματά της από την άποψη της ασφάλειας στα δίκτυα IoT. Η δυνατότητα ελέγχου του καναλιού μετάδοσης με τη χρήση RIS, αποτελεί σημαντικό παράγοντα για την ανάπτυξη προηγμένων PLS τεχνικών. Δεδομένου ότι το κανάλι του μεταδιδόμενου σήματος μπορεί εύκολα να αλλάξει με τη ρύθμιση της γωνίας φάσης του RIS, στις περιπτώσεις όπου οι κακόβουλοι επιτιθέμενοι αποκτούν πρόσβαση στο Channel State information των μεταδιδόμενων δεδομένων, το κανάλι μπορεί εύκολα να αλλάξει με την αλλαγή της γωνίας φάσης του RIS παρέχοντας έτσι επιπρόσθετη ασφάλεια στο φυσικό επίπεδο. Σύμφωνα με την έρευνα των (Sasaki M, 2011) προτάθηκε μια υλοποίηση, που βασίζεται σε RIS και εφαρμόζεται σε PLS με το όνομα user-specific RIS, ως λύση για τον περιορισμό που θέτουν οι Iot συσκευές λόγω του μικρού μεγέθους τους. Το προτεινόμενο σχήμα RIS μπορεί να ελέγξει εν μέρει το πλάτος του σήματος, ενώ οι συνηθισμένες RIS υλοποιήσεις μπορούν να ρυθμίσουν μόνο τη φάση ενός σήματος. Το προτεινόμενο σχήμα αυξάνει το βαθμό ελευθερίας για το σχεδιασμό διαμόρφωσης δέσμης RIS στα δίκτυα IoT,, δεδομένου ότι οι δυνατότητες διαμόρφωσης δέσμης είναι εξαιρετικά περιορισμένες. Με την προτεινόμενη λύση μπορούν πλέον να σχεδιαστούν και να βελτιστοποιηθούν συστήματα Iot, επιτυγχάνοντας αποτελεσματική επικοινωνία και λειτουργία, παρακάμπτοντας περιορισμούς που θέτον τα χαρακτηριστικά και οι προδιαγραφές τους όπως η εξοικονόμηση ενέργειας, η ασφάλεια, το μέγεθος τους κ.α.

ΣΥΝΟΨΗ ΤΩΝ ΛΥΣΕΩΝ PLS ΜΕ ΠΡΟΣΑΝΑΤΟΛΙΣΜΟ ΣΤΟ IoT

Σε σύγκριση με τις κλασικές στρατηγικές PLS, τα συστήματα που περιγράφονται στην προηγούμενη ενότητα είναι καλύτερα προσαρμοσμένα για το IOT, οι λόγοι των οποίων συνοψίζονται ως εξής. **Πρώτον**, τα σχήματα που αναπτύχθηκαν είναι ενεργειακά αποδοτικά, ικανοποιώντας έτσι τις απαιτήσεις χαμηλής κατανάλωσης ενέργειας του IoT.

Συγκεκριμένα, η προσέγγιση συνάθροισης θορύβου (noise aggregation) χρησιμοποιεί τον εγγενή θόρυβο στα ασύρματα κανάλια, αντί για τον τεχνητό θόρυβο, για να υποβαθμίσει την ποιότητα του λαμβανόμενου σήματος του υποκλοπέα και εγγυάται τη μυστικότητα στη μετάδοση χωρίς κόστος πρόσθετης ισχύος. Η (constellation rotation) μέθοδος, δημιουργεί ένα κατώτατο όριο σφάλματος στον αναξιόπιστο αναμεταδότη μέσω του βελτιστοποιημένου σχεδιασμού signal constellation, αποφεύγοντας έτσι την υπερβολική κατανάλωση ενέργειας για τη δημιουργία τεχνητού θορύβου. Η στρατηγική fountain-coding επιτυγχάνει την μυστικότητα εκμεταλλευόμενη τα χαρακτηριστικά της fountain κωδικοποιημένης μετάδοσης, ότι ολόκληρο το αρχείο μπορεί να ανακτηθεί μόνο αν συγκεντρωθεί επαρκής αριθμός κωδικοποιημένων πακέτων. Αυτή η μέθοδος δεν απαιτεί πρόσθετη ενέργεια για να εγγυηθεί τη μυστικότητα. **Δεύτερον**, τα συστήματα που περιεγραφήκαν παραπάνω απολαμβάνουν πολύ χαμηλή πολυπλοκότητα υλοποίησης, η οποία ταιριάζει με το χαρακτηριστικό χαμηλού κόστους συσκευών του IoT. Όπως αναφέρθηκε προηγουμένως, η συνάθροιση θορύβου (noise aggregation) είναι ουσιαστικά μια τεχνική αυτό-κρυπτογράφησης η οποία χρησιμοποιεί τα προηγούμενα μεταδιδόμενα μηνύματα για την κρυπτογράφηση νέων μηνυμάτων. Μόνο μια απλή λειτουργία XOR είναι απαραίτητη να εφαρμοστεί στον πομπό, η οποία είναι αποδεκτή από τις συσκευές IoT. Στο σχήμα constellation rotation η εφαρμογή της προκαλεί αμελητέα επιβάρυνση στις συσκευές IoT. Επιπλέον, οι γωνίες περιστροφής εξαρτώνται μόνο από τις υιοθετούμενες μορφές διαμόρφωσης και μπορούν να υπολογιστούν εκτός σύνδεσης πριν από τη μετάδοση δεδομένων, αποδίδοντας επίσης ασήμαντο υπολογιστικό φορτίο. Η επιπλέον επιβάρυνση που συνεπάγεται η fountain κωδικοποίηση περιλαμβάνουν κυρίως τις λειτουργίες κωδικοποίησης/ αποκωδικοποίησης και την ανατροφοδότηση καναλιού από τον Bob στην Alice. Ωστόσο, ο αλγόριθμος fountain κωδικοποίησης/αποκωδικοποίησης έχει γραμμική χρονική πολυπλοκότητα και η ποσότητα ανατροφοδότησης σε κάθε slot είναι μόνο δύο bits. Έτσι, το σύστημα που βασίζεται στην κωδικοποίηση fountain είναι επίσης ελκυστικό για εφαρμογές IoT. **Τρίτον**, από την οπτική γωνία των υπηρεσιών IoT, τα συστήματα που συζητήθηκαν στην προηγούμενη ενότητα, είναι επίσης πιο ανταγωνιστικά σε σύγκριση με τις κλασικές λύσεις PLS. Ειδικότερα, η χρήση της προσέγγισης συνάθροισης θορύβου (noise aggregation), βρίσκει υλοποίηση σε εφαρμογές βιντεοεπιτήρησης. Στο constellation rotation scheme, ο λόγος ισχύος του σήματος που φέρει πληροφορίες προς τον τεχνητό θόρυβο στα σύνθετα σήματα μπορεί να ρυθμιστεί προσαρμοστικά, παρέχοντας έτσι μια ευέλικτη αντιστάθμιση μεταξύ της αξιοπιστίας και της ασφάλειας. **Τέταρτον**, στο σύστημα ασφαλούς

μετάδοσης fountain-coding, το κατώφλι μπορεί να βελτιστοποιηθεί έτσι ώστε διάφορες επιλογές να ικανοποιήσουν τις απαιτήσεις υπηρεσιών, QoS του συστήματος να μπορούν να εξισορροπηθούν, συμπεριλαμβανομένης της μυστικότητας, της απόδοσης, καθώς και της καθυστέρησης μετάδοσης. **Τέλος**, στις RIS προσεγγίσεις, εάν και οι προοπτικές δείχνουν αρκετά ελπιδοφόρες από την άποψη της ασφάλειας και η τάση για έρευνα είναι γρήγορα εξελισσόμενη, εντούτοις στα ασύρματα δίκτυα είναι μια σχετικά νέα περιοχή προς έρευνα και οι πρακτικές εφαρμογές της δεν έχουν ακόμη προχωρήσει ικανοποιητικά.

Παρόλο που οι αναδυόμενες τεχνικές PLS που περιγράφονται στην προηγούμενη ενότητα έχουν αξιοσημείωτα πλεονεκτήματα, υπάρχουν επίσης ορισμένα μειονεκτήματα που συνδέονται με αυτές. Εν συντομία, και οι προαναφερθείς στρατηγικές απαιτούν ανατροφοδότηση καναλιού ή ανταλλαγή πληροφοριών μεταξύ των νόμιμων οντοτήτων, γεγονός που προκαλεί μια μικρή υποβάθμιση της απόδοσης του νόμιμου συστήματος. Ως εκ τούτου, αυτά τα συστήματα δεν είναι κατάλληλα για εφαρμογές πραγματικού χρόνου όπου η παράδοση δεδομένων έχει αυστηρούς περιορισμούς στην καθυστέρηση. Ωστόσο, οι υπηρεσίες IoT λειτουργούν συνήθως με πολύ χαμηλούς ρυθμούς μεταφοράς δεδομένων. Συνεπώς, τα μειονεκτήματα των συστημάτων δεν εμποδίζουν την υιοθέτησή τους στο μελλοντικό IoT.

Δεδομένου ότι η συντριπτική πλειονότητα των υφιστάμενων συστημάτων PLS δεν είναι ειδικά σχεδιασμένα για IoT δίκτυα, το PLS βρίσκεται ακόμη σε πρώιμο στάδιο για να χρησιμοποιηθεί αποτελεσματικά σε αυτόν τον τομέα. Επομένως, η ανάγκη ανάπτυξης και εφαρμογής νέων σχημάτων PLS για την ικανοποίηση των μοναδικών χαρακτηριστικών των συσκευών IoT είναι ζωτικής σημασίας.

ΚΕΦΑΛΑΙΟ 5: ΣΥΜΠΕΡΑΣΜΑΤΑ

Σε αυτό το άρθρο, είδαμε μια ολοκληρωμένη ανασκόπηση των τεχνικών ασφάλειας φυσικού επιπέδου στο Διαδίκτυο των πραγμάτων. Αρχικά συζητήθηκαν τα χαρακτηριστικά καθώς και οι απαιτήσεις ασφαλείας του IoT (Rojas, Alahmadi, & Bayoumi, 2021). Στη συνέχεια, παρουσιάστηκε η βασική αρχή της ασφάλειας φυσικού στρώματος και αρκετές αντιπροσωπευτικές τεχνικές λύσεις ασφάλειας φυσικού στρώματος με προσανατολισμό στο IoT συνοψίστηκαν. Τέλος, αναλύθηκαν οι προκλήσεις που αντιμετωπίζει ο σχεδιασμός ασφαλών πρωτοκόλλων μετάδοσης IoT και παρουσιάσαμε τρεις αναδυόμενες PLS λύσεις που μπορούν να αντιμετωπίσουν καλά αυτές τις προκλήσεις.

Παρόλο που η έρευνα για την ασφάλεια του φυσικού στρώματος έχει δημιουργήσει μεγάλο όγκο βιβλιογραφίας, με τις έρευνες να ξεκινούν από τη θεμελιώδη πληροφοριοθεωρητική ανάλυση έως τον πρακτικό σχεδιασμό στρατηγικών PLS, εξακολουθεί να αποτελεί πρόκληση η ανάπτυξη συστημάτων PLS που να ικανοποιούν τις πολυδιάστατες απαιτήσεις του μελλοντικού IoT. Ορισμένα ζητήματα που χρήζουν περαιτέρω μελέτης παρατίθενται στην συνέχεια:

(α) Ο σχεδιασμός ενός συστήματος PLS έχει στόχο την καταπολέμηση ενεργών επιθέσεων. Μέχρι τώρα, η πλειοψηφία των λύσεων PLS επικεντρώνονται στις τεχνικές κατά της υποκλοπής. Ωστόσο, η υποκλοπή είναι μια απλή και παθητική μορφή επίθεσης. Στο μελλοντικό IoT, θα υπάρχουν διάφορες μορφές ενεργών κακόβουλων επιθέσεων, π.χ. τροποποιητικό μήνυμα, αποκάλυψη πληροφοριών, πιλοτικές αναγνωριστικές επιθέσεις, παρεμβολές, επίθεση μεταμφίεσης κ.λπ. Παραμένει ως ανοιχτό πρόβλημα ο τρόπος αξιοποίησης των τεχνικών PLS για την αντιμετώπιση αυτών των επιθέσεων. Ο σχεδιασμός άμυνας όχι συγκεκριμένα για ένα επίπεδο αλλά για περισσότερα, μπορεί να είναι μια πολλά υποσχόμενη μέθοδος για την αντιμετώπιση αυτού του ζητήματος.

(β) Νέα μετρική για την αξιολόγηση των επιδόσεων. Στην έρευνα PLS, υιοθετούνται οι ευρέως χρησιμοποιούμενες μετρικές απόδοσης συμπεριλαμβανομένων των «επιτεύξιμο ρυθμό μυστικότητας» και την «πιθανότητα διακοπής μυστικότητας». Αυτές οι μετρικές προτείνονται από πληροφοριο-θεωρητική άποψη. Στο μελλοντικό IoT, η ετερογένεια των συσκευών και των υπηρεσιών προκαλεί την ποικιλομορφία στις απαιτήσεις των χρηστών. Αυτό με τη σειρά του απαιτεί την πρόταση για νέας μετρικής για την αξιολόγηση της απόδοσης των συστημάτων PLS. Η νέα μετρική θα πρέπει να λαμβάνει υπόψη τις πολυδιάστατες απαιτήσεις των χρηστών, π.χ. μυστικότητα, καθυστέρηση, ρυθμός μετάδοσης, ρυθμός απώλειας πακέτων, κ.λπ., και να παρέχει μια ολοκληρωμένη αξιολόγηση των συστημάτων που αναπτύχθηκαν.

(γ) Η χρήση των τεχνικών PLS σε νέα συστήματα και σενάρια. Οι τρέχουσες μελέτες αφορούν κυρίως τα ασύρματα δίκτυα αισθητήρων ως πεδίο εφαρμογής. Στο μελλοντικό IoT, αρκετά νέα συστήματα αναδύονται, και θα

εξεταστούν πολλά νέα σενάρια εφαρμογών. Συνεπώς, απαιτούνται καινοτόμες ερευνητικές εργασίες, συμπεριλαμβανομένων νέων μοντέλων, νέων αναλυτικών εργαλείων, κ.λπ.

ΠΑΡΑΡΤΗΜΑ Ι – ΕΥΡΕΤΗΡΙΟ ΟΡΩΝ

CNN

Το Convolutional Neural Network (CNN), ή Συνελικτικό Νευρωνικό Δίκτυο, είναι ένα είδος τεχνητού νευρωνικού δικτύου που έχει σχεδιαστεί ειδικά για την επεξεργασία δεδομένων που έχουν δομική διάταξη, όπως εικόνες, ήχος και βίντεο (LeCun, 2015). Τα δίκτυα CNN έχουν τη δυνατότητα να ανιχνεύουν και να εξάγουν χαρακτηριστικά από τα εισερχόμενα δεδομένα χρησιμοποιώντας συνελίξεις. Αυτό το κάνουν μέσω της εφαρμογής φίλτρων, ή κατάλληλα σχεδιασμένων μάσκων, στην είσοδο των δεδομένων για την εξαγωγή χαρακτηριστικών (Goodfellow, 2016). Αυτή η διαδικασία είναι κοινώς γνωστή ως συνέλιξη. Οι σημαντικότερες ιδιότητες των CNN περιλαμβάνουν την ικανότητά τους να μάθουν και να εξάγουν συντομεύσεις από τα δεδομένα, την αντοχή τους σε μετατοπίσεις και μεταστροφές στη θέση των στοιχείων των δεδομένων και την ικανότητά τους να μειώνουν τον αριθμό των παραμέτρων που απαιτούνται για την εκπαίδευσή τους, χάρη στην κοινή χρήση παραμέτρων (Krizhevsky, 2012).

Οι CNN βρίσκουν εφαρμογή σε πολλούς τομείς, συμπεριλαμβανομένης της αναγνώρισης εικόνων, της αναγνώρισης αντικειμένων, της αναγνώρισης προσώπων, της αναγνώρισης φωνής, της ανάλυσης κειμένου, της αυτόματης οδήγησης και πολλών άλλων.

DNN

Το Deep Neural Network (DNN), ή Βαθύ Νευρωνικό Δίκτυο, αναφέρεται σε ένα είδος τεχνητού νευρωνικού δικτύου που αποτελείται από πολλά επίπεδα νευρώνων (layers) (LeCun, 2015) . Κάθε επίπεδο λαμβάνει εισόδους από τα προηγούμενα επίπεδα και παράγει εξόδους που χρησιμοποιούνται ως είσοδοι για τα επόμενα επίπεδα. Τα DNN είναι ιδιαίτερα ισχυρά στην αναγνώριση προτύπων, την κατηγοριοποίηση δεδομένων, την πρόβλεψη και τη γενίκευση από πολύπλοκα δεδομένα (Goodfellow, 2016). Κάθε επίπεδο του δικτύου μπορεί να προσθέτει στην αναπαράσταση των χαρακτηριστικών των δεδομένων, επιτρέποντας στο δίκτυο να μάθει και να αναπαριστά σύνθετες συναρτήσεις (Bengio, 2013). Τα DNN έχουν εφαρμογές σε πολλούς τομείς, συμπεριλαμβανομένης της αναγνώρισης εικόνων, της επεξεργασίας φωνής, της αναγνώρισης κειμένου, της αυτόματης μετάφρασης, της ανάλυσης δεδομένων και άλλων. Η επιτυχία των DNN οφείλεται σε παράγοντες όπως η ικανότητά τους να μαθαίνουν από δεδομένα, η ευκολία υλοποίησης τους σε πολλούς τομείς και η ικανότητά τους να αντιμετωπίζουν σύνθετα προβλήματα (Schmidhuber, 2015).

MIC key

Το MIC key αναφέρεται στο προσωρινό κλειδί ακεραιότητας μηνυμάτων (Message Integrity Code key) που χρησιμοποιείται σε πρωτόκολλα ασφάλειας ασύρματων δικτύων, όπως το πρότυπο WPA (Wi-Fi Protected Access).

Το MIC key χρησιμοποιείται για τον υπολογισμό του Message Integrity Code (MIC) σε κάθε πακέτο δεδομένων που αποστέλλεται μέσω του ασύρματου δικτύου. Ο MIC είναι ένα μικρό κατακερματισμένο αποτέλεσμα υπολογισμού που προσδιορίζει αν έχει τροποποιηθεί το περιεχόμενο του πακέτου δεδομένων κατά τη μετάδοση. Με τη χρήση του MIC key, επαληθεύεται η ακεραιότητα των δεδομένων και προστατεύεται το δίκτυο από επιθέσεις που στοχεύουν στην παραποίηση των πακέτων.

Με τη χρήση του MIC key, ενισχύεται η ασφάλεια των ασύρματων δικτύων, καθώς προσφέρεται έλεγχος ακεραιότητας των δεδομένων που μεταδίδονται μέσω του δικτύου.

Στα ασύρματα δίκτυα, ιδίως σε πρωτόκολλα όπως το WPA (Wi-Fi Protected Access) και το WPA2, οι προκατασκευασμένες κλειδιά μπορούν να χρησιμοποιηθούν για να προστατεύσουν την ασύρματη επικοινωνία. Το PKM είναι υπεύθυνο για την αυθεντικοποίηση και τη διαχείριση αυτών των προκατασκευασμένων κλειδιών σε ένα ασύρματο δίκτυο.

Ουσιαστικά, το PKM είναι υπεύθυνο για τη διαχείριση των κλειδιών που χρησιμοποιούνται για την ασφάλεια του ασύρματου δικτύου. Αυτό συμπεριλαμβάνει την παραγωγή, τη διανομή και την επαλήθευση των κλειδιών μεταξύ των σταθμών του δικτύου.

MIMO

MIMO σημαίνει Πολλαπλές Εισόδους, Πολλαπλές Εξόδους (Multiple Input, Multiple Output). Το MIMO είναι μια τεχνική στην ασύρματη επικοινωνία που χρησιμοποιεί πολλές κεραίες τόσο στον πομπό όσο και στον δέκτη για να αυξήσει την απόδοση του ασύρματου συστήματος. Με τη χρήση της τεχνικής MIMO, μπορούν να μεταδοθούν πολλά σήματα ταυτόχρονα μέσω διαφορετικών κεραιών, βελτιώνοντας έτσι το ρυθμό μετάδοσης δεδομένων και την επίδοση του δικτύου. Η χρήση της τεχνικής MIMO επιτρέπει επίσης την αντιμετώπιση των προβλημάτων που σχετίζονται με τις παρεμβολές και την απώλεια σήματος σε ασύρματα δίκτυα. Συνολικά, η τεχνική MIMO βοηθάει στην βελτίωση της ασύρματης επικοινωνίας με την αύξηση της ταχύτητας μετάδοσης, τη μείωση των παρεμβολών και τη βελτίωση της αξιοπιστίας των επικοινωνιών.

PKM

Το PKM (Preshared Key Management) είναι ένα πρωτόκολλο που χρησιμοποιείται σε ασύρματα δίκτυα για τη διαχείριση των προκατασκευασμένων κλειδιών (preshared keys), τα οποία χρησιμοποιούνται για την αυθεντικοποίηση και την κρυπτογράφηση της επικοινωνίας.

RNN

Τα Recurrent Neural Networks (RNNs), ή Επαναλαμβανόμενα Νευρωνικά Δίκτυα, είναι μια κατηγορία νευρωνικών δικτύων που έχουν σχεδιαστεί ειδικά για την επεξεργασία ακολουθιών δεδομένων, όπως χρονοσειρές, ακολουθίες κειμένων και ηχητικά σήματα (Graves, 2005). Τα RNNs διαθέτουν μια ειδική δομή που επιτρέπει στις πληροφορίες να κυκλοφορούν προς τα εμπρός και προς τα πίσω μέσα στο δίκτυο, δημιουργώντας έναν εσωτερικό κατάσταση (state) που επιτρέπει στο δίκτυο να αντιμετωπίζει ακολουθιακά δεδομένα και να αντλεί συμπεράσματα από το παρελθόν κατά την επεξεργασία των δεδομένων στο παρόν (Cho, 2014).

TKIP

Το **TKIP** (**Temporal Key Integrity Protocol**) αποτελεί ένα πρωτόκολλο κρυπτογράφησης που χρησιμοποιείται στο πρότυπο ασφαλείας WPA (Wi-Fi Protected Access). Το κύριο χαρακτηριστικό του TKIP είναι η δημιουργία προσωρινών κλειδιών (temporal keys) που αλλάζουν με κάθε πακέτο δεδομένων που αποστέλλεται μέσω του ασύρματου δικτύου. Αυτό το χαρακτηριστικό βελτιώνει την ασφάλεια του συστήματος κρυπτογράφησης, καθώς δυσκολεύει τυχόν επιθέσεις κρυπτανάλυσης. Το TKIP εισήχθηκε για αντικατάσταση του πρωτοκόλλου WEP που είχε αδυναμίες στην ασφάλεια του. Μέσω του TKIP, επιτυγχάνεται κρυπτογράφηση των δεδομένων με πιο αξιόπιστο τρόπο, προσφέροντας μεγαλύτερη προστασία στα ασύρματα δίκτυα Wi-Fi.

WEP

Το **WEP (Wired Equivalent Privacy)** είναι ένας αλγόριθμος ασφάλειας για τα ασύρματα δίκτυα IEEE 802.11. Η εισαγωγή του έγινε το Σεπτέμβριο του 1999, σαν μέρος του αρχικού προτύπου. Η πρόθεσή του ήταν, όπως δηλώνει και το όνομά του, να παρέχει εμπιστευτικότητα δεδομένων συγκρίσιμη με τα παραδοσιακά ενσύρματα δίκτυα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

A. Whitmore, A. A. (2015). *The internet of things—a survey of topics and trends.* Inf. Syst. Front. 17 (2) (2015) 261–274, doi:10.1007.

Akyildiz, I. F. (2002). *A survey on sensor networks. .* IEEE Communications Magazine, 40(8), 102-114.

Barcelo-Llado, J., Morell, A., & Seco-Granados. (2014). *G. Amplify-and-forward compressed sensing as a physical-layer secrecy solution in wireless sensor networks. .* IEEE Trans. Inf. Forensics Secur. .

Barcelo-Llado, J., Morell, A., & Seco-Granados, G. (2014). *Amplify-and-forward compressed sensing as an energy-efficient solution in wireless sensor networks.* IEEE Sens.

Bo Cheng, M. I. (2017). *Situation-Aware Dynamic Service Coordination in an IoT Environment.* IEEE/ACM Transactions On Networking, vol. 25, no. 4, pp. 2082–2095.

C. Perera, A. Z. (2014). *Context aware computing for the Internet of Things: A survey.* IEEE Communication surveys and tutorials.

Choi, J. (2016). *Secure transmissions via compressive sensing in multicarrier systems. IEEE Signal Process. Lett.*

Dautov, R., & Tsouri, G. (2016). *Dautov, R.; Tsouri, G.R. Securing while sampling in wireless body area networks with application to electrocardiography.* IEEE J. Biomed. Health Inform.

Department, T. S. (2012). *Norton cybercrime report.* http://www.norton.com/2012cybercrimereport.

Dong, L., Han, Z., Petropulu, A., & Poor, H. (2010). *Improving wireless physical layer security via cooperative relays.* IEEE Trans. Signal Process.

Giaffreda, R., Capra, L., & Antonelli, F. (2016). *A pragmatic approach to solving IoT interoperability and security problems in an eHealth context.* Internet of Things (WF-IoT) IEEE 3rd World Forum.

Green, C. Z. (2015). *Communication Security in Internet of Thing: Preventive measure and avoid DDoS attack over IoT network.* IEEE Symposium on Communications & Networking.

H. ElSawy, E. H. (2013). *Stochastic geometry for modeling,analysis, and design of multi-tier and cognitive cellular wireless networks: A survey.* IEEE Commun. Surv. Tut., vol. 15, no. 3, pp. 996–1019.

Hu L. Wen, H. W. (2018). Cooperative jamming for physical layer security enhancement in internet of things. *IEEE Internet Things J.*

Hu, L., Wen, H., Wu, B., Pan, F., Liao, R., Song, H., . . . Wang, X. (2018). *Cooperative jamming for physical layer security enhancement in internet of things.* IEEE Internet Things.

Hussain, M., Du, Q., Sun, L., & Ren, P. (2016). *Security enhancement for video transmission via noise aggregation in.* Multimed. Tools Appl.

Hussain, M., Du, Q., Sun, L., & Ren, P. (2016). *Security enhancement for video transmission via noise aggregation in immersive systems.* Multimed. Tools Appl.

IEEE. (2021, Ιούνιος 14). *Physical Layer Security for IoT Communications - A Survey.* Ανάκτηση από ieeexplore.ieee.org: https://ieeexplore.ieee.org/document/9595025

Imperva Application Security. (2023). *1*. Ανάκτηση από OSI Model: https://www.imperva.com/learn/application-security/osi-model/

intellectsoft. (2020). *Top 10 Biggest IoT Security Issues*. Ανάκτηση από Top 10 Biggest IoT Security Issues: https://www.intellectsoft.net/blog/biggest-iot-security-issues/

ITU. (2013). *The World in 2013: ICT facts and figures.* http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf.

J. Santos, J. R. (2016). *An IoT-based mobile gateway for intelligent personal assistants on mobile health environments.* J. Netw. Comput. Appl. 71, 194–204.

Janna, S., Premnath, S., Clark, M., Kasera, S., Patwari, N., & Krishnamurthy, S. (2009). *On the effectiveness of secret key extraction from wireless signal strength in real environments.* Beijing, China: In Proceedings of the 15th ACM MobiCom.

Jeon, H., Choi, J., McLaughlin, S., & Ha, J. (2013). *Channel aware encryption and decision fusion for wireless networks.* IEEE Trans. Inf. Forensics Secur. .

Jeon, H., Hwang, D., Choi, J., Lee, H., & Ha, J. (2011). *Secure type-based multiple access.* IEEE Trans. Inf. Forensics Secur.

Jiawen Kang, R. Y. (χ.χ.). *Location Privacy Attacks and Defenses in Cloud-Enabled Internet of Vehicles.* 2016: IEEE Wireless Communications, pp. 52-59.

Karim, M., Esmaeilzadeh, M., & Sadeghi, P. (2017). *On reducing intercept probability for unsubscribed video layers using network coding.* IEEE Commun. Lett. .

Khan, A., Tassi, A., & Chatzigeorgiou, I. (2015). *Rethinking the intercept probability of random linear network coding.* IEEE Commun. Lett.

Krikidis, I., Thompson, J., & McLaughlin, S. (2009). *Relay selection for secure cooperative networks with jamming.* IEEE Trans. Wirel. Commun. .

Li, Y., Qi, Y., & Lu, L. (2017). *Secure and Efficient V2V Communications for Hetero geneous Vehicle Ad Hoc Networks.* in International Conference on Networking and Network Applications .

Luby, M. (2002). *LT codes. In Proceedings of the 43rd IEEE Annual Symposium on Foundations of Computer Science.* Vancouver, Canada: BC.

M. Abdel-Basset, G. M. (2018). *Internet of things (IoT) and its impact on supply chain: a framework for building smart, secure and efficient systems.* Fut. Gener. Comput. Syst. 86 (2018) 614–628, doi:10.1016/j.future.2018.04.051.

M.M. Rathore, A. P.-H. (2018). *Exploiting IoT and big data analytics: defining smart digital city using real-time urban data, Sustain. Cities Soc. 40.* doi:10.1016/j.scs.2017.12.022.

MacKay, D. (2005). *Fountain codes.* IEE Proc. Commun.

Mukherjee. (2015). *Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints.* IEEE.

Mullins, T. (2020). *osi-model-7-layers-of-security*. Ανάκτηση από The OSI Model: 7 Layers of Security: https://gofortress.com/osi-model-7-layers-of-security/

Nonenmacher, J., Biersack, E., & Towsley, D. (1998). *Partity-based loss recovery for reliable multicast transmission.* IEEE/ACM Trans. Netw.

Nordrum, A. (2016). *The Internet of Fewer Things.* IEEE Spectrum, vol. 10, pp. 12–13.

O. Aliu, A. I. (2013). *A survey of self organisation in future cellular networks.* IEEE Commun. Surv. Tut., vol. 15, no. 1, pp. 336–361,.

Premnath, S., Jana, S., Croft, J., Gowda, P., Clark, M., Kasera, S., . . . Krishnamurthy, S. (2013). *Secret key extraction from wireless signal strength in real environments.* IEEE Trans. Mob. Comput.

Q, L., Han, G., & Fu, X. (2018). *Physical layer security in multi-hop AF relay network based on compressed sensing.* IEEE Commun. Lett.

Ray, P. (2018). *A survey on internet of things architectures.* J. King Saud Univ. 30 (3) (2018) 291–319.

riarawal99. (2023, Jan 03). *OSI Security Architecture*. Ανάκτηση από OSI Security Architecture: https://www.geeksforgeeks.org/osi-security-architecture/

Rojas, P., Alahmadi, S., & Bayoumi, M. (2021). *Physical Layer Security for IoT Communications - A Survey.* IEEE.

S.A. Al-Qaseemi, H. A. (2016). *IoT architecture challenges and issues: lack of standardization.* Future Technologies Conference (FTC), IEEE, 2016, pp. 731–738.

Sadegh Dorri, R. J. (2016). *TIRIAC: A trust-driven risk-aware acces control framework for Grid enviroments.* Future Generation Computer Systems, vol. 55, pp. 238–254.

Shannon. (1949). C.E. Communication theory of secrecy systems. Στο Shannon. Bell Syst. Tech.

Shea, S. (2022). *10 IoT security challenges and how to overcome them*. Ανάκτηση από 10 IoT security challenges and how to overcome them: https://www.techtarget.com/iotagenda/tip/Internet-of-Things-IOT-Seven-enterprise-risks-to-consider

Shokrollahi, A. (2006). *Rapter codes. .* IEEE Trans. Inf. Theory .

Sun, L., & Xu, H. (2018). *Fountain-coding based secure communications exploiting outage prediction and limited feedback.* IEEE Trans. Veh. Technol. .

Sun, L., Ren, P., Du, Q., & Wang, Y. (2016). Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks. *IEEE Trans. Ind. Inform.*

Sun, L., Ren, P., Du, Q., & Wang, Y. (2016). *Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks.* IEEE Trans. Ind. Inform.

THELES. (2022). *IOT SECURITY ISSUES IN 2022: A BUSINESS PERSPECTIVE*. Ανάκτηση από IOT SECURITY ISSUES IN 2022: A BUSINESS PERSPECTIVE: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats

Wang, G., Meng, C., Heng, W., & Chen, X. (2018). Secrecy energy efficiency optimization in AN-aided distributed. *IEEE Access*.

Wei Zhou, Y. J. (2018). *The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved.* IEEE Internet of Things Journal, pp. 1–11.

Wilson, R., Tse, D., & Scholtz, R. (2007). *Channel identification: Secret sharing using reciprocity in ultrawideband channels.* IEEE Trans. Inf. Forensics Secur.

X. Jia, Q. F. (2012). *RFID technology and its applications in internet of things (IoT).* 2nd International Conference on Consumer.

Xu, H., Sun, L., Ren, P., & Du, Q. (2015). *Securing two-way cooperative systems with an untrusted relay: A constellation-rotation aided approach.* IEEE Commun. Lett.

Yu, N. (2017). *Indistinguishability of compressed encryption with circulant matrices for wireless security.* IEEE Signal Process. Lett. .

Yuankun Xue, J. L. (2017). *Fundamental Challenges Toward Making the IoT a Reachable Reality: A Model-Centric Investigation.* ACM Transactions on Design Automation of Electronic Systems, vol. 22, no. 3.

Zeng, K. (2015). *Physical layer key generation in wireless networks: Challenges and opportunities. .* IEEE Commun. Mag.

Zhang, X., McKay, M., Zhou, X., & Heath, R. (2015). Artificial-noise-aided secure multi-antenna transmission. *IEEE Trans. Wirel. Commun.*