ΠΑΝΕΠΙΣΤΥΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝΒΙΟΜΗΧΑΝΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ ΚΑΙ ΠΑΡΑΓΩΓΗΣ

MSc ΑΥΤΟΜΑΤΙΣΜΟΣ ΠΑΡΑΓΩΓΗΣ & ΥΠΗΡΕΣΙΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ:

ΕΦΑΡΜΟΓΕΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΤΩΝ ΠΡΑΓΜΑΤΩΝ ΣΕ ΚΡΙΣΙΜΑ ΕΠΙΚΟΙΝΩΝΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΣΙΜΟΠΟΥΛΟΣ ΣΥΜΕΩΝ

Α.Μ.: 80697720

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΔΡΟΣΟΣ ΧΡΗΣΤΟΣ

ΙΟΥΛΙΟΣ 2022

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

ΓΚΑΝΕΤΣΟΣ ΘΕΟΔΩΡΟΣ	Theodoros Gkanetsos Digitally signed by Theodoros Gkanetsos Date: 2022.08.10 18:23:24 +03'00'
ΠΑΠΟΥΤΣΙΔΑΚΗΣ ΜΙΧΑΗΛ	Michail Papoutsidakis Digitally signed by Michail Papoutsidakis Date: 2022.08.10 17:11:39 +03'00'
ΔΡΟΣΟΣ ΧΡΗΣΤΟΣ	Christos Drosos Digitally signed by Christos Drosos Date: 2022.08.10 09:26:52 +03'00'

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Σιμόπουλος Συμεών , με αριθμό μητρώου 80697720 φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής Μηχανικών του Τμήματος Μηχανικών Βιομηχανικής Σχεδίασης και Παραγωγής, δηλώνω υπεύθυνα ότι:

«Είμαι συγγραφέας αυτής της διπλωματικής 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.»

Ο Δηλών,
ΣΙΜΟΠΟΥΛΟΣ ΣΥΜΕΩΝ

Περίληψη

Θέμα της παρούσας διπλωματικής εργασίας είναι η αξιοποίηση του Internet of Things (IoT) στα επικοινωνιακά συστήματα. Στο πρώτο κεφάλαιο δίνεται ο ορισμός του IoT, παρουσιάζεται η Αρχιτεκτονική του και αναλύονται οι απαιτήσεις του. Στο δεύτερο κεφάλαιο δίνεται ο ορισμός των επικοινωνιακών συστημάτων, καταγράφονται τα διάφορα είδη επικοινωνιακών συστημάτων και παρουσιάζονται τα πλεονεκτήματα και τα μειονεκτήματα του κάθε είδους. Στο τρίτο, και τελευταίο, κεφάλαιο, αναλύεται η αξιοποίηση του IoT στα συστήματα επικοινωνίας. Πιο συγκεκριμένα παρουσιάζονται οι κυριότερες εφαρμογές του IoT στις επικοινωνίες, όπως το ZigBee, το Bluetooth, το WiFi και το Lora. Στα συμπεράσματα γίνεται ποιοτική σύγκριση των παραπάνω πρωτοκόλλων του IoT και αξιολογείται η συμβολή τους στα συστήματα επικοινωνίας.

Λέξεις – Κλειδιά

Το Δίκτυο των Πραγμάτων, Επικοινωνιακά Συστήματα, Πρωτόκολλα IoT

Abstract

The subject of this thesis is the utilization of the Internet of Things (IoT) in communication systems. In the first chapter the definition of IoT is given, its Architecture is presented and its requirements are analyzed. In the second chapter, the definition of communication systems is given, the various types of communication systems are recorded and the advantages and disadvantages of each type are presented. In the third, and last, chapter, the utilization of IoT in communication systems is analyzed. More specifically, the main applications of IoT in communications are presented, such as ZigBee, Bluetooth, WiFi and Lora. In the conclusions, a qualitative comparison of the above IoT protocols is made and their contribution to communication systems is evaluated.

Keywords

The Network of Things, Communication Systems, IoT Protocols

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

ΠΕΡΙΕΧΟΜΕΝΑ

Εισαγωγή

Το Διαδίκτυο έχει εξελιχθεί σε μια σειρά από κύματα [1]. Τα πρώτα τρία κύματα ήταν με επίκεντρο τις συσκευές. Στο πρώτο κύμα, πήγαμε σε μια συσκευή, συνήθως έναν επιτραπέζιο υπολογιστή, για πρόσβαση στο Διαδίκτυο. Καθώς ο φορητός υπολογιστής εξελισσόταν, σύντομα φέραμε τις δικές μας συσκευές μαζί μας και μπορούσαμε να έχουμε πρόσβαση στο Διαδίκτυο οπουδήποτε, ανά πάσα στιγμή. Σήμερα, βρισκόμαστε στη μέση του λεγόμενου Διαδικτύου των Πραγμάτων (IoT) όπου οι συσκευές (πράγματα) συνδέονται με το Διαδίκτυο και μεταξύ τους.

Αυτά τα πράγματα περιλαμβάνουν ένα πλήθος ετερογενών συσκευών που κυμαίνονται από καταναλωτικές συσκευές, όπως κινητά τηλέφωνα και φορητές συσκευές, έως βιομηχανικούς αισθητήρες και ενεργοποιητές. Η Gartner (2017) υπολόγισε ότι μόνο 8,4 δισεκατομμύρια πράγματα συνδέθηκαν το 2017, αντιπροσωπεύοντας λίγο περισσότερο από το 0,5% των συνολικών εκτιμώμενων συνδεόμενων φυσικών αντικειμένων παγκοσμίως [2].

Το Διαδίκτυο των Πραγμάτων (IoT) έχει αναδειχθεί γρήγορα τα τελευταία δέκα χρόνια και, ωστόσο, σημαίνει διαφορετικά πράγματα για διαφορετικούς ανθρώπους. Πράγματι, οι Whitmore et al. (2015) σημείωσαν ότι δεν υπάρχει καθολικός ορισμός του IoT. Υπάρχουν δύο κύριες εννοιολογήσεις—η τεχνική και η κοινωνικο-τεχνική προοπτική. Η πρώτη, η καθαρή τεχνική προοπτική, βλέπει το IoT ως ένα συγκρότημα και οικοσύστημα τεχνικών αντικειμένων[3].

Για παράδειγμα, οι Weyrich και Ebert (2016), όρισαν το IoT ως ένα καινοτόμο βήμα για τη λειτουργικότητα και την καλύτερη παραγωγικότητα μέσω της απρόσκοπτης σύνδεσης συσκευών [4].Αντίθετα, οι Tarkoma και Katasonov (2011) ορίζουν το IoT ως ένα παγκόσμιο δίκτυο και υποδομή υπηρεσιών μεταβλητής πυκνότητας και συνδεσιμότητας με δυνατότητες αυτορύθμισης που βασίζονται σε τυπικά και διαλειτουργικά πρωτόκολλα και μορφές το οποίο αποτελείται από ετερογενή πράγματα που έχουν ταυτότητες, φυσικές και εικονικές ιδιότητες και ενσωματώνονται απρόσκοπτα και με ασφάλεια στο Διαδίκτυο [5].

Ομοίως, οι Whitmore et al. (2015) ορίζουν το IoT ως ένα παράδειγμα όπου τα καθημερινά αντικείμενα μπορούν να εξοπλιστούν με δυνατότητες αναγνώρισης, ανίχνευσης, δικτύωσης και επεξεργασίας που θα τους επιτρέψουν να επικοινωνούν μεταξύ τους και με άλλες συσκευές και υπηρεσίες μέσω του Διαδικτύου για να επιτύχουν κάποιους συγκεκριμένους σκοπούς [3].

Η κοινωνικο-τεχνική προοπτική του IoT αναγνωρίζει όχι μόνο τα τεχνικά αντικείμενα, αλλά και τους συνεργαζόμενους φορείς και διαδικασίες με τους οποίους αλληλεπιδρά το IoT. Οι Haller et al. (2009) αναγνωρίζει το ρόλο των συνδεδεμένων αντικειμένων ως ενεργών συμμετεχόντων στις επιχειρηματικές διαδικασίες και ορίζουν το IoT ως έναν κόσμο όπου τα φυσικά αντικείμενα ενσωματώνονται απρόσκοπτα στο δίκτυο πληροφοριών και όπου τα φυσικά αντικείμενα μπορούν να γίνουν ενεργοί συμμετέχοντες στις επιχειρηματικές διαδικασίες. Οι υπηρεσίες είναι διαθέσιμες για αλληλεπίδραση με αυτά τα «έξυπνα αντικείμενα» μέσω του Διαδικτύου, για αναζήτηση της κατάστασής τους και οποιασδήποτε πληροφορίας που σχετίζεται με αυτά, λαμβάνοντας υπόψη ζητήματα ασφάλειας και απορρήτου [6].

Ο Shin (2014) υποστηρίζει ότι το IoT είναι μέρος ευρύτερων, κοινωνικο-τεχνικών συστημάτων, που περιλαμβάνουν ανθρώπους, ανθρώπινη δραστηριότητα, χώρους, τεχνουργήματα, εργαλεία και τεχνολογίες. Πράγματι, οι Shin et al. αναφέρουν ότι σε ορισμένες περιπτώσεις, μια βιολογική οντότητα μπορεί, στην πραγματικότητα, να θεωρηθεί το σημείο σύνδεσης, όπως για παράδειγμα ένας άνθρωπος με εμφύτευμα παρακολούθησης καρδιάς ή ένα ζώο φάρμας με αναμεταδότη βιοτσιπ. Υπάρχει ένα γενικό πλαίσιο το ότι μπορεί να χρησιμοποιηθεί για την κατανόηση προβλημάτων και ερευνητικών ερωτημάτων που σχετίζονται με το IoT σε συνδυασμό με ευρέως αποδεκτά επίπεδα γενίκευσης τόσο στις κοινωνικές επιστήμες (nano, micro, meso, macro) όσο και στις επιστήμες υπολογιστών (υπολογισμός, αλγοριθμική/αναπαραστατική, φυσική/υλοποίηση). Επιπλέον, παρέχει μια αρκετά γενική αφαίρεση του IoT, καθώς διευκολύνει τη δημιουργία νοημάτων χωρίς να φτάνει σε ένα μη γενικευμένο επίπεδο ευαισθησίας.

Σε αυτό το πλαίσιο, προσδιορίζονται και ορίζονται πέντε βασικές οντότητες. Κάθε μία από αυτές τις οντότητες έχει μια μυριάδα χαρακτηριστικών που μπορεί να αλλάξουν και να εξελιχθούν με την πάροδο του χρόνου και να επηρεάσουν την κατανόησή μας για το πώς μπορεί να δημιουργηθεί και να συλληφθεί αξία σε διαφορετικές μονάδες

ανάλυσης:

Οι κοινωνικοί δρώντες (S), ενώ είναι τυπικά άνθρωποι, δεν χρειάζεται να είναι. Το πλαίσιο είναι αρκετά ευέλικτο ώστε να προσαρμόζεται στην αναδυόμενη έννοια των υπολογιστών ως κοινωνικών παραγόντων [8]. Τα πράγματα (T) είναι κυρίως φυσικά, ωστόσο μπορεί επίσης να είναι εικονικά και να υπάρχουν σε επαυξημένη ή/και εικονική πραγματικότητα. Δύο βασικές λειτουργικές απαιτήσεις των πραγμάτων στο IoT και το IoE είναι η ανίχνευση δεδομένων (συλλογή δεδομένων) και η συνδεσιμότητα δικτύου. Τα δεδομένα (D) εδώ είναι διακριτά τεχνουργήματα που μπορούν να συνδεθούν με άλλες οντότητες συμπεριλαμβανομένων άλλων δεδομένων και μπορεί να προέρχονται από πηγές πρώτου μέρους, δεύτερου μέρους ή τρίτων. Αναγνωρίζει την ύπαρξη μιας αλυσίδας δεδομένων IoT.

Για παράδειγμα, η αναγνώριση ραδιοσυχνοτήτων (RFID) επιτρέπει την παρακολούθηση αντικειμένων μέσω ενός ηλεκτρονικού κωδικού προϊόντος (EPC) που χρησιμεύει ως σύνδεσμος προς δεδομένα σχετικά με το αντικείμενο που μπορούν να αναζητηθούν μέσω του Διαδικτύου [6]. Τα δίκτυα (N) είναι συστήματα διασυνδεδεμένων οντοτήτων και είναι και αγωγοί και οντότητες από μόνα τους. Το πλαίσιο μας φιλοξενεί δίκτυα μεταξύ διαφορετικών τύπων οντοτήτων IoT και του ίδιου τύπου, για παράδειγμα δίκτυα μηχανής με μηχανή (M2M). Τα συμβάντα (E) είναι περιστατικά ενδιαφέροντος σε δεδομένη στιγμή ή/και φυσικό ή εικονικό χώρο. Οι διεργασίες (P) είναι προφανώς κρίσιμες για τον τρόπο με τον οποίο οι οντότητες αλληλεπιδρούν στο IoT και περιλαμβάνουν γενικές (π.χ. επικοινωνία) και διαδικασίες ειδικές για τον τομέα. Είναι απαραίτητες για τον τρόπο δημιουργίας, σύλληψης και παράδοσης αξίας στο IoT.

Όλες οι οντότητες και οι διεργασίες λαμβάνουν χώρα σε ένα περιβάλλον υποδομής και το πλαίσιο αναγνωρίζει ότι στο IoT, επιπλέον δεδομένα και μεταδεδομένα δημιουργούνται και συγκεντρώνονται σε επίπεδο υποδομής. Καθώς το IoT μπορεί να διερευνηθεί από πολλές οπτικές γωνίες, υποστηρίζουμε ότι ένα τέτοιο ερευνητικό πλαίσιο μπορεί να διαδραματίσει σημαντικό ρόλο ώστε οι ερευνητές να κατανοήσουν ένα περίπλοκο και δυναμικό περιβάλλον και να απομονώσουν τα κύρια στοιχεία της εμπειρίας του IoT. Επιπλέον, το προτεινόμενο πλαίσιο μπορεί να χρησιμοποιηθεί ως ικρίωμα γενικής χρήσης για τη δημιουργία ερευνητικών ατζέντηδων στο IoT και την αποφυγή διπλών και μη εστιασμένων ερευνητικών προσπαθειών.

Το IoT περιστρέφεται γύρω από έναν αριθμό βασικών εννοιών και τεχνολογιών ενεργοποίησης, συμπεριλαμβανομένων της αναγνώρισης αντικειμένων (π.χ. IPv6), ανίχνευσης πληροφοριών (π.χ. RFID, αισθητήρες, GPS, κ.λπ.), τεχνολογίες επικοινωνιών για ανταλλαγή δεδομένων και τεχνολογίες ολοκλήρωσης δικτύου [6]. Είναι σημαντικό να σημειωθεί ότι οι αρχιτεκτονικές υπολογιστών και τηλεπικοινωνιών παλαιού τύπου δεν σχεδιάστηκαν με γνώμονα το IoT. Η κλίμακα των ετερογενών συσκευών και ο άνευ προηγουμένου όγκος, η ποικιλία και η ταχύτητα δεδομένων σε συνδυασμό με μια ακραία διακύμανση στο περιβάλλον χρήσης απαιτούν νέα παραδείγματα στον υπολογιστή. Ανάλογα με την περίπτωση χρήσης και τις απαιτήσεις επιπέδου υπηρεσίας, οι συσκευές IoT ενδέχεται να απαιτούν επεξεργασία και αποθήκευση τοπικά, στο cloud ή κάπου ενδιάμεσα. Επιπλέον, το cloud computing, το edge, το fog και το dew computing είναι τρία νέα μοντέλα υπολογιστών που έχουν σχεδιαστεί για να υποστηρίζουν το IoT. Αν και πέρα από το πεδίο αυτού του κεφαλαίου, είναι χρήσιμο να γνωρίζουμε αυτές τις έννοιες και τεχνολογίες όταν εξετάζουμε τις αρχιτεκτονικές στο IoT.

1. Το Δίκτυο των Πραγμάτων (Internet of Things, IoT)

1.1. Η Αρχιτεκτονική του Δικτύου των Πραγμάτων

Οι συσκευές IoT χρησιμοποιούνται σε ένα ευρύ φάσμα τομέων όπως η υγεία, η γεωργία, οι έξυπνες πόλεις και η αυτοματοποίηση διαδικασιών. Τα «πράγματα» που χρησιμοποιούνται μπορούν να χαρακτηριστούν από την ετερογένειά τους όσον αφορά τους υπολογιστικούς πόρους (επεξεργασία, μνήμη και αποθήκευση), τη συνδεσιμότητα δικτύου (πρωτόκολλα και πρότυπα επικοινωνίας) και την ανάπτυξη λογισμικού (υψηλός βαθμός διανομής, παραλληλισμός, δυναμικότητα).

Ενώ αυτή η ετερογένεια επιτρέπει το βάθος και το εύρος των εφαρμογών και των περιπτώσεων χρήσης, εισάγει επίσης πολυπλοκότητα, ιδιαίτερα σε σχέση με τις αναμενόμενες απαιτήσεις επιπέδου υπηρεσιών, για παράδειγμα, κινητικότητα χρήστη και συσκευής, αξιοπιστία λογισμικού, υψηλή διαθεσιμότητα, δυναμικότητα σεναρίου και επεκτασιμότητα. Ως εκ τούτου, απαιτείται ένα επίπεδο αφαίρεσης για την προώθηση της διαλειτουργικότητας μεταξύ των συσκευών IoT. Ωστόσο, η έλλειψη τυποποίησης σημαίνει ότι δεν υπάρχει τέτοια διαλειτουργικότητα [9]. Οι Αρχιτεκτονικές Αναφοράς μπορούν να βοηθήσουν τους προγραμματιστές λογισμικού IoT να κατανοήσουν, να συγκρίνουν και να αξιολογήσουν διαφορετικές λύσεις IoT ακολουθώντας μια ενιαία πρακτική.

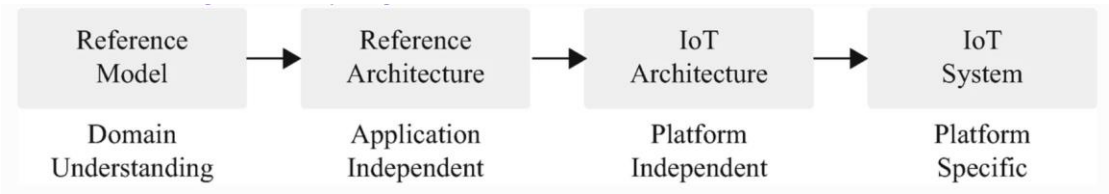
Έχουν προταθεί αρκετές Αρχιτεκτονικές Αναφοράς προκειμένου να τυποποιηθούν οι έννοιες και η εφαρμογή συστημάτων IoT σε διαφορετικούς τομείς. Ο Breivold, για παράδειγμα, πραγματοποίησε μια συγκριτική μελέτη με έντεκα διαφορετικές Αρχιτεκτονικές Αναφοράς. Αυτό το κεφάλαιο εστιάζει σε εκείνες τις Αρχιτεκτονικές Αναφοράς που επιτρέπουν την ενσωμάτωση του IoT με το cloud computing ή/και το fog and edge computing, δηλαδή σε όλο το συνεχές από το cloud το πράγμα (C2T) [10].

Το Σχήμα 1 δείχνει το χρονοδιάγραμμα που περιέχει τις κύριες Αρχιτεκτονικές Αναφοράς που υποστηρίζουν το IoT σε όλο το συνεχές C2T, συγκεκριμένα το μοντέλο IoT Architectural Reference (IoT ARM), IEEE P2413 (IEEE P2413 2014), Industrial Internet Reference Architecture (IIRA al.9) (L20) (L20) , WSO2 IRA, Intel SAS, Azure IRA και SAT-IoT.

Σχήμα 1. Χρονοδιάγραμμα επιλεγμένων αρχιτεκτονικών αναφοράς IoT[1]

1.2.1 Αρχιτεκτονικό μοντέλο αναφοράς Internet of Things (IoT ARM)

Το έργο IoT-A (IoT-A 2019) ομαδοποιεί τις ιδιαιτερότητες των λειτουργιών του IoT και ορίζει το Αρχιτεκτονικό Μοντέλο Αναφοράς IoT (IoT ARM) για να υποστηρίξει τη χρήση, την ανάπτυξη και την ανάλυση διαφορετικών συστημάτων IoT, από την επικοινωνία έως το επίπεδο εξυπηρέτησης. Σύμφωνα με τους Bauer et al., οι κύριες συνεισφορές του IoT ARM είναι δύο: (α) το ίδιο το Μοντέλο Αναφοράς, το οποίο περιέχει μια κοινή κατανόηση του τομέα IoT και τους ορισμούς των κύριων οντοτήτων IoT και τις βασικές σχέσεις και αλληλεπιδράσεις τους. και (β) την Αρχιτεκτονική Αναφοράς αυτή καθαυτή, η οποία παρέχει απόψεις και προοπτικές για τη δημιουργία αρχιτεκτονικών IoT προσαρμοσμένων στις συγκεκριμένες απαιτήσεις κάποιου [11]. Με αυτόν τον τρόπο, το Μοντέλο Αναφοράς και η Αρχιτεκτονική Αναφοράς παρέχουν επίπεδα αφαίρεσης (μοντέλα, όψεις και προοπτικές) για την εξαγωγή συγκεκριμένων λύσεων IoT (δηλαδή αρχιτεκτονικές και συστήματα IoT συμβατά με IoT ARM) (Σχ. 2).



Σχήμα 2. Προέλευση από κάθε βήμα IOT ARM[2]

Η Αρχιτεκτονική Αναφοράς είναι ανεξάρτητη από μια συγκεκριμένη περίπτωση χρήσης ή εφαρμογή και περιλαμβάνει τρεις όψεις: (α) λειτουργική, (β) πληροφορίες και (γ) ανάπτυξη και λειτουργία. Η λειτουργική προβολή περιγράφει τα λειτουργικά στοιχεία ενός συστήματος. Αυτές περιλαμβάνουν τις ευθύνες των στοιχείων, τις

[1] https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/12310/Pelekanos_MDE1633.pdf?sequence=1&isAllowed=y
[2] https://www.arm.com/solutions/iot/iot-technology

προεπιλεγμένες λειτουργίες, τις διεπαφές και τις αλληλεπιδράσεις. Η αρχιτεκτονική αποτελείται από πέντε διαμήκεις ομάδες λειτουργικότητας (FGs), δηλαδή οργάνωση υπηρεσιών, διαχείριση διεργασιών IoT, εικονική οντότητα, υπηρεσίες IoT, επικοινωνία και δύο εγκάρσιες ομάδες FG, δηλαδή διαχείριση και ασφάλεια.

Η προβολή πληροφοριών καλύπτει τον κύκλο ζωής των πληροφοριών στο σύστημα IoT, παρέχοντας μια επισκόπηση των δομών και των ροών πληροφοριών (δηλαδή πώς ορίζονται, δομούνται, ανταλλάσσονται, επεξεργάζονται και αποθηκεύονται οι πληροφορίες) και τη λίστα των στοιχείων που εμπλέκονται στη διαδικασία.

Τέλος, η άποψη ανάπτυξης και λειτουργίας διαδραματίζει σημαντικό ρόλο στην υλοποίηση των συστημάτων IoT καθώς συγκεντρώνουν έναν αριθμό συσκευών, καθεμία από τις οποίες έχει διαφορετικούς πόρους και διεπαφές σύνδεσης, οι οποίες μπορούν να διασυνδεθούν με πολλούς τρόπους. Η προβολή ανάπτυξης και λειτουργίας παρέχει ένα σύνολο οδηγιών για το σχεδιασμό του συστήματος, που καλύπτουν διαφορετικές πτυχές τεχνολογιών, πρωτοκόλλων επικοινωνίας, υπηρεσιών, πόρων και αποθήκευσης πληροφοριών.

Σύμφωνα με τους Bauer et al., η εξέλιξη και η διαλειτουργικότητα, η διαθεσιμότητα και η ανθεκτικότητα, η εμπιστοσύνη, η ασφάλεια και το απόρρητο και η απόδοση και η επεκτασιμότητα είναι τα πιο σημαντικά για τις προοπτικές για τα συστήματα IoT. Παρουσιάζουν επίσης μια αντίστροφη χαρτογράφηση για να δείξουν πώς οι έννοιες του IoT ARM μπορούν να παρουσιαστούν στις υπάρχουσες αρχιτεκτονικές και για να επικυρώσουν την πρότασή τους. Μία από τις περιπτώσεις χρήσης βασίστηκε στη χρήση RFID για τον εντοπισμό των πετσετών πριν, κατά τη διάρκεια και μετά το χειρουργείο για να αποφευχθεί η παραμονή πετσετών στην κοιλιά του ασθενούς. Αυτή η περίπτωση χρήσης βασίστηκε επίσης στη χρήση μιας υποδομής cloud για την αποθήκευση δεδομένων. Παρόλο που οι συγγραφείς υποστηρίζουν ότι η χαρτογράφηση IoT ARM έγινε με επιτυχία, δεν υπάρχει τρόπος να πούμε ότι μπορεί να εφαρμοστεί σε οποιαδήποτε υπάρχουσα αρχιτεκτονική σκυροδέματος [11].

1.2.2 Πρότυπο IEEE για ένα αρχιτεκτονικό πλαίσιο για το Διαδίκτυο των πραγμάτων (P2413)

Για να αποφευχθούν τα σιλό σε πρότυπα για συγκεκριμένο τομέα, το P2413 είναι ένα ενοποιημένο αρχιτεκτονικό πλαίσιο για το IoT. Εκτός από τον ορισμό του πλαισίου, περιλαμβάνει περιγραφές διαφόρων τομέων IoT, ορισμούς αφαιρέσεων τομέα IoT και προσδιορισμό κοινών σημείων μεταξύ διαφορετικών τομέων IoT (ενέργεια, μέσα, σπίτι, μεταφορές κ.λπ.). Παρέχει ένα μοντέλο αναφοράς που καθορίζει τις σχέσεις μεταξύ διαφόρων κάθετων IoT και κοινών αρχιτεκτονικών στοιχείων. Με αυτόν τον τρόπο έχει παρόμοιες αρχές σχεδίασης με το IoT ARM [48]

Η Αρχιτεκτονική Αναφοράς καλύπτει τον ορισμό των βασικών αρχιτεκτονικών δομικών στοιχείων και την ικανότητά τους να ενσωματώνονται σε συστήματα πολλαπλών επιπέδων. Η Αρχιτεκτονική Αναφοράς εξετάζει επίσης τον τρόπο τεκμηρίωσης και μετριασμού της απόκλισης αρχιτεκτονικής. Το P2413 περιλαμβάνει επίσης ένα σχέδιο για την αφαίρεση δεδομένων και αντιμετωπίζει την ανάγκη για εμπιστοσύνη μέσω της προστασίας, της ασφάλειας, του απορρήτου και της ασφάλειας. Εφαρμόζοντας το P2413, η αρχιτεκτονική διαφάνεια των συστημάτων IoT μπορεί να βελτιωθεί για να παρέχει αξιολογήσεις συγκριτικής αξιολόγησης, ασφάλειας και ασφάλειας.

Το P2413.1 είναι το Πρότυπο για μια Αρχιτεκτονική Αναφοράς για Έξυπνη Πόλη (RASC) (P2413.1 2019). Το RASC παρέχει έναν αρχιτεκτονικό σχεδιασμό για την υλοποίηση μιας έξυπνης πόλης, επιτρέποντας την αλληλεπίδραση και τη διαλειτουργικότητα μεταξύ τομέων και στοιχείων συστήματος. Οι εφαρμογές έξυπνων πόλεων μπορεί να περιλαμβάνουν διαχείριση νερού, διαχείριση απορριμμάτων, φωτισμό δρόμων, έξυπνο πάρκινγκ, περιβαλλοντική παρακολούθηση, έξυπνη κοινότητα, έξυπνη πανεπιστημιούπολη, έξυπνα κτίρια, ηλεκτρονική υγεία, ηλεκτρονική διακυβέρνηση κ.λπ. Το RASC περιλαμβάνει το Ευφυές Κέντρο Επιχειρήσεων (IoC) και IoT. [49]

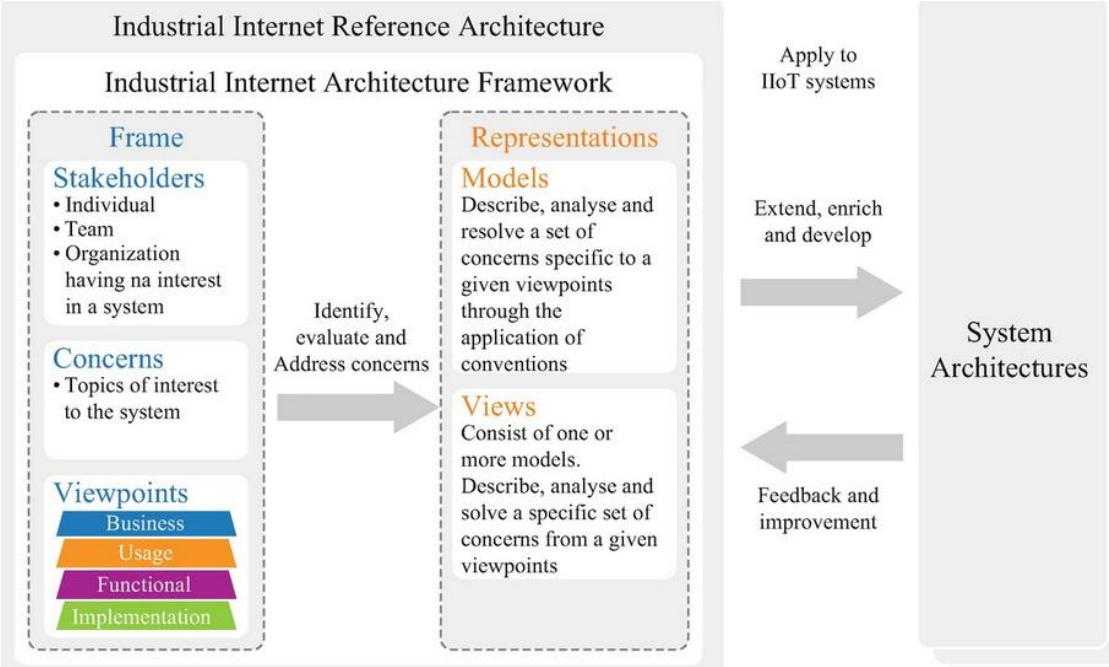
Το P2413.2 είναι το Πρότυπο για Αρχιτεκτονική Αναφοράς για Διανομή Ισχύος IoT (PDIoT) (P2413.2 2019). Ακολουθώντας μια παρόμοια ιδέα του RASC, το PDIoT παρέχει επίσης έναν αρχιτεκτονικό σχεδιασμό, αλλά για την υλοποίηση συστημάτων

διανομής ενέργειας, που καλύπτουν διαφορετικούς τομείς, όπως συστήματα δικτύου παλαιού τύπου, IoT και υπολογιστικό νέφος. Αυτό το πρότυπο ορίζει μια διανομή ενέργειας που βασίζεται στο cloud, η οποία υποστηρίζει μικροϋπηρεσίες και μετάβαση από παλαιού τύπου συστήματα σε πλατφόρμες που βασίζονται στο IoT. Ο όρος «Βιομηχανικό Διαδίκτυο» αποδίδεται σε μεγάλο βαθμό στην General Electric (GE). Σε μια κοινή έκθεση, οι Accenture και GE (2014) ορίζουν το βιομηχανικό διαδίκτυο ως μια αρχιτεκτονική που δίνει τη δυνατότητα στις εταιρείες να χρησιμοποιούν αισθητήρες, λογισμικό, εκμάθηση από μηχανή σε μηχανή και άλλες τεχνολογίες για τη συλλογή και ανάλυση δεδομένων από φυσικά αντικείμενα ή άλλες μεγάλες ροές δεδομένων—και στη συνέχεια να χρησιμοποιούν αυτές τις αναλύσεις για τη διαχείριση λειτουργιών και, σε ορισμένες περιπτώσεις, για να προσφέρουν νέα, υπηρεσίες προστιθέμενης αξίας [19].

Σήμερα, το Βιομηχανικό Διαδίκτυο έχει εξελιχθεί στο Βιομηχανικό Διαδίκτυο των Πραγμάτων (IIoT). Το IIoT ορίζεται Boyes et al. (2018) ως ένα σύστημα που περιλαμβάνει δικτυωμένα έξυπνα αντικείμενα, κυβερνοφυσικά περιουσιακά στοιχεία, σχετικές γενικές τεχνολογίες πληροφοριών και προαιρετικές πλατφόρμες υπολογιστικού νέφους ή αιχμής, που επιτρέπουν σε πραγματικό χρόνο, έξυπνη και αυτόνομη πρόσβαση, συλλογή, ανάλυση, επικοινωνίες και ανταλλαγή διαδικασιών, προϊόντων και/ ή πληροφορίες υπηρεσιών, εντός του βιομηχανικού περιβάλλοντος, ώστε να βελτιστοποιηθεί η συνολική αξία παραγωγής [20].

Κάπως όπως το IoT ARM και το P2413, το Industrial Internet Reference Architecture (IIRA) είναι ένα πλαίσιο αρχιτεκτονικής για την ανάπτυξη διαλειτουργικών συστημάτων IIoT για ποικίλες εφαρμογές σε βιομηχανικούς κλάδους [21]. Το IIRA αποτελείται από ένα πλαίσιο και διαφορετικές παραστάσεις (Σχ. 3). Πρόκειται για ένα πλαίσιο, μια συλλογή εννοιών που αντιπροσωπεύονται από ενδιαφερόμενα μέρη (άτομο, ομάδα, οργανισμός που ενδιαφέρεται για ένα σύστημα), ανησυχίες (οποιοδήποτε θέμα ενδιαφέροντος που σχετίζεται με το σύστημα) και απόψεις (πλαισίωση συμβάσεων την περιγραφή και ανάλυση συγκεκριμένων ανησυχιών του συστήματος). Οι αναπαραστάσεις ορίζονται ως όψεις και μοντέλα, τα οποία είναι συλλογές των αποτελεσμάτων που λαμβάνονται μέσω της εφαρμογής του πλαισίου αρχιτεκτονικής σε αφηρημένα ή συγκεκριμένα συστήματα. Αυτά τα μοντέλα και οι

απόψεις επιλέγονται για την αντιμετώπιση μιας συγκεκριμένης ανησυχίας σε κατάλληλο επίπεδο αφαίρεσης [21].



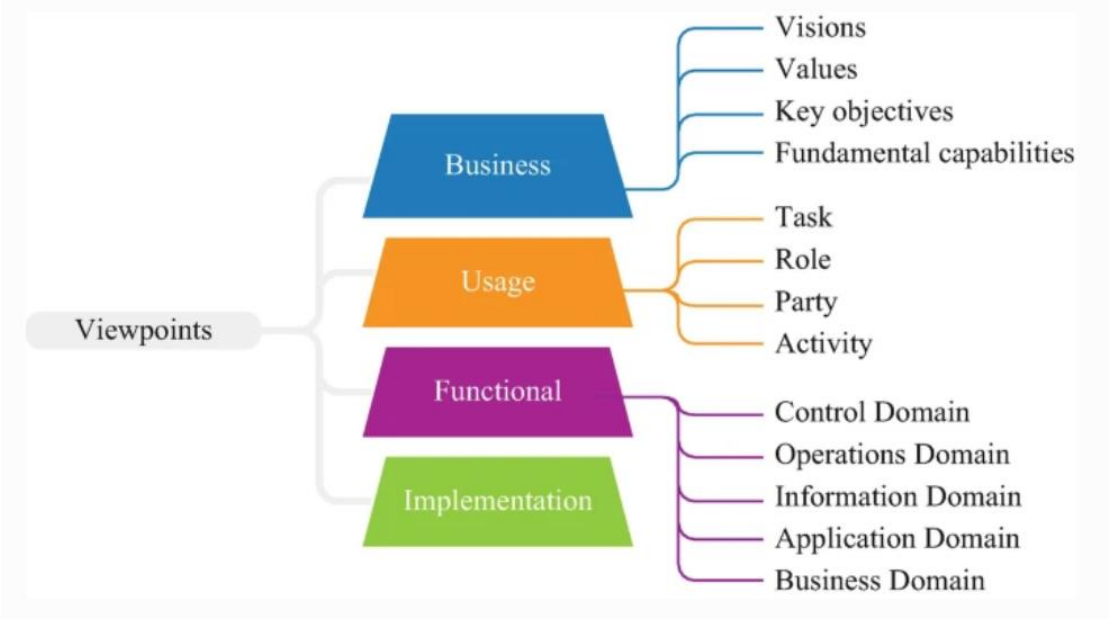
Σχήμα 3. Industrial internet Reference Architecture[3]

Το IIRA εντοπίζει τις κύριες αρχιτεκτονικές ανησυχίες που εντοπίζονται στα συστήματα IIoT και τις ταξινομεί σε απόψεις που σχετίζονται με τους αντίστοιχους ενδιαφερόμενους φορείς. Οι απόψεις είναι κρίσιμα στοιχεία στο IIRA. υπάρχουν τέσσερις διαφορετικές απόψεις (Σχ. 4).

Πρώτον, η Επιχειρηματική Άποψη είναι υπεύθυνη για την εισαγωγή του οράματος, των αξιών και των στόχων των επιχειρηματικών ενδιαφερομένων στο εμπορικό και ρυθμιστικό πλαίσιο. Δεύτερον, το Usage Viewpoint περιγράφει πώς ένα σύστημα IIoT πραγματοποιεί τις βασικές του δυνατότητες, παρέχοντας την ακολουθία δραστηριοτήτων που συντονίζει τα στοιχεία του συστήματος. Τρίτον, το Functional Viewpoint συσχετίζει τις λειτουργικές και δομικές δυνατότητες ενός συστήματος IIoT και των στοιχείων του. Αποσυντίθεται σε πέντε κύριους λειτουργικούς τομείς: τομέας ελέγχου, τομέας λειτουργίας, τομέας πληροφοριών, τομέας εφαρμογής και

[3] https://www.researchgate.net/figure/Industrial-Internet-Integrated-Reference-Model-I3RM_fig8_336693486

επιχειρηματικός τομέας. Τέλος, το Implementation Viewpoint παρέχει (1) μια περιγραφή της γενικής αρχιτεκτονικής ενός συστήματος IIoT, (2) μια τεχνική περιγραφή των στοιχείων του, (3) έναν χάρτη υλοποίησης των δραστηριοτήτων που προσδιορίζονται στο Usage Viewpoint. και (4) έναν χάρτη υλοποίησης για τα βασικά χαρακτηριστικά του συστήματος [21].



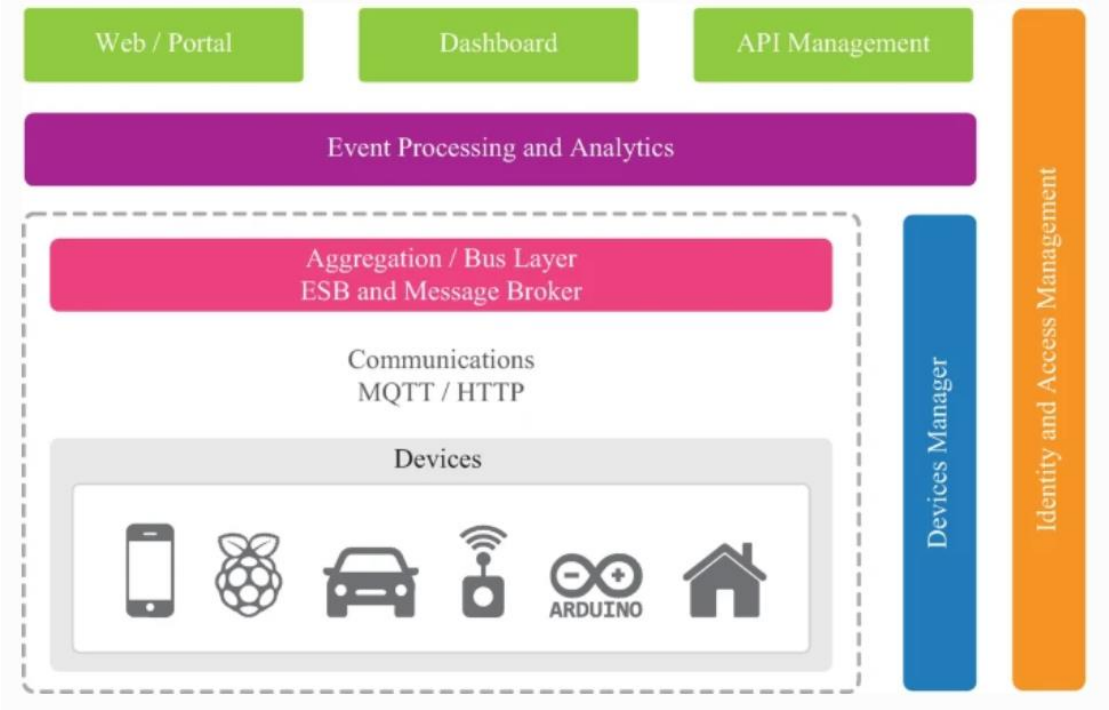
Σχήμα 4. Απόψεις IIRA[4]

Με την υιοθέτηση του IIRA, οι βιομηχανίες μπορούν να ενσωματώσουν τις βέλτιστες πρακτικές στις διαδικασίες τους, να χρησιμοποιήσουν μια γενική αρχιτεκτονική και ένα κοινό πλαίσιο και ως αποτέλεσμα να μειώσουν τις λειτουργικές δαπάνες. Θα πρέπει να σημειωθεί ότι το IIRA παρέχει αρχιτεκτονικά μοτίβα τόσο για το cloud όσο και για το edge computing.

Το WSO2 είναι ένας προμηθευτής ενοποίησης ανοιχτού κώδικα με έδρα τις ΗΠΑ. Η Αρχιτεκτονική αναφοράς WSO2 IoT (WSO2 IRA) απεικονίζεται στο Σχ. 5 και υποστηρίζει την παρακολούθηση, τη διαχείριση και την αλληλεπίδραση συσκευών IoT, καλύπτοντας τη διαδικασία επικοινωνίας μεταξύ του IoT και του cloud [22]. Το WSO2 IRA περιλαμβάνει πέντε οριζόντια επίπεδα (πελάτη/εξωτερική επικοινωνία, επεξεργασία συμβάντων και αναλυτικά στοιχεία, επίπεδο συγκέντρωσης, μεταφορές

[4]https://dspace.lib.ntua.gr/xmlui/bitstream/handle/123456789/52409/Athanasopoulos%20Athanasios%20Diploma%20Thesis.pdf?sequence=1

και συσκευές) και δύο επίπεδα διατομής (διαχείριση συσκευής και διαχείριση ταυτότητας και πρόσβασης).

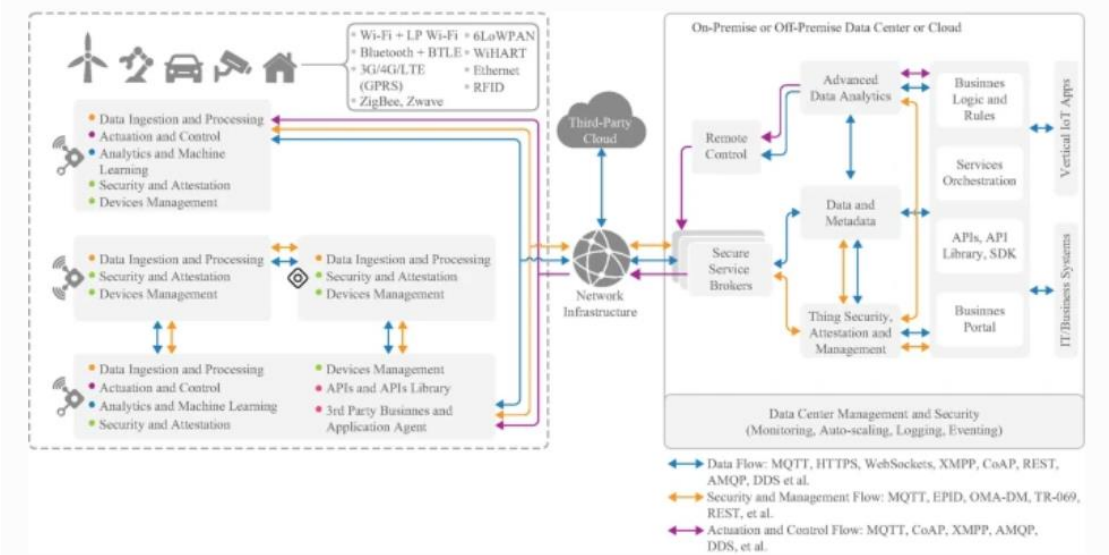


Σχήμα 5. Αρχιτεκτονική αναφοράς WSO2 IoT[5]

Ο σκοπός των προδιαγραφών αρχιτεκτονικής συστήματος Intel (SAS) είναι η σύνδεση οποιουδήποτε τύπου συσκευής στο cloud λαμβάνοντας υπόψη πέντε βασικά στοιχεία: (1) διαχείριση C2T, (2) αναλυτικά στοιχεία σε πραγματικό χρόνο, (3) διαλειτουργικότητα, (4) υπηρεσία και συσκευή ανακάλυψη και παροχή, και (5) ασφάλεια (Intel 2015).

Η Intel SAS έχει δύο ξεχωριστές εκδόσεις που συνυπάρχουν προκειμένου να καλύπτουν διαφορετικά επίπεδα ωριμότητας υποδομής: έκδοση 1.0 για σύνδεση μη συνδεδεμένων και έκδοση 2.0 για έξυπνα και συνδεδεμένα πράγματα. Η έκδοση 1.0 καθορίζει τον τρόπο με τον οποίο οι συσκευές παλαιού τύπου που δεν σχεδιάστηκαν αρχικά για να συνδέονται στο cloud μπορούν να χρησιμοποιούν μια πύλη IoT για να είναι συνδεδεμένες στο διαδίκτυο. Η έκδοση 2.0 καθορίζει τον τρόπο ενσωμάτωσης ετερογενών έξυπνων πραγμάτων με επίκεντρο την ασφάλεια, τη διαχειρισιμότητα και την κοινή χρήση δεδομένων σε πραγματικό χρόνο μεταξύ πραγμάτων και cloud (Σχ. 6)

[5] https://docs.wso2.com/display/IoTS100COPY/WSO2+IoT+Server+Architecture



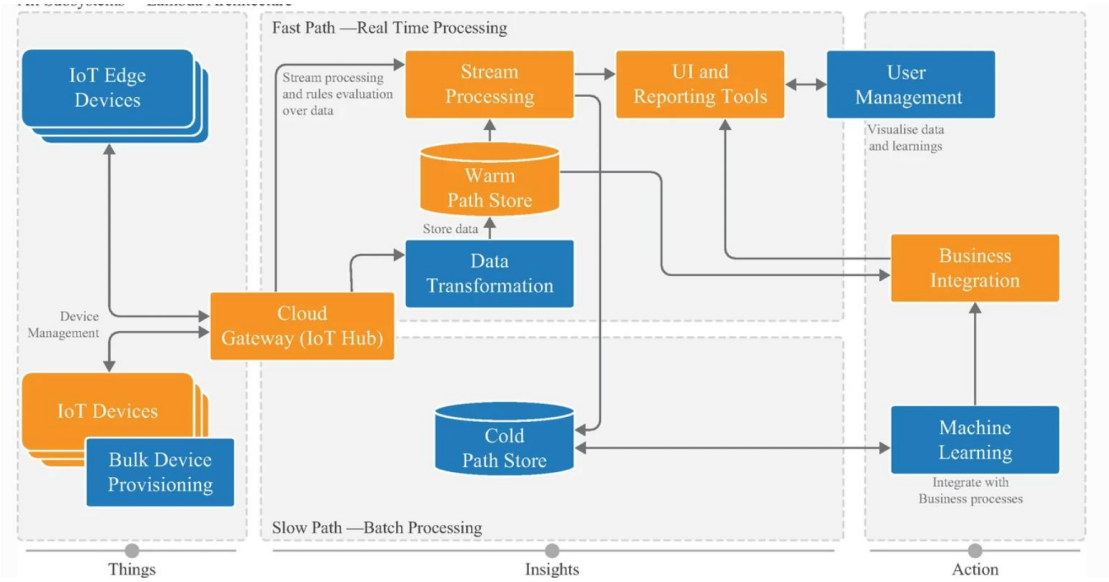
Σχήμα 6. Προδιαγραφές αρχιτεκτονικής συστήματος Intel[6]

Η Intel SAS συνιστά μια πολυεπίπεδη αρχιτεκτονική που περιλαμβάνει οριζόντια επίπεδα (χρήστες, χρόνο εκτέλεσης και προγραμματιστές) και κάθετα επίπεδα (επιχειρήσεις και ασφάλεια). Η ροή δεδομένων περιλαμβάνει έντεκα βήματα, συμπεριλαμβανομένων της μετατροπής αναλογικού σε ψηφιακό (ADC), των πυλών και της πρόσβασης στο σύννεφο. Η Intel συνιστά επίσης στοιχεία λογισμικού και διεπαφές για τη σύνδεση παλαιού τύπου συσκευών χωρίς λειτουργικότητα συνδεσιμότητας. Τα στοιχεία λογισμικού βρίσκονται σε συσκευές τελικού σημείου και στο cloud. Βασικά, τα στοιχεία λογισμικού cloud λαμβάνουν δεδομένα που συλλέγονται από στοιχεία εσωτερικής εγκατάστασης και είναι υπεύθυνα για την ανάλυση, την αποθήκευση και την ενορχήστρωση υπηρεσιών.

Το Azure IoT Reference Architecture (Azure IRA) που αναπαρίσταται στο Σχ. 7 βασίζεται στην πλατφόρμα Microsoft Azure για τη σύνδεση αισθητήρων με έξυπνες υπηρεσίες στο cloud. Ο κύριος στόχος του Azure IRA είναι να αναλάβει ενέργειες σχετικά με επιχειρηματικές πληροφορίες που δημιουργούνται μέσω της συλλογής δεδομένων από εφαρμογές IoT («πράγματα») [23] . Το έγγραφο αναφοράς προτείνει μια συνιστώμενη αρχιτεκτονική IoT, που περιγράφει θεμελιώδεις έννοιες και αρχές, λεπτομέρειες υποσυστημάτων IoT και ζητήματα σχεδιασμού λύσεων. Το Azure IRA εστιάζει στην ευελιξία. Ως εκ τούτου, οι λύσεις IoT είναι εγγενείς στο cloud και βασίζονται σε μικροϋπηρεσίες. Καθώς οι αναπτυσσόμενες υπηρεσίες είναι

[6] http://repfiles.kallipos.gr/html_books/1285/bookES.html

ανεξάρτητες μεταξύ τους, προτείνουν ότι είναι καλύτερο για κλιμάκωση, ενημέρωση μεμονωμένων υποσυστημάτων IoT και ευελιξία στην επιλογή τεχνολογιών ανά υποσύστημα IoT.



Σχήμα 7. Azure IoT Reference Architecture[7]

Το Σχήμα 7 δείχνει το προτεινόμενο Azure IRA που καλύπτει τόσο την ενσωμάτωση υβριδικού νέφους όσο και λύσεων ακμών. Σε πορτοκαλί χρώμα, μπορεί κανείς να δει τα βασικά υποσυστήματα IoT: συσκευές IoT, πύλη cloud (IoT Hub), επεξεργασία ροής και διεπαφή χρήστη. Η συσκευή IoT θα πρέπει να μπορεί να εγγραφεί στην πύλη cloud, η οποία είναι υπεύθυνη για τη διαχείριση των συσκευών. Ο επεξεργαστής ροής καταναλώνει και αποθηκεύει τα δεδομένα και ενσωματώνεται στην επιχειρηματική διαδικασία. Για κάθε υποσύστημα, το Azure IRA συνιστά μια συγκεκριμένη τεχνολογία που βασίζεται στις υπηρεσίες Azure. Υπάρχει επίσης ένα σύνολο προαιρετικών υποσυστημάτων IoT (με μπλε): συσκευές IoT edge, μετασχηματισμός δεδομένων, μηχανική εκμάθηση και διαχείριση χρηστών. Οι συσκευές ακμής είναι σε θέση να συγκεντρώνουν και/ή να μετασχηματίζουν και να επεξεργάζονται τα δεδομένα επί τόπου, ενώ ο μετασχηματισμός δεδομένων (στο cloud) μπορεί να χειρίζεται και να μεταφράζει δεδομένα τηλεμετρίας. Το υποσύστημα μηχανικής εκμάθησης επιτρέπει στο σύστημα IoT να μαθαίνει από προηγούμενα δεδομένα και να ενεργεί σωστά, όπως η ειδοποίηση πυροδότησης για την προγνωστική συντήρηση. Τέλος, το υποσύστημα

[7] https://www.researchgate.net/figure/Azure-IoT-Reference-Architecture-Adapted-from-Microsoft-2018_fig3_342744519

διαχείρισης χρηστών παρέχει λειτουργικότητα στους χρήστες για τη διαχείριση των συσκευών.

Το SAT IoT είναι μια πλατφόρμα που αναπτύχθηκε από την ισπανική εταιρεία SATEC, ως μέρος του έργου Horizon 2020 RECAP. Υποσημείωση 1 Οι έξυπνες πόλεις είναι μια κύρια περίπτωση χρήσης για το SAT IoT. Ως εκ τούτου, χρειαζόταν μια αρχιτεκτονική που θα μπορούσε (1) να διαχειρίζεται την τοπολογία του δικτύου δεδομένων έξυπνης πόλης κατά την εκτέλεση, (2) να χρησιμοποιεί τεχνικές βελτιστοποίησης που υποστηρίζουν την επεξεργασία συγκεντρωτικών δεδομένων ανά γεωγραφικές ζώνες και (3) να παρακολουθεί το σύστημα IoT και τη διαδικασία βελτιστοποίησης σε χρόνος εκτέλεσης [24].

Η διαφάνεια τοποθεσίας υπολογιστών άκρων/νέφους είναι ένα βασικό χαρακτηριστικό της πλατφόρμας που επιτρέπει την κοινή χρήση δεδομένων μεταξύ διαφορετικών ζωνών (γεωγραφικά και από το νέφος μέχρι την άκρη) και επομένως την επεξεργασία τους σε οποιονδήποτε από τους κόμβους άκρων, τους μεσαίους κόμβους ή τους κόμβους του νέφους . Αυτό υλοποιείται από δύο από τις οντότητες της αρχιτεκτονικής SaT IoT—την οντότητα δυναμικής δρομολόγησης ροής δεδομένων IoT και την οντότητα διαχείρισης τοπολογίας. Μαζί, επιτρέπουν στο SAT IoT να διαχειρίζεται την τοπολογία του δικτύου κατά το χρόνο εκτέλεσης, ενώ παρέχουν επίσης τις απαραίτητες δυνατότητες παρακολούθησης για την κατανόηση του προτύπου χρήσης και των περιορισμών χωρητικότητας της υποδομής. Η οντότητα δυναμικής δρομολόγησης ροής δεδομένων IoT και η οντότητα διαχείρισης τοπολογίας ενισχύονται από την ενσωμάτωση του RECAP Application Optimiser στο SAT IoT, που εξάγουν την καλύτερη δυνατή τοποθέτηση της λογικής επεξεργασίας δεδομένων.

Στον πίνακα 1 συνοψίζουμε τα βασικά λειτουργικά χαρακτηριστικά που αντιμετωπίζονται σε κάθε Αρχιτεκτονική Αναφοράς IoT, δηλαδή διαλειτουργικότητα, επεκτασιμότητα, ασφάλεια και απόρρητο, διαχείριση δεδομένων, αναλυτικά στοιχεία, οπτικοποίηση δεδομένων και διεπαφή χρήστη και υποστηριζόμενα μοντέλα υπολογιστών.

Πίνακας 1. Σύνοψη των βασικών χαρακτηριστικών που παρατίθενται από διαφορετικές Αρχιτεκτονικές Αναφοράς IoT

Αρχιτεκτονικές αναφορές	IoT ARM	IEEE P2413	IIRA	WSO2 IRA	Intel SAS	Azure IRA	SAT-IoT
Διαλειτουργικότητα	X	X	X	X	X	X	X
Επεκτασιμότητα	X	X	X	X	X	X	X
Ασφάλεια και	X	X	X	X	X	X	X
Διαχείριση δεδομένων	X	X	X	X	X	X	X
Αναλύσεις	-	-	X	X	X	X	X
Οπτικοποίηση δεδομένων	-	-		X	X	X	X
Υποστηριζόμενο λογισμικό	IoT και cloud	IoT και cloud	IoT και cloud	IoT και cloud	IoT και cloud	IoT, edge και cloud	IoT, edge, fog

Με τον όρο διαλειτουργικότητα συστήματος, εννοούμε ότι η αρχιτεκτονική θα πρέπει να αφορά τη συνδεσιμότητα, τη διαχείριση δεδομένων και την αυτόματη ενσωμάτωση με διαφανή τρόπο για τον τελικό χρήστη. Η επεκτασιμότητα αναφέρεται στην ικανότητα της αρχιτεκτονικής να χειρίζεται τις αυξήσεις στον αριθμό των συσκευών IoT και των τελικών σημείων. Η ικανότητα ασφάλειας και απορρήτου διασφαλίζει ότι οι πληροφορίες βρίσκονται εκεί που πρέπει και αποτρέπει τη διαρροή δεδομένων σε μη εξουσιοδοτημένα άτομα. Η διαχείριση δεδομένων αναφέρεται τόσο στη διαχείριση

όσο και στην ανταλλαγή δεδομένων μεταξύ αρχιτεκτονικών στοιχείων. Το Analytics αναφέρεται στην ικανότητα της αρχιτεκτονικής να συλλαμβάνει χρήσιμα δεδομένα από τον κατακλυσμό δεδομένων που ταξιδεύει στο δίκτυο. Η οπτικοποίηση δεδομένων και η διεπαφή χρήστη σχετίζεται με το εάν η αρχιτεκτονική παρέχει ανθρώπινη διεπαφή. Τέλος, το υπολογιστικό παράδειγμα αναφέρεται στο εάν η αρχιτεκτονική απευθύνεται σε υποστήριξη για νέα υπολογιστικά παραδείγματα και συγκεκριμένα υπολογιστές νέφους, ομίχλης, ακμών και δρόσου [81].

1.2. Απαιτήσεις του IoT

1.2.1. Ενέργεια

Το Διαδίκτυο των Πραγμάτων με την άφιξή του έφερε μερικά ενδιαφέροντα θέματα προς αντιμετώπιση. Αυτά περιλαμβάνουν θέματα όπως η ασφάλεια, η εργονομία, η τεχνολογία επικοινωνιών, αλλά κυρίως ο εξοπλισμός χαμηλής κατανάλωσης. Οι συσκευές IoT συχνά τροφοδοτούνται από μπαταρία επειδή δεν έχουν άμεση πρόσβαση σε τροφοδοτικό. Αυτό συχνά προκαλείται από το ότι βρίσκεται σε μέρη όπου η πρόσβαση στο ηλεκτρικό δίκτυο απλά δεν είναι δυνατή [80].

Η εύρεση τρόπων για τη διασφάλιση της χαμηλής κατανάλωσης ενέργειας σίγουρα δεν ήρθε με το IoT. Πριν από πολύ καιρό είχαμε αριθμομηχανές, τηλεχειριστήρια, ψηφιακά παιχνίδια και φορητούς υπολογιστές ή κινητά τηλέφωνα. Όλες αυτές οι συσκευές τροφοδοτούνταν από μπαταρίες. Ωστόσο, οι συσκευές IoT αντιπροσωπεύουν ένα ειδικό σύνολο συσκευών όπου αναμένεται να μπορούν να λειτουργούν χωρίς παρέμβαση χρήστη για μήνες ή χρόνια. Και προτού η μπαταρία εξαντληθεί, θα σας ειδοποιήσουν εκ των προτέρων ότι η μπαταρία πρέπει να αντικατασταθεί. Οι ενεργειακά αυτόνομες συσκευές είναι τα θεμελιώδη στοιχεία του IoT.

Στην περίπτωση των συσκευών IoT δεν μπορούμε να αντέξουμε οικονομικά όπως στην περίπτωση των τυπικών συσκευών που τροφοδοτούνται από το ηλεκτρικό δίκτυο και έτσι - μετατρέποντας την περίσσεια ενέργειας σε θερμότητα. Με τον αυξανόμενο αριθμό φορητών συσκευών, νέες και νέες τεχνολογίες αναπτύσσονται για την αύξηση της χωρητικότητας της μπαταρίας. Ομοίως, αναπτύσσονται διαδικασίες για τη διασφάλιση χαμηλής κατανάλωσης ενέργειας. Υπάρχουν αρκετές από αυτές τις διαδικασίες, αλλά κατ 'αρχήν μπορούν να χωριστούν σε δύο βασικές ομάδες:

διαδικασίες για τη μείωση της κατανάλωσης κατά το σχεδιασμό λογισμικού και διαδικασίες για τη μείωση της κατανάλωσης κατά το σχεδιασμό υλικού [72]

Οι συσκευές IoT συχνά δεν απαιτούν για τη δραστηριότητά τους να τροφοδοτείται συνεχώς. Για παράδειγμα, κατά τη μέτρηση της θερμοκρασίας δωματίου, δεν είναι απαραίτητο η ανάγνωση του αισθητήρα θερμοκρασίας να πραγματοποιείται κάθε δευτερόλεπτο. Σε αυτή την περίπτωση αρκεί να γίνονται οι μετρήσεις κάθε λίγα λεπτά [82]. Μέχρι να λήξει αυτό το διάστημα, η συσκευή δεν κάνει τίποτα. Τίποτα, μπορεί να σημαίνει ότι η διαδικασία αναστέλλεται για μια απαραίτητη χρονική περίοδο καλώντας την delay (για παράδειγμα, την πρωτότυπη πλακέτα Arduino Uno). Αυτό μπορεί να φαίνεται ότι ο μικροελεγκτής δεν κάνει τίποτα, επειδή η λειτουργία καθυστέρησης παρεμποδίζεται, αλλά η συσκευή θα εξακολουθεί να καταναλώνει ενέργεια. Ωστόσο, εάν μπει σε κατάσταση αναστολής λειτουργίας για ένα απαιτούμενο χρονικό διάστημα, η κατανάλωση ενέργειας θα είναι ελάχιστη [61]

Είναι, φυσικά, δυνατό να μειωθεί η κατανάλωση ρεύματος επιλέγοντας τα κατάλληλα εξαρτήματα. Συχνά, μπορεί να είναι τα περιττά LED που σε σύγκριση με άλλες πηγές φωτός, έχουν χαμηλή ζήτηση, αλλά μπορούν να αποφορτίσουν αξιόπιστα και γρήγορα την παροχή ρεύματος όταν είναι συνεχώς αναμμένα. Στην περίπτωση των συσκευών IoT, το ενδιαφέρον είναι τα στοιχεία που διασφαλίζουν την επικοινωνία. Υπάρχουν τεχνολογίες που είναι απολύτως ακατάλληλες για αυτόν τον τύπο επικοινωνίας, ενώ άλλες έχουν σχεδιαστεί για τέτοιου είδους συσκευές [51]

Κατά τη σχεδίαση υλικού, είναι επίσης καλό να θυμάστε ότι η συνολική κατανάλωση επηρεάζει την κατανάλωση μεμονωμένων εξαρτημάτων. Ορισμένοι πιο απαιτητικοί αισθητήρες βραχυπρόθεσμα, απαιτούν πολύ υψηλό ρεύμα, παρόλο που κατά την κανονική λειτουργία, η κατανάλωσή τους είναι ελάχιστη. Μετά την αφύπνιση ή τη σύνδεση (π.χ. ορισμένες μονάδες επικοινωνίας), μπορούν επίσης να απαιτούν 2A σε σύντομο χρονικό διάστημα. Έτσι, η μπαταρία πρέπει να προετοιμαστεί ανάλογα με τα εξαρτήματα IoT της συσκευής ακόμη και σε ένα τόσο βραχυπρόθεσμο φορτίο [56].

1.2.2. Νοημοσύνη

Η ευφυΐα και η εξυπνάδα θεωρούνται η κορυφαία αξία του το Διαδίκτυο των Πραγμάτων (IoT) [12]. Ο κύριος λόγος σύνδεσης είναι ότι δίνουν τη δυνατότητα αυτοματισμού, ειδικά το είδος του αυτοματισμού που μοιάζει με νοημοσύνη. Υπάρχει

μια αναμενόμενη έξυπνη συμπεριφορά από συστήματα IoT ή εφαρμογές ακόμα κι αν οι συσκευές δεν είναι μόνιμα συνδεδεμένες.

Η φύση μιας τέτοιας νοημοσύνης είναι τόσο ποικίλη όσο και ο αριθμός των εφαρμογές στο IoT. Έτσι, παράγοντας έξυπνες λειτουργίες για το IoT απαιτεί καλή γνώση σε τομείς εφαρμογών, το εγκατάσταση του συστήματος και των εμπλεκόμενων συσκευών. Μια πρόταση πλαίσιο παρουσιάστηκε στο [13] για να αντιμετωπιστεί η αυξανόμενη πολυπλοκότητα της ανάπτυξης εφαρμογών νοημοσύνης εναλλακτικό για το IoT. Το πλαίσιο εισάγει μια αφαίρεση των υπηρεσιών πληροφοριών σε ένα επίπεδο πληροφοριών που εξυπηρετεί τις εφαρμογές που ζητούν πληροφορίες.

Η κύρια ιδέα είναι να αποσύνδεση της υλοποίησης των λειτουργιών νοημοσύνης από τον πραγματικό κωδικό εφαρμογής, δίνοντας έτσι τη δυνατότητα διατηρώντας την ανεξάρτητη Διαχείριση Κύκλου Ζωής (LCM) του καθενός έξυπνη λειτουργία σε μία συσκευή. Το πλαίσιο διερευνά το δυνατότητα παροχής υπηρεσιών πληροφοριών απευθείας σε α συσκευή. Αντίθετα, εστιάζονται οι εμπορικά διαθέσιμες προσεγγίσεις σχετικά με την παροχή διεπαφών προγραμματισμού εφαρμογών (API) για εφαρμογές για πρόσβαση σε έξυπνες υπηρεσίες από ένα δίκτυο cloud.

Οι έξυπνες εφαρμογές και έξυπνες υπηρεσίες χρησιμοποιούνται ως εναλλάξιμοι όροι σε πολλές περιπτώσεις, ωστόσο οι τελικοί τους στόχοι είναι διαφορετικοί και έντονα διακριτοί. Μια έξυπνη εφαρμογή χρησιμοποιεί μία ή περισσότερες έξυπνες υπηρεσίες που επιτρέπει να εκπληρώσει το καθήκον του, το οποίο σχετίζεται στενά με μια χρήση υπόθεση. Για παράδειγμα, μια εφαρμογή επεξεργασίας κειμένου μπορεί να χρησιμοποιήσει μια υπηρεσία αναγνώρισης φωνής για την εκπλήρωση του έργου της δημιουργίας έγγραφα για έναν χρήστη. Η έξυπνη υπηρεσία αναγνώρισης είναι η ψηφιοποίηση της προφορικής εισόδου φυσικής γλώσσας σε μορφή κατανοητή και χειραγωγείται από άλλο στοιχείο λογισμικού. Σε αυτό το παράδειγμα, το στοιχείο λογισμικού που χρησιμοποιεί την υπηρεσία αναγνώρισης ομιλίας την εφαρμογή επεξεργασίας κειμένου [83].

Πολλαπλές έξυπνες υπηρεσίες μπορούν να ενσωματωθούν και να εξυπηρετήσουν μία εφαρμογή. Μπορούν να χρησιμοποιήσουν την έξοδο ή μέρος της εξόδου του μία ή πολλές άλλες υπηρεσίες για την παραγωγή ενός νέου αποτελέσματος. Αυτό αναφέρεται ως σύνθεση υπηρεσίας. Η σύνθεση της υπηρεσίας μπορεί να ενσωματωθεί σε μεγάλο

βαθμό στον κώδικα υλοποίησης του εφαρμογή ή χαλαρά συζευγμένο με αρθρωτό τρόπο. Η έννοια των ευφυών υπηρεσιών είναι πιο εμφανής και ορατή όταν η αρχιτεκτονική των εφαρμογών είναι αρθρωτή. Η ανάπτυξη έξυπνων υπηρεσιών είναι διαφορετική από την ανάπτυξη παραδοσιακών εφαρμογών. Ο προγραμματισμός γλώσσες, τη διαδικασία ανάπτυξης, τα απαιτούμενα δεδομένα υποστήριξης και η υποστήριξη επιτάχυνσης διαφέρουν ανάλογα με τις απαιτήσεις τους και τελικό αποτέλεσμα. Εάν οι ευφυείς υπηρεσίες είναι άμεσα ενσωματωμένες στις εφαρμογές, όλοι αυτοί οι παράγοντες περιπλέκουν τον κύκλο ζωής διαχείριση των εφαρμογών και κάνει την εξέλιξή τους πιο δύσκολο [14].

Είναι δυνατό να βρείτε ευφυείς υπηρεσίες υψηλής αποσύνδεσης από εφαρμογές σε συγκεκριμένους τομείς όπως η αναγνώριση αντικειμένων [15]. Οι εφαρμογές χρησιμοποιούν REST API για πρόσβαση σε πόρους σε απομακρυσμένες τοποθεσίες. Οι απομακρυσμένοι πόροι επεξεργάζονται δεδομένα εισόδου από την εφαρμογή και απαντήστε με πληροφορίες που έχουν υποστεί επεξεργασία με τους ευφυείς αλγόριθμους τους σε μορφή κατανοητή από εφαρμογές που ακολουθούν τον ορισμό του API. Αν και υπάρχει κάποιου βαθμού αποσύνδεση των υπηρεσιών από την εφαρμογή, ο κύριος λόγος για τη διάλυση της υπηρεσίας βρίσκεται στην ανάγκη εκφόρτωσης υπολογιστικής επεξεργασίας και μείωσης του μετάδοση δεδομένων για εκπαιδευτικούς σκοπούς. Κατά συνέπεια, οι υπηρεσίες πληροφοριών εκτελούνται κυρίως σε απομακρυσμένους διακομιστές και όχι απευθείας στις συσκευές όπου εκτελούνται οι εφαρμογές [84].

Παράλληλα, τα δεδομένα που απαιτούνται για την εκπαίδευση των μοντέλων είναι συλλέγονται κεντρικά και με τη σειρά τους διευκολύνουν τη διαδικασία εκπαίδευσης των μοντέλων που χρησιμοποιούνται από τις ευφυείς υπηρεσίες [16].

Το IoT είναι ένα ετερογενές και ποικιλόμορφο περιβάλλον από άποψη τοπολογιών, πρωτοκόλλων, περιπτώσεων χρήσης, επιχειρηματικών διαδικασιών και αναπτυγμένες τεχνολογίες. Οι εφαρμογές που στοχεύουν στο IoT είναι επίσης ποικίλα και ποικίλα ως προς τον σκοπό, τις απαιτήσεις και χαρακτηριστικά επεξεργασίας. Οι εφαρμογές αντιμετωπίζουν παρόμοιες προκλήσεις και απαιτούν υψηλό βαθμό ευελιξίας και προσαρμοστικότητας. Σε ορισμένες περιπτώσεις, ο ευφυής οι υπηρεσίες μπορεί να χρειαστεί να εκτελεστούν σε σχετικά περιορισμένο περιβάλλοντα με περιορισμούς στη

μνήμη και την επεξεργαστική ισχύ ή η επεξεργασία τους εκφορτώνεται σε απομακρυσμένο περιβάλλον εκτέλεσης- όπως το cloud [85].

Η ενοποίηση ή η συγκέντρωση των δεδομένων ενδέχεται επίσης να περιορίσουν περαιτέρω τον τρόπο λειτουργίας των υπηρεσιών πληροφοριών που αντιμετωπίζονται, συμπεριλαμβανομένων των εισροών και των εξόδων τους. Υπάρχουν διάφορες πτυχές της διανομής πληροφοριών στην Κατανομή Τεχνητής Νοημοσύνης. Η νοημοσύνη (D-AI) περιλαμβάνει στην πράξη, ειδικά στο IoT. Καταρχήν, υπάρχει μια λειτουργική κατανομή νοημοσύνης. Οι έξυπνες υπηρεσίες μπορούν να αποσυντεθούν σε μικρότερα εξαρτήματα ή λειτουργίες με συνδυασμένες εξόδους που τροφοδοτούν μια άλλη λειτουργία - βασικά, μια αρθρωτή προσέγγιση νοημοσύνης κατανομή της υπηρεσίας πληροφοριών σε όλες τις ενότητες. Μια δεύτερη πτυχή του D-AI είναι η κατανομή εκτέλεσης συμπερασμάτων. Το συμπέρασμα της υπηρεσίας πληροφοριών μπορεί να εκτελεστεί σε διαφορετικούς τομείς σύμφωνα με τη διαθεσιμότητα, τις ανάγκες και τις απαιτήσεις της περίπτωσης χρήσης. Αυτή η πτυχή είναι ιδιαίτερα κρίσιμη στο IoT περίπτωση με την ετερογένεια των αναπτύξεών τους [86].

Οι τομείς κυμαίνονται από μονάδα επεξεργαστή ή εξειδικευμένο υλικό, έως α συσκευή, πύλη ή κόμβο άκρης ή ένα κεντρικό κέντρο δεδομένων. Ο τομέας εκτέλεσης των υπηρεσιών πληροφοριών μπορεί να προσαρμοστεί σύμφωνα με τις συνθήκες σε πραγματικό χρόνο που βιώνονται όταν απαιτείται η υπηρεσία. Η εκτέλεση συμπερασμάτων δεν πρέπει να συγχέεται με την κατανομή εκτέλεσης της εκπαίδευσης, ακόμη και όταν σχετίζονται με την πτυχή του ίδιου τομέα. Η εκπαίδευση του μοντέλα είναι, σε ορισμένες περιπτώσεις, μια πολύ εντατική CPU και μνήμη πεινασμένη διαδικασία.

Σε συνέπεια, η παραλληλοποίηση των διαδικασιών κατάρτισης είναι σήμερα μια κοινή πρακτική που χρησιμοποιείται για την παροχή μικρότεροι χρόνοι προπονήσεων και, σε ορισμένες περιπτώσεις, επίσης για την προστασία της ιδιωτικής ζωής λόγους [17]. Μια τέταρτη πτυχή είναι η παροχή μοντέλων ή λειτουργίες νοημοσύνης στα περιβάλλοντα εκτέλεσής τους (είτε για εκπαίδευση ή συμπέρασμα). Εν τω μεταξύ οι δύο προηγούμενες πτυχές επικεντρώνονται στην εκτέλεση, εστιάζει η πτυχή παροχής στο πώς να συσκευάσετε τη νοημοσύνη (σενάρια, μορφές ανταλλαγής, εικονικές μηχανές, κοντέινερ κ.λπ.) και αποκαλύπτουν τη λειτουργικότητα σε εφαρμογές που κάνουν χρήση των τοπικών πόρων, παρακάτω τοπικών και απομακρυσμένων πολιτικών και

ενεργοποίησης της νοημοσύνης διαχείριση του κύκλου ζωής των λειτουργιών. Μια τελευταία πτυχή που πρέπει να λάβετε υπόψη είναι η λειτουργική κατανομή του πράκτορα. Οι ορθολογικοί παράγοντες μπορεί να αλληλεπιδρούν μεταξύ τους ακολουθώντας το σκοπό τους σε ένα άτομο και απομονωμένη μόδα, αλλά μπορεί επίσης να ακολουθήσει συνεργατικές συμπεριφορές (για παράδειγμα σε ένα ιεραρχικό μοντέλο ή ένα μοντέλο σμήνος), ή ακόμα και ανταγωνιστικές προσεγγίσεις (αντίπαλα μοντέλα ή παιχνίδι Βελτιστοποιήσεις που βασίζονται στη θεωρία) [18]. Ο τρόπος πώς ο ευφυής πράκτορες, οι οποίοι μπορεί να κάνουν χρήση μιας ή περισσότερων πληροφοριών υπηρεσίες, η αλληλεπίδραση με άλλους ευφυείς πράκτορες είναι επίσης σχετική όταν εξετάζετε το D-AI για IoT [87].

1.2.3. Επικοινωνία

Οι συσκευές Internet of Things (IoT) επικοινωνούν με δεκάδες διαφορετικούς τρόπους, χρησιμοποιώντας εκατοντάδες διαφορετικά πρωτόκολλα. Αυτό συμβαίνει επειδή ο τρόπος επικοινωνίας τους εξαρτάται από το τι βρίσκονται, πού βρίσκονται, με ποιες άλλες συσκευές και συστήματα πρέπει να μιλήσουν και τι έχουν να πουν. Δεν υπάρχει κανένα καλύτερο πρωτόκολλο, το οποίο είναι ουσιαστικά η κοινή "γλώσσα" που χρησιμοποιείται για τη δρομολόγηση μηνυμάτων από μια συσκευή IoT σε άλλη. Η σωστή επιλογή εξαρτάται πάντα από τις συγκεκριμένες ανάγκες της εφαρμογής.

Υπάρχουν επίσης περιορισμοί που πρέπει να ληφθούν υπόψη. Ποιος είναι ο προϋπολογισμός ισχύος της συσκευής; Ποιοι είναι οι περιορισμοί κόστους; Ποιες είναι οι απαιτήσεις για φυσικό μέγεθος, ασφάλεια, χρόνο για την αγορά, γεωγραφικές περιοχές και απομακρυσμένη συντήρηση; Σε αυτό το άρθρο θα ρίξουμε μια ματιά στα ενσωματωμένα στοιχεία ενός συστήματος επικοινωνίας IoT και θα συζητήσουμε πώς διαφορετικές ανάγκες και περιβάλλοντα καθορίζουν την καλύτερη λύση για κάθε περίπτωση χρήσης [67]

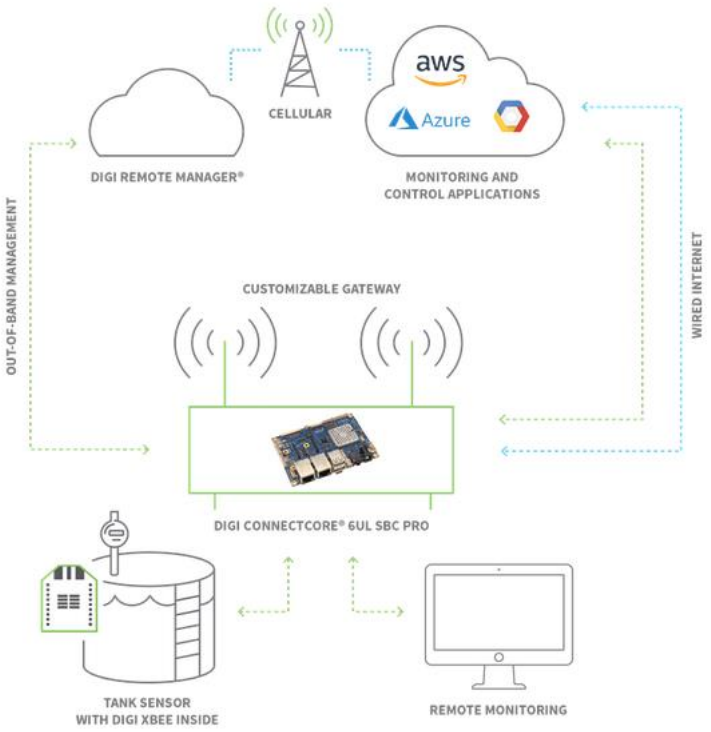
Ενώ τα συστήματα IoT διατίθενται σε πολλές διαφορετικές αρχιτεκτονικές, τα περισσότερα περιλαμβάνουν τα ακόλουθα στοιχεία:

- Συσκευή IoT – οτιδήποτε, από τον πιο μικροσκοπικό αισθητήρα θερμοκρασίας έως ένα γιγάντιο βιομηχανικό ρομπότ
- Τοπικές επικοινωνίες – η μέθοδος που χρησιμοποιεί η συσκευή για να μιλήσει με γειτονικές συσκευές

- Πρωτόκολλο εφαρμογής – το πλαίσιο που καθορίζει τον τρόπο μεταφοράς του περιεχομένου πληροφοριών
- Πύλες – μεταφράζουν και αναμεταδίδουν πληροφορίες, συνδέοντας συνήθως τα τοπικά δίκτυα συσκευών με το Διαδίκτυο
- Διακομιστές δικτύου – συστήματα που διαχειρίζονται την αποδοχή και τη μετάδοση δεδομένων IoT, που βρίσκονται συνήθως μέσα σε κέντρα δεδομένων cloud
- Εφαρμογές Cloud – επεξεργάζονται δεδομένα IoT σε χρήσιμες πληροφορίες, για παρουσίαση στους χρήστες
- Διεπαφή χρήστη – όπου οι άνθρωποι βλέπουν πληροφορίες IoT, τις χειρίζονται και εκδίδουν εντολές πίσω στις συσκευές IoT
- Συσκευές IoT

Όταν μιλάμε για συσκευές IoT, συνήθως περιγράφουμε πράγματα όπως περιβαλλοντικούς αισθητήρες, συνδεδεμένες συσκευές, ανιχνευτές οχημάτων ή ακόμα και μηχανές γραμμής συναρμολόγησης. Ενώ μια συσκευή IoT είναι αναμφισβήτητα οποιαδήποτε ηλεκτρονική συσκευή που μπορεί να επικοινωνήσει με το Διαδίκτυο, συνήθως δεν εννοούμε κινητά τηλέφωνα ή υπολογιστές γενικής χρήσης.

Συνήθως, εστιάζουμε σε συσκευές με στενότερο σκοπό, όπως τον έλεγχο των φώτων στο σπίτι σας ή την παρακολούθηση των επιπέδων της δεξαμενής για την κατασκευή χημικών. Για παράδειγμα, το ακόλουθο γραφικό δείχνει τη συνδεσιμότητα μεταξύ ενός αισθητήρα βιομηχανικής δεξαμενής που χρησιμοποιεί μια μονάδα ραδιοφώνου Digi XBee®, η οποία επικοινωνεί με μια πύλη που φιλοξενεί ένα σύστημα Digi ConnectCore® σε μονάδα (SOM) [59]



Σχήμα 8. Σύνδεση ασύρματων συσκευών[8]

Πολλές από αυτές τις συσκευές δεν δημιουργήθηκαν αρχικά με δυνατότητες Διαδικτύου και πρέπει να τροποποιηθούν με λύσεις μετά την αγορά για να συνδεθούν. Ωστόσο, οι δυνατότητες IoT σχεδιάζονται όλο και περισσότερο απευθείας σε νέες συσκευές, όπου μπορούν να μειώσουν σημαντικά το κόστος και να βελτιώσουν τη λειτουργικότητα. Ενώ οι συσκευές IoT ποικίλλουν ανάλογα με την ανάγκη που δημιουργήθηκαν για να καλύψουν, ορισμένα βασικά στοιχεία περιλαμβάνονται σχεδόν πάντα.

Για παράδειγμα, υπάρχει συνήθως ένας αισθητήρας για τον εντοπισμό φυσικών περιστατικών, όπως κίνηση ή διαρροή νερού. Μπορεί επίσης να υπάρχουν ενεργοποιητές που δημιουργούν φυσικές αλλαγές, όπως το άναμμα ενός φωτός ή το κλείσιμο μιας βαλβίδας. Αυτοί οι αισθητήρες και οι ενεργοποιητές συνδέονται με έναν ή περισσότερους μικροεπεξεργαστές που εκτελούν τη λογική που οδηγεί τη λειτουργικότητα του IoT. Ως συνδεδεμένη συσκευή, πρέπει να έχει τουλάχιστον ένα

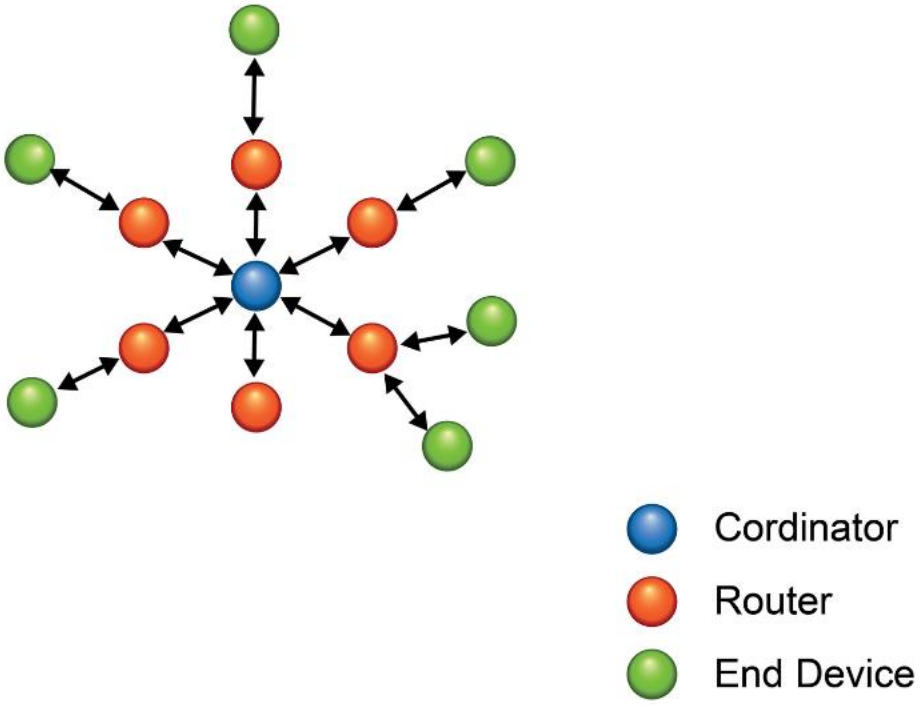
[8] http://users.sch.gr/jabatzo/files/yliko/live%20ebooks/diktya_ypolog_G_2018_final/_2.html

στοιχείο επικοινωνίας, είτε κάποιο τύπο ραδιοφώνου είτε μια ενσύρματη μέθοδο επικοινωνίας όπως το Ethernet [76]

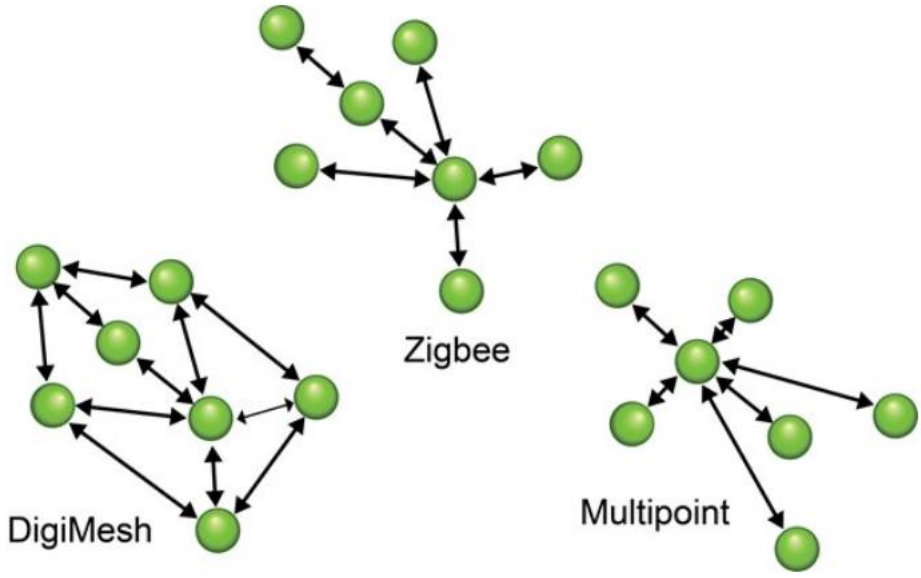
Οι συσκευές IoT λειτουργούν συχνά με μπαταρίες, καθιστώντας τη διαχείριση ενέργειας βασικό στοιχείο κατά την επιλογή εξοπλισμού, το σχεδιασμό λειτουργικότητας και τη δημιουργία στρατηγικών επικοινωνίας. Όλα αυτά τα εξαρτήματα θα στεγάζονται σε κάποιο τύπο περιβλήματος, συχνά αρκετά μικρό. Ανάλογα με το περιβάλλον, αυτό το περίβλημα μπορεί να χρειαστεί να σφραγιστεί και να στεγανοποιηθεί ή να εξαεριστεί πολύ για τη διαχείριση της θερμότητας [71]

Κάθε συσκευή IoT χρειάζεται να επικοινωνεί. Ορισμένες συσκευές στέλνουν μόνο πληροφορίες. πολλοί άλλοι στέλνουν και λαμβάνουν. Ενώ ορισμένες επικοινωνίες με ομότιμες συσκευές είναι άμεσες, οι απομακρυσμένες επικοινωνίες θα πρέπει συχνά να περάσουν από μια πύλη για να φτάσουν στον προορισμό τους. Ανεξάρτητα από το πού πρέπει να πάνε τα μηνύματα της συσκευής, κάθε ταξίδι ξεκινά με ένα πρώτο βήμα [78]

Το παρακάτω γράφημα απεικονίζει ένα μοντέλο για ασύρματες επικοινωνίες και πώς κάθε «κόμβος» στο ασύρματο δίκτυο παίζει έναν καθορισμένο ρόλο. Όπως μπορείτε να δείτε σε αυτό το παράδειγμα, το οποίο ονομάζεται "δίκτυο αστεριών", μια έξυπνη ασύρματη μονάδα συντονίζει τις επικοινωνίες σε συσκευές που λειτουργούν ως δρομολογητές και μεταφέρουν τις επικοινωνίες στις τελικές συσκευές.



Το σενάριο αλλάζει για διαφορετικούς συνδυασμούς ασύρματων συσκευών και πρωτοκόλλων. Στο παρακάτω διάγραμμα, μπορείτε να δείτε πώς μπορούν να κατασκευαστούν δίκτυα ώστε να συμπεριφέρονται με διάφορους τρόπους με τη χρήση διαφορετικών ασύρματων πρωτοκόλλων. Το καλύτερο πρωτόκολλο εξαρτάται από διάφορους παράγοντες, όπως η απόσταση μεταξύ των κόμβων επικοινωνίας στο δίκτυο.



Το πρώτο βήμα ή «hop» στην επικοινωνία IoT θα είναι είτε ενσύρματη είτε ασύρματη. Οι ενσύρματες συνδέσεις μπορεί να χρησιμοποιούν ένα απλό σειριακό πρωτόκολλο, αν και πιο συχνά θα χρησιμοποιηθεί ένα σύστημα δικτύωσης όπως το Ethernet, το οποίο επιτρέπει «άμεσες» συνδέσεις πρωτοκόλλου Διαδικτύου (TCP/IP) σε διακομιστή δικτύου ή εφαρμογή cloud. Τα μηνύματα που περνούν μέσω του Διαδικτύου δρομολογούνται μέσω πολλών διαφορετικών συσκευών, ωστόσο ως αρχιτέκτονες IoT, μπορούμε με ασφάλεια να αφαιρέσουμε αυτή τη διαδικασία. Οι ενσύρματες συνδέσεις είναι γρήγορες και αξιόπιστες, ωστόσο συχνά είναι πολύ δαπανηρό ή μη πρακτικό για την εκτέλεση φυσικής καλωδίωσης. Φυσικά για οτιδήποτε κινητό, καλώδια αποκλείονται [68]

Οι ασύρματες επικοινωνίες για το IoT γίνονται σχεδόν πάντα μέσω ραδιοφώνου και υπάρχουν εκατοντάδες πρωτόκολλα ραδιοφώνου εκεί έξω για να διαλέξετε. Αρκετά

είναι αρκετά δημοφιλή. Ακολουθεί μια επισκόπηση υψηλού επιπέδου ορισμένων δημοφιλών πρωτοκόλλων επικοινωνίας:

Ορισμένες συσκευές χρησιμοποιούν Wi-Fi, το οποίο έχει πολλά πλεονεκτήματα, εφόσον μπορούν να καλυφθούν οι απαιτήσεις ενέργειας και οι περίπλοκες ανάγκες επεξεργασίας και παροχής δεν δημιουργούν εμπόδια. Το Wi-Fi εκτελεί το TCP/IP εγγενώς, οπότε μόλις ρυθμιστεί, μπορούμε να αφαιρέσουμε την πολυπλοκότητα του ίδιου του Διαδικτύου.

Το Zigbee και το Z-wave είναι μεγάλα ονόματα στη δικτύωση οικιακού αυτοματισμού επειδή είναι βελτιστοποιημένα για επικοινωνίες χαμηλής κατανάλωσης και χαμηλού εύρους ζώνης και αμφότερα επιτρέπουν στις συσκευές στο σπίτι να συνομιλούν απευθείας μεταξύ τους για ταχύτητα και ασφάλεια. Κανένα από τα δύο δεν υποστηρίζει άμεσα πρωτόκολλο Διαδικτύου, επομένως οι επικοινωνίες εκτός της τοπικής περιοχής δρομολογούνται συνήθως μέσω μιας πύλης.
Το πρωτόκολλο LoRaWAN είναι ολοένα και πιο δημοφιλές και για IoT χαμηλού εύρους ζώνης. Συνδυάζει μεγάλη εμβέλεια με πολύ χαμηλό εύρος ζώνης, υποστηρίζοντας μίλια εύρους οπτικής επαφής για συσκευές που έχουν μόνο πολύ μικρά πράγματα να πουν [57]

Το Bluetooth και το BLE χαμηλής κατανάλωσης ενέργειας είναι εξαιρετικά δημοφιλή για απλές συσκευές IoT. Κανένας από τους δύο δεν μπορεί να επικοινωνήσει πολύ μακριά, επομένως μια άλλη συσκευή - συχνά ένα κινητό τηλέφωνο - θα χρησιμοποιηθεί για τη διευκόλυνση των μηνυμάτων μεγάλων αποστάσεων.
Τα κυψελωτά δίκτυα μπορούν πλέον να φιλοξενήσουν εύκολα συσκευές IoT. Νέα πρωτόκολλα κινητής τηλεφωνίας όπως το Cat-M και το NB-IoT επιτρέπουν στις συσκευές που λειτουργούν με μπαταρία να λειτουργούν για μήνες χωρίς επαναφόρτιση, στο εμπόριο για πολύ περιορισμένο εύρος ζώνης.
Άλλα πρωτόκολλα όπως το 4G LTE και το 5G απαιτούν πολύ περισσότερη ισχύ, αλλά μπορούν επίσης να χειριστούν μεγαλύτερα δεδομένα όπως το ψηφιακό βίντεο.
Υπάρχουν επίσης πολλά ιδιόκτητα πρωτόκολλα και πρωτόκολλα ενός κατασκευαστή ρυθμισμένα για μοναδικές ανάγκες απόστασης, ειδικές απαιτήσεις εύρους ζώνης, δύσκολα ραδιοφωνικά περιβάλλοντα και φυσικά βελτιστοποίηση κόστους. Δεν υπάρχει ένα πρωτόκολλο που να τα διέπει όλα. Κάθε έργο θα έχει τη δική του καλύτερη λύση [49]

Τα πλαίσια δικτύωσης υπολογιστών είναι συνήθως δομημένα σε εικονικά επίπεδα. Το χαμηλότερο επίπεδο ασχολείται με το φυσικό μέρος, τα καλώδια ή τα ραδιοκύματα. Ακολουθούν τα επίπεδα που συντονίζουν τον τρόπο σχηματισμού, διεύθυνσης, δρομολόγησης και επιβεβαίωσης των μηνυμάτων.

Πίνακας 2. Τα επίπεδα συντονισμού του τρόπου σχηματισμού, διεύθυνσης, δρομολόγησης και επιβεβαίωσης των μηνυμάτων.

Application Layer	This layer facilitates human-computer interactions and access to the network layer.
Presentation Layer	This layer performs data encryption and delivers data in a usable format.
Sessions Layer	The sessions layer manages ports and sessions, and maintains connections.
Transport Layer	This layer is responsible for transmitting data using protocols such as TCP/IP.
Network Layer	The network layer determines the data routing path.
Data Link Layer	The data link layer transmits data between network nodes.
Physical Layer	This layer facilitates human-computer interactions and access to the network layer.

Το υψηλότερο επίπεδο διαχειρίζεται το χρήσιμο περιεχόμενο, που συνήθως αναφέρεται ως "εφαρμογή, όπως φαίνεται στην εικόνα του "μοντέλου δικτύωσης OSI". Το OSI σημαίνει Open Systems Interconnection και το μοντέλο είναι ένα εννοιολογικό πλαίσιο που περιγράφει τα στοιχεία ή τα επίπεδα των λειτουργιών ενός δικτύου.

Το επίπεδο εφαρμογής είναι εκεί όπου γίνεται η πραγματική δουλειά του IoT και μπορεί να συμβεί με πολλούς διαφορετικούς τρόπους. Η ύπαρξη ενός τυπικού τρόπου επικοινωνίας για συγκεκριμένες εργασίες είναι απίστευτα χρήσιμη όταν συσκευές από πολλούς διαφορετικούς κατασκευαστές πρέπει να συνεργαστούν για να ολοκληρώσουν τη δουλειά τους. Ορισμένα ασύρματα πρωτόκολλα τυποποιούν την ανταλλαγή μηνυμάτων σχετικά με κοινές εργασίες όπως ο έλεγχος φωτισμού, η ασφάλεια ή η ροή ήχου.

Το Zigbee, το Bluetooth και το Z-Wave περιλαμβάνουν όλα πρωτόκολλα εφαρμογών που παρέχουν μια τυπική γλώσσα, έτσι ώστε, για παράδειγμα, ένας διακόπτης φώτων από μια εταιρεία να μπορεί να ανάβει τρεις διαφορετικούς λαμπτήρες που κατασκευάζονται από άλλες εταιρείες.

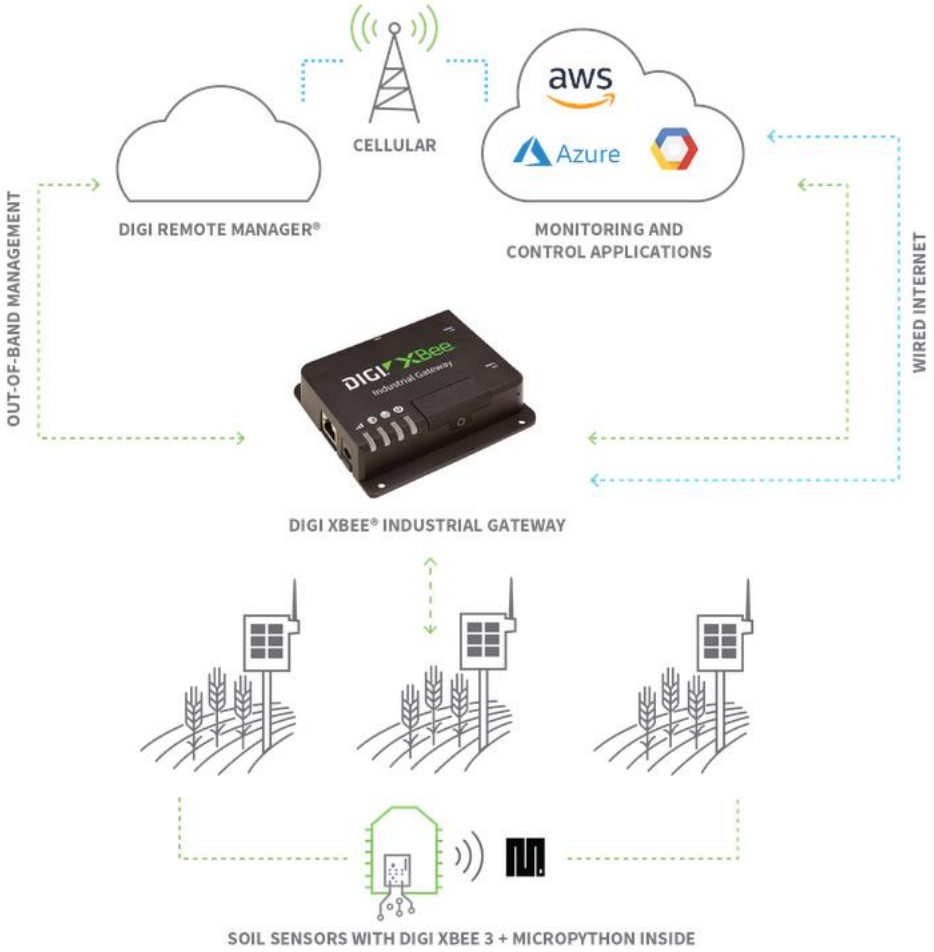
Άλλα πρωτόκολλα εφαρμογών είναι πιο γενικά. Το MQTT και το CoAP είναι και τα δύο πολύ ελαφριά πρωτόκολλα εφαρμογών που τυποποιούν τις επικοινωνίες μεταξύ διαφορετικών συσκευών χωρίς να περιορίζουν τα μηνύματα σε συγκεκριμένες εργασίες. Επειδή είναι ελαφριά, καταναλώνουν πολύ μικρό εύρος ζώνης και επομένως πολύ μικρή ισχύ, καθιστώντας τα ιδανικά για συσκευές που λειτουργούν με μπαταρία.

Οι συσκευές με μεγαλύτερη ισχύ και εύρος ζώνης ενδέχεται να χρησιμοποιούν RESTful επικοινωνίες μέσω HTTP — το πρωτόκολλο πίσω από τον ιστό. Αυτό το ευρέως εφαρμοσμένο πλαίσιο είναι επίσης αγνωστικό ως προς τις εργασίες, αλλά επειδή δεν σχεδιάστηκε με γνώμονα την εξαιρετική απόδοση, μπορεί γρήγορα να εξαντλήσει τόσο τις μπαταρίες όσο και το εύρος ζώνης μιας μικρής συσκευής IoT και θα πρέπει να εφαρμόζεται με προσοχή.

Όταν μια συσκευή δεν μπορεί να εκτελεί απευθείας το Πρωτόκολλο Διαδικτύου (TCP/IP), συνήθως περνά τα μηνύματά της σε μια άλλη συσκευή που ονομάζεται πύλη. Αυτή η πύλη θα επεξεργάζεται και θα προωθεί μηνύματα προς και από το Διαδίκτυο. Οι πύλες βοηθούν τις συσκευές IoT να παραμένουν μικρές, να λειτουργούν με μπαταρία και να είναι φθηνές, επειδή συνήθως χειρίζονται πολλές συσκευές ως τοπικό σταθμό βάσης. Για παράδειγμα, εδώ είναι μερικά σενάρια πραγματικής ζωής: Οι φορητές συσκευές που διαθέτουν Bluetooth/BLE συχνά χρησιμοποιούν ένα κινητό τηλέφωνο ως πύλη στο Διαδίκτυο. Αυτό λειτουργεί καλά εφόσον το τηλέφωνο και οι συσκευές βρίσκονται η μία κοντά στην άλλη. Τα πρωτόκολλα οικιακού αυτοματισμού όπως τα Zigbee, Z-Wave και LoRaWAN δεν μπορούν να χειριστούν απευθείας ένα κινητό τηλέφωνο, ούτε θα ήταν λογικό, καθώς τα κινητά τηλέφωνα δεν μένουν σε σταθερή τοποθεσία. Αυτά τα πρωτόκολλα, καθώς και τα ιδιόκτητα, χρησιμοποιούν συνήθως ένα κουτί πύλης συνδεδεμένο σε τροφοδοσία τοίχου και είτε Ethernet, Wi-Fi είτε κινητής τηλεφωνίας. Λαμβάνουν πληροφορίες από συσκευές που χρησιμοποιούν το εγγενές τους πρωτόκολλο, όπως το Zigbee, επεξεργάζονται ό,τι λαμβάνουν και, στη συνέχεια, τις διαβιβάζουν μέσω του Διαδικτύου [88].

Τα βιομηχανικά περιβάλλοντα, όπως τα ηλιακά πεδία και τα αιολικά πάρκα απαιτούν μια σκληρυμένη βιομηχανική πύλη για τη δρομολόγηση των επικοινωνιών από συσκευές που διανέμονται στο απομακρυσμένο δίκτυο συσκευών, όπως φαίνεται στο σχ. 8.

Αυτή η διαδικασία πύλης "multi-hop" επιτρέπει σε συσκευές με περιορισμένες δυνατότητες να συνδέονται με μακρινές τοποθεσίες, χρησιμοποιώντας συχνά μια ακολουθία διαφορετικών πρωτοκόλλων για να ολοκληρώσουν τη δουλειά. Οι πύλες χρησιμοποιούν γενικά πρωτόκολλα εφαρμογών όπως MQTT, REST ή CoAP για σύνδεση με διακομιστή δικτύου ή εφαρμογή cloud που συνήθως στεγάζεται σε κάποιο απομακρυσμένο κέντρο δεδομένων.



Σχήμα 9. Διάγραμμα δικτύου συσκευών IoT[9]

[9] https://pergamos.lib.uoa.gr/uoa/dl/frontend/file/lib/default/data/2866409/theFile

Οι περισσότερες επικοινωνίες IoT γίνονται αρχικά αποδεκτές και διαχειρίζονται από κάποιον τύπο διακομιστή δικτύου. Ορισμένα πρωτόκολλα το απαιτούν για την ολοκλήρωση εργασιών χαμηλού επιπέδου, όπως η αντιγραφή περιττών μηνυμάτων και η μετατροπή ειδικών μορφών πρωτοκόλλου. Ακόμη και όταν ένα πρωτόκολλο δεν απαιτεί πρόσθετη επεξεργασία, είναι απεριόριστα χρήσιμο να έχετε ένα σύστημα που όχι μόνο διαχειρίζεται τις επικοινωνίες, αλλά μπορεί να διαμορφώσει, να ασφαλίσει και να αναφέρει τις ίδιες τις συσκευές [89].

1.2.4. Ενσωμάτωση

Ένα έργο IoT απαιτεί μια σειρά εξοπλισμού με αισθητήρες, συνδεσιμότητα, επεξεργασία δεδομένων και διαχείριση δεδομένων μεταξύ των βασικών στοιχείων. Η ενσωμάτωση του συστήματος IoT είναι το καθήκον της συνένωσης αυτών των κομματιών για την αντιμετώπιση των περιπτώσεων χρήσης των πελατών και των απαιτήσεων της κάθετης αγοράς.

Η φύση της ολοκλήρωσης έχει αλλάξει με την πάροδο του χρόνου. Στις πρώτες μέρες της ανάπτυξης των επιχειρήσεων, τα συστήματα IoT με το κλειδί στο χέρι δεν υπήρχαν και η βαριά τεχνική ενσωμάτωση ήταν η σειρά της ημέρας. Σήμερα, τα προ-ενσωματωμένα κιτ εκκίνησης IoT, που ονομάζονται επίσης επιταχυντές, μπορούν να ξεκινήσουν τα έργα [90].

Ενώ οι πρωτοβουλίες IoT μπορεί να μην μοιάζουν πλέον με επιστημονικά έργα, οι τεχνολογίες παραμένουν ποικίλες. Ένας CIO δεν μπορεί να πάει σε έναν μόνο προμηθευτή και να περιμένει να αγοράσει ένα all-in-one σύστημα IoT. Η ενσωμάτωση παραμένει στο επίκεντρο. Αν μη τι άλλο, το εύρος της ολοκλήρωσης έχει αυξηθεί. Το στοιχείο επεξεργασίας δεδομένων του IoT εκτείνεται πλέον σε δημόσιες πλατφόρμες cloud και υπολογιστές αιχμής. Το Analytics και η τεχνητή νοημοσύνη έχουν γίνει επίσης κομμάτια του παζλ του IoT [53]

Ορισμένοι οργανισμοί διαθέτουν την εσωτερική τεχνογνωσία για να ολοκληρώσουν ένα έργο ενοποίησης IoT, αλλά πολλοί δεν το έχουν. Τα τμήματα πληροφορικής δεν δημιουργούν ένα σύστημα IoT κάθε μέρα, επομένως μπορεί να τους λείπουν οι κρίσιμες δεξιότητες, η εμπειρία και οι θεσμικές γνώσεις για να ολοκληρώσουν τη δουλειά τους. Οι CIO και οι διαχειριστές IT μπορούν να προσλάβουν μια εταιρεία ενοποίησης συστημάτων IoT τρίτου μέρους για να καλύψουν το κενό δεξιοτήτων με

γνώσεις που προέρχονται από την ολοκλήρωση έργων πολλών πελατών. Τέτοιες εταιρείες κυμαίνονται από τοπικούς ειδικούς έως μεγάλους, διεθνείς παρόχους υπηρεσιών. Στα παραδείγματα περιλαμβάνονται εταιρείες επαγγελματικών υπηρεσιών όπως η Accenture και η Deloitte. μεγάλους προμηθευτές πληροφορικής όπως η HPE και η IBM. και παγκόσμιες εταιρείες ενοποίησης συστημάτων όπως οι Cognizant, Insight, Tata Consultancy Services και Wipro [63]

Οι ολοκληρωτές συμβάλλουν περισσότερο από την τεχνική οξυδέρκεια. Φέρνουν επίσης σχέσεις με πολλούς παρόχους τεχνολογίας IoT, ένα σημαντικό στοιχείο σε έναν τομέα όπου καμία τεχνολογία δεν παρέχει τα αγαθά και η υποστήριξη των προμηθευτών είναι κρίσιμη για την πρόκληση της ολοκλήρωσης. Επιπλέον, οι πελάτες επιταχύνουν τα έργα τους όταν αποφεύγουν να συναρμολογήσουν τα δικά τους οικοσυστήματα IoT.

Τα έργα ενοποίησης συστημάτων IoT μπορεί να διαφέρουν δραματικά ανάλογα με το τι χρειάζονται οι οργανισμοί και τη θέση τους στην καμπύλη υιοθέτησης τεχνολογίας. Ένας οργανισμός που μόλις ξεκινάει το IoT, για παράδειγμα, μπορεί να διατηρήσει έναν ενοποιητή συστημάτων για να καθορίσει την περίπτωση χρήσης του και να ξεκινήσει ένα έργο απόδειξης ιδέας ή περιορισμένη ανάπτυξη [79].

Τα τμήματα πληροφορικής δεν δημιουργούν ένα σύστημα IoT κάθε μέρα, επομένως μπορεί να τους λείπουν οι κρίσιμες δεξιότητες, η εμπειρία και οι θεσμικές γνώσεις για να ολοκληρώσουν τη δουλειά τους. Οι οργανισμοί περαιτέρω μαζί με το IoT, από την άλλη πλευρά, μπορούν να χρησιμοποιήσουν έναν ολοκληρωτή για να κλιμακώσουν τις αρχικές τους αναπτύξεις σε ένα ευρύτερο εύρος, όπως από ένα μεμονωμένο κύτταρο παραγωγής σε πολλαπλές κυψέλες ή, ενδεχομένως, σε πολλαπλές εγκαταστάσεις. Οι ολοκληρωμένοι μπορούν επίσης να επεκτείνουν τις αναπτύξεις των πελατών με πρόσθετες περιπτώσεις χρήσης, όπως η ανάπτυξη της ανάπτυξης IoT ενός εστιατορίου από τη διαχείριση ενέργειας HVAC στην ασφάλεια των τροφίμων [44].

Η πολυπλοκότητα της ολοκλήρωσης συνήθως αυξάνεται με το εύρος του έργου. Η ενσωμάτωση με τα back-office συστήματα πληροφορικής καθίσταται απαραίτητη καθώς το IoT επεκτείνεται πέρα από το πιλοτικό στάδιο και περιλαμβάνει περισσότερες οργανωτικές λειτουργίες και τα υποκείμενα συστήματα πληροφορικής τους. Οι πληροφορίες που συλλέγονται από τα μηχανήματα στο πάτωμα του

εργοστασίου, για παράδειγμα, μπορεί να χρειαστεί να τροφοδοτηθούν σε ένα σύστημα ERP. Οι χρήστες του IoT μπορεί επίσης να χρειάζονται οργανωτική ενοποίηση. Οι CIO που συνδέουν περισσότερα μηχανήματα, συσκευές και άλλα περιουσιακά στοιχεία σε μια ανάπτυξη IoT θα βρεθούν σύντομα στη σφαίρα της επιχειρησιακής τεχνολογίας (OT). Η σύνδεση των ενδιαφερομένων μερών OT και IT αποκτά πρωταρχική σημασία σε αυτό το σημείο [91].

Η ενοποίηση του IoT ξεκινά συνήθως με συμβουλευτικές υπηρεσίες. Το πρώτο βήμα θα πρέπει να καθορίσει εάν το πρόβλημα ενός οργανισμού είναι κάτι που μπορεί πραγματικά να αντιμετωπίσει το IoT. Σε αυτό το σημείο, ο ολοκληρωμένος μπορεί επίσης να συμβουλεύσει τον πελάτη για άλλες τεχνολογίες που πρέπει να ενσωματωθούν, κάτι που θα μπορούσε να σημαίνει οτιδήποτε, από δικτύωση 5G έως σύγκλιση τεχνητής νοημοσύνης. Η φάση της διαβούλευσης θα πρέπει επίσης να αποτυπώσει την περίπτωση χρήσης ενός οργανισμού, ένα βασικό βήμα λαμβάνοντας υπόψη την πολλαπλότητα των πιθανών ρόλων IoT [55].

Οι περιπτώσεις χρήσης θα περιστρέφονται συχνά γύρω από την κάθετη αγορά ενός οργανισμού, γεγονός που καθιστά το υπόβαθρο του κλάδου ενός ολοκληρωμένου συστήματος ιδιαίτερα σημαντικό. Οι ολοκληρωτές εστιάζουν γενικά σε έναν αριθμό κάθετων αγορών ή υποτομέων κάθετων αγορών. Αυτή η επιχειρηματική γνώση επιτρέπει στον ενοποιητή να προσαρμόσει μια ανάπτυξη IoT για να καλύψει τις απαιτήσεις ενός πελάτη.

Με την αυξανόμενη ωρίμανση του IoT, οι CIO μπορούν γενικά να περιμένουν από τους ολοκληρωτές να παρέχουν κάποιο είδος κιτ εκκίνησης. Τέτοιες προσφορές μπορούν να ξεκινήσουν ένα έργο, αλλά μεγαλύτερες αναπτύξεις συνήθως απαιτούν υψηλότερο βαθμό προσαρμογής και ενοποίησης. Όσο μεγαλύτερη είναι η ανάπτυξη, τόσο μεγαλύτερη είναι η επίδραση στις λειτουργίες, στους υπαλλήλους και στους συνεργάτες μιας επιχείρησης. Οι ολοκληρωτές μπορούν επίσης να παρέχουν υπηρεσίες διαχείρισης οργανωτικών αλλαγών για να βοηθήσουν τους πελάτες να προσαρμοστούν στους νέους τρόπους επιχειρηματικής δραστηριότητας που προωθεί το IoT [92].

Οι CIO και οι διευθυντές IT που αξιολογούν τους ενοποιητές συστημάτων θα πρέπει να αναζητούν εταιρείες με ιστορικό επιτυχημένων αναπτύξεων IoT, τεχνογνωσία κάθετης αγοράς και συμβουλευτική προσέγγιση. Η ασφάλεια στον κυβερνοχώρο είναι

μια άλλη βασική απαίτηση, δεδομένης της συνεχώς διευρυνόμενης επιφάνειας επίθεσης που δημιουργούν οι συνδεδεμένες συσκευές. Ο ερευνητής αγοράς Statista προέβλεψε ότι ο πληθυσμός των συσκευών IoT θα φτάσει τα 30,9 δισεκατομμύρια το 2025, υπερδιπλασιάζοντας τα 13,8 δισεκατομμύρια συσκευές συνδεδεμένες με IoT που αναμένονται το 2024 [52]

Άλλα απαραίτητα χαρακτηριστικά εξαρτώνται από το επίπεδο υιοθέτησης του IoT από έναν οργανισμό. Ένας νεοεισερχόμενος στο IoT μπορεί να θέλει να αναζητήσει έναν ολοκληρωμένο με μια προκατασκευασμένη προσφορά IoT, ενώ ένας οργανισμός που δεσμεύεται για ανάπτυξη σε ολόκληρη την επιχείρηση μπορεί να δώσει μεγαλύτερη έμφαση στη διαχείριση αλλαγών [62]

Η γεωγραφική εμβέλεια ενός ενοποιητή θα αναδειχθεί ως κριτήριο επιλογής όταν τα σχέδια IoT απαιτούν εθνική ή διεθνή κάλυψη. Ένας άλλος παράγοντας που πρέπει να ληφθεί υπόψη είναι το βάθος του οικοσυστήματος IoT του ενοποιητή. Τα απαιτούμενα εξαρτήματα και τα σημεία ολοκλήρωσης θα πολλαπλασιαστούν σε συνδυασμό με τη φιλοδοξία του έργου IoT. Ένα μεγαλύτερο οικοσύστημα παρέχει περισσότερες επιλογές για τους διαχειριστές IT και διευκολύνει την προμήθεια και τις προμήθειες [93].

Οι δημόσιες πλατφόρμες cloud έχουν γίνει αναπόσπαστο μέρος των αναπτύξεων IoT, οι οποίες, μόλις πριν από λίγα χρόνια, ήταν σε μεγάλο βαθμό ως ιδιωτικά έργα εντός εγκαταστάσεων. Το cloud προσφέρει στους οργανισμούς έναν επεκτάσιμο πόρο για ανάλυση δεδομένων IoT. Τα δημόσια σύννεφα όπως το AWS, η Google Cloud Platform και το Microsoft Azure παρέχουν υπηρεσίες IoT. Οι CIO θα πρέπει να βεβαιωθούν ότι οι ενοποιητές έχουν δεξιότητες υπολογιστικού νέφους, είτε χρειάζονται βοήθεια για τη δημιουργία του cloud σε μια νέα ανάπτυξη είτε για τη μετεγκατάσταση ενός παλαιότερου συστήματος IoT στο cloud [63].

1.2.5. Αξιοπιστία

Δεδομένης της εκκολαπτόμενης φύσης αυτού του πεδίου, όπως περιγράφηκε προηγουμένως σε αυτήν την ενότητα, καθίσταται απαραίτητο να διατυπωθεί ένας ορισμός για το IoT. Ενώ η αξιοπιστία είναι ένα ώριμο πεδίο στους σχετικούς κλάδους της μηχανικής [25] και της μηχανικής λογισμικού [26] δεν υπάρχει συμφωνημένος ορισμός για το IoT. Ως εκ τούτου, καθίσταται απαραίτητο να αναθεωρηθούν οι βασικές

αρχές της αξιοπιστίας σε αυτούς τους άλλους τομείς. Οι δημοσιεύσεις με μεγάλη αναφορά και βασισμένες σε αυτές επιλέχθηκαν από τους κλάδους της μηχανικής, της βιοϊατρικής μηχανικής και της πληροφορικής, οι οποίες περιέγραφαν την πρακτική του ορισμού και της ποσοτικοποίησης της αξιοπιστίας. Από αυτές τις εργασίες, αναπτύσσεται στη συνέχεια ένας σαφής ορισμός της αξιοπιστίας. Αυτός ο βασικός ορισμός της αξιοπιστίας λαμβάνεται στη συνέχεια και εφαρμόζεται στο πλαίσιο του IoT. Αυτό διασφαλίζει ότι η εφαρμογή οποιουδήποτε ορισμού αξιοπιστίας είναι σταθερά θεμελιωμένη σε ακαδημαϊκά και επιστημονικά άρθρα με υψηλή αναφορά. Ο ορισμός της αξιοπιστίας του IoT επεκτείνεται στη συνέχεια περαιτέρω και εξετάζεται από άκρο σε άκρο, χρησιμοποιώντας τη βασική φυσική αρχιτεκτονική του IoT ως δομή για να συζητηθούν οι εφαρμογές της αξιοπιστίας στο IoT [93].

Με την αξιοπιστία να ορίζεται σταθερά με μια ευρύτερη έννοια, στη συνέχεια να περιορίζεται σε ένα συγκεκριμένο πεδίο εφαρμογής και ορισμό για το IoT, επιλέχθηκαν έργα για να καταδειχθεί η τρέχουσα κατάσταση της τέχνης στην εκτέλεση ανάλυσης αξιοπιστίας στο IoT. Η αξιοπιστία, σε θεμελιώδες επίπεδο, ασχολείται με τη μελέτη των αστοχιών [27] . Πιο συγκεκριμένα, ασχολείται με το πώς προκαλούνται οι αστοχίες, πώς μπορούν να αντιμετωπιστούν και πώς μπορούν να προληφθούν. Υπάρχουν πολλές παρανοήσεις σχετικά με το τι αντιπροσωπεύει στην πραγματικότητα η αξιοπιστία. Δεν είναι τόσο απλό όσο η δοκιμή και η εκ νέου δοκιμή μιας συσκευής μέχρι να επιτευχθεί σχετική ικανοποίηση. Η αξιοπιστία μπορεί να αναπαρασταθεί από έναν επίσημο ορισμό που περιλαμβάνει τέσσερις βασικές απαιτήσεις. Ο Fries (2006) ορίζει αυτές τις απαιτήσεις αξιοπιστίας δηλώνοντας ότι οι συσκευές πρέπει να είναι σε θέση να εκτελέστε μια απαιτούμενη λειτουργία, εκτελέστε χωρίς αποτυχία, εκτελέστε υπό καθορισμένες συνθήκες και λειτουργήστε για μια συγκεκριμένη χρονική περίοδο [27]. Επομένως, η προδιαγραφή για την αξιοπιστία απαιτεί να προσδιορίσουμε πλήρως τις αναμενόμενες συνθήκες χρήσης, τι συνιστά σωστή λειτουργία και τι συνιστά αστοχία [28]. Το υπόλοιπο αυτής της ενότητας θα καλύψει τους βασικούς τομείς για την καθιέρωση της μηχανικής αξιοπιστίας. Πρώτον, παρουσιάζεται ένας ορισμός για να απεικονιστεί η διαφορά μεταξύ δύο όρων που χρησιμοποιούνται συχνά. ποιότητα και αξιοπιστία. Στη συνέχεια, συζητούνται τα βασικά πρότυπα αποτυχίας και πώς επηρεάζουν τις νέες υπηρεσίες. Τέλος, παρουσιάζεται μια περιγραφή της αξιοπιστίας όπως ισχύει στον τομέα των υπολογιστών, παράλληλα με τις τυπικές μετρήσεις που χρησιμοποιούνται για την ποσοτικοποίηση της αξιοπιστίας στους υπολογιστές

Οι όροι «ποιότητα» και «αξιοπιστία» συχνά παρεξηγούνται. Μερικές φορές, αυτοί οι όροι χρησιμοποιούνται εναλλακτικά, ωστόσο, υπάρχουν σημαντικές διακρίσεις μεταξύ των δύο όρων. Και οι δύο όροι υπάρχουν για να περιγράψουν ένα χαρακτηριστικό ενός προϊόντος ή συστήματος. Ο Fries (2006) προσδιορίζει ότι η κύρια διαφορά μεταξύ αυτών των δύο όρων είναι η χρονική φύση της ποιότητας [27]. Ο όρος «ποιότητα», όπως ορίζεται στο ISO 9000 είναι η «ικανότητα να παρέχεις με συνέπεια προϊόντα και υπηρεσίες σύμφωνα με τις απαιτήσεις τους» [29].

Σε αυτόν τον ορισμό της ποιότητας, δεν προσδιορίζεται χρονική περίοδος για την οποία αυτές οι απαιτήσεις πρέπει να πληρούνται ή να συνεχίσουν να πληρούνται στο μέλλον. Επομένως, μια δοκιμή ποιότητας αντικατοπτρίζει μόνο ένα στιγμιότυπο μιας συγκεκριμένης στιγμής κατά την οποία οι απαιτήσεις ποιότητας είτε πληρούνται είτε δεν πληρούνται. Η αξιοπιστία, ωστόσο, αναφέρεται στην απόδοση ενός συστήματος ή ενός προϊόντος σε ένα συγκεκριμένο χρονικό διάστημα. Αυτή είναι μια σημαντική διάκριση μεταξύ των δύο όρων, ειδικά όταν πρόκειται για τη διασφάλιση συνεχούς επαρκούς απόδοσης μιας συσκευής ή συστήματος με την πάροδο του χρόνου. Ουσιαστικά, μπορούμε να αξιολογήσουμε την ποιότητα στο IoT, ωστόσο, αυτό δεν θα μας προσφέρει καμία διασφάλιση για τη συνεχή επιτυχή λειτουργία της ανάπτυξης.

Ένα προϊόν ή ένα σύστημα μπορεί να σχεδιαστεί και να κυκλοφορήσει με πολύ υψηλό επίπεδο ποιότητας, ωστόσο, αυτό δεν παρέχει καμία πληροφορία σχετικά με το πόσο συχνά αποτυγχάνει το προϊόν. Επιπλέον, δεν μπορούμε να χρησιμοποιήσουμε την ποιότητα για να εξακριβώσουμε την πιθανότητα το σύστημα ή το προϊόν να λειτουργεί χωρίς σφάλμα σε μια δεδομένη στιγμή. Τα ποσοτικά μέτρα αξιοπιστίας, από την άλλη πλευρά, μας επιτρέπουν να εξακριβώσουμε ζωτικής σημασίας πληροφορίες σχετικά με την ενημερωμένη επιχειρησιακή κατάσταση της ανάπτυξης του IoT. Αυτές οι πληροφορίες μπορούν να περιλαμβάνουν, πόσο συχνά αποτυγχάνει μια συσκευή, το μέσο διάστημα μεταξύ των βλαβών, τον μέσο χρόνο που απαιτείται για την επισκευή ενός στοιχείου και την πιθανότητα ότι ένα εξάρτημα θα χρειαστεί να αντικατασταθεί έως μια συγκεκριμένη ημερομηνία [94].

Υπάρχουν τρία κύρια πρότυπα αστοχίας που ορίζονται στον τομέα της μηχανικής αξιοπιστίας. βρεφική θνησιμότητα, σταθερό ποσοστό αποτυχίας και αποτυχία φθοράς [25]. Η βρεφική θνησιμότητα αναφέρεται σε αστοχίες που συμβαίνουν κυρίως νωρίς στον κύκλο ζωής ενός προϊόντος και σταδιακά εξουδετερώνονται με την πάροδο του

χρόνου. Μοτίβα αποτυχίας φθοράς παρατηρούνται όταν μια συσκευή αρχίζει να εμφανίζει εκθετικά μεγαλύτερο αριθμό σφαλμάτων σε σύγκριση με έναν σταθερά χαμηλό αριθμό σφαλμάτων στο παρελθόν. Αυτό το μοτίβο αστοχίας υποδεικνύει ότι μια συσκευή πλησιάζει στο τέλος της ωφέλιμης περιόδου ζωής της [27]. Το σταθερό ποσοστό αποτυχίας περιγράφει ένα μοτίβο όπου ο αριθμός των σφαλμάτων σε μια δεδομένη χρονική περίοδο παραμένει σταθερός. Για παράδειγμα, για να έχει μια συσκευή σταθερό ποσοστό αποτυχίας, θα περιμέναμε να εμφανίζεται ο ίδιος συνολικός αριθμός σφαλμάτων σε κάθε ημερολογιακό μήνα, αν και αυτά δεν χρειάζεται απαραίτητα να συμβαίνουν τις ίδιες ώρες κάθε μήνα.

Υπάρχουν πολλοί τρόποι αξιολόγησης της αξιοπδχιστίας στους υπολογιστές. Η καταλληλότερη μέθοδος μπορεί να εξαρτάται από τη φύση και τη λειτουργία του συστήματος που αξιολογείται. Η αξιοπιστία πρέπει να είναι ένα ποσοτικό μέτρο που αντιπροσωπεύει σε γενικές γραμμές την ικανότητα ενός συστήματος υπολογιστή να εκτελεί την προβλεπόμενη λειτουργία του [26]. Οι Xie et al. (2004) σκιαγραφούν διάφορες βασικές μετρήσεις που βοηθούν στον καθορισμό της αξιοπιστίας στους υπολογιστές. Ο μέσος χρόνος αποτυχίας (MTTF), στενά συνδεδεμένος με τον μέσο χρόνο μεταξύ βλαβών (MTBF) είναι η αναμενόμενη διάρκεια ζωής που το σύστημα θα λειτουργεί κανονικά πριν συμβεί μια αστοχία. Η συνάρτηση ποσοστού αστοχίας, γνωστή και ως συνάρτηση κινδύνου, είναι μια μέτρηση που βοηθά στον καθορισμό του ρυθμού γήρανσης του συστήματος. Το ποσοστό αποτυχίας είναι η πιθανότητα να αποτύχει μια συσκευή μέσα σε ένα καθορισμένο χρονικό διάστημα. Η συνάρτηση του ποσοστού αστοχίας όταν χρησιμοποιείται για την αξιολόγηση του υλικού αναμένεται να ακολουθεί μια εκθετική κατανομή, η οποία μας επιτρέπει έτσι να συλλογιστούμε για τη γήρανση και τη φθορά του υλικού. Όταν χρησιμοποιείται σε λογισμικό, ωστόσο, το ποσοστό αποτυχίας θα παραμείνει σταθερό επειδή το λογισμικό δεν γερνάει ούτε φθείρεται φυσικά.

Συντηρησιμότητα, σύμφωνα με τους Xie et al. (2004), είναι μια μέτρηση που αντιπροσωπεύει την πιθανότητα ότι ένα αποτυχημένο σύστημα μπορεί να επανέλθει σε κανονική λειτουργία μέσα σε μια δεδομένη χρονική περίοδο. Η διαθεσιμότητα είναι μια μέτρηση που αντιπροσωπεύει την πιθανότητα ένα σύστημα να λειτουργεί κανονικά σε μια δεδομένη χρονική περίοδο [26]. Η διαθεσιμότητα και η συντηρησιμότητα συνδέονται στενά, ωστόσο, διαφέρουν σε μία βασική πτυχή: η διαθεσιμότητα αφορά

τη χρονική περίοδο κατά την οποία ένα σύστημα αναμένεται να λειτουργεί κανονικά, ενώ η δυνατότητα συντήρησης αφορά τη χρονική περίοδο κατά την οποία προέκυψε ένα σφάλμα. Φυσικά, πέρα από αυτόν τον τεχνικό ορισμό, η δυνατότητα συντήρησης αφορά επίσης τη συνεχή και συνεχή λειτουργία ενός συστήματος - αυτό μπορεί να σχετίζεται με εργασίες όπως η ικανοποίηση νέων απαιτήσεων, ο κώδικας ανακατασκευής και αναδιάρθρωσης και άλλες εργασίες συντήρησης που συμβάλλουν στη μεγιστοποίηση της ωφέλιμης διάρκειας ζωής του ένα σύστημα.

Στο πλαίσιο της μελέτης της υπολογιστικής αξιοπιστίας, υπάρχουν τέσσερις βασικοί τομείς που έχουν διαφορετικές προσεγγίσεις για τον καθορισμό της αξιοπιστίας. υλικό, λογισμικό, δίκτυο και σύστημα [26]. Αυτές οι διαφορετικές περιοχές έχουν καθεμία μεθόδους ανάλυσης αξιοπιστίας που ταιριάζουν μοναδικά στις απαιτήσεις και τα ζητήματα της περιοχής. Η αξιοπιστία υλικού αφορά την αξιοπιστία με την πάροδο του χρόνου για τα φυσικά στοιχεία ενός συστήματος υπολογιστή, όπως η CPU, ο δίσκος και οι αισθητήρες. Αυτά τα εξαρτήματα είναι επιρρεπή στη φθορά, και επομένως θα περιμέναμε να μειωθεί η αξιοπιστία με την πάροδο του χρόνου για αυτά τα εξαρτήματα. Τα στοιχεία λογισμικού, από την άλλη, δεν θα πρέπει να υπόκεινται σε φυσική φθορά, επομένως δεν θα περιμέναμε να παρατηρήσουμε μείωση της αξιοπιστίας με την πάροδο του χρόνου [28]. Η αξιοπιστία δικτύου αφορά την απόδοση του δικτύου για μια δεδομένη χρονική περίοδο, η οποία καθορίζεται από ένα μείγμα υλικού και λογισμικού. Η αξιοπιστία συστημάτων είναι ένας συνδυασμός όλων των στοιχείων που συνδυάζονται και υπάρχουν εξειδικευμένες τεχνικές για την ανάλυση αυτού.

Οι μέθοδοι ποσοτικοποίησης της αξιοπιστίας στους υπολογιστές είναι καλά καθιερωμένες και κατανοητές, όπως παρουσιάζονται σε αυτήν την ενότητα. Με την έναρξη του νέου παραδείγματος IoT, ωστόσο, είναι σημαντικό να διατυπώσουμε μεθόδους ποσοτικοποίησης της αξιοπιστίας με επίκεντρο το IoT. Αυτές οι μέθοδοι πρέπει να ταιριάζουν με τη μοναδική φύση και τους περιορισμούς του IoT, που συζητείται στην επόμενη ενότητα. Τα τέσσερα επίπεδα της αρχιτεκτονικής του IoT. επίπεδο cloud, επίπεδο διαχείρισης υπηρεσιών, στρώμα ομίχλης και επίπεδο συσκευής.

Ο ορισμός για το IoT είναι θεμελιώδης για την κατανόηση του προβλήματος της αξιοπιστίας εντός του παραδείγματος. Ο ορισμός του IoT συχνά υποεκπροσωπείται και δεν ορίζεται σωστά [30]. Συχνά, το IoT ορίζεται χονδροειδώς ως το ότι μπορεί να προσθέσει συνδεσιμότητα στο Διαδίκτυο σε καθημερινές συσκευές, επιτρέποντας στην

πραγματικότητα «η τοστιέρα σας να μιλά στο ψυγείο σας». Αν και αυτή η δήλωση ισχύει για κάποιο μέρος του IoT, δεν περιλαμβάνει ολόκληρο το παράδειγμα του IoT. Ένα χρήσιμο σημείο εκκίνησης για τον ορισμό του παραδείγματος IoT είναι η εξέταση των βασικών στοιχείων του IoT. Αυτά τα εξαρτήματα είναι? αίσθηση, ενεργοποίηση, επικοινωνία, υπηρεσίες και εφαρμογές [31]. Αυτά τα τέσσερα στοιχεία μπορούν στη συνέχεια να αντιστοιχιστούν σε μια αρχιτεκτονική για το IoT. Η ανίχνευση και η ενεργοποίηση εκτελούνται στο χαμηλότερο επίπεδο της αρχιτεκτονικής, που αναφέρεται επίσης ως επίπεδο συσκευής. Το επόμενο επίπεδο επάνω, το επίπεδο ακμής, επιτρέπει την επικοινωνία μεταξύ των συσκευών και του επιπέδου εφαρμογής. Τυπικά, αυτή η επικοινωνία ενεργοποιείται από ημι-δυνατές συσκευές που συμπεριφέρονται ως διανομείς, συλλέγουν δεδομένα από τους αισθητήρες και τα αναμεταδίδουν στο νέφος και στέλνουν εντολές στους ενεργοποιητές όπως απαιτείται.

Έχοντας κατά νου τα βασικά στοιχεία του IoT, μπορούμε τώρα να διαμορφώσουμε έναν πλήρη ορισμό του IoT, το οποίο είναι ένα παράδειγμα που επιτρέπει τη διασύνδεση σε οτιδήποτε και τα πάντα για τη δημιουργία υποδομής παρακολούθησης και ελέγχου που μπορεί να χρησιμοποιηθεί σε εφαρμογές για τον εμπλουτισμό της καθημερινής εμπειρίας χρήστη [31].

Από την άποψη της συσκευής, δηλαδή των αισθητήρων και των ενεργοποιητών, το πρώτο πρόβλημα που μπορούμε να παρατηρήσουμε είναι η εξαιρετικά περιορισμένη φύση αυτών των συσκευών [32]. Αυτοί οι περιορισμοί αφορούν την μπαταρία, τη μνήμη και την υπολογιστική χωρητικότητα [33]. Η μπαταρία προκαλεί ανησυχία για τις εφαρμογές IoT, επειδή συχνά το επίπεδο εφαρμογής δεν γνωρίζει την εναπομείνασα μπαταρία στη συσκευή, καθιστώντας έτσι δύσκολο τον προσδιορισμό πότε η συσκευή χρειάζεται αντικατάσταση μπαταρίας [34]. Αυτή η ανησυχία για τη διάρκεια ζωής της μπαταρίας επιδεινώνεται ακόμη περισσότερο όταν λάβουμε υπόψη ότι οι συσκευές ενδέχεται να βρίσκονται σε μέρη που είναι φυσικά δύσκολο ή επικίνδυνο να αντικατασταθούν. Οι περιορισμοί μνήμης και CPU στις συσκευές περιορίζουν την ικανότητα της συσκευής να αποθηκεύει πολύπλοκες μεθόδους κρυπτογράφησης, πράγμα που σημαίνει ότι οι συσκευές IoT πρέπει να βασίζονται σε ελαφριά κρυπτογράφηση για την προστασία των δεδομένων που μεταδίδονται από τη συσκευή [35].

Ένα άλλο ζήτημα εξελίσσεται από την περιορισμένη φύση των συσκευών όταν πρόκειται για την ενημέρωση του περιορισμένου υλικολογισμικού αυτών των αισθητήρων χαμηλής κατανάλωσης. Δεν είναι πρακτικό, λόγω της έλλειψης ισχύος και των επιπτώσεων στη διάρκεια ζωής της μπαταρίας για τη συσκευή, να συνδέεστε σε μια υπηρεσία cloud τακτικά και να ελέγχετε εάν χρειάζεται λήψη και εγκατάσταση νέου υλικολογισμικού στη συσκευή [36]. Αυτό οδηγεί σε ένα σενάριο όπου οι συσκευές θα μπορούσαν ενδεχομένως να λειτουργούν με ξεπερασμένο υλικολογισμικό, αφήνοντάς τες έτσι ευάλωτες σε παραβιάσεις ασφάλειας.

Οι αισθητήρες και οι ενεργοποιητές που χρησιμοποιούνται στο IoT συχνά αναπτύσσονται σε απομακρυσμένες και απομακρυσμένες τοποθεσίες και συχνά υπόκεινται σε σκληρές περιβαλλοντικές συνθήκες όπως θερμότητα, θερμοκρασίες παγώματος, μηχανική φθορά, κραδασμούς και υγρασία [31]. Σε αυτήν την αναφορά, υπάρχει ανάγκη να προσδιοριστεί η περίοδος «ωφέλιμης ζωής» μιας συσκευής, ώστε να μπορούμε να προσδιορίσουμε πότε η συσκευή πρέπει να αποσυρθεί. Αυτή η ωφέλιμη ζωή θα μειωθεί εάν η συσκευή χρησιμοποιείται σε σκληρό περιβάλλον, επομένως, θα μπορούσαμε να περιμένουμε να δούμε μεγάλες αποκλίσεις στη διάρκεια ζωής της συσκευής για πανομοιότυπες συσκευές που αναπτύσσονται σε διαφορετικά περιβάλλοντα, γεγονός που έχει ως αποτέλεσμα τη δυσκολία διαχείρισης της αξιοπιστίας του συστήματος.

Μια άλλη πτυχή που αφορά την αξιοπιστία της συσκευής στο IoT, είναι η τάση των αισθητήρων να «αποτυχαίνουν-βρώμικα» [37]. Αυτό το φαινόμενο αφορά ένα σενάριο όπου ένας αισθητήρας συνεχίζει να στέλνει λανθασμένες μετρήσεις αφού έχει υποστεί βλάβη. Αυτό είναι ένα πολύ γνωστό, αλλά ελάχιστα κατανοητό, πρόβλημα που είναι διάχυτο σε περιβάλλοντα IoT. Συγκεκριμένα, αυτό το ζήτημα είναι δύσκολο να διαγνωστεί επειδή ο αισθητήρας φαίνεται να λειτουργεί κανονικά. Ο αντίκτυπος μιας λανθασμένης ανάγνωσης που αποστέλλεται σε περιβάλλον IoT μπορεί να είναι κρίσιμος, όταν λάβουμε υπόψη ότι η ενεργοποίηση έχει συχνά φυσικές επιπτώσεις στις ανθρώπινες ζωές.

Η κινητικότητα είναι μία από τις βασικές προσδοκίες ενός δικτύου IoT όπου οι χρήστες του δικτύου μπορούν να μετακινούνται δυναμικά μεταξύ των εφαρμογών, ενώ η ενσωμάτωση και η αναγνώριση της συσκευής γίνονται απρόσκοπτα στο παρασκήνιο [38]. Η παγκόσμια διευθυνσιοδότηση, ωστόσο, είναι μια δυσκολία στο IoT, δεδομένου

ότι οι κατασκευαστές δεν συντονίζονται για να παρέχουν παγκοσμίως μοναδικά αναγνωριστικά για όλες τις συσκευές IoT [39]. Αυτό σημαίνει ότι η ευθύνη της εκχώρησης μοναδικής αναγνώρισης ανήκει στο ίδιο το δίκτυο IoT. Όταν θεωρούμε ότι οι συσκευές IoT αναμένεται να είναι κινητές, αυτό δημιουργεί πρόβλημα δεδομένου ότι το αναγνωριστικό συσκευής μπορεί να διαφέρει σε διαφορετικά δίκτυα, πράγμα που σημαίνει ότι μπορεί να χάσουμε την ιχνηλασιμότητα της συσκευής. Αυτό στη συνέχεια εισάγει μια ανησυχία για την αξιοπιστία όταν πρόκειται για παρακολούθηση ή έλεγχο της συσκευής καθώς κινείται μέσω διαφορετικών εφαρμογών IoT.

Το Πρωτόκολλο Διαδικτύου (IP) είναι το σημερινό de-facto πρότυπο για επικοινωνία και αναγνώριση σε παραδοσιακά δίκτυα. Η IP στην τρέχουσα κατάστασή της, ωστόσο, δεν είναι κατάλληλη για το IoT [40]. Η εισαγωγή νέων πρωτοκόλλων σε αυτόν τον χώρο προβλημάτων θα απαιτήσει αυτά τα νέα πρωτόκολλα να ωριμάσουν γρήγορα, κάτι που δεν είναι πάντα εύκολο. Αυτό το πρόβλημα επιδεινώνεται περαιτέρω όταν εξετάζουμε τις συνέπειες της μοναδικής αντιμετώπισης. Το IPv4 έχει μια διεύθυνση μήκους 32 bit, η οποία δημιουργεί χώρο για 4,3 δισεκατομμύρια διευθύνσεις, λαμβάνοντας υπόψη τις προβλέψεις 50 δισεκατομμυρίων συσκευών που συζητήθηκαν προηγουμένως σε αυτό το έγγραφο, γίνεται σαφές ότι το IPv4 δεν είναι κατάλληλο για να εκπληρώσει το όραμα του IoT. Αυτό το πρόβλημα επιδεινώνεται περαιτέρω από το γεγονός ότι το IPv4 εξαντλήθηκε από διευθύνσεις το 2010 [41]. Ως εκ τούτου, καθίσταται απαραίτητο να εφαρμοστεί ένα πρωτόκολλο με κατάλληλο χώρο διευθύνσεων, όπως το IPv6, το οποίο διαθέτει χώρο διευθύνσεων 128 bit, αφήνοντας χώρο για 3,4×1038 διευθύνσεις. Αυτός ο νέος χώρος διευθύνσεων, ωστόσο, δημιουργεί προβλήματα για περιορισμένες συσκευές, οι οποίες δεν είναι όλες ικανές να χειριστούν τα γενικά έξοδα που απαιτούνται για τη διεύθυνση [40].

Μια λύση σε αυτό το μεγάλο κόστος διεύθυνσης προσφέρεται από το πρωτόκολλο 6LoWPAN [42]. Το 6LoWPAN είναι σε θέση να συμπιέζει το μέγεθος της κεφαλίδας των πακέτων IPv6 προκειμένου να τα καταστήσει συμβατά με το πρότυπο IEEE 802.15.4 [40] και επομένως να ταιριάζουν καλύτερα στο IoT. Αυτά τα νέα και αναδυόμενα πρότυπα για την αντιμετώπιση των νέων απαιτήσεων του IoT συμβάλλουν στη δημιουργία ενός τοπίου διαφορετικών προτύπων και πρωτοκόλλων μεταξύ συσκευών IoT και αναπτύξεων που στοχεύουν στην επικοινωνία για περιορισμένες συσκευές σε δίκτυα IoT. Δεδομένου του ελαφρού και περιορισμένου χαρακτήρα

ορισμένων από αυτά τα πρωτόκολλα, δεν διαθέτουν όλα εγγυήσεις ποιότητας υπηρεσίας (QoS), πράγμα που σημαίνει ότι η αξιοπιστία της σύνδεσης δικτύου γίνεται πιο δύσκολο να αξιολογηθεί.

Οι Karkouch et al. (2016) αναφέρουν στη μελέτη τους ότι λόγω των σπάνιων πόρων και της διακοπτόμενης επικοινωνίας, το δίκτυο είναι πιθανό να σταματήσει τις αναγνώσεις ή να παράγει αναξιόπιστες αναγνώσεις[42]. Αυτή η αντίληψη ότι οι αναγνώσεις μπορούν να διαγραφούν λόγω της εγγενούς φύσης των δικτύων IoT προκαλεί ανησυχία, ειδικά δεδομένου ότι η υποδομή IoT είναι συχνά υπεύθυνη για τη διαχείριση κρίσιμων για την αποστολή εφαρμογών [43].

Το επίπεδο εφαρμογής του παραδείγματος IoT δεν υπόκειται στους ίδιους περιορισμούς είτε του δικτύου είτε του επιπέδου συσκευής της αρχιτεκτονικής. Είναι σημαντικό να σημειωθεί ότι σε πολλές περιπτώσεις η αξιοπιστία του επιπέδου εφαρμογής είναι συνάρτηση του πόσο αξιόπιστα είναι τα κατώτερα στρώματα της αρχιτεκτονικής. Εάν αποστέλλονται ανώμαλα δεδομένα από τη συσκευή μέσω του δικτύου στο επίπεδο εφαρμογής, αυτό θα μειώσει την αξιοπιστία της εφαρμογής. Από αυτή την άποψη, είναι σημαντικό το επίπεδο εφαρμογής να διαθέτει επαρκείς τεχνικές ανίχνευσης ανωμαλιών για την εξάλειψη των σφαλμάτων και τη διατήρηση της αξιοπιστίας της εφαρμογής. Δεδομένου ότι τα δίκτυα IoT διαθέτουν μια ετερογενή σειρά περιορισμένων συσκευών που μεταδίδουν πολλές πληροφορίες σε διαφορετικές μορφές, αυτό το έργο μπορεί να είναι δύσκολο [44].

Ενώ το επίπεδο εφαρμογής δεν υποφέρει από τους φυσικούς περιορισμούς του επιπέδου της συσκευής, εξακολουθεί να υπάρχει ανάγκη διαχείρισης της αξιοπιστίας των εφαρμογών που αναπτύσσονται. Μια μελέτη παρατήρησε τον αντίκτυπο των ανώμαλων δεδομένων στην ταξινόμηση στην εφαρμογή IoT της αναγνώρισης ανθρώπινης δραστηριότητας διαπίστωσε ότι ορισμένοι ταξινομητές ήταν πολύ πιο ευάλωτοι σε σφάλματα από άλλους και ότι η μέθοδος προετοιμασίας των δεδομένων μπορεί επίσης να καταστήσει την εφαρμογή πιο ευάλωτη σε αποτυχία . Έχοντας αυτό κατά νου, οι προγραμματιστές πρέπει να καταβάλουν συνειδητή προσπάθεια να εδραιώσουν και να κατανοήσουν την αξιοπιστία των εφαρμογών που φιλοξενούνται στην υποδομή IoT, προκειμένου να αποφευχθεί η είσοδος κρίσιμων σφαλμάτων στο σύστημα [45].

Τα ζητήματα αξιοπιστίας στα τρία επίπεδα της αρχιτεκτονικής στο IoT συνδυάζονται για να δημιουργήσουν ένα ευάλωτο τοπίο για το IoT, το οποίο συχνά οδηγεί σε ανώμαλα δεδομένα που παράγονται και αποστέλλονται μέσω του δικτύου. Αυτή η ιδέα καταδεικνύει την έντονη ανάγκη για αποτελεσματικά, ποσοτικοποιήσιμα μέτρα αξιοπιστίας που θα μας επιτρέψουν να συλλογιστούμε σχετικά με την καταλληλότητα για τους σκοπούς των συστημάτων μας IoT. Το ζήτημα των ανώμαλων δεδομένων είναι εξαιρετικά προβληματικό για το όραμα του IoT, δεδομένου ότι θα γίνουν ενεργοποιήσεις με βάση αυτά τα δεδομένα που θα μπορούσαν, στις πιο σοβαρές περιπτώσεις, να απειλήσουν ανθρώπινες ζωές [43]. Ως εκ τούτου, είναι σημαντικό κάθε πλαίσιο που στοχεύει στην αξιολόγηση και ποσοτικοποίηση της αξιοπιστίας στο IoT πρέπει να μπορεί να ανιχνεύει την παρουσία ανωμαλιών στο σύστημα. Μόλις ποσοτικοποιηθεί η αξιοπιστία, αυτό ανοίγει μια νέα ευκαιρία για περαιτέρω ενίσχυση της στιβαρότητας του συστήματος τοποθετώντας έναν άνθρωπο στο βρόχο (HITL). Το HITL είναι ένα ουσιαστικό συστατικό για το μέλλον της αξιοπιστίας στο IoT και αναγνωρίστηκε ως βασικός τομέας μελλοντικής έρευνας του Stankovic (2014) [46]. Το παράδειγμα HITL ανοίγει ευκαιρίες για τον εντοπισμό και την επίλυση ζητημάτων αξιοπιστίας σε κρίσιμες υποδομές IoT. Η χρήση ενός ανθρώπινου παρατηρητή φέρνει ένα στοιχείο ειδικών γνώσεων τομέα στην εφαρμογή, το οποίο επιτρέπει στον άνθρωπο να συνθέσει πληροφορίες που παρουσιάζονται από το σύστημα με τις δικές του ειδικές γνώσεις για να καταλήξει σε τεκμηριωμένο συμπέρασμα σχετικά με την αξιοπιστία του συστήματος.

Επιπλέον, οι άνθρωποι επιτρέπουν την αξιολόγηση της αλήθειας του εδάφους, όπως μια πραγματική τιμή θερμοκρασίας, η οποία μπορεί να βοηθήσει στην επαλήθευση μιας μηχανής ανάγνωσης. Αυτή η ιδέα είναι σχετικά νέα στην έρευνα του IoT και, μέχρι σήμερα, καμία μελέτη αξιοπιστίας δεν έχει επιλέξει τη χρήση μιας μεθόδου HITL για να βοηθήσει στην αξιολόγηση της αξιοπιστίας σε συνδυασμό με κλασικά μοντέλα αξιοπιστίας. Αυτός ο νέος συνδυασμός θα ήταν ένα βήμα προς μια νέα και αποτελεσματική λύση. Το ευάλωτο τοπίο που καταλαμβάνει το IoT παρουσιάζει μια σαφή απαίτηση για την ερευνητική κοινότητα να σχεδιάσει και να εφαρμόσει πλαίσια και λύσεις που θα μπορούσαν να βοηθήσουν στην αξιολόγηση και την κατανόηση της αξιοπιστίας της βασικής μας υποδομής IoT.

Ο ορισμός της αξιοπιστίας, όπως συζητήθηκε στις προηγούμενες ενότητες, έχει ένα ισχυρό στοιχείο ποσοτικοποίησης που σχετίζεται με αυτόν. Αξιοπιστία, δεν είναι μια υποκειμενική επιστήμη, και ως εκ τούτου οι μηχανισμοί που στοχεύουν στην αξιολόγηση της αξιοπιστίας θα πρέπει να είναι αντικειμενικοί και ποσοτικοποιήσιμοι στη φύση τους. Υπάρχει επίσης μεγάλη έμφαση στην αξιοπιστία στον καθορισμό και τη χρήση μετρήσεων για την αξιολόγηση της αξιοπιστίας εξαρτημάτων και συστημάτων. Έρευνα στον τομέα της αξιοπιστίας του IoT έχει διεξαχθεί για την ενίσχυση της αξιοπιστίας σε διάφορα επίπεδα της αρχιτεκτονικής του IoT. Αυτή η ενότητα συνοψίζει τη διαθέσιμη έρευνα στους τομείς της αξιοπιστίας συσκευών, της ποιότητας δεδομένων, της αξιοπιστίας δικτύου και της ανίχνευσης ανωμαλιών, οι οποίες αντιπροσωπεύουν βασικούς τομείς για τη βελτίωση της αξιοπιστίας του IoT.

Αρκετοί συγγραφείς που ερευνούν την αξιοπιστία συσκευών IoT ενσωμάτωσαν κλασικές μετρήσεις αξιοπιστίας σε λύσεις με επίκεντρο το IoT. Η αξιοπιστία, το ποσοστό αποτυχίας, η διαθεσιμότητα και το MTTR ποσοτικοποιήθηκαν από τους Zin et al. [47]. Η εργασία πρότεινε ένα πιθανολογικό μοντέλο για τη μέτρηση της αξιοπιστίας σε συνδεδεμένες συσκευές IoT που θέτει ότι οι δομές αστοχίας των συσκευών IoT τηρούν μια ορισμένη κατανομή πιθανοτήτων. Οι συγγραφείς ορίζουν το μέτρο αξιοπιστίας R(t) ως την πιθανότητα η συσκευή να λειτουργεί σωστά στο χρονικό διάστημα [0, t]. Αυτή η πιθανολογική συνάρτηση επιτρέπει την εκτίμηση του αναμενόμενου χρόνου μέχρι την αποτυχία, της διαθεσιμότητας και της αξιοπιστίας για μια δεδομένη συσκευή IoT. Εν τω μεταξύ, οι Μαυρογιώργου κ.ά. (2018), συμπεριέλαβαν στη δουλειά τους μετρήσεις Μέσος Χρόνος για Επισκευή (MTTR), MTTF, MTBF και διαθεσιμότητας, οι οποίες πρότειναν έναν μηχανισμό για την καταγραφή της αξιοπιστίας των ετερογενών συσκευών IoT. Αυτός ο μηχανισμός εξέταζε τόσο γνωστούς όσο και άγνωστους τύπους συσκευών και προσπάθησε να διαφοροποιήσει ποιες συσκευές ήταν αξιόπιστες και ποιες όχι, με στόχο τη συλλογή δεδομένων από τις αξιόπιστες και την απόρριψη δεδομένων από αναξιόπιστες συσκευές. Ο μηχανισμός αποτελούνταν από τέσσερα στάδια: αναγνώριση συσκευών, ταξινόμηση προδιαγραφών, εκτίμηση αξιοπιστίας και επικύρωση αξιοπιστίας. Χρησιμοποιώντας αυτόν τον μηχανισμό, οι συγγραφείς μπόρεσαν να δημιουργήσουν μια κατάταξη των συνδεδεμένων συσκευών γυμναστικής με βάση τα αποτελέσματα αξιοπιστίας τους από γνωστές μετρήσεις αξιοπιστίας. Τέλος, ο Kim (2016) χρησιμοποίησε την αξιοπιστία, το ποσοστό αποτυχίας και την ανάκτηση στη μελέτη

του, η οποία πρότεινε ένα σταθμισμένο μοντέλο για την ποσοτικοποίηση της αξιοπιστίας στο IoT. Το μοντέλο αποτελούνταν από τέσσερα κριτήρια ποιότητας. λειτουργικότητα, αξιοπιστία, αποτελεσματικότητα και φορητότητα. Οι μετρήσεις ορίστηκαν μέσα σε αυτά τα κριτήρια στα οποία εκχωρήθηκαν βάρη, έτσι ώστε το μοντέλο να μπορεί να παρέχει μια συνολική βαθμολογία για την ποιότητα της εφαρμογής IoT. Το μοντέλο στη συνέχεια αξιολογήθηκε σε ένα εικονικό περιβάλλον και παρήχθησαν βαθμολογίες για κάθε μία από τις μετρήσεις. Αυτό το μοντέλο παρέχει στάθμιση, ωστόσο, κάθε κριτήριο σταθμίστηκε ομοιόμορφα σε αυτό το πείραμα. Αυτές οι κλασικές μετρήσεις παρέχουν ένα χρήσιμο σημείο εκκίνησης για την ποσοτικοποίηση της αξιοπιστίας του IoT, αλλά δεν έχουν ακόμη ωριμάσει σε ικανότητες και δεν μπορούν να επιβεβαιώσουν την αξιοπιστία σε όλα τα επίπεδα της αρχιτεκτονικής του IoT.

Πέρα από το να μπορούμε να συλλογιστούμε για την καταλληλότητα των συσκευών μας IoT, πρέπει επίσης να είμαστε σε θέση να πιστοποιήσουμε την αξιοπιστία της υποδομής δικτύου που αποτελεί τη ραχοκοκαλιά της επικοινωνίας IoT. Σε γενικές γραμμές, υπάρχουν δύο μορφές μελετών αξιοπιστίας δικτύου που συζητούνται σε αυτήν την ενότητα. μελέτες για τη βελτίωση της QoS σε δίκτυα και μελέτες που στοχεύουν στον ποσοτικό προσδιορισμό μετρήσεων αξιοπιστίας για δίκτυα. Αυτή η ενότητα παρουσιάζει την τρέχουσα έρευνα αιχμής στην αξιοπιστία των δικτύων IoT.

Μια νέα μέτρηση QoS δικτύου IoT προτάθηκε από τους Maalel et al. (2013) στην εργασία τους, η οποία σχεδίασε ένα ελαφρύ και ενεργειακά αποδοτικό πρωτόκολλο δρομολόγησης για τη βελτίωση και τη μέτρηση της αξιοπιστίας σε εφαρμογές IoT, ειδικά σε εφαρμογές έκτακτης ανάγκης. Οι εφαρμογές έκτακτης ανάγκης στο IoT απαιτούν ταχεία απόκριση για συναγερμούς που έχουν σημάνει. Η εργασία πρότεινε έναν μηχανισμό που ονομάζεται AJIA (Adaptive Joint Protocol based on Implicit ACK) για απώλεια πακέτων και αξιολόγηση ποιότητας διαδρομής. Ο μηχανισμός βασίζεται στη φύση εκπομπής του πρωτοκόλλου, όπου τα μηνύματα μεταδίδονται σε όλους τους κοντινούς κόμβους. Οι κοντινοί κόμβοι μπορούν επομένως να «ακούν» το μήνυμα που αποστέλλεται. Αυτή η λειτουργία ακρόασης χρησιμοποιείται αντί για τα παραδοσιακά μηνύματα ACK για να διασφαλιστεί η αξιοπιστία του μηνύματος που αποστέλλεται. Στη συνέχεια, οι σύνδεσμοι μεταξύ των κόμβων αξιολογούνται με μια μέτρηση που ονομάζεται Δείκτης Ποιότητας Συνδέσμου (LQI), η οποία χρησιμοποιεί

το ιστορικό απώλειας πακέτων στη σύνδεση για να προσδιορίσει την αξιοπιστία αυτής της συγκεκριμένης διαδρομής. Άλλες μετρήσεις QoS, όπως η απόδοση καθυστέρησης και η απώλεια πακέτων, ποσοτικοποιήθηκαν από τον Kamyod (2018). Αυτή η εργασία χρησιμοποίησε τα Optimized Network Engineering Tools (OPNET) της Riverbed για να παρατηρήσει αυτές τις παραμέτρους αξιοπιστίας δικτύου σε ένα έξυπνο σενάριο γεωργίας. Αυτές οι παράμετροι παρακολουθήθηκαν έτσι ώστε να μπορούν να παρέχουν κάποιες πληροφορίες σχετικά με το πόσο αξιόπιστο ήταν το συνολικό σύστημα IoT από άκρο σε άκρο. Η μελέτη διαπίστωσε ότι η αύξηση του αριθμού των κόμβων στο δίκτυο είχε μεγαλύτερες καθυστερήσεις πακέτων και σημαντικά μεγαλύτερους χρόνους μετάδοσης και απώλεια πακέτων. Οι Brogi και Forti (2017) πρότειναν ένα γενικό μοντέλο για μια υποδομή IoT με επίγνωση του QoS, με βάση το παράδειγμα υπολογισμού ομίχλης. Το μοντέλο επιτρέπει στις εφαρμογές IoT να δημιουργούν προφίλ QoS προκειμένου να ζητούν ορισμένα χαρακτηριστικά QoS από τα πράγματα με τα οποία αλληλεπιδρά. Κάθε σύνδεσμος επικοινωνίας στο σύστημα IoT έχει ένα συσχετισμένο προφίλ QoS, το οποίο επιτρέπει στο μοντέλο να προσδιορίζει τον πιθανό λανθάνοντα χρόνο και το εύρος ζώνης για μια εφαρμογή για επικοινωνία πραγμάτων. Το μοντέλο λαμβάνει υπόψη μόνο την καθυστέρηση και το εύρος ζώνης, το οποίο είναι ένα περιορισμένο υποσύνολο χαρακτηριστικών QoS που δεν θα αντιπροσωπεύει πλήρως την αξιοπιστία του δικτύου σε μια δεδομένη χρονική στιγμή.

Περαιτέρω μετρήσεις QoS δικτύων IoT, ενσωματωμένες σε ένα πλαίσιο διαχείρισης, εξετάστηκαν σε μια μελέτη από τον Al-Masri (2018), η οποία παρουσίασε ένα πλαίσιο διαχείρισης QoS μικροϋπηρεσιών (mQoSM) για χρήση στο Industrial IoT (IIoT), το οποίο έχει επίγνωση του QoS ενδιάμεσο λογισμικό που παρακολουθεί τη συμπεριφορά των μικροϋπηρεσιών προκειμένου να προσδιορίσει την «καλύτερη» μικρουπηρεσία μεταξύ όλων των μικρουπηρεσιών που ανακαλύφθηκαν. Αυτές οι πληροφορίες μπορούν στη συνέχεια να χρησιμοποιηθούν από αρχιτέκτονες IoT για να αποφασίσουν εάν επιθυμούν να ενσωματώσουν τη μικρουπηρεσία. Αυτό το πλαίσιο παρακολουθεί τις ακόλουθες παραμέτρους. χρόνος απόκρισης, απόδοση, διαθεσιμότητα, αξιοπιστία και κόστος. Το μοντέλο παρουσιάζει ένα χρήσιμο βήμα προς τη δημιουργία μιας συνειδητοποίησης της κατάστασης του συστήματος IoT όσον αφορά την αξιοπιστία και την απόδοση, ωστόσο, δεν έχει κλιμακωθεί πέρα από τις μικροϋπηρεσίες σε περιβάλλον IoT.

Μια προσέγγιση μοντελοποίησης αξιοπιστίας χρησιμοποιώντας Γενικευμένο Στοχαστικό Δίκτυο Petri (GSPN) προτάθηκε από τους Li και Huang (2017). Αυτή η προσέγγιση θεώρησε τα μαθηματικά μοντέλα σε κόμβους ακμών για να παρέχουν στατιστικά στοιχεία σχετικά με την απόδοση των συσκευών IoT. Οι μετρήσεις που υπολογίστηκαν ήταν η κατανάλωση χρόνου, ο χρόνος απόκρισης, το ποσοστό αστοχίας και οι χρόνοι επισκευής. Αυτές οι μετρήσεις μιλούν μόνο για την απόδοση του επιπέδου από τη συσκευή σε άκρη και προσφέρουν μια πολύ περιορισμένη άποψη της απόδοσης του δικτύου, η οποία δεν παρουσιάζει μια ολιστική άποψη της αξιοπιστίας του IoT. Ένα μοντέλο πλεονασμού πύλης προτάθηκε από τους Sinche et al. (2018). Αυτή η εργασία έκανε χρήση του πλεονασμού τόσο σε επίπεδο ISP (Internet Service Provider) όσο και σε επίπεδο Gateway (κόμβος άκρης). Αυτό το μοντέλο δοκίμασε τρεις περιπτώσεις, μια υποδομή IoT χωρίς πλεονασμό, ένα IoT με πλεονασμό πύλης και ένα IoT με πλεονασμό πύλης και ISP και πύλης. Το μοντέλο δοκιμάστηκε χρησιμοποιώντας μια φυσική κλίνη δοκιμής IoT, όπου οι συσκευές επικοινωνούσαν χρησιμοποιώντας το πρωτόκολλο διαύλου I2C. Ως μέτρηση απόδοσης χρησιμοποιήθηκε RTT (χρόνος ταξιδιού επιστροφής) για τον προσδιορισμό της αποτελεσματικότητας του μοντέλου. Τα αποτελέσματα που φαίνονται στη μελέτη διαπίστωσαν ότι το μοντέλο που δεν χρησιμοποίησε την προσέγγιση πλεονασμού είδε το RTT να αυξάνεται κατά 14% σε συνθήκες σφάλματος, ενώ τα μοντέλα πλεονασμού είχαν ως αποτέλεσμα μόνο 1% αύξηση του RTT. Αυτή η μελέτη εξετάζει την αξιοπιστία μόνο σε επίπεδο δικτύου και cloud. Επομένως, δεν λαμβάνει υπόψη την αξιοπιστία των φυσικών συσκευών ή την τάση τους να αποτυγχάνουν σε οποιαδήποτε δεδομένη στιγμή. Αυτή η μελέτη επίσης δεν εξετάζει την ετερογενή φύση των πρωτοκόλλων επικοινωνίας IoT. Ο Alam (2018) παρουσίασε ένα πλαίσιο για τη διαχείριση ζητημάτων αξιοπιστίας στο IoT με βάση το TCP (Transmission Control Protocol). Υπάρχουν τρία στοιχεία στο πλαίσιο. τον υπολογιστή αξιοπιστίας, τον ελεγκτή αξιοπιστίας και τον χειριστή αξιοπιστίας. Το πλαίσιο χρησιμοποιεί καθυστέρηση για να προσδιορίσει την κατάσταση αστοχίας του συστήματος IoT. Εάν παρατηρηθούν υψηλά επίπεδα καθυστέρησης από την αριθμομηχανή αξιοπιστίας, ο ελεγκτής αξιοπιστίας θα επιχειρήσει αναμετάδοση και ο χειριστής αξιοπιστίας θα ξεκινήσει μια λειτουργία μετάδοσης και θα εισέλθει σε κατάσταση εξοικονόμησης ενέργειας. Αυτό το πλαίσιο ασχολείται μόνο με τη μέτρηση καθυστέρησης QoS στο IoT, επομένως δεν μπορεί να αντιπροσωπεύει την πλήρη κατάσταση αξιοπιστίας στο δίκτυο.

Η έρευνα που παρουσιάζεται σε αυτή την ενότητα δείχνει ότι ενώ έχουν γίνει κάποιες προσπάθειες για να ενισχυθεί η αξιοπιστία στα δίκτυα IoT, τόσο με την ενίσχυση της QoS του δικτύου όσο και με την παρακολούθηση και ποσοτικοποίηση της αξιοπιστίας του δικτύου, δεν υπάρχει επί του παρόντος μια ερευνητική προσέγγιση που να συνδυάζει με επιτυχία την αξιοπιστία συσκευών και δικτύου σε ένα πλαίσιο.

Ορισμένες έρευνες έχουν επίσης διεξαχθεί για την αξιολόγηση της αξιοπιστίας του IoT σε επίπεδο συστήματος. Αυτές οι προσεγγίσεις βρίσκονται σε υψηλό επίπεδο και δεν αποτυπώνουν τις μεμονωμένες λεπτομέρειες για αξιοπιστία, όπως ποιες συσκευές είναι υπεύθυνες για βλάβες ή ποια μέρη του δικτύου ευθύνονται για προβλήματα κυκλοφορίας [98].

Οι Behera et al. (2015) πρότειναν μια μέθοδο μοντελοποίησης της αξιοπιστίας σε ένα IoT προσανατολισμένο στις υπηρεσίες. Συγκεκριμένα, προτάθηκαν αλγόριθμοι για την αξιολόγηση της αξιοπιστίας σε ένα Κεντρικό Ετερογενές Σύστημα Υπηρεσιών IoT (CHISS). Οι συγγραφείς πρότειναν ότι η αξιοπιστία θα μπορούσε να μετρηθεί με μοντελοποίηση της διαθεσιμότητας του προγράμματος για την εκτέλεση της υπηρεσίας, της διαθεσιμότητας εισόδου που απαιτείται για την εκτέλεση της υπηρεσίας και της αξιοπιστίας υπηρεσίας των υποσυστημάτων που σχετίζονται με το σύστημα. Οι αλγόριθμοι δοκιμάστηκαν σε μια μελέτη περίπτωσης ενός συστήματος συναγερμού πυρκαγιάς, το οποίο λειτουργούσε υπό κανονική λειτουργία εκείνη τη στιγμή. Οι αλγόριθμοι ήταν σε θέση να προσδιορίσουν εάν το πρόγραμμα και το αρχείο ήταν διαθέσιμα για κάθε στοιχείο στο σύστημα IoT. Ωστόσο, αυτή η μεθοδολογία δεν εξέτασε την ιδέα ότι τα στοιχεία του IoT θα μπορούσαν να αποτύχουν ανά πάσα στιγμή και να αρχίσουν να στέλνουν ανώμαλα δεδομένα ή ότι το δίκτυο θα μπορούσε να πέσει θύμα μιας εξαπλούμενης απειλής ή ιού. Προκειμένου να παρουσιαστεί μια αληθινή αντανάκλαση της αξιοπιστίας, είναι απαραίτητο να υπάρχει ένας μηχανισμός που να μπορεί να ειδοποιεί τον χρήστη για αστοχίες στο σύστημα πριν πραγματοποιηθούν κρίσιμες ενεργοποιήσεις [99].

Οι Kharchenko et al. (2017) πρότεινε τη χρήση ενός μοντέλου Markov για την πρόβλεψη των απαιτήσεων αξιοπιστίας ενός συστήματος IoT. Το μοντέλο Markov θεώρησε ότι η εφαρμογή θα μπορούσε να είναι σε ένα εύρος 15 καταστάσεων, από κανονική κατάσταση έως πλήρη αποτυχία. Η πιθανοτική φύση του μοντέλου Markov

διευκολύνει την πρόβλεψη ότι το σύστημα θα μετακινηθεί από τη μια κατάσταση στην άλλη και μπορεί να καθορίσει την πιθανότητα αποτυχίας σε μια δεδομένη χρονική στιγμή. Αυτό το μοντέλο λαμβάνει υπόψη μόνο τις καταστάσεις που καθορίζονται στη σχεδίαση του μοντέλου και δεν είναι ικανό να αντιδράσει σε νέες καταστάσεις που δεν ελήφθησαν υπόψη στο σχεδιασμό του μοντέλου.

Με την ευάλωτη κατάσταση των δικτύων IoT, δεδομένων των περιορισμένων συσκευών τους και της εξαιρετικά φορητής φύσης τους, είναι σημαντικό κάθε πλαίσιο που σκοπεύει να ποσοτικοποιήσει την αξιοπιστία μιας υποδομής IoT πρέπει να έχει γνώση της πιθανής παρουσίας ανώμαλων δεδομένων στις εφαρμογές του. Αυτά τα ανώμαλα δεδομένα θα μπορούσαν να έχουν σοβαρές συνέπειες εάν αφεθούν αδιάγνωστα για να σταλούν στο επίπεδο εφαρμογής και να χρησιμοποιηθούν σε κρίσιμες καταστάσεις ενεργοποίησης. Αυτή η ενότητα παρουσιάζει την τρέχουσα έρευνα για τον εντοπισμό ανωμαλιών του IoT. Η ανίχνευση ανωμαλιών ειδικά για το IoT είναι ένας δύσκολος τομέας, επειδή οι λύσεις πρέπει να είναι ελαφριές και ικανές να χειρίζονται το ετερογενές φάσμα των συσκευών IoT.

Οι Stiawan et al. (2017) πρότεινε μια τεχνική για την έγκαιρη ανίχνευση ανωμαλιών χρησιμοποιώντας ανάλυση κίνησης δικτύου. Αυτή η τεχνική χρησιμοποίησε το SNMP (Simple Network Mapping Protocol) για τη συλλογή επισκεψιμότητας από μια ετερογενή σειρά συσκευών IoT. Αυτή η κίνηση στη συνέχεια απεικονίστηκε σε γραφήματα για περαιτέρω αναλύσεις. Στη συνέχεια, τα κατώφλια θα μπορούσαν να οριστούν με βάση τη χρήση της CPU και της μνήμης, η οποία μπορεί να καθορίσει την παρουσία μιας ανώμαλης επικοινωνίας στο δίκτυο. Αυτή η προσέγγιση είναι ελαφριά και κατάλληλη για το IoT, ωστόσο, η λύση δεν περιλαμβάνει μέθοδο για τον αυτόματο ή στατιστικό προσδιορισμό ενός ορίου για αστοχίες, οι οποίες θα μπορούσαν να δημιουργήσουν μεγάλο όγκο ψευδών συναγερμών [100].

Χρήσιμη αποδείχθηκε μια ενεργειακά αποδοτική τεχνική ανίχνευσης ανωμαλιών που εξυπηρετεί συσκευές IoT χαμηλών πόρων. Η τεχνική χρησιμοποιεί μια μεθοδολογία θεωρητικής παιγνίων προκειμένου να επιτευχθεί η βέλτιστη ενεργειακή απόδοση συνδυάζοντας δύο γνωστές τεχνικές για την ανίχνευση εισβολών στο IoT. ανίχνευση με βάση την υπογραφή και ανίχνευση ανωμαλιών. Το στοιχείο ανίχνευσης ανωμαλίας μαθαίνει τη δραστηριότητα και δημιουργεί έναν κανόνα ταξινόμησης, ο οποίος στη

συνέχεια περνά στο στοιχείο ανίχνευσης υπογραφής, έτσι ώστε την επόμενη φορά που θα εμφανιστεί η ανωμαλία να μπορεί να αναγνωριστεί από την υπογραφή του αντί να χρειάζεται να ξανατρέξει ο ταξινομητής για να την ανιχνεύσει. Στη συνέχεια, η θεωρία παιγνίων εφαρμόστηκε σε αυτήν την υβριδική τεχνική για να δημιουργήσει περαιτέρω εξοικονόμηση ενέργειας, η οποία έρχεται σε αντίθεση με δύο «παίκτες» μεταξύ τους, ο ένας είναι ο εισβολέας που εκτοξεύει τις νέες υπογραφές επίθεσης και ο άλλος που εκτελεί τον αλγόριθμο για τον εντοπισμό ανώμαλων νέων υπογραφών. Όταν τελειώσει το παιχνίδι, τα ιστορικά δεδομένα μπορούν να εξεταστούν για να προσδιοριστεί η πιθανότητα μιας νέας υπογραφής και, επομένως, μπορεί να οριστεί μια στιγμή κατά την οποία θα πρέπει να εκτελεστεί η ανίχνευση ανωμαλιών για τη δημιουργία νέων κανόνων. Η μελέτη συνέκρινε την προτεινόμενη ελαφριά τεχνική θεωρητικής παιγνίων με άλλες γνωστές υβριδικές τεχνικές στην ερευνητική βιβλιογραφία. Η μελέτη διαπίστωσε ότι η ακρίβεια μειώθηκε στην τεχνική της θεωρίας παιγνίων, κάτι που ήταν αναμενόμενο δεδομένης της προγνωστικής φύσης της τεχνικής. Κατά τη σύγκριση της κατανάλωσης ενέργειας, ωστόσο, η μελέτη διαπίστωσε ότι ήταν δυνατή η εξοικονόμηση έως και 6000 mJ ενέργειας κατά την εκτέλεση της ελαφριάς τεχνικής, η οποία αντιπροσωπεύει μια αξιόλογη εξοικονόμηση ενέργειας δεδομένης της φύσης του IoT με χαμηλούς πόρους [101].

Οι μετρήσεις αξιοπιστίας της συσκευής, ανεξάρτητα από το αν είναι τυπικές ή μη, προσφέρουν πολλές ευκαιρίες για επέκταση και περαιτέρω έρευνα. Πρώτον, ίσως αυτές οι μετρήσεις θα μπορούσαν επίσης να επεκταθούν για να συμπεριλάβουν την υποδομή δικτύου και τα πρωτόκολλα επικοινωνιών. Κάτι τέτοιο θα επιτρέψει στη λύση να είναι πιο ολιστική και θα την φέρει πιο κοντά στη διαχείριση της αξιοπιστίας για την πλήρη στοίβα από άκρο σε άκρο. Δεύτερον, αυτές οι μετρήσεις είναι σε θέση να επιβεβαιώσουν την αξιοπιστία των συσκευών IoT σε μια συγκεκριμένη χρονική στιγμή - θα μπορούσαν στη συνέχεια αυτές οι μετρήσεις να επεκταθούν για να επιτρέψουν στα συστήματα να προβλέψουν και να προλάβουν την αποτυχία; Κάνοντας αυτό θα ήταν ένα πολύτιμο βήμα προς ένα πιο αξιόπιστο IoT, ειδικά σε σενάρια όπου το IoT υποστηρίζει κρίσιμες εφαρμογές. Αυτό οδηγεί στην τρίτη περιοχή για επέκταση εδώ - ενώ αυτές οι μετρήσεις είναι πολύτιμες για την επίλυση της αξιοπιστίας για ένα δεδομένο σύνολο αισθητήρων σε ένα δεδομένο περιβάλλον, απαιτείται έρευνα για να κατανοηθεί πώς αυτό γενικεύεται σε άλλες εφαρμογές. Είναι σημαντικό, χρειάζεται να εφαρμόζονται διαφορετικά όρια όταν εξετάζεται ένας κατακόρυφος IoT έναντι του

άλλου; Απαιτείται επίσης κάποια έρευνα για να κατανοηθεί πώς μπορεί να αντιδράσουν αυτές οι μετρήσεις αξιοπιστίας καθώς προστίθενται στις εφαρμογές νέες και προηγουμένως αφανείς συσκευές. Θα περίμενε κανείς ότι οι νέες συσκευές ενδέχεται να έχουν ένα σημαντικά διαφορετικό προφίλ αποτυχίας και, επομένως, να επηρεάζουν τις μετρήσεις αξιοπιστίας με διαφορετικούς τρόπους. Η έρευνα για την αξιοπιστία των συσκευών IoT, επομένως, θα πρέπει να επεκταθεί όπου είναι δυνατόν, ώστε να συμπεριλάβει το σενάριο στο οποίο το IoT είναι ικανό να χειρίζεται νέες και μη ορατές συσκευές, που λειτουργούν σε ένα ευρύ φάσμα πρωτοκόλλων επικοινωνίας. Τέλος, υπάρχει μια αλληλεπίδραση μεταξύ της αξιοπιστίας της συσκευής IoT και της ανίχνευσης ανωμαλιών, η οποία δεν αξιοποιήθηκε πλήρως στα έργα που ερευνήθηκαν. Δεδομένου ότι γνωρίζουμε ότι οι συσκευές IoT είναι επιρρεπείς τόσο σε αυθόρμητη αποτυχία όσο και σε επιθέσεις από κακόβουλους χρήστες, αυτή η ιδέα θα έχει ισχυρή επίδραση στην αξιοπιστία των συσκευών IoT. Επομένως, απαιτείται έρευνα για την κατανόηση του αντίκτυπου των ανωμαλιών στην αξιοπιστία των συσκευών IoT. Για παράδειγμα, ορισμένες εφαρμογές μπορεί να είναι πολύ ευαίσθητες σε θόρυβο και ανωμαλίες, ενώ άλλες εφαρμογές μπορεί να αποτύχουν εντελώς με την παρουσία μιας μεμονωμένης ανωμαλίας. Ως εκ τούτου, οι μέθοδοι ανίχνευσης ανωμαλιών παρέχουν μια πολύτιμη εικόνα για την τρέχουσα κατάσταση αξιοπιστίας για τις συσκευές IoT. Ένα πιθανό ερευνητικό ερώτημα υπάρχει εδώ στην προσπάθεια να κατανοήσουμε εάν οι πληροφορίες αξιοπιστίας μπορούν να συντεθούν από μοντέλα ανίχνευσης ανωμαλιών [102].

Όσον αφορά τις εργασίες που ερευνούν την αξιοπιστία του δικτύου, μπορούμε και πάλι να παρατηρήσουμε ότι προτάθηκαν ορισμένες μετρήσεις, τόσο τυπικές [103] όσο και μη τυπικές [104]. Μπορούμε επίσης να παρατηρήσουμε ότι ορισμένα νέα πρωτόκολλα επικοινωνίας προτάθηκαν για να καταστεί δυνατό ένα πιο αξιόπιστο IoT. Διεξήχθη επίσης κάποια έρευνα για να βοηθήσει στην αντιμετώπιση της ανάγκης οι λύσεις IoT να λαμβάνουν υπόψη τις διάφορες κάθετες αγορές, για παράδειγμα τις εφαρμογές IoT έκτακτης ανάγκης [105]. Εισήχθησαν επίσης μέθοδοι σε συσκευές προφίλ προτού ενταχθούν στην ανάπτυξη του IoT, χρησιμοποιώντας δεδομένα αξιοπιστίας ως παράγοντα απόφασης [106]. Η έρευνα που διεξήχθη σχετικά με την αξιοπιστία του δικτύου ανοίγει πολλούς τομείς για μελλοντική έρευνα για να καταστεί δυνατή ένα πιο αξιόπιστο IoT. Πρώτον, ενώ έχει διεξαχθεί κάποια έρευνα για την κατανόηση της ευαισθησίας των διαφορετικών κάθετων IoT, εξακολουθεί να υπάρχει αυξανόμενη

ανάγκη για έρευνα σε αυτόν τον τομέα για να βοηθήσει στην κατανόηση του αντίκτυπου που έχουν αυτές οι κάθετες αγορές στη μηχανική αξιοπιστίας στο IoT. Δεδομένων των μεγάλων προβλέψεων για ανάπτυξη στις υπηρεσίες IoT, μπορούμε μόνο να περιμένουμε αύξηση της ζήτησης και διαφοροποίηση όσον αφορά τις εφαρμογές που προσφέρονται. Επομένως, για να είναι πλήρως αξιόπιστο, το IoT πρέπει να γνωρίζει αυτές τις κάθετες αγορές και να μετρά την αξιοπιστία με προσαρμοσμένο τρόπο [107]. Για παράδειγμα, τα σφάλματα πρέπει να αναφέρονται σε πραγματικό χρόνο, όπως με εφαρμογές έκτακτης ανάγκης; Ή ίσως μπορούμε να ανεχτούμε την αναφορά σφαλμάτων σε μεγαλύτερα χρονικά παράθυρα, όπως μια μέρα, όπως συμβαίνει με τις εφαρμογές έξυπνου σπιτιού. Ένα από τα κύρια ζητήματα με τις μελέτες που στοχεύουν στην αξιολόγηση της αξιοπιστίας του δικτύου είναι ότι δεν έχουν επίγνωση της αξιοπιστίας των ίδιων των συσκευών. Ως εκ τούτου, είναι σκόπιμο να διεξαχθεί κάποια έρευνα για να βοηθήσει στη σύνδεση αυτών των δύο πτυχών, προκειμένου να καταστεί δυνατή η αξιοπιστία σε ολόκληρη τη στοίβα IoT [108].

Όπως και με την αξιοπιστία της συσκευής, μπορούμε επίσης να υποθέσουμε τη σημασία των ανωμαλιών και των εισβολών στην κυκλοφορία του δικτύου. Είναι σημαντικό να κατανοήσουμε τον αντίκτυπο που έχουν αυτές οι ανωμαλίες στην αξιοπιστία μιας συγκεκριμένης εφαρμογής. Επιπλέον, εάν είμαστε σε θέση να αξιοποιήσουμε μεθόδους ανίχνευσης εισβολής και μεθόδους ανίχνευσης ανωμαλιών για δίκτυα και να τις χρησιμοποιήσουμε για να εξακριβώσουμε πληροφορίες αξιοπιστίας, τότε αυτό αντιπροσωπεύει ένα βήμα προς ένα πιο αξιόπιστο IoT. Επίσης, παρόμοια με την περίπτωση της συσκευής, θα ήταν χρήσιμη κάποια έρευνα για να γίνει κατανοητό εάν ήταν δυνατόν να προβλεφθούν σφάλματα προτού εμφανιστούν σε επίπεδο δικτύου. Η ικανότητα εκτέλεσης αυτής της πρόβλεψης θα επέτρεπε στους αρχιτέκτονες του IoT να διαχειρίζονται προληπτικά την αποτυχία, με αποτέλεσμα ένα πιο αξιόπιστο IoT—ειδικά στην περίπτωση εφαρμογών IoT κρίσιμων για την αποστολή [109].

Οι εργασίες μοντελοποίησης αξιοπιστίας συστήματος που εξετάζονται σε αυτό το έγγραφο δεν αφορούσαν ούτε τη συσκευή ούτε το στοιχείο δικτύου της αρχιτεκτονικής IoT. Ωστόσο, οι μέθοδοι σε αυτές τις εργασίες βρίσκονται σε πρώιμο στάδιο ανάπτυξης και δεν διαθέτουν την απαιτούμενη πολυπλοκότητα για την αντιμετώπιση ενός πολύπλοκου περιβάλλοντος IoT [110].

Αναφερόμενοι στις εργασίες που εξετάστηκαν για ανίχνευση ανωμαλιών, είναι σαφές από αυτές τις εργασίες ότι η ανίχνευση ανωμαλιών είναι ένας αναπτυσσόμενος τομέας στο IoT και στους υπολογιστές γενικότερα. Ενώ οι μέθοδοι ανίχνευσης ανωμαλιών που περιλαμβάνονται ήταν ικανές να ανιχνεύουν ανωμαλίες, εξακολουθεί να υπάρχει έλλειψη έρευνας και γνώσης σχετικά με το πώς θα μπορούσαμε να αξιοποιήσουμε αυτές τις πληροφορίες ανωμαλιών για να ποσοτικοποιήσουμε την αξιοπιστία μιας ανάπτυξης IoT. Ένας βασικός τομέας μελλοντικής έρευνας εδώ θα είναι η χρησιμοποίηση αυτών των μεθόδων ανίχνευσης ανωμαλιών και η προσπάθεια σύνθεσης πληροφοριών αξιοπιστίας από αυτές. Οι πέντε ερευνητικές κατευθύνσεις για την αξιοπιστία του IoT [111].

Έχοντας καταγράψει και αναλύσει τις συνδυασμένες προσπάθειες που καταβάλλονται από την ερευνητική κοινότητα αξιοπιστίας IoT, μπορούν να γίνουν ορισμένες εκτιμήσεις ως προς το πώς θα πρέπει να είναι η ιδανική λύση αξιοπιστίας. Ενώ κανένα από τα έργα που ερευνήθηκαν σε αυτό το έγγραφο δεν ικανοποιεί πλήρως την αξιοπιστία από άκρο σε άκρο στο IoT, το καθένα προσθέτει ένα κομμάτι του παζλ προς αυτόν τον στόχο. Ως εκ τούτου, μπορούμε να αντλήσουμε από αυτές τις εργασίες πέντε κρίσιμα στοιχεία που πρέπει να τηρεί ένα σύστημα διαχείρισης αξιοπιστίας από άκρο σε άκρο για το IoT [112].

Εάν το IoT έχει ρυθμιστεί να διαχειρίζεται κρίσιμες υποδομές, όπως η ασφάλεια και τα κρίσιμα συστήματα κυκλοφορίας, τότε πρέπει να είμαστε σε θέση να επιβεβαιώσουμε την αξιοπιστία του συστήματος σε πραγματικό χρόνο ή όσο το δυνατόν πιο κοντά σε πραγματικό χρόνο. Όπως φαίνεται στη μελέτη των Maalel et al. (2013), είναι απαραίτητο να δώσουμε ιδιαίτερη προσοχή σε εκείνες τις εφαρμογές που λειτουργούν υπηρεσίες έκτακτης ανάγκης και απαιτούν ταχεία και αξιόπιστη απόκριση. Επιπλέον, υπάρχει ανάγκη να καθοριστούν απαιτήσεις αξιοπιστίας σε κάθε επιμέρους τομέα. Για παράδειγμα, μια λύση έξυπνης κατασκευής μπορεί να έχει ανοχή καθυστέρησης έως και μερικά δευτερόλεπτα. Μια βιομηχανική διαδικασία, από την άλλη πλευρά, πιθανότατα θα είναι σε θέση να ανεχθεί μόνο καθυστερήσεις μικροδευτερόλεπτων. Ως εκ τούτου, απαιτείται έρευνα για την κατηγοριοποίηση αυτών των απαιτήσεων και τον σχεδιασμό αποτελεσματικών λύσεων για τη διαχείριση της αξιοπιστίας σε καθέναν από αυτούς τους κάθετους τομείς [113].

Αυτή η έρευνα έδειξε το πολύ ευρύ φάσμα πρωτοκόλλων και συσκευών που έχουν ρυθμιστεί να συνδέονται και να καταναλώνουν υπηρεσίες από το IoT. Τα πρότυπα για τα πρωτόκολλα επικοινωνίας συνεχίζουν να εξελίσσονται καθημερινά με τις προσπάθειες πολλών ερευνητικών ομάδων που στοχεύουν να σχεδιάσουν πιο ελαφριά και αποτελεσματικά πρωτόκολλα επικοινωνίας. Επιπλέον, νέες συσκευές και υλικό IoT συνεχίζουν να εμφανίζονται καθημερινά στην καταναλωτική αγορά. Ως εκ τούτου, η ιδανική λύση αξιοπιστίας πρέπει να είναι τόσο το υλικό, όσο και το λογισμικό και το πρωτόκολλο επικοινωνίας αγνωστικιστικά [61]

Ένα από τα συμπεράσματα που προέκυψαν από την ανασκόπηση της βιβλιογραφίας ήταν ότι, ενώ πολλοί ερευνητές είχαν λύσει επιτυχώς ένα συγκεκριμένο πρόβλημα ή υποσύνολο προβλημάτων, στην έρευνα αξιοπιστίας του IoT, δεν έχει πραγματοποιηθεί καμία μελέτη που να έχει πλήρη επίγνωση της αξιοπιστίας από άκρο σε άκρο. Δεδομένης της κλίμακας και της πολυπλοκότητας των αναδυόμενων αναπτύξεων IoT, αυτό δεν είναι εύκολο έργο. Αυτό δεν σημαίνει, ωστόσο, ότι οι ερευνητές θα πρέπει να επιδιώκουν να σχεδιάσουν μια προσέγγιση αξιοπιστίας «ένα μέγεθος για όλους», καθώς αυτό θα έρχεται σε αντίθεση με την πρώτη ερευνητική κατεύθυνση που περιγράφεται σε αυτήν την εργασία. Αντίθετα, θα πρέπει να προτείνονται μεμονωμένες λύσεις αξιοπιστίας για κάθε κλάδο IoT που να περιλαμβάνει την πλήρη αρχιτεκτονική του IoT. Ωστόσο, ο σχεδιασμός μιας λύσης αξιοπιστίας από άκρο σε άκρο για το IoT θα ήταν ένα σημαντικό και νέο ερευνητικό εύρημα με τη δυνατότητα να βελτιώσει σημαντικά την εμπειρία του τελικού χρήστη του IoT [59]

Έχει γίνει πολλή δουλειά για τον εντοπισμό και την αναφορά ανωμαλιών όταν εμφανίζονται σε υπηρεσίες IoT. Αν και αυτή η εργασία είναι και χρήσιμη και απαραίτητη, δεν βοηθά απαραίτητα την αξιοπιστία χωρίς ένα επιπλέον βήμα. Η γνώση μιας ανωμαλίας δεν λέει απαραίτητα στον χρήστη εάν το σύστημα IoT έχει γίνει λιγότερο αξιόπιστο. Ως εκ τούτου, υπάρχει ανάγκη να ερευνήσουμε πώς μπορούμε να συνθέσουμε πληροφορίες σχετικά με έκτακτες ανωμαλίες στα συστήματα IoT σε πληροφορίες σχετικά με τον τρόπο με τον οποίο έχει επηρεαστεί η αξιοπιστία. Για παράδειγμα, εάν ένας αισθητήρας σπάσει σε ένα έξυπνο σπίτι που παρακολουθεί ένα σενάριο υποβοηθούμενης διαβίωσης, μπορεί να μην υπάρχει απαραίτητα άμεσος κίνδυνος για τη ζωή. Ενώ, εάν ένας θερμικός αισθητήρας αρχίσει να στέλνει

λανθασμένες μετρήσεις σε ένα έξυπνο εργοστάσιο, υπάρχει πιθανότητα δυσλειτουργίας επικίνδυνου μηχανήματος [58]

Η μέτρηση της αξιοπιστίας είναι η εργασία που συζητείται εκτενώς σε αυτήν την εργασία. Εάν η έρευνα πρόκειται να προχωρήσει ένα βήμα πέρα από αυτόν τον στόχο, τότε μπορεί να εξεταστεί το έργο της προγνωστικής συντήρησης. Εάν είμαστε σε θέση να αιτιολογήσουμε την ποσοτικοποιημένη αξιοπιστία ενός συστήματος, μπορούμε στη συνέχεια να το προεκθέσουμε σε μια ακριβή ημερομηνία συντήρησης; Επιπλέον, μπορεί αυτό να ταξινομηθεί περαιτέρω σε επίπεδο συνιστώσας και να είναι μια δυναμική διαδικασία που καθορίζει αποτελέσματα με βάση δεδομένα αξιοπιστίας σε πραγματικό χρόνο, αντί να χρησιμοποιεί ένα ιστορικό προηγούμενων αστοχιών για την εκτίμηση μιας μελλοντικής ημερομηνίας αστοχίας; Η επίλυση αυτού του ερευνητικού ερωτήματος θα αντιπροσώπευε ένα πολύτιμο βήμα στην έρευνα της αξιοπιστίας του IoT [114].

1.2.6. Σημασιολογικές Τεχνολογίες και IoT

Με την έλευση του IoT εκατοντάδες αισθητήρες, έξυπνες συσκευές και smartphone έχουν έχουν εφαρμοστεί στην καθημερινότητά μας. Το αποτέλεσμα αυτού είναι τεράστιες ποσότητες δεδομένα με μεγάλες διαφορές σε μορφές και τομείς. Αυτό έχει δημιουργήσει μεγάλες προκλήσεις

ώστε οι μηχανές να κατανοούν πληροφορίες και να εξάγουν γνώση από αυτά τα δεδομένα. Για καλύτερη αναπαράσταση του IoT, διαφορετικές ερευνητικές μελέτες δεδομένων έχουν προτείνει διαφορετικές τεχνικές που επιτρέπουν στις μηχανές να κατανοούν έξυπνα ετερογενή δεδομένα [115].

Το Semantic Web of Things (SWoT) είναι μια συνέχεια του World Wide Web που προσπαθεί να το κάνει επιλύει τα προβλήματα που προκύπτουν από τα ετερογενή συστήματα και παρέχει μια καλύτερη κατανόηση των διαφορετικών τομέων IoT. Ο κύριος σκοπός του Web of Things είναι να ενεργοποιήσει διαλειτουργικότητα σε πλατφόρμες IoT και τομείς εφαρμογών. Συνολικά, τα WoT σκοπός είναι η υποστήριξη και συμπλήρωση των υφιστάμενων προτύπων και λύσεων IoT [150].

Με τη σημασιολογική τεχνολογία στο Web of Things η γνώση τομέα και Οι πληροφορίες παρασκηνίου συνδυάζονται με δεδομένα αισθητήρων, διευκολύνοντας

τις μηχανές κατανοήσουν και επεξεργαστούν. Επιπλέον, η σημασιολογία παρέχει μια συνεκτική περιγραφή αρχιτεχνολογίες που ενισχύουν τις πληροφορίες και την ανταλλαγή γνώσεων μεταξύ μεταβλητών κόμβους αισθητήρων. Πριν από το WOT, οι αισθητήρες και ο κόσμος του Ιστού είχαν εντελώς απορριφθεί φιδωτός. Με τα δεδομένα που σχετίζονται με το WOT IoT στον Ιστό θα βοηθούσαν τους χρήστες σε διαφορετικούς τομείς με άμεση πρόσβαση σε δεδομένα αισθητήρων και παρακολούθηση των ενσωματωμένων παραμέτρων του πραγματικού κόσμου με παρόμοιες πληροφορίες περιβάλλοντος από τον Ιστό.

Για να συναντήσετε το WOT στον κόσμο του IoT, μεγάλης κλίμακας ανοιχτές διεπαφές και μορφές δεδομένων πρέπει να βελτιστοποιηθούν και να ενσωματωθούν με τα σχετικά αντίστοιχα IoT [151].

Γενικά, οι χρήστες του IoT ενδιαφέρονται μάλλον για πραγματικές καταστάσεις και γνώσεις παρά στα συστήματα ανίχνευσης και τα πρωτογενή δεδομένα τους. Μέσω του SWoT υπάρχουν τα κατάλληλα αφαιρέσεις για τη χαρτογράφηση αισθητήρων και την ακατέργαστη παραγωγή τους σε οντότητες του πραγματικού κόσμου με πραγματικό σημασιολογία. Για να συνειδητοποιήσουμε ότι οι ερευνητές SWoT επεκτείνουν το IoT με όλα τα αξιοσημείωτα χαρακτηριστικά του Σημασιολογικού Ιστού: α) ευρεία χρήση URI και HTTP, β) σύνδεση τομέα μοντέλα μέσω διαλειτουργικών αναφορών, γ) χρήση κοινών τυπικών γλωσσών και δ) εκφραστικότητα τομέα μέσω παρέκτασης λογικών ακολουθιών.

Το Διαδίκτυο των Πραγμάτων (IoT) γίνεται όλο και πιο δημοφιλές και η εφαρμογή του Τα δεδομένα αντιμετωπίζουν τεράστιο πολλαπλασιασμό που οδηγεί σε ένα νέο ψηφιακό οικοσύστημα. πλατφόρμες IoT αποτελούν ουσιαστικά τον ακρογωνιαίο λίθο μιας ολοκληρωμένης λύσης IoT καθώς επιτρέπουν στον συν- συλλογή και ανάλυση των δεδομένων που παράγονται στα τελικά σημεία, με αποτέλεσμα την ανάπτυξη μεγάλων δεδομένων αναλυτικά στοιχεία και εφαρμογές. Η ταχεία αύξηση του αριθμού των δικτυακών ελαττώματα που αναπτύσσονται στον πραγματικό κόσμο, ενισχύονται από τις δυνατότητες επεξεργασίας πληροφοριών δημιούργησε τεράστιες ποσότητες βάσεων δεδομένων. Καθώς το IoT βασίζεται σε μια μεγάλη ποικιλία διαφορετικών για ετερογενή συστήματα και τεχνολογίες, δεν υπάρχει τυποποιημένη γλώσσα αναπαράσταση και επεξεργασία δεδομένων. Αυτό συνέβαλε σε μεγάλο αριθμό IoT συστήματα που δεν είναι συμβατά. Έτσι, είναι πολύ δύσκολο για τους επιστήμονες

δεδομένων να εξαγάγουν πληροφορίες από τον τεράστιο αριθμό δεδομένων που παρέχονται από τις εφαρμογές IoT κάθε δεύτερος [116].

Οι τεχνολογίες του σημασιολογικού ιστού προσπαθούν να ξεπεράσουν τέτοιες προκλήσεις. Μοχλός σημασιολογικού ιστού- ηλικιακά πρότυπα ιστού και σημασιολογικές τεχνολογίες για τη διασύνδεση όλων των τύπων συσκευών μετατρέποντας τα ακατέργαστα δεδομένα αισθητήρων σε γνώση υψηλού επιπέδου που είναι κατανοητή από ανθρώπους και μηχανές. Η διαλειτουργικότητα είναι μια από τις σημαντικότερες προκλήσεις σε περιβάλλον IoT, όπου διαφορετικές συσκευές, υπηρεσίες και οντότητες προσπαθούν να συνδεθούν ο ένας τον άλλον. Η σημασιολογική μοντελοποίηση παράγει ένα συγκεκριμένο σχήμα των δεδομένων που σημαίνουν δομημένο τρόπο συνδυάζοντας γνώσεις εφαρμογής και πληροφορίες σχετικές με το πλαίσιο με δεδομένα αισθητήρα. Η ανάπτυξη που βασίζεται στην οντολογία, η οποία είναι τομέας του η σημασιολογική μοντελοποίηση, των πλαισίων IoT μπορεί να οδηγήσει σε καθολικές λύσεις IoT πολλαπλασιάζονται- αξιοποιώντας τα οφέλη του IoT [152].

1.2.7. Μοντελοποίηση και Σχεδιασμός

Ο σχεδιασμός ενός συστήματος IoT σήμερα παρουσιάζει σημαντικό περίπλοκο. Διάφοροι παράγοντες συμβάλλουν σε αυτήν την πολυπλοκότητα: πρώτον, η κατανόηση του IoT εξακολουθεί να είναι πολύ εστιασμένη στην τεχνολογία IoT-nologies και αντικείμενα (τύποι συσκευών, πρωτόκολλα επικοινωνίας, σύννεφο, τύπος βάσης δεδομένων, κ.λπ.). Ένα τέτοιο όραμα χάνει τα μάτια του

Ο πραγματικός σκοπός του συστήματος να αναπτυχθεί και να οδηγεί τα περισσότερα από τα καιρός για μη ικανοποιητικές λύσεις. Στη συνέχεια, η μεγάλη ποικιλία από Τα συστήματα IoT, όσον αφορά την ανάπτυξή τους, είναι μια τεχνολογία πηγή πολυπλοκότητας: Τα συστήματα IoT μπορούν να θεωρηθούν με α «τοπική» ανάπτυξη όπως ένα αυτόματο σύστημα φωτισμού ένα σπίτι (μέτρηση, αποθήκευση, ανάλυση και εκτέλεση δεδομένων της εφαρμογής σε μία μόνο «συσκευή» που είναι συνδεδεμένη στο smartphone του ιδιοκτήτη), ή συστήματα με "υψηλή κατανομή" αρχιτεκτονική όπως ένα σύστημα πρόγνωσης καιρού (αισθητήρας δίκτυα για δυνατότητες λήψης δεδομένων, συν ένα σύννεφο για αποθήκευση, ανάλυση δεδομένων και εκτέλεση της εφαρμογής τελικού χρήστη). Άλλο η πτυχή αφορά την ανάγκη ενσωμάτωσης παλαιών

συστημάτων, π.χ. Τα συστήματα IoT δεν έχουν σχεδιαστεί από το «μηδέν», το πρόβλημα είναι τότε για τη δημιουργία νέων καινοτόμων υπηρεσιών με βάση τις υπάρχουσες υποδομές. Σε αυτή την περίπτωση, είναι απαραίτητο να "συνδέσετε" τι υπάρχει και στη συνέχεια αναπτύξτε / ενσωματώστε υποστηρικτικά στοιχεία (έλεγχος ταυτότητας, παρακολούθηση, διανομή δεδομένων, ανάλυση δεδομένων, και τα λοιπά.) [117].

Για αυτό το πεδίο, η προτεινόμενη λύση πρέπει να επιτρέπει i) μοντελοποίηση πολλών πτυχών ενός συστήματος IoT: το φυσικό επίπεδο, τις συσκευές IoT, το επίπεδο συστήματος, τις συμπεριφορές του συστήματος και τις αλληλεπιδράσεις μεταξύ των συστατικών. ii) Σύνθεση Οι υπηρεσίες IoT παρέχονται επίσης από διαφορετικές πλατφόρμες IoT, χρησιμοποιώντας μια προσέγγιση σχεδιασμού που βασίζεται σε μοντέλο και σημειώνεται σημασιολογικά μορφές δεδομένων για την υποστήριξη της διαλειτουργικότητας μεταξύ ετερογενών συστήματα. iii) Επίσημη επαλήθευση και επικύρωση των μοντέλων σχεδιασμένο με το πλαίσιο. iv) Η αυτόματη παραγωγή κώδικα από τα μοντέλα που πρόκειται να αναπτυχθούν σε πραγματικές συσκευές. v) Υποστήριξη της προσέγγισης συν-προσομοίωσης, με τη δημιουργία ένα περιβάλλον μικτής πραγματικότητας, όπου εικονικές και πραγματικές οντότητες μπορούν να αλληλεπιδράσουν μεταξύ τους. vi) Παρακολούθηση της εφαρμογής IoT- θέσεις κατά το χρόνο εκτέλεσης, διατηρώντας τα μοντέλα και τον φυσικό κόσμο συγχρονίζονται μεταξύ τους. Η επόμενη ενότητα θα παρέχει α τελευταίας τεχνολογίας (sota) των λύσεων που είναι διαθέσιμες για το σχεδιασμό και διαχείριση εφαρμογών IoT επόμενης γενιάς [153]

2. Επικοινωνιακά Συστήματα

2.1. Ορισμός Επικοινωνιακών Συστημάτων

Ένα σύστημα επικοινωνιών είναι μια συλλογή εξοπλισμού επικοινωνιών που είναι ενσωματωμένος σε ένα συνεκτικό σύστημα. Αυτά επιτρέπουν σε διαφορετικούς ανθρώπους να παραμένουν σε επαφή μέσω ενός γεωγραφικού συστήματος. Μια σημαντική εφαρμογή είναι η αντιμετώπιση καταστροφών. Με ένα σύστημα επικοινωνιών, οι πυροσβέστες, η αστυνομία και οι παραϊατρικοί μπορούν να συντονίσουν τις προσπάθειές τους με άλλους κυβερνητικούς αξιωματούχους. Ένα σύστημα επικοινωνιών είναι ένα ολοκληρωμένο σύστημα υλικού επικοινωνιών. Αυτό μπορεί να περιλαμβάνει εξοπλισμό μετάδοσης, σταθμούς αναμετάδοσης, σταθμούς παραπόταμου και άλλο τερματικό εξοπλισμό δεδομένων. Ένα σύστημα επικοινωνιών μπορεί να περιλαμβάνει ακόμη και άλλα συστήματα επικοινωνιών. Ένα καλό παράδειγμα θα ήταν ένα περιφερειακό σύστημα επικοινωνίας απόκρισης έκτακτης ανάγκης που συνδέει πολλές διαφορετικές πόλεις και τους επιτρέπει να ανταποκρίνονται σε μια καταστροφή ενσωματώνοντας συστήματα που έχουν εγκαταστήσει για τους δικούς τους αστυνομικούς και πυροσβέστες [78]

Τα συστήματα επικοινωνιών μπορούν να περιλαμβάνουν δίκτυα οπτικών επικοινωνιών, όπως καλώδια οπτικών ινών, ραδιόφωνο, ακόμη και επικοινωνίες με γραμμές ηλεκτρικής ενέργειας. Ένα εξελιγμένο σύστημα μπορεί να συνδυάζει και να ταιριάζει με αυτούς τους διαφορετικούς τύπους μέσων. Μια άλλη διάκριση στους τύπους επικοινωνίας είναι οι αμφίδρομες επικοινωνίες. Οι επικοινωνίες διπλής όψης επιτρέπουν στα δύο μέρη να επικοινωνούν μεταξύ τους την ίδια στιγμή.

Παραδείγματα συστημάτων επικοινωνιών σε δράση περιλαμβάνουν τακτικά δίκτυα που επιτρέπουν στις ένοπλες δυνάμεις να παραμένουν σε επαφή με την κεντρική διοίκηση με ασφάλεια. Μια άλλη σημαντική εφαρμογή είναι τα συστήματα επικοινωνιών έκτακτης ανάγκης που επιτρέπουν στους υπαλλήλους και τους πρώτους ανταποκριτές να στέλνουν μηνύματα μεταξύ τους και στο κοινό, όπως μέσω του Συστήματος Ειδοποίησης Έκτακτης Ανάγκης των ΗΠΑ (EAS) και των εξωτερικών προειδοποιητικών σειρήνων. Ένας άλλος τύπος συστήματος επικοινωνίας είναι ένας αυτόματος διανομέας κλήσεων, ο οποίος παραθέτει κλήσεις από έξω από έναν

οργανισμό για δρομολόγηση σε συγκεκριμένα άτομα. Αυτά εμφανίζονται συνήθως σε τηλεφωνικά κέντρα [75]

2.2. Είδη Επικοινωνιακών Συστημάτων

- Σύστημα Οπτικής Επικοινωνίας

Όταν το φως χρησιμοποιείται για την αποστολή μηνύματος από το ένα μέσο στο άλλο, τότε χρησιμοποιείται το οπτικό σύστημα επικοινωνίας. Το μήνυμα μετατρέπεται σε σήματα και τα σήματα μεταφέρονται από τον αποστολέα στον δέκτη. Ο δέκτης λαμβάνει το σήμα, το αποκωδικοποιεί και κατανοεί και αποκρίνεται ανάλογα. Ολόκληρο το σύστημα οπτικής επικοινωνίας εξαρτάται από το φως. Για παράδειγμα, τα ελικόπτερα και οι προσγειώσεις αεροπλάνων λειτουργούν με την ίδια αρχή του συστήματος οπτικής επικοινωνίας. Τα φωτεινά σήματα λαμβάνονται από τη βάση και στη συνέχεια αποφασίζονται τα επόμενα βήματα. Τα συστήματα οπτικών επικοινωνιών χρησιμοποιούνται επίσης από τους σιδηροδρόμους και ακόμη και στους δρόμους με τη μορφή σημάτων κυκλοφορίας. Το πράσινο φως είναι για να πάει, ενώ το κόκκινο φως είναι ένα σήμα για να σταματήσει. Τα σήματα SOS χρησιμοποιούν επίσης συστήματα οπτικής επικοινωνίας [73]

- Σύστημα ραδιοεπικοινωνίας

Όπως υποδηλώνει το όνομα, το σύστημα ραδιοεπικοινωνίας χρησιμοποιεί ραδιόφωνο για τη μετάδοση μιας επικοινωνίας από τον αποστολέα στον δέκτη. Αυτό το σύστημα επικοινωνίας απαιτεί τη χρήση δέκτη κεραίας και στα δύο άκρα.
Τα σήματα παράγονται με τη βοήθεια μιας κεραίας, η οποία μεταδίδεται στο σήμα στο άκρο του δέκτη. Το μήνυμα επικοινωνίας μεταφέρεται με τη βοήθεια κυμάτων.
Το ραδιόφωνο διαθέτει φίλτρο σήματος για φιλτράρισμα διαφορετικών σημάτων. Οι πληροφορίες για ορισμένα σήματα είναι ανεπιθύμητες, ενώ ορισμένα σήματα απαιτούνται. Επομένως, τα ραδιόφωνα διαθέτουν μια δυνατότητα συντονισμού με την οποία ο δέκτης μπορεί να συντονιστεί σε μια συγκεκριμένη συχνότητα στην οποία μπορείτε να λάβετε το επιδιωκόμενο μήνυμα του αποστολέα.
Τα σήματα αποκωδικοποιούνται από το ραδιόφωνο και είναι εύκολα κατανοητά από τους ακροατές [73]

- Συστήματα Διπλής Επικοινωνίας

Όπως υποδηλώνει το όνομα, τα συστήματα επικοινωνίας διπλής όψης περιλαμβάνουν τη χρήση δύο διαφορετικών τύπων εξοπλισμού για την επικοινωνία μεταξύ τους. Αυτοί οι δύο τύποι εξοπλισμού χρησιμοποιούνται ταυτόχρονα. Για παράδειγμα, στη βιντεοκλήση, και οι δύο καλούντες μπορούν να δουν ο ένας τον άλλον και να μιλήσουν ταυτόχρονα. Ο άλλος μπορεί να ακούσει και να μιλήσει ταυτόχρονα. Επομένως, αυτό το σύστημα μπορεί να θεωρηθεί προηγμένο σε σύγκριση με τα συστήματα ραδιοεπικοινωνίας και φωτός. Η διαδικασία επικοινωνίας στα συστήματα αμφίδρομης επικοινωνίας λαμβάνει χώρα ταυτόχρονα, ενώ τα συστήματα ραδιοεπικοινωνίας και φωτός δεν το επιτρέπουν [73]

- Συστήματα επικοινωνίας μισής διπλής όψης

Σε αυτό το σύστημα επικοινωνίας, σε αντίθεση με το σύστημα επικοινωνίας διπλής όψης, και τα δύο μέρη δεν μπορούν να επικοινωνήσουν ταυτόχρονα. Ένα άτομο πρέπει να σταματήσει να στέλνει το σήμα στο άλλο άτομο και να περιμένει μέχρι να ανταποκριθεί το άλλο άτομο. Για παράδειγμα, ένα φορητό ραδιόφωνο ακολουθεί ένα σύστημα επικοινωνίας ημι-αμφίδρομης λειτουργίας. Στο τέλος κάθε πρότασης στο Walkie Talkie, ο αποστολέας αναμένεται να λέει «πάνω» έτσι ώστε ο παραλήπτης να μπορεί να αρχίσει να στέλνει σχόλια με βάση το μήνυμα που έστειλε ο αποστολέας [73]

- Σύστημα τακτικής επικοινωνίας

Σε ένα σύστημα τακτικής επικοινωνίας, η επικοινωνία ποικίλλει καθώς ποικίλλει οι περιβαλλοντικές συνθήκες σε αυτά. [77]

<u>Κοινά Στοιχεία Συστημάτων Επικοινωνίας</u>

- Πληροφορίες

Πληροφορίες είναι το μήνυμα που πρόκειται να μεταφερθεί από τον αποστολέα στον παραλήπτη ή από τον παραλήπτη στον αποστολέα ως ανατροφοδότηση. Η μορφή των πληροφοριών μπορεί να είναι οτιδήποτε, από κείμενο, έως βίντεο ή συνδυασμός οποιασδήποτε μορφής διαθέσιμων μορφών μηνυμάτων.

- Σήμα

Το σήμα είναι ο φορέας της πληροφορίας. Το μήνυμα μετατρέπεται σε σήμα για μετάδοση από το ένα άκρο στο άλλο.

- Μετατροπέας

Ο μορφοτροπέας μπορεί επίσης να ονομαστεί μετατροπέας αφού μετατρέπει ενέργεια από τη μια μορφή στην άλλη. Ο μετατροπέας μπορεί να μετατρέψει θερμοκρασία, πίεση, δύναμη σε αντίστοιχα ηλεκτρικά σήματα. Για παράδειγμα, μια τηλεφωνική κλήση μπορεί να μεταφέρει τη φωνή μας στον αποστολέα μετατρέποντας τη φωνή σε σήματα ήχου.

- Ενισχυτής

Η συσκευή που βοηθά στην αύξηση της ισχύος του μεταδιδόμενου σήματος ονομάζεται Ενισχυτής. Η ενίσχυση γίνεται για να αυξηθεί η συχνότητα του μηνύματος που αποστέλλεται.

- Διαμορφωτής

Μερικές φορές το μήνυμα πρόκειται να μεταδοθεί σε μεγάλες αποστάσεις. Αυτά τα μηνύματα τείνουν να έχουν χαμηλή συχνότητα και πλάτος. Για να αυξηθεί η εμβέλειά τους, αυτά τα μηνύματα συνδυάζονται με φέροντα κύματα, τα οποία είναι κύματα υψηλού πλάτους και υψηλής συχνότητας. Αυτή η διαδικασία σύλληψης κυμάτων υψηλής συχνότητας με το μήνυμα ονομάζεται διαμόρφωση. Το προκύπτον κύμα διαμόρφωσης είναι το μήνυμα που πρόκειται να μεταδοθεί.

Υπάρχουν τρεις διαφορετικοί τύποι διαμορφώσεων που υπάρχουν με βάση τις αλλαγές που πραγματοποιήθηκαν:

- Διαμόρφωση πλάτους – Όταν το πλάτος αλλάζει και υπερτίθεται στο φέρον κύμα υψηλής συχνότητας, ονομάζεται διαμόρφωση πλάτους.
- Διαμόρφωση συχνότητας – Σε αυτή την τεχνική, η συχνότητα μεταβάλλεται με την παρακίνηση του σήματος με ένα φέρον κύμα. Η διαμόρφωση συχνότητας είναι καλύτερη και πιο αποτελεσματική από το κίνητρο πλάτους, καθώς οι θόρυβοι εξαλείφονται από διαφορετικές πηγές.

- Διαμόρφωση φάσης – Η φάση του φέροντος κύματος αλλάζει τη φάση του κύματος σήματος[74] .

- Πομπός

Το μήνυμα μετατρέπεται σε σήμα με τη βοήθεια εξοπλισμού, ο οποίος ονομάζεται πομπός. Ο πομπός είναι παρών στην τοποθεσία του αποστολέα και στη θέση του παραλήπτη, μπορεί να υπάρχει ως δέκτης.

- Κεραία

Η δομή ή η συσκευή που δέχεται ηλεκτρομαγνητικά κύματα από τον αέρα, που μεταδίδονται από τον αποστολέα, ονομάζεται κεραία. Ορίζεται επίσης ως η δομή που μπορεί να μετατρέψει το μήνυμα σε κύματα για να το μεταδώσει περαιτέρω ονομάζεται κεραία. Η κεραία είναι μεταλλική και απαιτεί πολλά καλώδια για να λειτουργήσει.

- Κανάλι

Όταν η κεραία μετατρέπει το μήνυμα, μεταφέρεται μέσω καλωδίου ή καλωδίου ή διαστήματος, που ονομάζεται κανάλι.

- Θόρυβος

Το εμπόδιο μεταξύ του αποστολέα και του παραλήπτη ονομάζεται θόρυβος. Ο θόρυβος κυρίως διακόπτει ή διακόπτει το μήνυμα που μεταφέρεται από τον αποστολέα στον παραλήπτη. Αυτή η παρεμβολή μπορεί να έχει τη μορφή φυσικής διακοπής, κεραυνού, ηλιακής ακτινοβολίας ή οποιουδήποτε άλλου σχετικού τύπου απόσπασης της προσοχής.

Τα κανάλια είναι σχεδιασμένα με τέτοιο τρόπο ώστε να εξαλείφουν την εξωτερική καταστροφή ή να ελαχιστοποιούν. Ο θόρυβος μπορεί να συμβεί λόγω της τυχαίας σύγκρουσης ηλεκτρονίων στους αγωγούς. Γίνονται προσπάθειες μείωσης ή εξάλειψης του θορύβου εσωτερικά με τη χρήση ψηφιακής τεχνολογίας.

- Εξασθένηση

Η εξασθένηση είναι το πρόβλημα που προκαλείται από το μέσο όταν το σήμα διανύει μεγάλες αποστάσεις από ένα μέσο. Αυτό εξαρτάται από το μήκος του μέσου. Το εύρος του μέσου είναι ευθέως ανάλογο με την απώλεια αρχικής ισχύος. Τα ψηφιακά σήματα είναι λιγότερο επιρρεπή σε εξασθένηση σε σύγκριση με τα αναλογικά.

- Παραμόρφωση

Είναι ένα από τα προβλήματα του καναλιού. Το μεταδιδόμενο μήνυμα βρίσκεται σε συγκεκριμένο εύρος ζώνης και συχνότητα. Ωστόσο, όταν παραμορφώνεται αυτό, η συχνότητα και το εύρος ζώνης.

- Δέκτης

Ο δέκτης βρίσκεται στο μακρινό άκρο του συστήματος επικοινωνίας και λειτουργεί ως δέκτης για το μήνυμα που στέλνει ο αποστολέας. Είναι μια συσκευή που έχει σχεδιαστεί για να δίνει μια έξοδο στο σήμα λήψης. Ο δέκτης μεταφράζει επίσης το μήνυμα στο άτομο στο άκρο λήψης. Σε αμφίδρομη επικοινωνία, ο δέκτης λειτουργεί επίσης ως συσκευή αποστολής και μεταδίδει το μήνυμα πίσω στον αποστολέα.

- Αποδιαμορφωτής

Η συνάρτηση της αποδιαμόρφωσης είναι ακριβώς το αντίθετο της διαμόρφωσης. Στη διαμόρφωση, το μήνυμα συνδέεται με τον φορέα, ενώ στην αποδιαμόρφωση, το μήνυμα διαχωρίζεται από το φέρον κύμα.

- Επαναληπτικοί

Οι επαναλήπτες υπάρχουν σε πολλαπλές θέσεις μεταξύ του δέκτη και του πομπού. Η κύρια λειτουργία του επαναλήπτη είναι να ενισχύει το σήμα που λαμβάνει και να το στέλνει στον επόμενο επαναλήπτη διασφαλίζοντας παράλληλα ότι το μήνυμα δεν παραμορφώνεται [118].

Τα συστήματα επικοινωνίας αποτελούν ουσιαστικό μέρος της διαδικασίας επικοινωνίας. Αυτά τα συστήματα επιτρέπουν τη μεταφορά πληροφοριών και την ανταλλαγή ιδεών από απομακρυσμένα μέρη. Ενώ το σύστημα είναι πολύπλοκο με τη

συμμετοχή πολλαπλών στοιχείων, η διαδικασία της επικοινωνίας παραμένει η ίδια σε όλες σχεδόν τις πτυχές ή τους τύπους συστημάτων επικοινωνίας [119].

2.3. Πλεονεκτήματα και Μειονεκτήματα Επικοινωνιακών Συστημάτων

Τα οφέλη της ψηφιακής επικοινωνίας έναντι της αναλογικής αναφέρονται ως εξής:

- Στα ψηφιακά σήματα, η επίδραση της παρεμβολής θορύβου, η παραμόρφωση είναι μικρότερη.
- Διευκολύνει τη τηλεδιάσκεψη που εξοικονομεί χρόνο, χρήμα και προσπάθεια.
- Μπορούμε να πραγματοποιήσουμε τηλεδιάσκεψη με κάποιον ή μια ομάδα ατόμων χωρίς να ταξιδέψουμε. Στη τηλεδιάσκεψη, μπορούμε να δούμε τις εκφράσεις του προσώπου, οι οποίες βοηθούν στην ανάγνωση της αντίδρασης των ανθρώπων.
- Είναι εύκολο στην εφαρμογή, λιγότερο ακριβό.
- Χρησιμοποιείται σε στρατιωτικές εφαρμογές.
- Η διόρθωση και η ανίχνευση σφαλμάτων είναι εύκολη στην ψηφιακή επικοινωνία, καθώς υπάρχει χρήση κωδικοποίησης καναλιών.
- Σε σύγκριση με τα αναλογικά σήματα, είναι εύκολο να αποθηκεύσετε και να ανακτήσετε ψηφιακά σήματα.
- Στα ψηφιακά σήματα, η διαδικασία διαμόρφωσης είναι εύκολη σε σύγκριση με τα αναλογικά σήματα.
- Υπάρχει μια κοινή τεχνική κωδικοποίησης στα περισσότερα ψηφιακά κυκλώματα, επομένως για μια σειρά διεργασιών, μπορούν να χρησιμοποιηθούν παρόμοιες συσκευές.
- Η πιθανότητα αλληλεπίδρασης είναι πολύ μικρότερη στην ψηφιακή επικοινωνία.
- Η υλοποίηση του υλικού είναι πιο ευέλικτη στην ψηφιακή επικοινωνία.
- Στην ψηφιακή επικοινωνία, για την αποφυγή εμπλοκής σήματος, χρησιμοποιείται η τεχνική του φάσματος διασποράς.
- Μας διευκολύνει επίσης με ηχητική διάσκεψη μέσω της οποίας μπορούμε να μιλήσουμε με κάποιον ή μια ομάδα ατόμων σε άλλη τοποθεσία χωρίς να ταξιδέψουμε. Έτσι, εξοικονομεί χρόνο, κόπο και χρήμα.

- Για να διατηρηθεί το απόρρητο των πληροφοριών, οι λειτουργίες επεξεργασίας σήματος όπως η συμπίεση και η κρυπτογράφηση χρησιμοποιούνται σε ψηφιακά κυκλώματα.
- Η ψηφιακή επικοινωνία είναι φθηνότερη και απλούστερη σε σύγκριση με τα αναλογικά σήματα λόγω της προόδου των τεχνολογιών IC [65]

Οι περιορισμοί της ψηφιακής επικοινωνίας αναφέρονται ως εξής:

- Υπάρχει υψηλή κατανάλωση ενέργειας στην ψηφιακή επικοινωνία.
- Υπάρχει απαίτηση για συγχρονισμό στην περίπτωση της σύγχρονης διαμόρφωσης.
- Υπάρχει δειγματοληπτικό σφάλμα.
- Ο πιο συνηθισμένος περιορισμός της ψηφιακής επικοινωνίας είναι ότι απαιτεί μεγαλύτερο εύρος ζώνης μετάδοσης. Οφείλεται στον υψηλότερο ρυθμό μετάδοσης δεδομένων λόγω της μετατροπής αναλογικής σε ψηφιακή.
- Η ψηφιακή επικοινωνία απαιτεί μετατροπή αναλογικού σε ψηφιακό με υψηλό ρυθμό.
- Μπορεί να υπάρχει πιθανότητα εσφαλμένης επικοινωνίας εάν ένας χρήστης δεν καταλαβαίνει κάτι [66]

3. Το Δίκτυο των Πραγμάτων στα Επικοινωνιακά Συστήματα

3.1. Εφαρμογές του IoT στα Επικοινωνιακά Συστήματα

3.1.1. ZigBee

Το Zigbee είναι μια ασύρματη τεχνολογία που αναπτύχθηκε ως πρότυπο συνδεσιμότητας ανοικτής παγκόσμιας αγοράς για να καλύψει τις μοναδικές ανάγκες των χαμηλού κόστους και χαμηλής κατανάλωσης ασύρματων δικτύων δεδομένων IoT. Το πρότυπο συνδεσιμότητας Zigbee λειτουργεί με την προδιαγραφή ραδιοφώνου φυσικής πλακέτας IEEE 802.15.4 και λειτουργεί σε ζώνες ραδιοφώνου χωρίς άδεια, συμπεριλαμβανομένων των 2,4 GHz, 900 MHz και 868 MHz [120].

Η ασύρματη προδιαγραφή 802.15.4 βάσει της οποίας λειτουργεί η στοίβα Zigbee κέρδισε την επικύρωση της πλακέτας από το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE) το 2003. Η προδιαγραφή είναι ένα πρωτόκολλο πλακέτας ραδιοφώνου που βασίζεται σε πακέτα και προορίζεται για συσκευές χαμηλού κόστους που λειτουργούν με μπαταρία και προϊόντα. Το πρωτόκολλο επιτρέπει στις συσκευές να επικοινωνούν δεδομένα σε μια ποικιλία τοπολογιών δικτύου και μπορεί να έχουν διάρκεια ζωής της μπαταρίας αρκετά χρόνια [121].

Το πρωτόκολλο Zigbee έχει δημιουργηθεί και επικυρωθεί από εταιρείες-μέλη της Zigbee Board Alliance. Πάνω από 300 κορυφαίοι κατασκευαστές ημιαγωγών, εταιρείες τεχνολογίας, OEM και εταιρείες παροχής υπηρεσιών αποτελούν το συμβούλιο μελών της Zigbee Alliance. Το πρωτόκολλο Zigbee σχεδιάστηκε για να παρέχει μια εύχρηστη λύση ασύρματων δεδομένων που χαρακτηρίζεται από ασφαλείς, αξιόπιστες αρχιτεκτονικές ασύρματων δικτύων [122].

Το πρωτόκολλο Zigbee 3.0 έχει σχεδιαστεί για την επικοινωνία δεδομένων μέσω θορυβωδών περιβαλλόντων ραδιοσυχνοτήτων που είναι κοινά σε εμπορικές και βιομηχανικές εφαρμογές της αγοράς. Η έκδοση 3.0 βασίζεται στο υπάρχον πρότυπο συνδεσιμότητας Zigbee, αλλά ενοποιεί τα ειδικά προφίλ εφαρμογών της αγοράς για να επιτρέπει σε όλες τις συσκευές να συνδέονται ασύρματα στο ίδιο δίκτυο, ανεξάρτητα από την ονομασία και τη λειτουργία τους στην αγορά. Επιπλέον, ένα σύστημα πιστοποίησης Zigbee 3.0 διασφαλίζει τη διαλειτουργικότητα προϊόντων από

διαφορετικούς κατασκευαστές συσκευών. Η σύνδεση των δικτύων Zigbee 3.0 στον τομέα IP ανοίγει την ασύρματη παρακολούθηση και τον έλεγχο από συσκευές ραδιοφώνου όπως smartphone και tablet σε LAN ή WAN, συμπεριλαμβανομένου του Διαδικτύου, και φέρνει στην πράξη το αληθινό Internet of Things [123].

3.1.1.1. Τα χαρακτηριστικά του πρωτοκόλλου Zigbee

Τα χαρακτηριστικά του πρωτοκόλλου Zigbee περιλαμβάνουν:

- Υποστήριξη πολλαπλών τοπολογιών δικτύου, όπως point-to-point, δίκτυα από σημείο σε πολλαπλά σημεία και πλέγμα
- Χαμηλός κύκλος λειτουργίας – παρέχει μεγάλη διάρκεια ζωής της μπαταρίας
- Χαμηλή καθυστέρηση
- Φάσμα εξάπλωσης απευθείας ακολουθίας (DSSS)
- Έως 65.000 κόμβοι ανά δίκτυο
- Κρυπτογράφηση AES 128-bit για ασφαλείς συνδέσεις δεδομένων
- Αποφυγή σύγκρουσης, επαναλήψεις και επιβεβαιώσεις Η στοίβα λογισμικού Zigbee 3.0 ενσωματώνει μια «συσκευή βάσης» που παρέχει συνεπή συμπεριφορά για τη θέση σε λειτουργία κόμβων και συσκευών σε ένα δίκτυο.
- Παρέχεται ένα κοινό σύνολο μεθόδων ανάθεσης, συμπεριλαμβανομένου του Touchlink, μιας μεθόδου εγγύτητας σε λειτουργία [124].

3.1.1.2. Zigbee Wireless Security

Το Zigbee 3.0 παρέχει βελτιωμένη ασφάλεια δικτύου. Υπάρχουν δύο μέθοδοι ασφάλειας που δημιουργούν δύο τύπους δικτύου:

- Κεντρική ασφάλεια: Αυτή η μέθοδος χρησιμοποιεί έναν συντονιστή/κέντρο εμπιστοσύνης που σχηματίζει το δίκτυο και διαχειρίζεται την κατανομή των κλειδιών ασφαλείας του δικτύου και τη σύνδεση με τους κόμβους που συνδέονται.
- Κατανεμημένη ασφάλεια: Αυτή η μέθοδος δεν έχει συντονιστή/κέντρο εμπιστοσύνης και σχηματίζεται από δρομολογητή. Οποιοσδήποτε κόμβος δρομολογητή Zigbee μπορεί στη συνέχεια να παρέχει το κλειδί δικτύου για τη σύνδεση κόμβων.

Οι κόμβοι υιοθετούν οποιαδήποτε μέθοδο ασφαλείας χρησιμοποιείται από το δίκτυο διανομέων στο οποίο εντάσσονται. Το Zigbee 3.0 υποστηρίζει την αυξανόμενη κλίμακα και την πολυπλοκότητα των ασύρματων δικτύων και αντιμετωπίζει μεγάλα τοπικά δίκτυα άνω των 250 κόμβων. Το Zigbee χειρίζεται επίσης τη δυναμική συμπεριφορά αυτών των δικτύων (με τους κόμβους να εμφανίζονται, να εξαφανίζονται και να επανεμφανίζονται στο δίκτυο) και επιτρέπει στους ορφανούς κόμβους, που προκύπτουν από την απώλεια ενός γονέα, να ενταχθούν ξανά στο δίκτυο μέσω διαφορετικού γονέα. Η αυτο-θεραπευτική φύση των δικτύων Zigbee Mesh επιτρέπει επίσης στους κόμβους να εγκαταλείψουν το δίκτυο χωρίς καμία διακοπή στην εσωτερική δρομολόγηση [125].

3.1.1.3. Συμβατότητα πρωτοκόλλου Zigbee

Η συμβατότητα προς τα πίσω του Zigbee 3.0 σημαίνει ότι οι εφαρμογές και οι έξυπνες οικιακές συσκευές που έχουν ήδη αναπτυχθεί στο πλαίσιο του προφίλ Zigbee Light Link 1.0 ή Home Automation 1.2 είναι έτοιμες για το Zigbee 3.0. Το προφίλ Zigbee Smart Energy είναι επίσης συμβατό με το Zigbee 3.0 σε λειτουργικό επίπεδο, αλλά το Smart Energy έχει πρόσθετες απαιτήσεις ασφαλείας που αντιμετωπίζονται μόνο εντός του προφίλ [126]

3.1.1.4. Δεδομένα συσκευής Zigbee

Η δυνατότητα αναβάθμισης Over-The-Air (OTA) του Zigbee για ενημερώσεις λογισμικού κατά τη λειτουργία της συσκευής διασφαλίζει ότι οι εφαρμογές σε συσκευές που έχουν ήδη αναπτυχθεί στο πεδίο/αγορά μπορούν να μετεγκατασταθούν απρόσκοπτα στο Zigbee 3.0. Η αναβάθμιση OTA είναι μια προαιρετική λειτουργία που οι κατασκευαστές ενθαρρύνονται να υποστηρίζουν στο επίπεδο εφαρμογής των προϊόντων Zigbee [126]

3.1.1.5. Zigbee Mesh Networks

Ένα βασικό στοιχείο του πρωτοκόλλου Zigbee είναι η δυνατότητα υποστήριξης δικτύωσης πλέγματος. Σε ένα δίκτυο πλέγματος, οι κόμβοι διασυνδέονται με άλλους κόμβους έτσι ώστε πολλαπλά μονοπάτια να συνδέουν κάθε κόμβο. Οι συνδέσεις μεταξύ των κόμβων ενημερώνονται δυναμικά και βελτιστοποιούνται μέσω εξελιγμένου, ενσωματωμένου πίνακα δρομολόγησης πλέγματος.

Τα δίκτυα πλέγματος έχουν αποκεντρωμένο χαρακτήρα. κάθε κόμβος είναι ικανός να αυτοανακαλύπτεται στο δίκτυο. Επίσης, καθώς οι κόμβοι εγκαταλείπουν το δίκτυο, η τοπολογία πλέγματος επιτρέπει στους κόμβους να διαμορφώνουν εκ νέου τις διαδρομές δρομολόγησης με βάση τη νέα δομή του δικτύου. Τα χαρακτηριστικά της τοπολογίας πλέγματος και της ad-hoc δρομολόγησης παρέχουν μεγαλύτερη σταθερότητα σε μεταβαλλόμενες συνθήκες κυμάτων ή αστοχία σε μεμονωμένους κόμβους [127]

3.1.1.6. Ασύρματες εφαρμογές Zigbee

Το Zigbee επιτρέπει την ανάπτυξη κυμάτων ευρείας βάσης ασύρματων δικτύων με λύσεις χαμηλού κόστους και χαμηλής κατανάλωσης. Παρέχει τη δυνατότητα να λειτουργεί για χρόνια με φθηνές μπαταρίες για μια σειρά από εφαρμογές παρακολούθησης και ελέγχου. Έξυπνο ενεργειακό/έξυπνο δίκτυο, AMR (Automatic Meter Reading), έλεγχοι φωτισμού, συστήματα αυτοματισμού κτιρίων, παρακολούθηση δεξαμενών, έλεγχος HVAC, ιατρικές συσκευές, ραδιόφωνο dbm, ασύρματα πρωτόκολλα ghz, ασύρματα δίκτυα αισθητήρων και εφαρμογές στόλου είναι μόνο μερικοί από τους πολλούς χώρους όπου Η τεχνολογία Zigbee κάνει σημαντικές προόδους [128].

3.1.1.7.Τεχνολογία Digi XBee 3 Zigbee

Η Digi είναι μέλος της Zigbee Alliance και έχει αναπτύξει ένα ευρύ φάσμα λύσεων δικτύωσης δεδομένων που βασίζονται στο πρωτόκολλο Zigbee. Το Digi XBee 3 είναι το πιο πρόσφατο σε μια μακρά σειρά ραδιοφωνικών συσκευών που παρέχουν μια εύκολη στην εφαρμογή λύση που παρέχει λειτουργικότητα για σύνδεση με μεγάλη ποικιλία συσκευών με ισχυρά πρότυπα συνδεσιμότητας [126].

3.1.2. RF Links

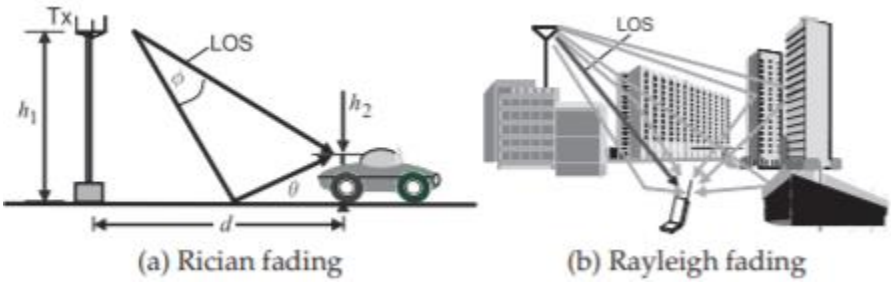
Η σύνδεση RF είναι μεταξύ μιας κεραίας εκπομπής και μιας κεραίας λήψης. Μερικές φορές η σύνδεση RF περιλαμβάνει την κεραία και μερικές φορές όχι, αυτό θα είναι ξεκάθαρο από τα συμφραζόμενα, αλλά συνήθως περιλαμβάνει τις κεραίες. Η βασική πηγή απώλειας συνδέσμου είναι η εξάπλωση του πεδίου EM καθώς διαδίδεται. Ελλείψει άλλων επιπτώσεων (όπως ατμοσφαιρικές απώλειες και αντανακλάσεις), η πυκνότητα ισχύος μειώνεται ως 1/d2, όπου d είναι η απόσταση, και αυτό ονομάζεται κατάσταση οπτικής επαφής (LOS). Σε αυτήν την ενότητα περιγράφεται πρώτα η διαδρομή διάδοσης μαζί με τις βλάβες της, συμπεριλαμβανομένης της διάδοσης σε

πολλαπλές διαδρομές μεταξύ μιας κεραίας εκπομπής και μιας κεραίας λήψης. Περιγράφεται η σκέδαση συντονισμού καθώς και πολλαπλά φαινόμενα εξασθένισης λόγω αντανακλάσεων, περίθλασης, βροχής και άλλων ατμοσφαιρικών επιδράσεων [130].

3.1.2.1. Διαδρομή Διάδοσης

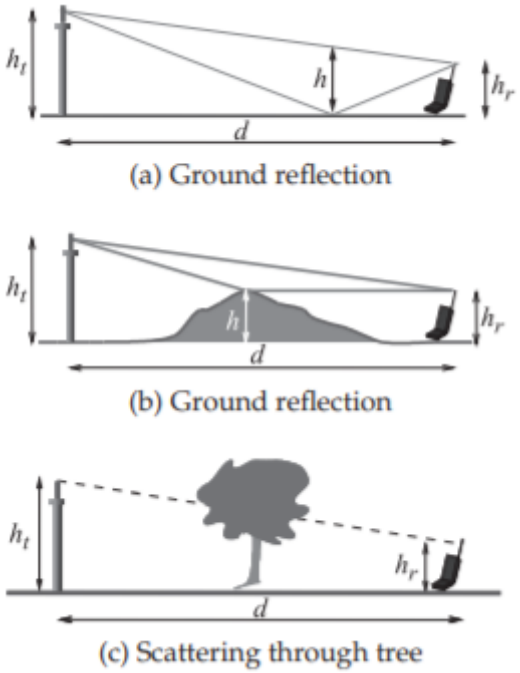
Όταν το ακτινοβολούμενο σήμα ανακλάται υπάρχουν πολλαπλές διαδρομές διάδοσης που έχουν ως αποτέλεσμα αυτό που ονομάζεται εξασθένιση, καθώς οι διαδρομές συνδυάζονται εποικοδομητικά και καταστροφικά στον δέκτη. Η άμεση διαδρομή και άλλες διαδρομές, που ονομάζονται πολλαπλές διαδρομές, οι οποίες ανακλώνται ή διαθλώνται από το έδαφος, τα κτίρια και άλλα αντικείμενα δεν φτάνουν στον δέκτη σε φάση που οδηγεί σε χρονικά μεταβαλλόμενο εποικοδομητικό και καταστροφικό συνδυασμό, που ονομάζεται παρεμβολή πολλαπλών διαδρομών. Από αυτούς ο καταστροφικός συνδυασμός είναι πολύ χειρότερος καθώς μπορεί να μειώσει ένα επίπεδο σήματος κάτω από αυτό που θα ήταν αν η διάδοση ήταν σε ελεύθερο χώρο. Σε αστικές περιοχές, 10 ή 20.Τα μονοπάτια μπορούν να έχουν σημαντική ισχύ σε αυτά και αυτά συνδυάζονται στην κεραία λήψης [6].

Όταν το σήμα σε μία από τις διαδρομές κυριαρχεί, αυτή είναι συνήθως η διαδρομή LOS, η εξασθένηση ονομάζεται Rician fading. Με LOS και μια ενιαία ανάκλαση εδάφους, η κατάσταση είναι η κλασική εξασθένιση του Rician όπως φαίνεται στο σχήμα 10α. Αυτή είναι μια ειδική κατάσταση, καθώς το έδαφος αλλάζει τη φάση του σήματος κατά την ανάκλαση, γενικά κατά 180∘. Όταν ο δέκτης απέχει πολύ από το σταθμό βάσης, τα μήκη των δύο διαδρομών είναι σχεδόν ίδια και το επίπεδο των σημάτων στις δύο διαδρομές είναι σχεδόν το ίδιο. Το καθαρό αποτέλεσμα είναι ότι αυτά τα δύο σήματα σχεδόν ακυρώνονται, και έτσι αντί να πέσει η ισχύς κατά 1/d2, πέφτει κατά 1/d3. Όταν υπάρχουν πολλά μονοπάτια και όλα έχουν παρόμοια σήματα πλάτους, η εξασθένηση ονομάζεται εξασθένιση Rayleigh. Σε μια αστική περιοχή όπως αυτή που φαίνεται στο σχήμα 10β, υπάρχουν πολλές σημαντικές πολλαπλές διαδρομές και η ισχύς μειώνεται κατά 1/d4 και μερικές φορές πιο γρήγορα [131].



Σχήμα 10. Διάδοση πολλαπλών διαδρομών: (α) οπτική γραμμή (LOS) και μονοπάτια ανάκλασης εδάφους μόνο και (β) σε αστικό περιβάλλον[10]

Οι κοινές διαδρομές που συναντώνται στο κυψελοειδές ραδιόφωνο φαίνονται στο σχήμα 11:

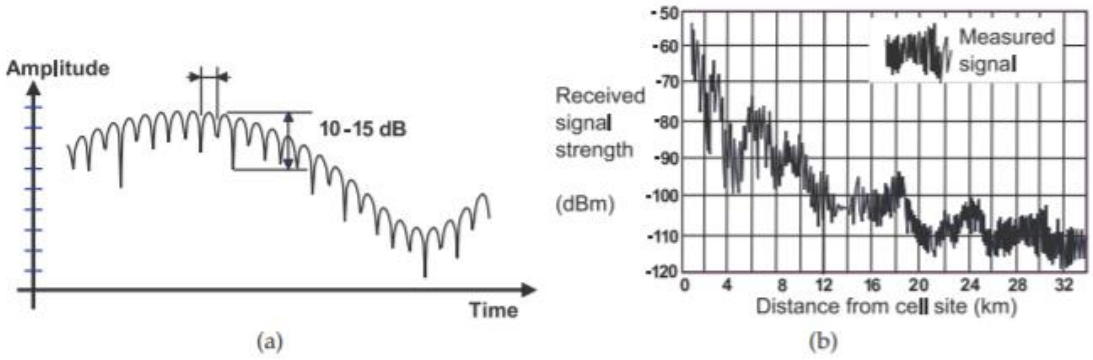


Σχήμα 11. Κοινά μονοπάτια που συμβάλλουν στη διάδοση πολλαπλών διαδρομών[11]

[10] http://artemis.cslab.ece.ntua.gr:8080/jspui/bitstream/123456789/14546/1/DT2006-0063.pdf
[11] http://telematics.upatras.gr/telematics/system/files/bouras_site/ergasies_foithtwn/Babatsikou_thlematiki.pdf

3.1.2.1. Ξεθώριασμα

Το Fading αναφέρεται στη μεταβολή του λαμβανόμενου σήματος με το χρόνο ή όταν αλλάζει η θέση των κεραιών εκπομπής ή λήψης. Η διακύμανση στην ισχύ του σήματος είναι πολύ μεγαλύτερη από ό,τι θα περίμενε κανείς από αλλαγές στη διαδρομή



Σχήμα 12. Γρήγορο και αργό ξεθώριασμα: (α) στο χρόνο καθώς κινείται ο ασύρματος και τα εμπόδια και (β) σε απόσταση[12]

3.1.2.1.1. Επίπεδο ξεθώριασμα

Οι διακυμάνσεις της θερμοκρασίας της ατμόσφαιρας μεταξύ της κεραίας εκπομπής και της κεραίας λήψης προκαλούν αυτό που ονομάζεται επίπεδη εξασθένιση και μερικές φορές ονομάζεται θερμική εξασθένηση. Αυτή η εξασθένιση ονομάζεται επίπεδη επειδή είναι ανεξάρτητη από τη συχνότητα. Μια μορφή επίπεδης εξασθένισης οφείλεται στη διάθλαση, η οποία συμβαίνει όταν διαφορετικά στρώματα της ατμόσφαιρας έχουν διαφορετικές πυκνότητες και επομένως η διηλεκτρική διαπερατότητα αυξάνεται ή μειώνεται μακριά από την επιφάνεια της γης. Το προφίλ θερμοκρασίας μπορεί να αυξηθεί μακριά από την επιφάνεια της γης ή να μειωθεί ανάλογα με το αν η θερμοκρασία της γης είναι υψηλότερη από αυτή του αέρα και συνήθως σχετίζεται με την αρχή και το τέλος της ημέρας. Αναστροφές θερμοκρασίας μπορούν επίσης να συμβούν όπου το προφίλ θερμοκρασίας στον αέρα δεν αυξάνεται ή μειώνεται

12 https://eclass.uth.gr/modules/document/file.php/DS_U_129/%CE%94%CE%B9%CE%B1%CF%86%CE%AC%CE%BD%CE%B5%CE%B9%CE%B5%CF%82%20%CE%BC%CE%B1%CE%B8%CE%AE%CE%BC%CE%B1%CF%84%CE%BF%CF%82/dspTopics.pdf

ομοιόμορφα, προκαλώντας έτσι ένα στρώμα με υψηλότερη διαπερατότητα από αυτό του αέρα πάνω ή κάτω. Η ενέργεια ραδιοσυχνοτήτων παγιδεύεται σε αυτό το στρώμα, αντανακλώντας από το πάνω και το κάτω μέρος του στρώματος αναστροφής. Αυτό ονομάζεται αγωγός. Στα συστήματα επικοινωνίας από σημείο σε σημείο, οι κεραίες εκπομπής και λήψης είναι τοποθετημένες ψηλά σε πύργους και στη συνέχεια η ανάκλαση από τα αντικείμενα του εδάφους είναι συχνά μικρή. Σε τέτοιες περιπτώσεις, το επίπεδο ξεθώριασμα είναι το πιο συχνά παρατηρούμενο φαινόμενο και οι μικρές διακυμάνσεις αρκετών ντεσιμπέλ στη στάθμη του σήματος λήψης είναι συχνές κατά τη διάρκεια της ημέρας. Ωστόσο, όταν οι διακυμάνσεις της θερμοκρασίας είναι ακραίες, ο αγωγός μπορεί να επηρεάσει σοβαρά τις επικοινωνίες μειώνοντας τα επίπεδα σήματος έως και 20 dB [132].

3.1.2.1.2. Ξεθώριασμα σκιάς

Η εξασθένηση της σκιάς εμφανίζεται όταν η διαδρομή LOS μπλοκάρεται από ένα εμπόδιο όπως ένα κτίριο ή ένα λόφο. Η πλήρης ισχύς του σήματος επιστρέφει όταν το εμπόδιο ή ο δέκτης μετακινηθεί για να αποκαταστήσει την άμεση διαδρομή. Το ξεθώριασμα σκιάς ονομάζεται επίσης αργό ξεθώριασμα και το χαρακτηριστικό του καναλιού θεωρείται ότι είναι σχετικά σταθερό σε σύντομο χρονικό διάστημα. Η απόκριση του πλάτους ποικίλλει σε χρόνο και απόσταση και φαίνεται στο Σχήμα 4.6.5 . Αυτό το σχήμα δείχνει τόσο γρήγορες αποσβέσεις με βάθος 10 έως 15 dB όσο και αργές ή σκιώδεις αποσβέσεις που είναι 20 έως 30 dB βαθιές [133].

3.1.2.1.3. Εξασθένιση πολλαπλών διαδρομών

Το ξεθώριασμα πολλαπλών διαδρομών είναι το πιο συνηθισμένο ξεθώριασμα όταν είτε η κεραία εκπομπής είτε η κεραία λήψης βρίσκονται κοντά στο έδαφος, κοντά σε κτίρια ή εδάφη που εμποδίζουν ή μέσα σε ένα κτίριο. Σε τέτοιες καταστάσεις υπάρχουν πολλοί προβληματισμοί που συνδυάζονται καταστροφικά και εποικοδομητικά. Η εξασθένηση πολλαπλών διαδρομών ονομάζεται επίσης γρήγορη εξασθένηση, καθώς τα χαρακτηριστικά του καναλιού μπορούν να αλλάξουν σημαντικά σε λίγα χιλιοστά του δευτερολέπτου. Θα ληφθούν υπόψη δύο τύποι εξασθένισης πολλαπλών διαδρομών—εξασθένιση Rician και εξασθένιση Rayleigh—θα ληφθούν υπόψη.

Η πολλαπλή διαδρομή είναι κυρίως πρόβλημα όταν η οπτική γωνία μεταξύ της κεραίας εκπομπής και λήψης είναι ασαφής. Ωστόσο, όπου υπάρχει οπτική επαφή, το σήμα που

αντανακλάται από το έδαφος αμέσως μπροστά από μια κεραία λήψης μπορεί μερικές φορές να ακυρώσει σε μεγάλο βαθμό το σήμα οπτικής επαφής. Με τον καιρό, τα αντικείμενα που παρεμβάλλονται μπορούν να μετακινηθούν και τα χαρακτηριστικά διάδοσης των διαφόρων μονοπατιών μπορούν να αλλάξουν λόγω θερμικών διακυμάνσεων. Όλα αυτά προσθέτουν στην τυχαιότητα των fast fades. Εξασθένιση πολλαπλών διαδρομών 20 dB μπορεί να συμβεί για ένα μικρό ποσοστό του χρόνου σε χρονικές κλίμακες πολλών δευτερολέπτων όταν υπάρχουν λίγα μονοπάτια διάδοσης (π.χ. σε μια αγροτική περιοχή) έως ένα μεγάλο ποσοστό του χρόνου πολλές φορές ανά δευτερόλεπτο σε ένα πυκνό αστικό περιβάλλον όταν υπάρχουν πολλά μονοπάτια. Ο εποικοδομητικός συνδυασμός αυξάνει το επίπεδο σήματος στιγμιαία, αλλά δεν υπάρχει κανένα πλεονέκτημα σε αυτό. Ο καταστροφικός συνδυασμός μπορεί να οδηγήσει σε βαθιές διαλείψεις των 20 dB, επηρεάζοντας τις επικοινωνίες και αναγκάζοντας το σύστημα επικοινωνίας να προσαρμοστεί είτε χρησιμοποιώντας υψηλότερες μέσες δυνάμεις είτε χρησιμοποιώντας στρατηγικές όπως πολλαπλές κεραίες ή διασπορά του σήματος επικοινωνίας σε μεγάλο εύρος ζώνης, καθώς οι εξασθενίσεις τείνουν να είναι 500 kHz έως 1 Εύρος MHz σε όλες τις συχνότητες [134].

3.1.3. Bluetooth

Εφευρέθηκε από την Ericsson το 1994, το Bluetooth προοριζόταν να ενεργοποιήσει ασύρματα ακουστικά. Έκτοτε, το Bluetooth έχει επεκταθεί σε μια ευρεία ποικιλία εφαρμογών, όπως ακουστικά Bluetooth, ηχεία, εκτυπωτές, ελεγκτές βιντεοπαιχνιδιών και πολλά άλλα.

Το Bluetooth είναι επίσης σημαντικό για το ταχέως αναπτυσσόμενο Internet of Things, συμπεριλαμβανομένων των έξυπνων κατοικιών και των βιομηχανικών εφαρμογών. Είναι μια επιλογή συνδεσιμότητας χαμηλής ισχύος, χαμηλής εμβέλειας και υψηλού εύρους ζώνης. Όταν οι συσκευές Bluetooth συνδέονται μεταξύ τους (για παράδειγμα, το τηλέφωνό σας και το ασύρματο ηχείο σας), ακολουθεί το μοντέλο γονέα-παιδιού, που σημαίνει ότι μια συσκευή είναι ο γονέας και οι άλλες συσκευές είναι τα παιδιά. Ο γονέας μεταδίδει πληροφορίες στο παιδί και το παιδί ακούει πληροφορίες από τον γονέα. Ένας γονέας Bluetooth μπορεί να έχει έως και 7 παιδιά, γι' αυτό ο υπολογιστής σας μπορεί να συνδεθεί μέσω Bluetooth σε πολλές συσκευές ταυτόχρονα. Όταν οι συσκευές συνδέονται μεταξύ τους μέσω Bluetooth, ονομάζεται "piconet".

Όχι μόνο μια συσκευή μπορεί να είναι γονέας σε ένα piconet και παιδί σε διαφορετικό piconet ταυτόχρονα, αλλά η σχέση γονέα-παιδιού μπορεί επίσης να αλλάξει. Όταν βάζετε τη συσκευή σας Bluetooth σε λειτουργία σύζευξης για να τη συνδέσετε, γίνεται προσωρινά ο γονέας, ώστε να μπορεί να δημιουργήσει μια σύνδεση και να συνεχίσει να συνδέεται ως παιδί [135].

Σε αντίθεση με το WiFi, το οποίο εξερευνήσαμε στο προηγούμενο κεφάλαιο, το Bluetooth προοριζόταν για φορητό εξοπλισμό και σχετικές εφαρμογές, επομένως υπερέχει όταν χρειάζεται να συνδέσετε δύο συσκευές με ελάχιστη διαμόρφωση. Επίσης, επειδή το Bluetooth χρησιμοποιεί αδύναμα σήματα, υπάρχουν περιορισμένες παρεμβολές και οι συσκευές μπορούν να επικοινωνούν σε περιβάλλοντα "θορυβώδους" [132].

Στο Βιομηχανικό Διαδίκτυο των Πραγμάτων, οι μηχανές χρειάζεται συχνά να στέλνουν σύντομες εκρήξεις δεδομένων σε εξαιρετικά θορυβώδη περιβάλλοντα. Με δυνητικά εκατοντάδες αισθητήρες και συσκευές που στέλνουν δεδομένα, το WiFi δημιουργεί υπερβολική ταλαιπωρία για τη ρύθμιση. Ένα μειονέκτημα του Bluetooth είναι το χαμηλότερο εύρος ζώνης, αλλά για πολλές βιομηχανικές εφαρμογές αυτό το υψηλότερο εύρος ζώνης απλά δεν χρειάζεται. Το Bluetooth είναι επίσης χρήσιμο σε μια ρύθμιση έξυπνου σπιτιού. Και πάλι, πολλές συσκευές στο έξυπνο σπίτι δεν χρειάζονται συνδέσεις υψηλού εύρους ζώνης και είναι πολύ πιο εύκολο να ρυθμίσετε το Bluetooth [136].

Επιπλέον, οι νεότερες εκδόσεις του Bluetooth μπορούν να δημιουργήσουν ένα αυτο-θεραπευόμενο δίκτυο πλέγματος, το οποίο σημαίνει ότι μεμονωμένες συσκευές μπορούν ακόμα να επικοινωνούν ακόμα και αν μια συσκευή εξαντληθεί ή αποσυνδεθεί. Εάν οι κλειδαριές της πόρτας, το σύστημα HVAC, το πλυντήριο, το στεγνωτήριο, το ψυγείο και τα φώτα είναι όλα συνδεδεμένα, σίγουρα δεν θα θέλατε να χαλάσουν όλα μόνο και μόνο επειδή πέσει το ένα [137]

3.1.3.1. Bluetooth Έκδοση 5

Η Ομάδα Ειδικού Ενδιαφέροντος Bluetooth υιοθέτησε επίσημα το Bluetooth 5 ως την τελευταία έκδοση του Bluetooth τον Δεκέμβριο του 2016. «Με το Bluetooth 5, το Bluetooth συνεχίζει να φέρνει επανάσταση στον τρόπο με τον οποίο οι άνθρωποι

βιώνουν το IoT. Το Bluetooth συνεχίζει να αγκαλιάζει τις τεχνολογικές εξελίξεις και να ωθεί τις απεριόριστες δυνατότητες του IoT».

Όπως είναι σαφές από την ανακοίνωση της Bluetooth SIG, το Bluetooth 5 στοχεύει ειδικά στο Internet of Things. Διαθέτει τετραπλάσια εμβέλεια, διπλάσια ταχύτητα και ενισχύει την ικανότητα μετάδοσης μηνυμάτων κατά 800%. Εισάγει επίσης τη δυνατότητα δικτύωσης πλέγματος που αναφέρθηκε παραπάνω.

Το Bluetooth 5 είναι συμβατό με τις προηγούμενες εκδόσεις του Bluetooth, αλλά απαιτείται νέο υλικό για να επωφεληθείτε από τα νέα πλεονεκτήματα που αναφέρονται παραπάνω. Μπορεί λοιπόν να χρειαστεί λίγος χρόνος μέχρι να δούμε όλα τα πλεονεκτήματα που έχει να προσφέρει το Bluetooth 5, αλλά είναι μια συναρπαστική εξέλιξη καθώς το Internet of Things συνεχίζει να κερδίζει έδαφος [138].

Εκτός από τις δυνατότητες που εξερευνήθηκαν παραπάνω, το Bluetooth μπορεί επίσης να παρέχει παρακολούθηση περιουσιακών στοιχείων σε εσωτερικούς χώρους χρησιμοποιώντας πολλαπλούς φάρους Bluetooth και χρησιμοποιώντας τη σχετική ισχύ του σήματος για τον τριγωνισμό της θέσης. Το GPS είναι εξαιρετικό για εφαρμογές εξωτερικού χώρου, αλλά έχει εγγενείς περιορισμούς ακρίβειας και αποτυγχάνει σε εσωτερικούς χώρους όταν οι αισθητήρες/συσκευές δεν μπορούν να λάβουν το σήμα από τους δορυφόρους GPS.

Μαζί με τα πλεονεκτήματα σε θορυβώδη περιβάλλοντα και την ευκολία εγκατάστασης, το Bluetooth είναι επομένως μια ισχυρή επιλογή για πολλές εφαρμογές Internet of Things εσωτερικού χώρου [139].

3.1.3.2. Bluetooth 4.0 LE

Όπως αναφέρθηκε προηγουμένως, το Bluetooth Low Energy ή το Bluetooth 4.0 κυκλοφόρησε στην αγορά το 2011. Όταν μιλάμε για Bluetooth Low Energy έναντι Bluetooth, η βασική διαφορά έγκειται στην ικανότητα χαμηλής κατανάλωσης ενέργειας του Bluetooth LE. Με χαμηλή κατανάλωση ενέργειας, οι εφαρμογές μπορούν να λειτουργούν με μια μικρή μπαταρία για μεγαλύτερο χρονικό διάστημα. Αν και αυτό δεν είναι ιδανικό για να μιλάτε στο τηλέφωνο, είναι ζωτικής σημασίας για εφαρμογές που ανταλλάσσουν περιοδικά μικρές ποσότητες δεδομένων [140].

3.1.4. Εφαρμογές Bluetooth Low Energy M2M και IoT

Παρόμοια με το Bluetooth, το Bluetooth LE λειτουργεί στη ζώνη των 2,4 GHz. Η κρυφή διαφορά είναι ότι το Bluetooth Low Energy παραμένει σε κατάσταση αναστολής λειτουργίας εκτός εάν ξεκινήσει μια σύνδεση. Οι πραγματικοί χρόνοι σύνδεσης διαρκούν μόνο μερικά χιλιοστά του δευτερολέπτου, σε αντίθεση με το Bluetooth, το οποίο συνδέεται για λίγα δευτερόλεπτα ή μερικές ώρες τη φορά. Αυτές οι σύντομες συνδέσεις είναι απαραίτητες επειδή οι ρυθμοί δεδομένων είναι σημαντικά υψηλότεροι (1 Mb ανά δευτερόλεπτο). Ακολουθούν ορισμένα κοινά παραδείγματα συσκευών που χρησιμοποιούν Bluetooth LE:

- Παρακολούθηση αρτηριακής πίεσης
- Συσκευές Fitbit
- Βιομηχανικοί αισθητήρες παρακολούθησης
- Στοχευμένες προωθήσεις με βάση τη γεωγραφία
- Εφαρμογές δημόσιας συγκοινωνίας
- Άλλες διάφορες εφαρμογές IoT [141].

Οι λύσεις Bluetooth μπορούν να εφαρμοστούν τόσο σε περιπτώσεις καταναλωτικής όσο και σε εμπορική χρήση. Οι περισσότεροι καταναλωτές έχουν πρόσβαση σε Bluetooth και Bluetooth Low Energy καθημερινά χωρίς καν να το συνειδητοποιούν – και οι εμπορικές βιομηχανίες αρχίζουν επίσης να κάνουν το ίδιο. Από το 2011, το Bluetooth συνέχισε να κάνει αναθεωρήσεις και βελτιώσεις. Μια σημαντική αλλαγή σημειώθηκε το 2016 όταν το Bluetooth 5.0 αύξησε σημαντικά την εμβέλεια, την ταχύτητα και τη χωρητικότητα δεδομένων. Το 2020 η Ομάδα Ειδικού Ενδιαφέροντος Bluetooth (SIG) εισήγαγε τον ήχο χαμηλής ενέργειας Bluetooth. Αυτή η τεχνολογία επιτρέπει σε μια συσκευή να μοιράζεται ήχο με πολλές άλλες συσκευές. Για παράδειγμα, ένα smartphone μπορεί να μοιράζεται ήχο με πολλά ακουστικά ταυτόχρονα. Αν και αυτή η περίπτωση χρήσης απευθύνεται στην καταναλωτική αγορά, είναι ένα άλλο παράδειγμα του πώς αυτή η τεχνολογία ασύρματης επικοινωνίας συνεχίζει να αναπτύσσεται. Δεν θα αργήσει να γίνει πραγματικότητα οι εφαρμογές για το Bluetooth 6.0. [142].

3.1.5. Bluetooth έναντι Bluetooth χαμηλής ενέργειας – Η διαφορά του IoT

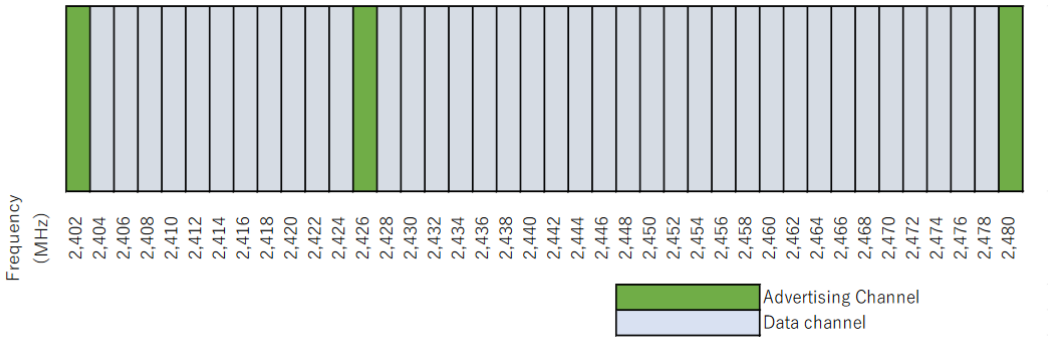
Συνοπτικά, το Bluetooth και το Bluetooth Low Energy είναι παρόμοια καθώς βοηθούν τους χρήστες να συνδέονται με τις πιο αγαπημένες και σημαντικές συσκευές τους τόσο για καταναλωτική όσο και για εμπορική χρήση. Η διαφορά έγκειται στον τρόπο διανομής των δεδομένων για εξοικονόμηση ενέργειας. Το Bluetooth μπορεί να χειριστεί πολλά δεδομένα, αλλά καταναλώνει γρήγορα τη διάρκεια ζωής της μπαταρίας και κοστίζει πολύ περισσότερο. Το Bluetooth Low Energy χρησιμοποιείται για εφαρμογές που δεν χρειάζονται ανταλλαγή μεγάλων ποσοτήτων δεδομένων και μπορούν να λειτουργούν με μπαταρία για χρόνια με φθηνότερο κόστος [143].

3.2. Δίκτυο περιοχής (WPAN)

Τα WPAN διαθέτουν ανταλλαγή δεδομένων σε απόσταση 10 περίπου μέτρων καταναλώνει πολύ λιγότερη ενέργεια από οποιαδήποτε άλλη ασύρματη τεχνολογία. Διάφοροι τύποι WPAN

είναι διαθέσιμα; Το ZigBee® και το Bluetooth είναι τα δύο κύρια τυποποιημένα ασύρματα δίκτυα, ενώ υπάρχουν και πολλά ανεξάρτητα, μη τυποποιημένα πρωτόκολλα επικοινωνίας διαθέσιμος. Το Bluetooth Low Energy χρησιμοποιείται σε πολλές εφαρμογές smartphone, γεγονός που το καθιστά η πιο ευρέως χρησιμοποιούμενη μορφή στην αγορά. Όταν συζητάτε για την τεχνολογία επικοινωνίας Bluetooth χαμηλής ενέργειας, είναι σημαντικό να να θυμάστε ότι αυτή η ασύρματη τεχνολογία Bluetooth δεν είναι η ίδια προδιαγραφή με την ασύρματη τεχνολογία Bluetooth που αναφέρεται στις συμβατικές φωνητικές επικοινωνίες. Bluetooth. Η τεχνολογία χαμηλής ενέργειας λειτουργεί σε ζώνη 80 MHz με εύρος από 2.400 GHz έως 2.480GHz και χωρίζεται σε 40 κανάλια με απόσταση 2MHz [144]. Υπάρχουν δύο τύποι καναλιών:

- Διαφημιστικά κανάλια: 3
- Κανάλια δεδομένων: 37



Σχήμα 12. Bluetooth Κανάλια Επικοινωνίας Συχνότητας Χαμηλής Ενέργειας[13]

Οι δύο τύποι καναλιών χρησιμοποιούνται ως εξής:

Οι περιφερειακές συσκευές στέλνουν διαφημιστικά πακέτα στα διαφημιστικά κανάλια. Η διαφήμιση το πακέτο εκπέμπει (μεταδίδει) τη θέση της συσκευής του σε άλλες συσκευές της περιοχής μέσω τριών διαφορετικά κανάλια σε διαφημιστικά διαστήματα. Στη συνέχεια ανιχνεύει και συνδέεται ασύρματα με άλλους

Συσκευές χαμηλής ενέργειας Bluetooth. Το διάστημα διαφήμισης είναι μεταξύ 20 χιλιοστών του δευτερολέπτου και 10,24 δευτερόλεπτα, όπως ορίζεται στις προδιαγραφές Bluetooth. Το μήκος του διαστήματος επηρεάζει την ευκολία της σύνδεσης και την ποσότητα ισχύος που καταναλώνεται [145].

Τα κανάλια δεδομένων χρησιμοποιούνται για επικοινωνία μεταξύ συσκευών μετά τη σύνδεση ολοκληρώθηκε το. Με το Bluetooth Low Energy, τα κανάλια δεδομένων χρησιμοποιούν Adaptive Frequency Hopping (AFH) για ισχυρή επικοινωνία στην οποία η μετάδοση αλλάζει από κανάλι σε κανάλι με βάση το διάστημα σύνδεσης. Ο όρος "προσαρμοστικό" χρησιμοποιείται για να υποδείξει την εναλλαγή καναλιού για την εξουδετέρωση των παρεμβολών συχνότητας. Το Bluetooth Low Energy εφαρμόζει επίσης ένα χρονικό όριο αναμονής, εφαρμογή hopping για να εξασφαλιστεί η συνεχής επικοινωνία ακόμη και όταν, για παράδειγμα,

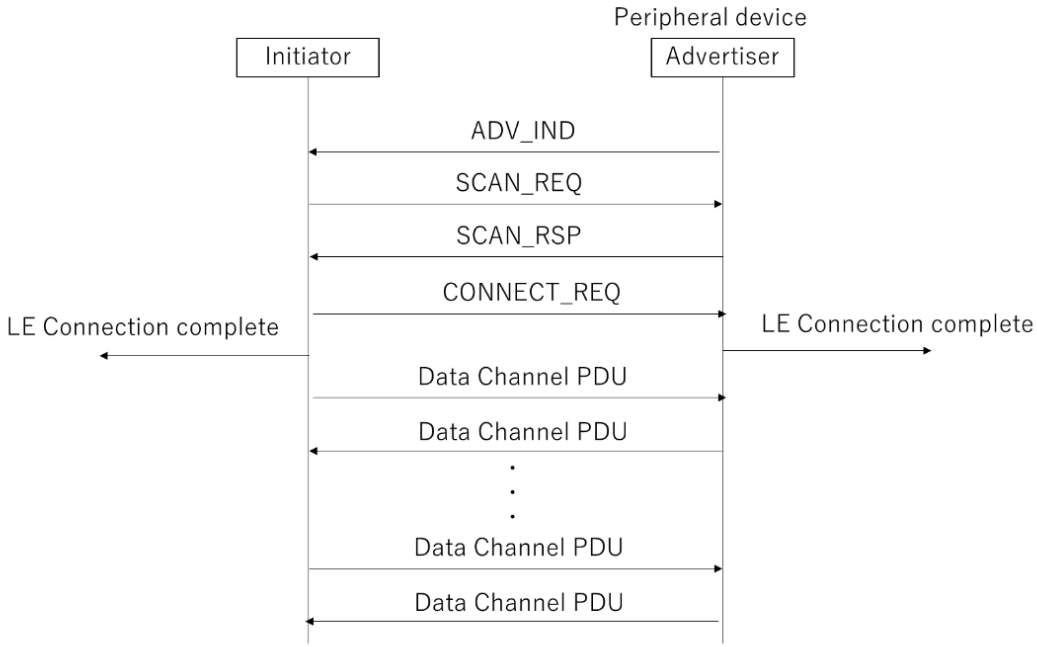
13 http://artemis.cslab.ece.ntua.gr:8080/jspui/bitstream/123456789/17494/1/%CE%B4%CE%B9%CF%80%CE%BB%CF%89%CE%BC%CE%B1%CF%84%CE%B9%CE%BA%CE%AE%20%CE%94%CE%AE%CE%BC%CE%BF%CF%82%20%CE%9A%CF%89%CE%BD%CF%83%CF%84%CE%B1%CE%BD%CF%84%CE%AF%CE%BD%CE%BF%CF%82%20%20%CE%9F%CE%BA%CF%84%CF%8E%CE%B2%CF%81%CE%B9%CE%BF%CF%82%202019.pdf

Η επικοινωνία θα διακοπεί διαφορετικά λόγω πολλαπλών μεταδόσεων. Χαμηλό Bluetooth Η ενεργειακή επικοινωνία είναι δομημένη έτσι ώστε οι επικοινωνίες να μην διακόπτονται ακόμη και όταν ορισμένα κανάλια παρουσιάζουν παρεμβολές. Οι προδιαγραφές Bluetooth καθορίζουν τη σύνδεση [146].

Οι δύο τύποι καναλιών χρησιμοποιούνται ως εξής:

Οι περιφερειακές συσκευές στέλνουν διαφημιστικά πακέτα στα διαφημιστικά κανάλια. Η διαφήμιση το πακέτο εκπέμπει (μεταδίδει) τη θέση της συσκευής του σε άλλες συσκευές της περιοχής μέσω τριών διαφορετικά κανάλια σε διαφημιστικά διαστήματα. Στη συνέχεια ανιχνεύει και συνδέεται ασύρματα με άλλους Συσκευές χαμηλής ενέργειας Bluetooth. Το διάστημα διαφήμισης είναι μεταξύ 20 χιλιοστών του δευτερολέπτου και 10,24 δευτερόλεπτα, όπως ορίζεται στις προδιαγραφές Bluetooth. Το μήκος του διαστήματος επηρεάζει την ευκολία της σύνδεσης και την ποσότητα ισχύος που καταναλώνεται. Τα κανάλια δεδομένων χρησιμοποιούνται για επικοινωνία μεταξύ συσκευών μετά τη σύνδεση ολοκληρώθηκε το. Με το Bluetooth Low Energy, τα κανάλια δεδομένων χρησιμοποιούν Adaptive Frequency Hopping (AFH) για ισχυρή επικοινωνία στην οποία η μετάδοση αλλάζει από κανάλι σε κανάλι με βάση το διάστημα σύνδεσης. Ο όρος "προσαρμοστικό" χρησιμοποιείται για να υποδείξει την εναλλαγή καναλιού για την εξουδετέρωση των παρεμβολών συχνότητας. Το Bluetooth Low Energy εφαρμόζει επίσης ένα χρονικό όριο αναμονής, εφαρμογή hopping για να εξασφαλιστεί η συνεχής επικοινωνία ακόμη και όταν, για παράδειγμα, Η επικοινωνία θα διακοπεί διαφορετικά λόγω πολλαπλών μεταδόσεων.

Η ενεργειακή επικοινωνία είναι δομημένη έτσι ώστε οι επικοινωνίες να μην διακόπτονται ακόμη και όταν ορισμένα κανάλια παρουσιάζουν παρεμβολές. Οι προδιαγραφές Bluetooth ορίζουν τη χρονική περίοδο σύνδεσης από 7,5 χιλιοστά του δευτερολέπτου έως τέσσερα δευτερόλεπτα. Η διάρκεια του διαστήματος επηρεάζει την απόδοση και την κατανάλωση ενέργειας [147].



Σχήμα 13. Παράδειγμα Λειτουργικής Ροής Χαμηλής Ενέργειας Bluetooth[14]

Οι μεταδόσεις δεδομένων Bluetooth μπορούν να κρυπτογραφηθούν. Για να ενεργοποιήσετε τις κρυπτογραφημένες μεταδόσεις, πρώτα μοναδικές πληροφορίες ανταλλάσσονται μεταξύ δύο συσκευών, μια διαδικασία που αναφέρεται ως "σύζευξη". Η σύζευξη οδηγεί σε «δέσμευση», όπου ανταλλάσσονται μοναδικές πληροφορίες ασφάλειας και αναγνώρισης και αποθηκεύονται. Με άλλα λόγια, οι συσκευές αντιστοιχίζονται ανταλλάσσοντας χαρακτηριστικά ασφαλείας και στη συνέχεια συνδέεται με την αποθήκευση της συσκευής και τη σύζευξη πληροφοριών που ανταλλάσσονται από τις συσκευές [148].

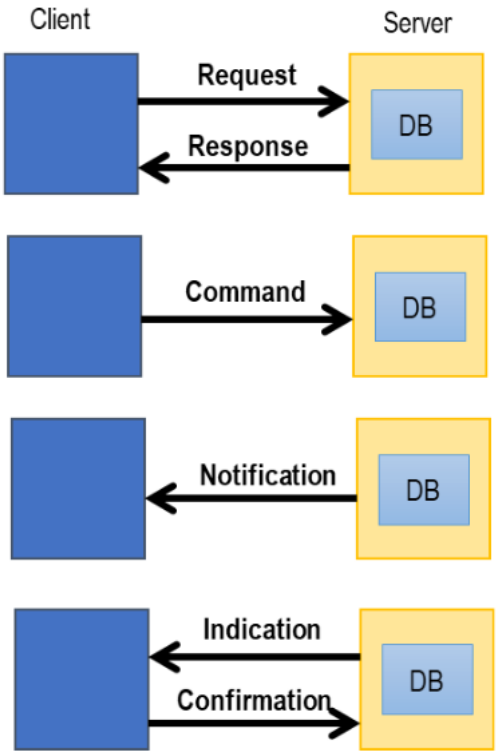
Οι απαιτήσεις ασφάλειας Bluetooth Low Energy περιγράφονται με τους όρους "λειτουργία ασφαλείας" και «επίπεδο ασφαλείας». Απαιτείται σύζευξη για την ικανοποίηση κάθε απαίτησης ασφάλειας. Υπάρχουν δύο τύποι σύζευξης: πιστοποιημένη σύζευξη, η οποία προστατεύει από το Man-in-the-Middle (MITM) επιθέσεις και μη επιβεβαιωμένη σύζευξη, η οποία δεν προστατεύει από τέτοιες

[14] http://gr.feasyblue.com/ble-module/bluetooth-5-ble-module/bluetooth-low-energy-chip.html

επιθέσεις Λευκή Βίβλος — Τεχνολογία χαμηλής ενέργειας Bluetooth® που ζωντανεύει το IoT [149]

Το Bluetooth Low Energy χρησιμοποιεί τέσσερις τύπους σύζευξης, όπως περιγράφεται εδώ.

- Εισαγωγή κωδικού πρόσβασης: Σύζευξη με βάση την εισαγωγή ενός 6ψήφιου κωδικού ελέγχου ταυτότητας. Αυτό είναι το LE
- Λειτουργία ασφαλείας 1 Επίπεδο 3; πιστοποιημένη ταυτότητα και προστασία MITM.
- Εκτός ζώνης (OOB): Σύζευξη με τύπους επικοινωνίας διαφορετικούς από Bluetooth (ενσύρματο, NFC, κ.λπ.) Αυτό είναι LE Security Mode 1 Level 3. πιστοποιημένη ταυτότητα και προστασία MITM.
- Αριθμητική σύγκριση: Σύζευξη που είναι ίδια με το «Just Works», αλλά με προσθήκη βήμα στο οποίο κάθε συσκευή δημιουργεί και εμφανίζει έναν 6ψήφιο κωδικό, που απαιτεί αντιστοίχιση να επιβεβαιωθεί. Αυτή η μέθοδος μπορεί να χρησιμοποιηθεί μόνο για Ασφαλείς Συνδέσεις LE που προστέθηκαν στο Bluetooth 4.2.



Σχήμα 13. Η προδιαγραφή ανταλλαγής δεδομένων Bluetooth Low Energy περιγράφηκε νωρίτερα λεπτομερώς.[15]

Η αρχική ιδέα του Bluetooth Low Energy, όπως υποδεικνύεται από το όνομά του, ήταν να παρέχει χαμηλή ενέργεια λειτουργίες κατανάλωσης ενέργειας. Για να γίνει αυτό, ήταν πιο αποτελεσματικό να αποστέλλονται μικρές ποσότητες δεδομένα. Αυτή η ιδέα επέκτεινε τη διάρκεια ζωής των μπαταριών, επιτρέποντας τη χρήση για αρκετά χρόνια χωρίς αντικατάσταση. Ο στόχος ήταν η χρήση συνδέσεων Bluetooth για τη σύνδεση συσκευών χαμηλής κατανάλωσης και εφαρμογές που λειτουργούν με μπαταρία και, στη συνέχεια, μεταδώστε τα δεδομένα μέσω σύνδεσης στο Διαδίκτυο.

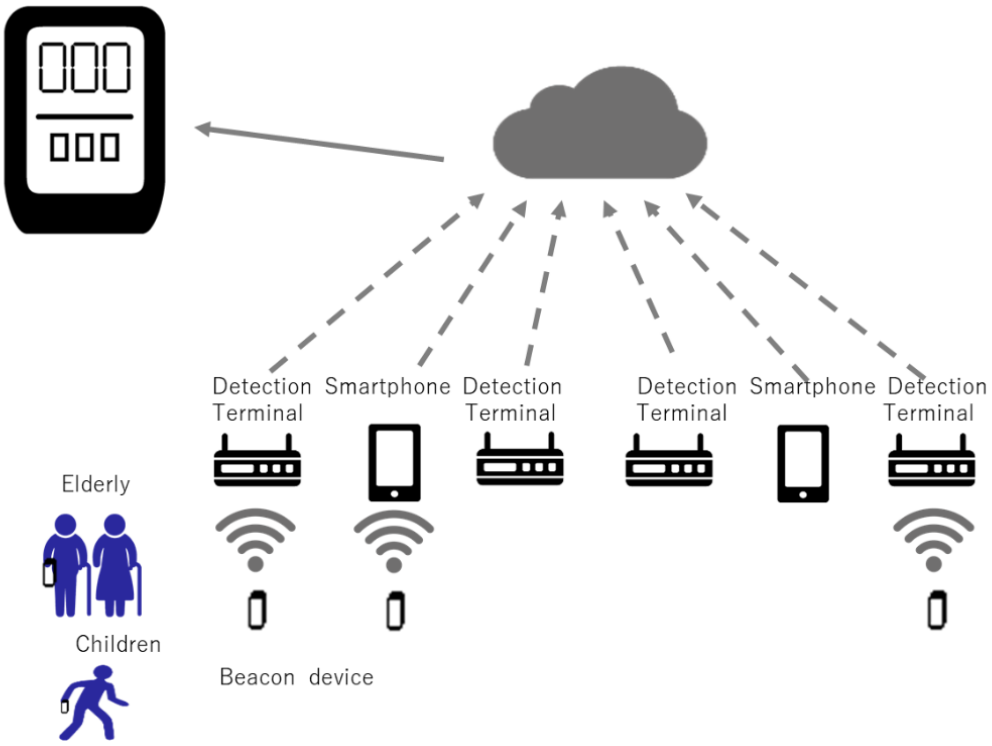
Πρόσφατα, το Bluetooth Low Energy στην προδιαγραφή Bluetooth αναθεωρήθηκε με βάση Bluetooth 4.0. Η προδιαγραφή πρόσθεσε μεγάλη χωρητικότητα, επικοινωνίες υψηλής ταχύτητας και τηλεπικοινωνίες μεγάλων αποστάσεων. Το Bluetooth 5 κυκλοφόρησε το 2016 με αυτές τις δυνατότητες προσφέρονται ως επιλογές. Στο μέλλον, το βασικό πρότυπο του Bluetooth Low Energy (όπως καθιερώθηκε στο Bluetooth 4.0) θα είναι μια απαιτούμενη λειτουργία και θα υποστηρίζει όλα τα έτοιμα προϊόντα χαμηλής κατανάλωσης Bluetooth. Χρησιμοποιώντας αυτή η προδιαγραφή πυρήνα χαμηλής ενέργειας Bluetooth θα εξασφαλίσει αξιόπιστες συνδέσεις και ως εκ τούτου, να εφαρμοστεί σε μια πληθώρα συσκευών στο μέλλον. Μπορούμε επίσης να περιμένουμε Bluetooth Low Energy για αποφυγή προβλημάτων συνδεσιμότητας.

Ας προχωρήσουμε σε μερικά δείγματα εφαρμογών. Αρχικά, εξετάζουμε μια συσκευή φάρου που δίνει ζωή σε μια εφαρμογή μεταδίδοντας ένα διαφημιστικό πακέτο, μια δυνατότητα που δεν είναι διαθέσιμη σε συμβατικό Bluetooth.

Οι συσκευές Beacon χρησιμοποιούνται συχνά ως εντοπιστές που μεταφέρονται από ηλικιωμένους ή μικρά παιδιά. ΕΝΑ Το τερματικό ανίχνευσης είναι εγκατεστημένο σε μια σχετική εγκατάσταση για τη λήψη ραδιοκυμάτων από το beacon συσκευή. Τερματικά ανίχνευσης θα πρέπει, για παράδειγμα, να εγκατασταθούν σε σχολεία για παιδιά και κοινοτικά κέντρα για ηλικιωμένα μέλη, καθώς και στο σπίτι και σε άλλους δημόσιους χώρους. Ένα άλλο παράδειγμα θα ήταν να έχετε τοπικούς εθελοντές να μεταφέρουν ένα smartphone εγκατεστημένο με ειδική εφαρμογή που επιτρέπει στο

[15] https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/9207/Tzanidakis_Marios.pdf?sequence=1&isAllowed=y

smartphone να λαμβάνει ραδιοκύματα από το συσκευή φάρου. Οι λαμβανόμενες πληροφορίες beacon αποθηκεύονται στο cloud μαζί με το πληροφορίες θέσης του τερματικού εντοπισμού ή του smartphone. Τα αποθηκευμένα δεδομένα χρησιμοποιούνται στη συνέχεια υποδεικνύουν τη θέση του φάρου σε έναν χάρτη smartphone, τον οποίο μόνο μέλη της οικογένειας ή κηδεμόνες που συνδέεται με τη συσκευή beacon μπορεί να έχει πρόσβαση. Χρήση Bluetooth Low Energy σε συσκευή beacon επιτρέπει στους φροντιστές να προσέχουν και να προστατεύουν τις χρεώσεις τους, ακόμη και όταν δεν βρίσκονται στο ίδια γειτονιά [150].



Σχήμα 14. Protective Locator Terminal[16]

3.3. 6LoWPAN

Το σύστημα 6LoWPAN χρησιμοποιείται για μια ποικιλία εφαρμογών, συμπεριλαμβανομένων των ασύρματων δικτύων αισθητήρων. Αυτή η μορφή ασύρματου δικτύου αισθητήρων στέλνει δεδομένα ως πακέτα και χρησιμοποιώντας IPv6 - παρέχοντας τη βάση για το όνομα - IPv6 μέσω ασύρματων δικτύων προσωπικής περιοχής χαμηλής ισχύος.

[16] https://www.semanticscholar.org/paper/A-protection-strategy-for-fault-detection-and-for-Monadi-Koch-Ciobotaru/6b5f260942d42532f6bf9e945e53963e9058d62b

Το 6LoWPAN παρέχει ένα μέσο μεταφοράς δεδομένων πακέτων με τη μορφή IPv6 μέσω του IEEE 802.15.4 και άλλων δικτύων. Παρέχει IPv6 από άκρο σε άκρο και ως εκ τούτου είναι σε θέση να παρέχει άμεση συνδεσιμότητα σε μια τεράστια ποικιλία δικτύων, συμπεριλαμβανομένης της άμεσης σύνδεσης με το Διαδίκτυο. Με αυτόν τον τρόπο, το 6LoWPAN υιοθετεί μια διαφορετική προσέγγιση από τις άλλες λύσεις ασύρματου δικτύου αισθητήρων χαμηλής ισχύος 6LoWPAN και IETF [49].

Το 6LoWPAN είναι ένα ανοιχτό πρότυπο που ορίζεται από την Ομάδα Εργασίας Μηχανικής Διαδικτύου, το IETF στο έγγραφό τους RFC 6282. Το IETF είναι το σώμα προτύπων που ορίζει πολλά από τα ανοιχτά πρότυπα που χρησιμοποιούνται στο Διαδίκτυο, συμπεριλαμβανομένων των HTTP, TCP, UDP και πολλών άλλων [50]

Ενώ το 6LoWPAN σχεδιάστηκε αρχικά για να βασίζεται στο IEEE 802.15.4, ένα πρότυπο που καθόριζε τα κατώτερα επίπεδα για ένα ασύρματο σύστημα χαμηλής ισχύος 2,4 GHz, τώρα αναπτύσσεται και προσαρμόζεται για να λειτουργεί με πολλούς άλλους φορείς ασύρματου δικτύου, συμπεριλαμβανομένου του Bluetooth Smart. Έλεγχος γραμμής ρεύματος, PLC και Wi-Fi χαμηλής ισχύος [140]

Στη συνέχεια, η ομάδα 6LoWPAN όρισε τους μηχανισμούς ενθυλάκωσης και συμπίεσης που επιτρέπουν τη μεταφορά δεδομένων IPv6 από το ασύρματο δίκτυο. Η ανάπτυξη του συστήματος 6LoWPAN δεν ήταν τόσο εύκολη όσο θα μπορούσε να θεωρηθεί, καθώς οι βασικές φύσεις των δύο συστημάτων είναι πολύ διαφορετικές. Ωστόσο, πιστεύεται ότι η χρήση πακέτων δεδομένων σε ασύρματο δίκτυο αισθητήρων χαμηλής ισχύος θα προσέφερε σημαντικά πλεονεκτήματα όσον αφορά το χειρισμό και τη διαχείριση δεδομένων.

3.3.1. Περιοχές εφαρμογής LoWPAN

Με πολλά ασύρματα δίκτυα αισθητήρων χαμηλής ισχύος και άλλες μορφές ad hoc ασύρματων δικτύων, είναι απαραίτητο κάθε νέο ασύρματο σύστημα ή τεχνολογία να έχει μια καθορισμένη περιοχή στην οποία απευθύνεται. Ενώ υπάρχουν πολλές μορφές ασύρματων δικτύων, συμπεριλαμβανομένων των ασύρματων δικτύων αισθητήρων, το 6LoWPAN απευθύνεται σε μια περιοχή που επί του παρόντος δεν αντιμετωπίζεται από κανένα άλλο σύστημα, δηλαδή αυτή της χρήσης IP, και ειδικότερα το IPv6 για τη μεταφορά των δεδομένων. Το συνολικό σύστημα στοχεύει στην παροχή ασύρματης

σύνδεσης στο Διαδίκτυο με χαμηλούς ρυθμούς δεδομένων και με χαμηλό κύκλο λειτουργίας [132].Ωστόσο, υπάρχουν πολλές εφαρμογές όπου χρησιμοποιείται το 6LoWPAN:

- Γενικός Αυτοματισμός: Υπάρχουν τεράστιες ευκαιρίες για χρήση του 6LoWPAN σε πολλούς διαφορετικούς τομείς αυτοματισμού.
- Οικιακός αυτοματισμός: Υπάρχει μεγάλη αγορά για οικιακούς αυτοματισμούς. Με τη σύνδεση χρησιμοποιώντας IPv6, είναι δυνατό να αποκτήσετε ξεχωριστά πλεονεκτήματα σε σχέση με άλλα συστήματα IoT. Η πρωτοβουλία Thread έχει δημιουργηθεί για να τυποποιηθεί σε ένα πρωτόκολλο που τρέχει πάνω από 6LoWPAN για να ενεργοποιήσει τον οικιακό αυτοματισμό.
- Έξυπνο δίκτυο: Τα έξυπνα δίκτυα επιτρέπουν στους έξυπνους μετρητές και άλλες συσκευές να δημιουργήσουν ένα δίκτυο μικροπλέγματος και μπορούν να στείλουν τα δεδομένα πίσω στο σύστημα παρακολούθησης και χρέωσης του διαχειριστή δικτύου χρησιμοποιώντας τον κορμό IPv6.
- Βιομηχανική παρακολούθηση: Τα αυτοματοποιημένα εργοστάσια και βιομηχανικές εγκαταστάσεις παρέχουν μια εξαιρετική ευκαιρία για το 6LoWPAN και η χρήση αυτοματισμού μπορεί να επιτρέψει την πραγματοποίηση σημαντικών εξοικονομήσεων. Η ικανότητα του 6LoWPAN να συνδέεται με το cloud ανοίγει πολλές διαφορετικές περιοχές για παρακολούθηση και ανάλυση δεδομένων. 6 Βασικά στοιχεία του LoWPAN

Η τεχνολογία 6LoWPAN χρησιμοποιεί το IEEE 802.15.4 για να παρέχει τα χαμηλότερα επίπεδα για αυτό το ασύρματο σύστημα δικτύου χαμηλής κατανάλωσης. Αν και αυτή φαίνεται μια απλή προσέγγιση για την ανάπτυξη ενός ασύρματου δικτύου πακέτων δεδομένων ή ασύρματου δικτύου αισθητήρων, υπάρχουν ασυμβατότητες μεταξύ της μορφής IPv6 και των μορφών που επιτρέπονται από το IEEE 802.15.4. Αυτές οι διαφορές ξεπερνιούνται μέσα στο 6LoWPAN και αυτό επιτρέπει στο σύστημα να χρησιμοποιηθεί ως στρώμα πάνω από το βασικό 802.15.4.

Για την αποστολή δεδομένων πακέτων, IPv6 μέσω 6LowPAN, είναι απαραίτητο να υπάρχει μια μέθοδος μετατροπής των δεδομένων πακέτων σε μορφή που μπορεί να χειριστεί το σύστημα κατώτερου επιπέδου IEEE 802.15.4. Το IPv6 απαιτεί η μέγιστη μονάδα μετάδοσης (MTU) να έχει μήκος τουλάχιστον 1280 byte. Αυτό είναι πολύ

μεγαλύτερο από το τυπικό μέγεθος πακέτου των 127 οκτάδων του IEEE802.15.4, το οποίο είχε ρυθμιστεί για να κρατά τις μεταδόσεις σύντομες και συνεπώς να μειώνει την κατανάλωση ενέργειας. Για να ξεπεραστεί το πρόβλημα επίλυσης διευθύνσεων, οι κόμβοι IPv6 λαμβάνουν διευθύνσεις 128 bit με ιεραρχικό τρόπο. Οι συσκευές IEEE 802.15.4 μπορούν να χρησιμοποιούν είτε εκτεταμένες διευθύνσεις IEEE 64 bit είτε διευθύνσεις 16 bit που είναι μοναδικές σε ένα PAN μετά τη συσχέτιση των συσκευών. Υπάρχει επίσης ένα PAN-ID για μια ομάδα συσκευών IEEE802.15.4 που βρίσκονται σε φυσική τοποθεσία [90].

3.3.2. Ασφάλεια LoWPAN

Αναμένεται ότι το Διαδίκτυο των Πραγμάτων, το IoT θα προσφέρει στους χάκερ μια τεράστια ευκαιρία να πάρουν τον έλεγχο συσκευών με κακή ασφάλεια και επίσης να τις χρησιμοποιήσουν για να βοηθήσουν στην επίθεση σε άλλα δίκτυα και συσκευές. Συνεπώς, η ασφάλεια είναι ένα σημαντικό ζήτημα για οποιοδήποτε πρότυπο όπως το 6LoWPAN και χρησιμοποιεί ασφάλεια επιπέδου σύνδεσης AES-128 που ορίζεται στο IEEE 802.15.4. Αυτό παρέχει έλεγχο ταυτότητας και κρυπτογράφηση συνδέσμου. Περαιτέρω ασφάλεια παρέχεται από τους μηχανισμούς ασφαλείας του επιπέδου μεταφοράς που περιλαμβάνονται επίσης. Αυτό ορίζεται στο RFC 5246 και εκτελείται μέσω TCP. Για συστήματα όπου χρησιμοποιείται UDP, μπορεί να χρησιμοποιηθεί το πρωτόκολλο επιπέδου μεταφοράς που ορίζεται στο RFC 6347, αν και αυτό μπορεί να απαιτεί ορισμένες συγκεκριμένες απαιτήσεις υλικού. 6Διαλειτουργικότητα LoWPAN Ένα βασικό ζήτημα οποιουδήποτε προτύπου είναι αυτό της διαλειτουργικότητας. Είναι ζωτικής σημασίας ο εξοπλισμός διαφορετικών κατασκευαστών να λειτουργεί μαζί. Κατά τη δοκιμή για διαλειτουργικότητα, είναι απαραίτητο να διασφαλιστεί ότι όλα τα επίπεδα της στοίβας OSI είναι συμβατά. Για να διασφαλιστεί ότι αυτό μπορεί να επιτευχθεί, υπάρχουν πολλές διαφορετικές προδιαγραφές που ισχύουν. Οποιοδήποτε στοιχείο μπορεί να ελεγχθεί ώστε να συμμορφώνεται με το πρότυπο και επίσης να ελεγχθεί άμεσα για διαλειτουργικότητα.

Το 6LoWPAN είναι ένα πρότυπο στυλ ασύρματου / IoT που έχει κερδίσει αθόρυβα σημαντικό έδαφος. Αν και αρχικά στόχευε στη χρήση με το IEEE 802.15.4, είναι εξίσου ικανό να λειτουργήσει με άλλα ασύρματα πρότυπα, καθιστώντας το ιδανική επιλογή για πολλές εφαρμογές. Το 6LoWPAN χρησιμοποιεί IPv6 και αυτό από μόνο του πρέπει να το παραμερίσει από τα άλλα με ένα ξεχωριστό πλεονέκτημα. Καθώς ο

κόσμος μεταναστεύει προς τα δεδομένα πακέτων IPv6, ένα σύστημα όπως το 6LoWPAN προσφέρει πολλά πλεονεκτήματα για ασύρματα δίκτυα αισθητήρων χαμηλής ισχύος και άλλες μορφές ασύρματων δικτύων χαμηλής ισχύος [49]

3.4. Z-Wave

Καθώς αυξάνονταν οι εφαρμογές που βασίζονται στα ασύρματα δίκτυα αισθητήρων, τον οικιακό αυτοματισμό και το IoT, η ανάγκη για εναλλακτικό πρωτόκολλο επικοινωνίας εκτός από τα κανονικά πρωτόκολλα Bluetooth, Wi-Fi και GSM γινόταν εμφανής. Αρκετές τεχνολογίες όπως το Zigbee και το Bluetooth Low Energy (BLE) αναπτύχθηκαν ως εναλλακτικές, αλλά μια τεχνολογία που ξεχωρίζει, που αναπτύχθηκε για να εξυπηρετεί ειδικά εφαρμογές οικιακού αυτοματισμού ήταν το Z-Wave. Για το σημερινό άρθρο, θα εξετάσουμε τις τεχνικές λεπτομέρειες του Z-wave, τα διαφοροποιητικά χαρακτηριστικά του, το Standard και πολλά άλλα.

Το Z-Wave είναι ένα πρωτόκολλο ασύρματης επικοινωνίας που αναπτύχθηκε κυρίως για χρήση σε εφαρμογές οικιακού αυτοματισμού. Αναπτύχθηκε το 1999 από την Zensys με έδρα την Κοπεγχάγη ως αναβάθμιση σε ένα καταναλωτικό σύστημα ελέγχου φωτός που δημιούργησαν. Σχεδιάστηκε για να παρέχει την αξιόπιστη, χαμηλής καθυστέρησης μετάδοση μικρών πακέτων δεδομένων χρησιμοποιώντας ραδιοκύματα χαμηλής ενέργειας με ρυθμούς δεδομένων έως 100 kbit/s με απόδοση έως και 40 kbit/s (9,6 kbit/s χρησιμοποιώντας παλιά τσιπ) και είναι κατάλληλο για εφαρμογές ελέγχου και αισθητήρων [21].

Με βάση την τοπολογία του δικτύου πλέγματος και λειτουργούν εντός της ζώνης συχνοτήτων ISM χωρίς άδεια 800-900 MHz (η πραγματική συχνότητα ποικίλλει), οι συσκευές που βασίζονται στο Z-Wave μπορούν να επιτύχουν απόσταση επικοινωνίας έως και 40 μέτρα, με την πρόσθετη δυνατότητα των μηνυμάτων να αναπηδούν μεταξύ έως και 4 κόμβων. Όλα αυτά τα χαρακτηριστικά το καθιστούν κατάλληλο πρωτόκολλο επικοινωνίας για εφαρμογές οικιακού αυτοματισμού όπως έλεγχος φωτισμού, θερμοστάτες, χειριστήρια παραθύρων, κλειδαριές, ανοιχτήρια γκαραζόπορτας και πολλά άλλα, αποφεύγοντας παράλληλα τις προβληματικές συμφορήσεις που σχετίζονται με το Wi-Fi και το Bluetooth λόγω της χρήσης του Ζώνες

Για να κατανοήσουμε τη λειτουργία του πρωτοκόλλου Z-Wave, ας αναλύσουμε το θέμα σε τρεις κύριες ενότητες, δηλαδή την Αρχιτεκτονική του συστήματος Z-Wave, τη

μετάδοση/λήψη δεδομένων και τη δρομολόγηση και σύνδεση στο Διαδίκτυο [30]

3.4.1. Αρχιτεκτονική συστήματος Z-Wave

Κάθε δίκτυο κυμάτων Z αποτελείται από δύο ευρείες κατηγορίες συσκευών.

- Ελεγκτής/Κύριος(οι)
- Σκλάβοι

Το master συνήθως χρησιμεύει ως κεντρικός υπολογιστής του δικτύου Z-Wave στο οποίο μπορούν να συνδεθούν άλλες συσκευές (Slaves). Συνήθως συνοδεύεται από προ-προγραμματισμένο NetworkID (μερικές φορές ονομάζεται HomeID) που εκχωρείται σε κάθε slave (το οποίο δεν συνοδεύεται από ένα προ-προγραμματισμένο ID) όταν προστίθενται στο δίκτυο μέσω μιας διαδικασίας που ονομάζεται "inclusion". Εκτός από το HomeID, για κάθε συσκευή που προστίθεται στο δίκτυο Z-wave, συνήθως εκχωρείται από τον ελεγκτή ένα αναγνωριστικό που ονομάζεται NodeID. Το NodeID είναι μοναδικό σε κάθε δίκτυο (για κάθε HomeID), ως εκ τούτου, χρησιμοποιείται για τη διεύθυνση και κυρίως την αναγνώριση κάθε συσκευής σε ένα συγκεκριμένο δίκτυο. Η συμπερίληψη είναι παρόμοια ως προς τον τρόπο με τον οποίο ένας δρομολογητής εκχωρεί διευθύνσεις IP σε συσκευές στο δίκτυό του, ενώ οι κύριοι είναι παρόμοιοι με τους δρομολογητές/πύλες/διανομείς συσκευών, με τη μόνη διαφορά να είναι η σχέση πλέγματος που έχουν οι κύριοι με τους υποτελείς στο δίκτυο. Για την αφαίρεση κόμβων από ένα δίκτυο Z-Wave εκτελείται μια διαδικασία που ονομάζεται «Εξαίρεση». Κατά την εξαίρεση, το αναγνωριστικό Home και το αναγνωριστικό κόμβου διαγράφονται από τη συσκευή. Η συσκευή επαναφέρεται στην προεπιλεγμένη εργοστασιακή κατάσταση (οι ελεγκτές έχουν το δικό τους Home ID και οι slaves δεν έχουν Home ID).

Το HomeID και το NodeID που αναφέρονται παραπάνω είναι τα δύο συστήματα αναγνώρισης που ορίζονται από το πρωτόκολλο Z-wave για εύκολη οργάνωση του δικτύου Z-wave. Το HomeID είναι η κοινή αναγνώριση όλων των κόμβων που αποτελούν μέρος ενός συγκεκριμένου δικτύου Z-Wave, ενώ το NodeID είναι η διεύθυνση μεμονωμένων κόμβων σε ένα δίκτυο. Τα HomeID είναι συνήθως προ-προγραμματισμένα και μοναδικά και καθορίζουν το συγκεκριμένο δίκτυο κυμάτων Z. Έρχονται σε μήκος 32 bit, που σημαίνει ότι είναι δυνατή η δημιουργία έως και 4

δισεκατομμυρίων (2^32) διαφορετικών HomeID και διαφορετικών δικτύων κυμάτων Z. Το αναγνωριστικό κόμβου, από την άλλη πλευρά, έχει μήκος μόνο ένα byte (8 bit) που σημαίνει ότι θα μπορούσαμε να έχουμε έως και 256 (2^8) κόμβους σε ένα δίκτυο.

Εκτός από το ότι επιτρέπει την εύκολη διευθυνσιοδότηση των κόμβων, το σύστημα αναγνώρισης βοηθά στην αποφυγή παρεμβολών σε δίκτυα κυμάτων Z, επειδή δύο κόμβοι με διαφορετικά HomeID δεν μπορούν να επικοινωνήσουν ακόμα κι αν έχουν το ίδιο NodeID. Αυτό σημαίνει ότι θα μπορούσατε να αναπτύξετε δύο δίκτυα κυμάτων z το ένα δίπλα στο άλλο χωρίς να λαμβάνεται από τον Β παρεμβαλλόμενος χάρτης από το Δίκτυο Α [119].

3.4.2. Μετάδοση δεδομένων, λήψη και δρομολόγηση

Σε τυπικά ασύρματα δίκτυα, ο κεντρικός ελεγκτής/κύριος έχει μια απευθείας ασύρματη σύνδεση ένας προς έναν με τους κόμβους του Δικτύου. Όσο χρήσιμη και αν είναι αυτή η διάταξη για αυτά τα πρωτόκολλα, δημιουργεί έναν περιορισμό σχετικά με τη μετάδοση δεδομένων, έτσι ώστε η "συσκευή Α" να μην μπορεί να αλληλεπιδράσει με τη "συσκευή Β" εάν υπάρξει διακοπή της σύνδεσης μεταξύ κάποιου από αυτά και του κύριου. Αυτό, ωστόσο, δεν ισχύει για τα κύματα Z χάρη στην τοπολογία του δικτύου Mesh και στην ικανότητα των κόμβων του κυμάτων Z να προωθούν και να επαναλαμβάνουν μηνύματα σε άλλους κόμβους. Αυτό διασφαλίζει ότι η επικοινωνία μπορεί να πραγματοποιηθεί σε κάθε κόμβο σε ένα δίκτυο ακόμη και όταν δεν βρίσκονται στην άμεση εμβέλεια του ελεγκτή. Για να το κατανοήσετε καλύτερα, λάβετε υπόψη την παρακάτω εικόνα.

3.4.3. Τοπολογία Δικτύου Πλέγματος

Η εικόνα του δικτύου Z-wave δείχνει ότι ο ελεγκτής μπορεί να επικοινωνήσει απευθείας με τις συσκευές 1, 2 και 4, ενώ ο Κόμβος 6 βρίσκεται εκτός της εμβέλειάς του. Ωστόσο, λόγω των χαρακτηριστικών που περιγράφηκαν προηγουμένως, ο Κόμβος 2 θα λάβει μια κατάσταση επαναλήπτη/προωθητή και θα επεκτείνει το εύρος του ελεγκτή στον Κόμβο 6 έτσι ώστε οποιοδήποτε μήνυμα που κατευθύνεται στον Κόμβο 6 θα περάσει μέσω του Κόμβου 2. Κόμβοι όπως ο Κόμβος 2 σε μεγάλα δίκτυα ονομάζονται διαδρομές και συμβάλλουν στην ευελιξία και την ευρωστία των Δικτύων Z-wave. Για να καθορίσουν ποια από τις διαδρομές θα πρέπει να ταξιδεύουν τα

μηνύματα για να φτάσουν σε έναν συγκεκριμένο Κόμβο, τα δίκτυα κυμάτων Z χρησιμοποιούν ένα εργαλείο που ονομάζεται πίνακας δρομολόγησης [108].

3.4.4. Πρωτόκολλο Z-Wave

Κάθε κόμβος σε ένα δίκτυο κυμάτων Z είναι σε θέση να προσδιορίσει τους άλλους κόμβους (που ονομάζονται Neighbors) στην περιοχή άμεσης ασύρματης κάλυψης και κατά τη διάρκεια της Συμπερίληψης ή αργότερα, ο κόμβος ενημερώνει τον ελεγκτή για αυτούς τους γείτονες. Χρησιμοποιώντας τη λίστα των γειτόνων από κάθε Κόμβο, ο ελεγκτής δημιουργεί έναν πίνακα δρομολόγησης που χρησιμοποιείται για τη χαρτογράφηση διαδρομών σε Κόμβους που βρίσκονται εκτός της άμεσης ασύρματης εμβέλειας του ελεγκτή.

Είναι σημαντικό να σημειωθεί ότι δεν μπορούν να ρυθμιστούν όλοι οι κόμβοι ως προωθητές. Το πρωτόκολλο Z-wave επιτρέπει μόνο σε κόμβους που είναι συνδεδεμένοι (δεν τροφοδοτούνται από μπαταρία) να λειτουργούν ως "Κόμβοι δρομολόγησης".

3.4.5. Σύνδεση στο Διαδίκτυο

Χρησιμοποιώντας την πρόσφατη προσέγγιση «Gateway/Aggregator» από άλλα πρωτόκολλα, ένα σύστημα Z-Wave μπορεί να ελεγχθεί μέσω Διαδικτύου χρησιμοποιώντας μια πύλη Z-Wave ή μια συσκευή Controller(κύρια) που χρησιμεύει τόσο ως ελεγκτής διανομέα όσο και ως πύλη προς τα έξω. Ένα παράδειγμα αυτού είναι το

- Delock78007 Z-Wave® Gateway.
- Z-Wave Gateway
- Z-Wave Alliance

Ενώ οι πρώτες συσκευές βασισμένες στο Z-wave κυκλοφόρησαν ήδη από το 1999, η τεχνολογία δεν έπιασε πραγματικά μέχρι το 2005 όταν μια ομάδα εταιρειών, συμπεριλαμβανομένου του γίγαντα οικιακού αυτοματισμού Leviton, Danfoss και Ingersoll-Rand υιοθέτησαν το Z-Wave και σχημάτισαν μια συμμαχία. που ονομάζεται Z-Wave Alliance.

Η Συμμαχία δημιουργήθηκε για να προωθήσει τη χρήση και τη διαλειτουργικότητα της τεχνολογίας Z-Wave και των συσκευών που βασίζονται σε αυτήν. Σύμφωνα με αυτό, η συμμαχία αναπτύσσει και διατηρεί το πρότυπο Z-wave και πιστοποιεί όλες τις συσκευές που βασίζονται στο Z-Wave για να διασφαλίσει ότι συμμορφώνονται με το πρότυπο. Η συμμαχία ξεκίνησε με 5 εταιρείες μέλη, αλλά τώρα έχει πάνω από 600 εταιρείες που παράγουν περισσότερες από 2600 συσκευές με πιστοποίηση Z-Wave. Διαφορά μεταξύ Z-Wave και άλλων πρωτοκόλλων

Για να καταλάβουμε γιατί είναι λογικό να έχουμε ένα άλλο πρωτόκολλο επικοινωνίας όπως το Z-wave, θα το συγκρίνουμε με ορισμένα άλλα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται στον οικιακό αυτοματισμό, όπως: Bluetooth, WiFi και Zigbee

3.4.5.1. Z-wave έναντι Bluetooth

Το πιο έντονο πλεονέκτημα του Z-Wave έναντι του Bluetooth είναι το Range. Τα κύματα Z έχουν αποτελεσματικά μεγαλύτερη περιοχή κάλυψης από το Bluetooth. Επίσης, τα σήματα Bluetooth είναι επιρρεπή σε παρεμβολές και διακοπές επειδή στέλνουν και λαμβάνουν πληροφορίες στη ζώνη των 2,4 GHz, ανταγωνίζονται έτσι για το εύρος ζώνης με συσκευές που βασίζονται σε WiFi που χρησιμοποιούν την ίδια ζώνη συχνοτήτων. Με το Z-wave, αντί να κάνει το δίκτυο πιο αργό ή θορυβώδες, κάθε επαναλήπτης σήματος Z-wave συνεργάζεται για να κάνει το δίκτυο ισχυρότερο, έτσι ώστε όσο περισσότερες συσκευές έχετε, τόσο πιο εύκολο είναι να δημιουργήσετε ένα ισχυρό δίκτυο, ικανό να παρακάμψει εμπόδια.

3.4.5.2. Z-wave έναντι WiFi

Όπως το Bluetooth, τα δίκτυα που βασίζονται σε WiFi είναι επίσης ευαίσθητα σε παρεμβολές, διακοπές και ζητήματα που σχετίζονται με το εύρος και ως εκ τούτου λειτουργούν κάτω από δίκτυα που βασίζονται σε κύμα Z υπό αυτές τις συνθήκες. Εκτός από τον ανταγωνισμό για το εύρος ζώνης με συσκευές Bluetooth, οι συσκευές WiFi ανταγωνίζονται επίσης μεταξύ τους και αυτό θα μπορούσε να επηρεάσει την ισχύ του σήματος και την ταχύτητα του δικτύου σε σπίτια όπου πολλές συσκευές βασίζονται σε WiFi. Αυτό δεν συμβαίνει με το Z-wave καθώς το δίκτυο ανθίζει με την προσθήκη περισσότερων συσκευών στο Δίκτυο.

Οι συσκευές που βασίζονται σε WiFi, ωστόσο, έχουν ένα πλεονέκτημα σε σύγκριση με τα κύματα Z. Μπορούν να στείλουν μεγαλύτερες πληροφορίες, όπως ροές βίντεο

HD και άλλα, ενώ τα δίκτυα που βασίζονται σε κύμα Z μπορούν να χειρίζονται μικρά byte δεδομένων όπως δεδομένα αισθητήρα ή οδηγίες για την ενεργοποίηση/απενεργοποίηση μιας λάμπας.

3.4.5.3. Z-wave εναντίον Zigbee

Το Zigbee είναι μια άλλη ασύρματη τεχνολογία και όπως το Z-wave, σχεδιάστηκε με γνώμονα τον Οικιακό Αυτοματισμό και τα κοντινά ασύρματα δίκτυα αισθητήρων. Όπως το Z-wave, βασίζεται στην τοπολογία του δικτύου Mesh και κάθε συσκευή σε ένα δίκτυο Zigbee βοηθά στην ενίσχυση του σήματος. Ωστόσο, σε αντίθεση με το Z-wave, λειτουργεί στη ζώνη συχνοτήτων 2,4 GHz, που σημαίνει ότι ανταγωνίζεται επίσης για εύρος ζώνης με WiFi και Bluetooth και μπορεί επίσης να είναι επιρρεπής στις προκλήσεις παρεμβολών και ταχύτητας δικτύου που σχετίζονται με αυτά. Μια άλλη διαφορά της οποίας τη σημασία θα σας αφήσω να αποφασίσετε είναι το γεγονός ότι, ενώ το Z-Wave είναι μια αποκλειστική τεχνολογία (αν και υπάρχουν σχέδια να γίνει το λογισμικό ανοιχτού κώδικα), το Zigbee είναι ανοιχτού κώδικα.

Μερικά από τα πλεονεκτήματα των κυμάτων Z περιλαμβάνουν:

- Δυνατότητα υποστήριξης 232 συσκευών στη θεωρία και τουλάχιστον 50 στην πράξη.
- Τα σήματα μπορούν να ταξιδέψουν έως και 50 πόδια σε εσωτερικούς χώρους επιτρέποντας εμπόδια και έως και 100 πόδια ανεμπόδιστα. Αυτή η εμβέλεια επεκτείνεται σημαντικά σε εξωτερικούς χώρους. Με τα τέσσερα άλματα μεταξύ συσκευών να ενισχύουν περαιτέρω την εμβέλεια, η κάλυψη δεν θα είναι πρόβλημα στα μεγάλα συνδεδεμένα σπίτια.
- Η συμμαχία Z-wave αποτελείται από έως και 600 κατασκευαστές που παράγουν περισσότερες από 2600 πιστοποιημένες συσκευές για να διασφαλίσουν τη συμβατότητα.
- Λιγότερες παρεμβολές λόγω της χρήσης της ζώνης ISM.
- Λιγότερα νεκρά σημεία σε σύγκριση με άλλα δίκτυα, χάρη στην ισχυρή τοπολογία πλέγματος
- Είναι προσιτό και εύκολο στη χρήση.

Μειονεκτήματα Z-Wave

- Σε αντίθεση με ορισμένα από τα άλλα πρωτόκολλα επικοινωνίας, το Z-Waves σχεδιάστηκε ειδικά για χρήση σε εφαρμογές Οικιακού Αυτοματισμού, ως εκ τούτου, ήταν προσαρμοσμένο στις ανάγκες της εφαρμογής και φέρει πολύ λίγα μειονεκτήματα. Ωστόσο, τα λειτουργικά όρια των 50 συσκευών αντί για τις πλασματικές 232, μπορεί να είναι μια πρόκληση σε σπίτια όπου πρέπει να αναπτυχθούν περισσότερες από 50 συσκευές.
- Επίσης, η αδυναμία του να διατηρήσει τη μεταφορά μεγάλων byte δεδομένων το καθιστά όχι τόσο χρήσιμο σε εφαρμογές όπως η παρακολούθηση βίντεο, όπου τα megabyte δεδομένων πρέπει να μεταδίδονται σε ροή μεταξύ τελικών συσκευών.

Τα κύματα Z είναι για τον οικιακό αυτοματισμό ό,τι το LoRa για το ευρύτερο τοπίο του IoT. Το μεγαλύτερο πλεονέκτημα που έχει σε σχέση με όλα τα άλλα πρωτόκολλα στη θέση του Home Automation είναι το γεγονός ότι σχεδιάστηκε για αυτήν τη θέση. Αυτό σημαίνει ότι γενικά θα έχει καλύτερη απόδοση από άλλα πρωτόκολλα που έχουν σχεδιαστεί για ευρύτερη κατανάλωση και θα έχει σχετικά καλή απόδοση, τουλάχιστον, για το 80% των εφαρμογών σε αυτήν τη θέση.

3.4.6. WiFi

Η τάση για υποστήριξη μιας ποικιλίας συνδεσιμότητας σε μια κοινή πλατφόρμα δεν περιορίζεται στην ασύρματη ευρυζωνική σύνδεση. Καθώς το Internet of Things (IoT) επιταχύνεται, θα υπάρχει πολύ μεγαλύτερη ζήτηση για συνδέσεις μηχανής με μηχανή (M2M), πολλές από αυτές ασύρματες. Αυτές θα έχουν ακόμη μεγαλύτερη ποικιλία απαιτήσεων απόδοσης, αντανακλώντας τον τεράστιο αριθμό διαφορετικών Εφαρμογών που μπορεί να προκύψουν κάτω από την ομπρέλα του IoT.

Καμία ενιαία τεχνολογία δεν θα καλύψει όλες αυτές τις απαιτήσεις και υπάρχει ένας μακρύς κατάλογος πρωτοκόλλων ασύρματου IoT. Αυτό είναι πιθανό να παγιωθεί με την πάροδο του χρόνου, αλλά σίγουρα θα υπάρξει ανάγκη για τουλάχιστον μία ανοιχτή, τυποποιημένη τεχνολογία για πολλά βασικά προφίλ IoT. Αυτά τα προφίλ ποικίλλουν ανάλογα με το βαθμό στον οποίο υποστηρίζουν:

i. Εξαιρετικά χαμηλής ισχύος έναντι μέτριας ισχύος

ii. Μεγάλη εμβέλεια έναντι τοπικής εμβέλειας έναντι πολύ μικρής εμβέλειας
iii. Χαμηλή ταχύτητα μετάδοσης δεδομένων έναντι μέτριας ταχύτητας δεδομένων
iv. Εξαιρετικά χαμηλή καθυστέρηση έναντι χαμηλής καθυστέρησης
v. Κρίσιμη διαθεσιμότητα έναντι τυπικής διαθεσιμότητας
vi. Χωρίς άδεια έναντι αδειοδοτημένου φάσματος

Το WiFi έχει το πλεονέκτημα ότι απευθύνεται σε μια πολύ μεγάλη ποικιλία προφίλ λόγω της διάδοσης της οικογένειας προτύπων του. Αυτό σημαίνει ότι θα παίξει ρόλο στα περισσότερα περιβάλλοντα IoT, μόνο του ή σε συνεργασία με πιο εξειδικευμένα πρωτόκολλα ή με κυψελοειδές. Ορισμένες εφαρμογές IoT, όπως υπηρεσίες οχημάτων ή εφαρμογές που βασίζονται σε βίντεο, όπως συνδεδεμένες κάμερες ασφαλείας, θα χρειαστούν το εύρος ζώνης του ασύρματου ευρυζωνικού δικτύου, που θα υλοποιηθεί για να ενεργοποιηθούν άλλες απαιτήσεις, όπως η χαμηλή καθυστέρηση (σε κρίσιμα περιβάλλοντα αυτό μπορεί να λάβει χώρα σε ιδιωτικό δίκτυο ή φέτα).

Το WiFi είναι μοναδικά τοποθετημένο για να υποστηρίζει ευρυζωνικές και στενής ζώνης εφαρμογές IoT από μια κοινή πλατφόρμα που μπορεί να λειτουργήσει σε διαφορετικά επίπεδα κατανάλωσης ενέργειας και εμβέλειας σήματος. Η επόμενη έκδοση των προτύπων 5G, η Έκδοση 16, θα δώσει προτεραιότητα στις δυνατότητες που εστιάζουν στο IoT, όπως η καθυστέρηση κάτω από τέσσερα χιλιοστά του δευτερολέπτου και η πολύ υψηλή διαθεσιμότητα, για την υποστήριξη αναδυόμενων περιπτώσεων στην κατηγορία URLLC (εξαιρετικά αξιόπιστες επικοινωνίες χαμηλής καθυστέρησης).

3.4.7. LPWAN

Οι συνδέσεις ευρείας περιοχής χαμηλής ισχύος (LPWAN) είναι ένα ιδιαίτερα ενδιαφέρον παράδειγμα της ανάγκης για πολλαπλές τεχνολογίες για το IoT, ενδεχομένως με το WiFi, το πιο ευρέως εγκατεστημένο σε δίκτυα και συσκευές, ως ενοποιητικό σύνδεσμο. Αυτός είναι ο κύριος τομέας, μαζί με τα καθιερωμένα πρότυπα WPAN, όπου υπάρχουν τεχνολογίες μη WiFi που λειτουργούν σε κλίμακα σε ένα μη αδειοδοτημένο φάσμα. Το WiFi και το LoRaWAN είναι δύο από τις πιο υιοθετημένες τεχνολογίες χωρίς άδεια και μαζί αντιμετωπίζουν ένα μεγάλο ποσοστό Εφαρμογών IoT. Οι προσεγγίσεις για αυτές τις τεχνολογίες διαταράσσουν τα ιδιωτικά-δημόσια επιχειρηματικά μοντέλα και επίσης επιτρέπουν τη συμμετοχή στην επιτυχία του 5G.

Το WBA και η LoRa Alliance δημοσίευσαν μια κοινή λευκή βίβλο για να δείξουν πώς αυτές οι δύο ευρέως αναπτυγμένες τεχνολογίες συνδεσιμότητας IoT μπορούν να χρησιμοποιηθούν παράλληλα για την αποτελεσματική υποστήριξη μιας τεράστιας σειράς Εφαρμογών. Το LPWAN θα υποστηρίξει εφαρμογές όπως η έξυπνη μεταφορά, ο έξυπνος φωτισμός και η παρακολούθηση περιουσιακών στοιχείων, για να αναφέρουμε μερικά παραδείγματα. Το LPWAN παρέχει ένα καλό παράδειγμα για το πώς θα συνυπάρχουν πολλαπλές τεχνολογίες φάσματος χωρίς άδεια και αδειοδότηση. Το HaLOW, το εμπορικό σήμα για το πρότυπο 802.11ah, επιτρέπει την ανάπτυξη WiFi στο μη αδειοδοτημένο φάσμα sub-GHz για την υποστήριξη εφαρμογών LPWAN. Άλλες επιλογές φάσματος χωρίς άδεια περιλαμβάνουν το LoRa και το Sigfox, ενώ υπάρχουν δύο επιλογές που βασίζονται σε LTE για ζώνες με άδεια χρήσης, το LTE Cat-M και το LTE Cat-IoT. Κάθε μία από αυτές τις τεχνολογίες υποστηρίζει διαφορετική ισορροπία μεταξύ κατανάλωσης ενέργειας και ρυθμών δεδομένων, καθιστώντας τις βέλτιστες για διαφορετικές εφαρμογές.

Πολλοί πάροχοι υπηρεσιών αναπτύσσουν ήδη δύο ή περισσότερες από αυτές τις τεχνολογίες παράλληλα για να υποστηρίξουν την ευρεία ποικιλία υπηρεσιών που θα αποτελέσουν το IoT. Για παράδειγμα, σε ένα σύνθετο περιβάλλον όπως μια έξυπνη πόλη, η δυνατότητα χρήσης συνδυασμού τεχνολογιών συνδεσιμότητας για την υποστήριξη Εφαρμογών με διαφορετικές απαιτήσεις και την ενσωμάτωσή τους σε μια κοινή πλατφόρμα διαχείρισης θα είναι το κλειδί για μια οικονομικά βιώσιμη και πλούσια λειτουργική λύση.

Αν και είναι σημαντικό να υπάρχει ποικιλία τεχνολογιών για την υποστήριξη των ευρέως ποικίλων απαιτήσεων του IoT, είναι επίσης σημαντικό αυτές οι τεχνολογίες να μπορούν να λειτουργούν απρόσκοπτα για να αποφευχθεί η δημιουργία νησίδων επικοινωνίας, καθώς θα περιόριζε σοβαρά τη δυνατότητα δημιουργίας μιας ευρείας πλατφόρμας στην οποία διαφορετικές εφαρμογές μπορούν να ανταλλάσσουν δεδομένα εύκολα.

Τα 6 κορυφαία πρωτόκολλα επικοινωνίας IoT

Η ραχοκοκαλιά του IoT είναι ένα δίκτυο συνδεδεμένων, έξυπνων συσκευών. Αυτές οι συσκευές επικοινωνούν μεταξύ τους για να συλλέγουν και να ανταλλάσσουν δεδομένα για να κάνουν τις συσκευές που προορίζονται να λειτουργούν όπως θέλουν οι χρήστες.

Το IoT στον έξυπνο φωτισμό και τις ποικίλες εφαρμογές του έχει βελτιώσει δραστικά την απόδοση και την αποδοτικότητα με αποτέλεσμα καλύτερη εμπειρία χρήστη. Όντας ένα συνδεδεμένο σύστημα, τα στοιχεία έξυπνου φωτισμού όπως προγράμματα οδήγησης, ελεγκτές, πύλες, διεπαφές εφαρμογών και λύσεις cloud πρέπει να επικοινωνούν μεταξύ τους.

Τούτου λεχθέντος, ποια τεχνολογία επικοινωνίας θα χρησιμοποιήσουν αυτές οι έξυπνες συσκευές για την ανταλλαγή δεδομένων ή πληροφοριών; Μπορούν αυτές οι έξυπνες συσκευές που αναφέραμε να υποστηρίξουν και να λειτουργήσουν με όλες τις εξέχουσες τεχνολογίες επικοινωνίας της αγοράς;

Οι έξυπνες συσκευές που υποστηρίζουν πολλαπλά πρωτόκολλα επικοινωνίας αναφέρονται ως διαλειτουργικές συσκευές και η διαλειτουργικότητα σήμερα είναι ένας βασικός παράγοντας που συζητείται περισσότερο από ποτέ. Υπάρχουν πολλές τέτοιες τεχνολογίες και πρωτόκολλα ασύρματης επικοινωνίας που δημιουργούν ισχυρές ικανότητες εντός του πεδίου λειτουργίας τους.

Τι είναι το πρωτόκολλο ασύρματης επικοινωνίας στο IoT;

Το πρωτόκολλο ασύρματης επικοινωνίας στο IoT είναι το σύνολο κανόνων που χρησιμοποιούνται για την ανταλλαγή δεδομένων μεταξύ ηλεκτρονικών συσκευών. Τα πρωτόκολλα Bluetooth, ZigBee, LoRa, NBIoT, WiFi και Thread είναι τα πιο συχνά χρησιμοποιούμενα πρωτόκολλα. Ας εξερευνήσουμε κάθε πρωτόκολλο σε βάθος. ZigBee

Από την ενεργό ανάπτυξή του το 2005, το ZigBee είναι ένα αποτελεσματικό πρωτόκολλο επικοινωνίας για δίκτυα IoT. Μπορεί να φιλοξενήσει υψηλούς αριθμούς κόμβων και να επιτύχει δυνατότητες εμβέλειας έως και 900 πόδια. Το ZigBee αποδίδεται με πλεονεκτήματα για χαμηλή κατανάλωση ενέργειας, υψηλή επεκτασιμότητα, ισχυρή ασφάλεια και ανθεκτικότητα. Χρησιμοποιεί επίσης δρομολόγηση βάσει προορισμού, καθιστώντας το ένα ισχυρό δίκτυο πλέγματος παράλληλα με το ότι είναι ισχυρό, ανθεκτικό και ευέλικτο.

Το τυπικό πρωτόκολλο IEEE 802.15.4 είναι ιδανικά σχεδιασμένο για οικιακούς αυτοματισμούς και για μεγάλες βιομηχανικές εφαρμογές όπως το Bluetooth. Υπάρχουν

πολλά πιστοποιημένα προϊόντα ZigBee για οικιακούς αυτοματισμούς και μια μεγάλη γκάμα χρηστών που αναπτύσσουν προϊόντα συμβατά με ZigBee.

Πλεονεκτήματα του Zigbee

Καλύτερη επεκτασιμότητα

Τυχαιοποίηση

Μεγάλη διάρκεια ζωής μπαταρίας

Καλύτερη επεκτασιμότητα

Το ZigBee προσφέρει καλύτερη επεκτασιμότητα με εντυπωσιακό αριθμό συσκευών έως και 65.000 εκτός από την τεράστια κάλυψη παρά τη σχετικά χαμηλή γκάμα μεμονωμένων μονάδων.

Τυχαιοποίηση

Το ZigBee χρησιμοποιεί τυχαιοποίηση που επιτρέπει τη συνεχή αξιοπιστία επικοινωνίας των εφαρμογών ZigBee ακόμα και όταν το δίκτυο είναι πυκνό.

Μεγάλη διάρκεια ζωής μπαταρίας

Οι αποτελεσματικές δυνατότητες χαμηλής ισχύος του επιτρέπουν την προσέγγιση «εφαρμογή και λήθη», καθώς μπορεί να φτάσει για μήνες μετά την ανάπτυξη.

Το ZigBee 3.0, η πιο πρόσφατη έκδοση, συνδυάζει πολλά πρότυπα ασύρματης σύνδεσης ZigBee με όλες τις δυνατότητες τους σε ένα μόνο πακέτο. Τώρα χρησιμοποιείται καλύτερα σε αστικές περιοχές για φωτισμό δρόμων και ηλεκτρικούς μετρητές που απαιτούν χαμηλή κατανάλωση ενέργειας

3.4.8. LoRa

Το LoRa χρησιμοποιείται ως τεχνολογία δικτύου ευρείας περιοχής και το LoRaWAN είναι ένα πρωτόκολλο χαμηλής ισχύος, ευρείας περιοχής δικτύωσης (LPWAN) που βασίζεται στην τεχνολογία LoRa. Το δίκτυο ευρείας περιοχής μεγάλης εμβέλειας έχει σχεδιαστεί κυρίως για ασύρματες συσκευές IoT μεγάλης εμβέλειας που λειτουργούν με μπαταρία.

Από την έναρξή του το 2015, αναπτύσσεται καλύτερα σε περιφερειακά, εθνικά και παγκόσμια δίκτυα. Είναι γνωστό για τις δυνατότητές του να επικοινωνεί σε μεγάλες αποστάσεις με τη μικρότερη κατανάλωση ενέργειας και να ανιχνεύει σήματα σε μια σειρά από χαμηλά έως υψηλά επίπεδα σήματος. Είναι ειδικά σχεδιασμένο για να φιλοξενεί εκατομμύρια συσκευές εκτός από την υποστήριξη χαμηλού κόστους κινητής ασφαλούς επικοινωνίας σε IoT, έξυπνες πόλεις ή βιομηχανικές εφαρμογές.

Πλεονεκτήματα του LoRa

- Μεγάλης εμβέλειας
- Αμφίδρομη επικοινωνία με υψηλή ασφάλεια
- Απρόσκοπτη διάθεση στην αγορά
- Μεγάλης εμβέλειας
- Επιτρέπει στιβαρή επικοινωνία έως και 10 μίλια χωρίς ενσύρματες συνδέσεις.
- Αμφίδρομη επικοινωνία με υψηλή ασφάλεια
- Το σύστημα LoRa αναγνωρίζεται για τη διασφάλιση ασφαλείας τόσο των συσκευών όσο και του δικτύου.
- Απρόσκοπτη διάθεση στην αγορά
- Το LoRa συνοδεύεται από ένα ολοκληρωμένο πακέτο τεχνολογίας που παρέχει ενσωμάτωση από άκρο σε άκρο από την υλοποίηση έως τις υπηρεσίες.

Αυτό το πρωτόκολλο είναι διαλειτουργικό εκτός από το ότι είναι ευέλικτο στο να επιτρέπει στις λύσεις να κλιμακώνονται ή να εξελίσσονται, ένας λόγος για τον οποίο έχει υιοθετηθεί σε διάφορες περιπτώσεις χρήσης και μοντέλα εφαρμογών φωτισμού.

3.4.9. NB-IoT

Ταξινομημένο στην τεχνολογία a5G, το Narrow Band IoT είναι ειδικά σχεδιασμένο για δίκτυα που απαιτούν χαμηλό εύρος ζώνης για την υποστήριξη τεράστιας πυκνότητας σύνδεσης. Το σύστημα παρέχει εκτεταμένη κάλυψη με χαμηλή καθυστέρηση, εκτός από τη διασφάλιση δοκιμασμένων και χρονικά δοκιμασμένων χαρακτηριστικών ασφαλείας. Από την τυποποίησή του το 2016, το NB-IoT έχει αναπτυχθεί σε σενάρια με απαιτητικές απαιτήσεις για εκτεταμένη κάλυψη, όπως σε αγροτικούς και σε εσωτερικούς χώρους. Επιπλέον, αποδίδει επίσης εξαιρετικά χαμηλή πολυπλοκότητα

συσκευής και θεωρείται ως η τελική λύση για τη σύνδεση μαζικής κλίμακας συσκευών σε μία μόνο ανάπτυξη.

Πλεονεκτήματα του NB-IoT

- Η καλύτερη διάρκεια ζωής της μπαταρίας στην κατηγορία του
- Ευρύτερη ανάπτυξη
- Αξιοπιστία
- Η καλύτερη διάρκεια ζωής της μπαταρίας στην κατηγορία του
- Το NB-IoT καταναλώνει τη λιγότερη ενέργεια για να προσφέρει την καλύτερη διάρκεια ζωής της μπαταρίας του κλάδου για περισσότερα από 10 χρόνια.
- Ευρύτερη ανάπτυξη
- Με χαμηλότερους ρυθμούς bit, καλύτερους προϋπολογισμούς συνδέσεων και δυνατότητες παροχής συνδεσιμότητας χωρίς πύλες θα επιτρέψουν ευρύτερες αναπτύξεις σε ποικίλες εφαρμογές.
- Αξιοπιστία
- Δεδομένου ότι το NB-IoT λειτουργεί σε ένα αδειοδοτημένο φάσμα, η ασφάλεια και η αξιοπιστία είναι εγγυημένες εκτός από την ποιότητα των υπηρεσιών.

3.4.10. WiFi

Μεταξύ όλων των πρωτοκόλλων επικοινωνίας IoT, το Wireless Fidelity (WiFi) είναι το πιο δημοφιλές για ασύρματο τοπικό δίκτυο. Βάσει του προτύπου IEEE 802.11, το WiFi επιτρέπει την ισχυρή επικοινωνία μεταξύ συνδεδεμένων συσκευών σε εύρος 115-230 ποδιών. Αυτό το σύστημα απαιτεί χαμηλό κόστος υποδομής ή συσκευής εκτός από την υποστήριξη εύκολων αναπτύξεων και χρησιμοποιείται καλύτερα για εφαρμογές εσωτερικού χώρου και οικιακούς αυτοματισμούς. Από την έναρξή της, αυτή η τεχνολογία προσπαθεί να είναι η πιο πανταχού παρούσα τεχνολογία ασύρματης επικοινωνίας και κλιμακώνεται συνεχώς για να βελτιώνει την εμβέλεια και την ταχύτητά της.

Πλεονεκτήματα του WiFi

- Ασφάλεια δεδομένων και προστασία απορρήτου
- Εύκολη εγκατάσταση και σύνδεση
- Ταχύτερες μεταφορές δεδομένων

- Ασφάλεια δεδομένων και προστασία απορρήτου
- Η κρυπτογραφημένη και ασφαλής επικοινωνία δεδομένων έχει κάνει το WiFi μια ισχυρή τεχνολογία στο σύγχρονο σύστημα ασφάλειας και ελέγχου πρόσβασης για ένα μικρό και μεγάλο κτίριο και οργανισμούς.
- Εύκολη εγκατάσταση και σύνδεση
- Το WiFi χρησιμοποιεί απλά βήματα για τη σύνδεση συσκευών και εύκολες στην εγκατάσταση διαδικασίες, προσφέροντας ευκολία στον χρήστη και εύκολη χρήση.
- Ταχύτερες μεταφορές δεδομένων
- Η υποδομή ευρείας εμβέλειας υποστηρίζει εκατοντάδες megabits ανά δευτερόλεπτο για ικανότητες που επιτρέπουν τεράστιες ποσότητες μεταφοράς δεδομένων.

Το WiFi βασίζεται στα πρότυπα IEEE 802.11 με την πρώτη του έκδοση που κυκλοφόρησε το 1997 και έχει δυνατότητες να παρέχει ταχύτητες σύνδεσης έως και 2 Mbit/s.

3.4.11. Bluetooth χαμηλής ενέργειας

Το Bluetooth Low Energy είναι μια βελτιωμένη έκδοση Bluetooth για επικοινωνίες IoT μικρής εμβέλειας έως και 300 πόδια. Συγκαταλέγεται στις πιο χρησιμοποιούμενες ασύρματες τεχνολογίες στον έξυπνο φωτισμό και σε άλλες εφαρμογές IoT από την έναρξή της το 1989. Το Bluetooth εξελίχθηκε γρήγορα για να λανσάρει την έκδοση 4.0 με τις προδιαγραφές πυρήνα Bluetooth το 2010, παρουσιάζοντας το Bluetooth Low Energy. Έκαψε την εποχή του έξυπνου φωτισμού και του έξυπνου συνδεδεμένου IoT. Αυτή η τεχνολογία ανοιχτού προτύπου θεωρείται μια εύλογα ασφαλής ασύρματη τεχνολογία που κρυπτογραφεί τα σήματα επικοινωνίας, τόσο σε επίπεδο δικτύου όσο και σε επίπεδο εφαρμογής, για να αποτρέψει την περιστασιακή υποκλοπή από συσκευές εκτός δικτύου.

Πλεονεκτήματα του Bluetooth Low Energy

- Χαμηλή καθυστέρηση και καλύτερη απόκριση
- Επεκτασιμότητα
- Αξιοπιστία και στιβαρότητα

- Χαμηλή καθυστέρηση και καλύτερη απόκριση
- Ο υψηλός ρυθμός μεταφοράς δεδομένων αποτρέπει την καθυστέρηση και το άλμα συχνότητας ελαχιστοποιεί τις παρεμβολές εκτός δικτύου
- Επεκτασιμότητα
- Το Bluetooth Low Energy μπορεί να κλιμακωθεί για να συνδέσει χιλιάδες συσκευές φωτισμού χωρίς ένα μόνο σημείο αστοχίας
- Αξιοπιστία και στιβαρότητα
- Υποστηρίζει πολλές προς πολλές επικοινωνίες ταυτόχρονα μεταξύ όλων των συσκευών σε ένα δίκτυο για γρήγορη και αξιόπιστη μετάδοση δεδομένων ακόμη και σε δίκτυο μεγάλων συσκευών

Το Bluetooth Mesh, ένα πρότυπο δικτύου που βασίζεται στο Bluetooth Low Energy, θεωρείται ισχυρό και αξιόπιστο, καθιερώνοντας τον εαυτό του ως ένα σταθερό πλαίσιο επικοινωνίας.

Η προδιαγραφή μοντέλου πλέγματος Bluetooth Low Energy υποστηρίζει τη διαλειτουργικότητα μεταξύ προμηθευτών και συμμορφώνεται με όλα τα κύρια λειτουργικά συστήματα. Επιπλέον, επιτρέπει επίσης την εύκολη ενσωμάτωση μεγάλου αριθμού συσκευών. Διαβάστε περισσότερα για το μοντέλο Bluetooth Mesh.

Η διαχείριση του γίνεται από μία μόνο οντότητα, το Bluetooth SIG, δίνοντάς του τη δυνατότητα να πραγματοποιεί γρήγορα και ανεξάρτητα αλλαγές ή τροποποιήσεις στην τεχνολογία Bluetooth για να ανταποκρίνεται στις κλιμακούμενες απαιτήσεις της βιομηχανίας σε σύγκριση με άλλες κορυφαίες τεχνολογίες ασύρματης επικοινωνίας.

Συμπεράσματα

Η σύνδεση IoT είναι η τεχνολογία ενεργοποίησης που τροφοδοτεί το IoT, αλλά είναι η επικοινωνία της συσκευής IoT μέσω του Διαδικτύου που πραγματικά επιτρέπει σε μια λύση IoT να δημιουργήσει αξία. Η επικοινωνία μεταξύ της συσκευής IoT και της πύλης IoT και μετά στο cloud καθιστά δυνατή την εκτέλεση επεξεργασίας δεδομένων, ανάλυσης και αποθήκευσης. Το IoT γεφυρώνει τόσο τα πρωτόκολλα τηλεπικοινωνιών όσο και τα πρωτόκολλα IT και αρκετά πρωτόκολλα ειδικά για το IoT έχουν προκύψει για να βοηθήσουν στην τυποποίηση και τον εξορθολογισμό των διαδικασιών επικοινωνίας του IoT.

Ο ρόλος μιας πύλης IoT είναι σημαντικός εδώ επειδή λειτουργεί ως συσσωρευτής δεδομένων από συνδεδεμένες συσκευές IoT, οι οποίες μπορούν στη συνέχεια να επικοινωνούν στο σύννεφο. Η πύλη IoT είναι μια συσκευή που συνδέει τερματικά σημεία IoT, συστήματα εξοπλισμού, αισθητήρες και πόρους cloud. Μια πύλη IoT μπορεί να είναι ένα στοιχείο υλικού ή μια εικονική συσκευή και σε κάθε περίπτωση αποτελεί θεμελιώδη παράγοντα διευκόλυνσης της επικοινωνίας IoT.

Το Cloud και το IoT πάνε χέρι-χέρι, επειδή οι πόροι cloud επιτρέπουν στους οργανισμούς IoT να επεξεργάζονται δεδομένα από τη συσκευή IoT σε συστήματα πληροφορικής και στη συνέχεια να επικοινωνούν δεδομένα από το cloud στη συσκευή IoT. Αυτή η αναγκαιότητα για αμφίδρομη επικοινωνία είναι ζωτικής σημασίας για τα οφέλη του IoT, ειδικά για εφαρμογές που προσαρμόζονται συνεχώς και χρειάζονται πληροφορίες από έναν κεντρικό διαχειριστή – αυτοματοποιημένο ή ανθρώπινο.

Τα πρωτόκολλα επικοινωνιών που χρησιμοποιούνται σε αναπτύξεις IoT περιλαμβάνουν το Lightweight M2M (Machine-to-Machine) το οποίο είναι ένα πρωτόκολλο διαχείρισης συσκευών που έχει σχεδιαστεί για δίκτυα αισθητήρων και τους όγκους συσκευών που σχετίζονται με περιβάλλοντα M2M. Το Machine Type Communications (MTC) και το Massive Machine Type Communications (mMTC) καλύπτουν επίσης αυτό το άκρο υψηλού όγκου συσκευών της αγοράς IoT και επιτρέπουν την πλήρως αυτοματοποιημένη παραγωγή, ανταλλαγή, επεξεργασία και ενεργοποίηση δεδομένων μεταξύ έξυπνων μηχανών, με χαμηλή ή καθόλου ανθρώπινη παρέμβαση.

Συνήθως, τα πρωτόκολλα που χρησιμοποιούνται στο IoT περιλαμβάνουν χαμηλή ισχύ και χαμηλό φορτίο επεξεργασίας που ταιριάζουν με τις απαιτήσεις συσκευών αισθητήρων και συσκευών όπως οι έξυπνοι μετρητές που έχουν μεγάλο κύκλο ζωής. Ωστόσο, καθώς η μεγαλύτερη πολυπλοκότητα καθίσταται απαίτηση για πιο εξελιγμένες περιπτώσεις χρήσης IoT, πρόκειται να υιοθετηθούν πρωτόκολλα που απαιτούν περισσότερη επεξεργαστική ισχύ και μεγαλύτερη κατανάλωση ενέργειας. Το προηγμένο πρωτόκολλο ουράς μηνυμάτων (AMQP) είναι ένα παράδειγμα πρωτοκόλλου IoT για τη λήψη και την τοποθέτηση μηνυμάτων σε ουρές και τη δημιουργία μιας σχέσης μεταξύ των στοιχείων. Ωστόσο, δεν είναι κατάλληλο για συσκευές IoT που έχουν περιορισμένη μνήμη.

Ένα άλλο παράδειγμα είναι η υπηρεσία διανομής δεδομένων (DDS), η οποία είναι ένα επεκτάσιμο πρωτόκολλο IoT που επιτρέπει την επικοινωνία IoT υψηλής ποιότητας. Σε σύγκριση με το IoT, το DDS επιτρέπει τη διαλειτουργική ανταλλαγή δεδομένων ανεξάρτητα από μια πλατφόρμα υλικού και λογισμικού. Ωστόσο, υπάρχουν πολλές επιλογές για πρωτόκολλα επικοινωνίας και δεδομένων στο IoT. Ποια από αυτά θα επιλεγούν θα εξαρτηθεί από την εφαρμογή και την περίπτωση χρήσης.

Όπως και η συνδεσιμότητα που επιλέχθηκε για μια περίπτωση χρήσης, η στοίβα πρωτοκόλλων επικοινωνιών IoT προσφέρει επιλογές για όλα τα επίπεδα απαιτήσεων IoT και ωριμάζει γρήγορα. Μια σημαντική πτυχή αυτής της ωριμότητας είναι να γεφυρωθούν οι διαφορές μεταξύ των πρωτοκόλλων συνδεσιμότητας, διαδικτύου και δεδομένων. Αυτό επιτρέπει βελτιωμένες επικοινωνίες μεταξύ όλων των εμπλεκόμενων συστημάτων και προετοιμάζει επίσης την αρχιτεκτονική για πρόσθετες λειτουργίες που βασίζονται σε σύννεφο και εικονικές λειτουργίες, όπως τεχνητή νοημοσύνη, μηχανική μάθηση και μεγαλύτερη εξάρτηση από συστήματα ανοιχτού κώδικα στο μέλλον.

Πρωτόκολλα επικοινωνίας

- AMQP

Σύνθετο πρωτόκολλο ουράς μηνυμάτων

Το AMQP είναι ένα ανοιχτό πρότυπο πρωτόκολλο επιπέδου εφαρμογής που χρησιμοποιείται για μηνύματα συναλλαγών μεταξύ διακομιστών. Οι κύριες λειτουργίες περιλαμβάνουν τη λήψη και την τοποθέτηση μηνυμάτων σε ουρές, την

αποθήκευση μηνυμάτων και τη δημιουργία μιας σχέσης μεταξύ των στοιχείων. Δεν είναι κατάλληλο για συσκευές αισθητήρων IoT με περιορισμένη μνήμη.

- DDS

Υπηρεσία Διανομής Δεδομένων

Το DDS είναι ένα επεκτάσιμο πρωτόκολλο IoT που επιτρέπει την επικοινωνία υψηλής ποιότητας στο IoT. Παρόμοια με το MQTT, το DDS λειτουργεί και σε μοντέλο εκδότη-συνδρομητή. Σε αντίθεση με το MQTT, το DDS επιτρέπει τη διαλειτουργική ανταλλαγή δεδομένων ανεξάρτητα από το υλικό και την πλατφόρμα λογισμικού.

- CoAP

Πρωτόκολλο περιορισμένης εφαρμογής

Το CoAp είναι ένα πρωτόκολλο επιπέδου εφαρμογής που έχει σχεδιαστεί για να ανταποκρίνεται στις ανάγκες των συστημάτων IoT που βασίζονται σε HTTP. Το HTTP είναι το θεμέλιο της επικοινωνίας δεδομένων για τον Παγκόσμιο Ιστό, αλλά, ενώ είναι ελεύθερα διαθέσιμο και χρησιμοποιήσιμο από οποιαδήποτε συσκευή IoT, μπορεί να καταναλώσει υπερβολική ενέργεια για εφαρμογές IoT. Το CoAp έχει αντιμετωπίσει αυτόν τον περιορισμό μεταφράζοντας το μοντέλο HTTP σε χρήση σε περιοριστικές συσκευές και περιβάλλοντα δικτύου.

- Ελαφρύ M2M

Ένα πρωτόκολλο διαχείρισης συσκευών σχεδιασμένο για δίκτυα αισθητήρων και τις απαιτήσεις ενός περιβάλλοντος μηχανής με μηχανή (M2M).

- Modbus

Ένα πρωτόκολλο σειριακής επικοινωνίας για χρήση με προγραμματιζόμενους λογικούς ελεγκτές (PLC) που χρησιμοποιείται για τη σύνδεση βιομηχανικών ηλεκτρονικών συσκευών.

- MQTT

Μεταφορά τηλεμετρίας σε ουρά μηνυμάτων

Ένα πρωτόκολλο σχεδιασμένο να συνδέει τις φυσικές συσκευές και τα δίκτυα με εφαρμογές και ενδιάμεσο λογισμικό, καθιστώντας το ιδανικό πρωτόκολλο συνδεσιμότητας για IoT και M2M.

- MTC

Επικοινωνίες τύπου μηχανήματος

Ένας περιγραφικός όρος για την πλήρως αυτόματη παραγωγή, ανταλλαγή, επεξεργασία και ενεργοποίηση δεδομένων μεταξύ ευφυών μηχανών, με χαμηλή ή καθόλου ανθρώπινη παρέμβαση.

- Τεχνητή νοημοσύνη

Η θεωρία και η ανάπτυξη συστημάτων υπολογιστών ικανών να εκτελούν εργασίες που συνήθως απαιτούν ανθρώπινη νοημοσύνη, όπως οπτική αντίληψη, αναγνώριση ομιλίας και λήψη αποφάσεων. Η τεχνητή νοημοσύνη επιτρέπει επίσης στις μηχανές να μαθαίνουν από την εμπειρία.

- Υπολογιστική όραση

Ένα μέρος της επιστήμης των υπολογιστών που εργάζεται για να επιτρέπει στους υπολογιστές να βλέπουν, να αναγνωρίζουν και να επεξεργάζονται εικόνες με τρόπο παρόμοιο με την ανθρώπινη όραση.

- Βαθιά μάθηση

Μια τεχνική μηχανικής μάθησης που διδάσκει στους υπολογιστές να μαθαίνουν με το παράδειγμα.

- Μηχανική μάθηση

Η μηχανική μάθηση είναι μια μέθοδος ανάλυσης δεδομένων που αυτοματοποιεί την κατασκευή αναλυτικών μοντέλων, βασισμένη στην ιδέα ότι τα συστήματα μπορούν να μάθουν από δεδομένα, να αναγνωρίσουν πρότυπα και να λάβουν αποφάσεις με ελάχιστη ανθρώπινη παρέμβαση.

- Νευρωνικά δίκτυα

Ένα σύστημα υπολογιστών με πρότυπο τον ανθρώπινο εγκέφαλο και το νευρικό σύστημα που έχει σχεδιαστεί για να βοηθά τις μηχανές να λογίζονται περισσότερο σαν ανθρώπους.

- Υπολογισμός και το Cloud
- API
- Διεπαφή προγραμματισμού εφαρμογών

Ένα σύνολο συνηθισμένων ορισμών, πρωτοκόλλων και εργαλείων για την κατασκευή λογισμικού και εφαρμογών. Ένα API συνδέει τις επιχειρηματικές διαδικασίες, τις υπηρεσίες, το περιεχόμενο και τα δεδομένα σας με συνεργάτες καναλιών, εσωτερικές ομάδες και ανεξάρτητους προγραμματιστές με εύκολο και ασφαλή τρόπο. Τα API γίνονται το de facto πρότυπο με το οποίο οι εταιρείες ανταλλάσσουν δεδομένα και δημιουργούν συνεπείς εμπειρίες πελατών μεταξύ καναλιών.

- APN - Όνομα σημείου πρόσβασης

Μια πύλη που μεταφράζει τις επικοινωνίες μεταξύ τηλεπικοινωνιών και δικτύων υπολογιστών (συχνότερα το Διαδίκτυο).

- Cloud computing

Υπολογιστής που βασίζεται στο Διαδίκτυο που επιτρέπει την πρόσβαση σε δεδομένα από διαφορετικούς υπολογιστές ή συσκευές. Συνήθως αναφέρεται σαν το ίδιο το «σύννεφο» να αποθηκεύει τα δεδομένα, αλλά τα δεδομένα αποθηκεύονται σε φυσικούς υπολογιστές που επιτρέπουν την πρόσβαση ανά πάσα στιγμή στα δεδομένα μέσω του Διαδικτύου.

- Υπολογισμός ακμών

Ένα μοντέλο στο οποίο ο υπολογισμός εκτελείται σε μεγάλο βαθμό ή εξ ολοκλήρου σε κατανεμημένους κόμβους συσκευών γνωστούς ως έξυπνες συσκευές ή συσκευές ακμής σε αντίθεση με το να πραγματοποιείται σε ένα κεντρικό περιβάλλον cloud.

- Προγραμματισμός με βάση τη ροή

Ένας τύπος προγραμματισμού ροής δεδομένων στον οποίο τα βήματα του προγράμματος επικοινωνούν μεταξύ τους μεταδίδοντας δεδομένα μέσω κάποιου

είδους καναλιού. Η διαχείριση των καναλιών γίνεται από το μεγαλύτερο σύστημα, αφήνοντας τα συνδεδεμένα εξαρτήματα ελεύθερα να επικεντρωθούν στην επεξεργασία εισόδου και στην παραγωγή εξόδου.

- Υβριδικό σύννεφο

Ένα περιβάλλον υπολογιστικού νέφους που χρησιμοποιεί έναν συνδυασμό από εσωτερικής εγκατάστασης, ιδιωτικού cloud και τρίτων, δημόσιων υπηρεσιών cloud με ενορχήστρωση μεταξύ των δύο πλατφορμών.

- Java/JSON

Μια γλώσσα προγραμματισμού υπολογιστών γενικής χρήσης που έχει σχεδιαστεί για την παραγωγή προγραμμάτων που θα εκτελούνται σε οποιοδήποτε σύστημα υπολογιστή. Το JavaScript Object Notation είναι μια ελαφριά τεχνολογία που βασίζεται σε κείμενο για τη δημιουργία μορφοποιημένων δεδομένων αναγνώσιμα από τον άνθρωπο.

- OTA

Η παροχή OTA αναφέρεται σε διάφορες μεθόδους διανομής νέου λογισμικού, ρυθμίσεων διαμόρφωσης και ακόμη και ενημέρωση κλειδιών κρυπτογράφησης σε συσκευές του είδους.

- Ανοιχτή πηγή

Περιγράφει λογισμικό για το οποίο ο αρχικός πηγαίος κώδικας είναι ελεύθερα διαθέσιμος και μπορεί να αναδιανεμηθεί ή να τροποποιηθεί.

- Peer-to-peer

Ο υπολογισμός ή η δικτύωση peer-to-peer είναι μια κατανεμημένη αρχιτεκτονική εφαρμογών που κατατμεί εργασίες ή φόρτους εργασίας μεταξύ ομοτίμων. Οι ομότιμοι είναι εξίσου προνομιούχοι, ισοδύναμοι συμμετέχοντες στην εφαρμογή.

- RESTful API

Αναφέρεται επίσης ως υπηρεσία ιστού RESTful, ένα RESTful API βασίζεται στην τεχνολογία μεταφοράς κατάστασης αναπαράστασης (REST), ένα αρχιτεκτονικό στυλ και προσέγγιση στις επικοινωνίες που χρησιμοποιούνται συχνά στην ανάπτυξη υπηρεσιών Ιστού.

- SOAP API

Το Simple Object Access Protocol (SOAP) είναι ένα πρωτόκολλο επικοινωνίας για την ανταλλαγή πληροφοριών μεταξύ διαφόρων λειτουργικών συστημάτων χρησιμοποιώντας επεκτάσιμη γλώσσα σήμανσης (XML).

- Μεγάλα δεδομένα

Ποσότητες δεδομένων που είναι τόσο μεγάλες που οι παραδοσιακές τεχνολογίες δεν μπορούν να χειριστούν τη μεταφορά ή την ανάλυσή τους. Ορισμένες τεχνολογίες IoT ειδικεύονται στο χειρισμό και τη μεταφορά μεγάλων δεδομένων, καθώς θεωρείται κλειδί για τον στόχο των μεγάλων εταιρειών να μεγιστοποιήσουν την αποδοτικότητα.

- Blockchain

Μια αυξανόμενη λίστα εγγραφών, που ονομάζονται μπλοκ, τα οποία συνδέονται χρησιμοποιώντας κρυπτογραφία. Για χρήση ως κατανεμημένο καθολικό, μια αλυσίδα μπλοκ τυπικά διαχειρίζεται ένα δίκτυο peer-to-peer που τηρεί συλλογικά ένα πρωτόκολλο για επικοινωνία μεταξύ κόμβων και επικύρωση νέων μπλοκ. Φιλτράρισμα/φιλτράρισμα δεδομένων

Περιγράφει ένα ευρύ φάσμα στρατηγικών για τη βελτίωση των συνόλων δεδομένων, ώστε να παρέχουν αυτό που χρειάζεται ένας χρήστης ή ένα σύνολο χρηστών χωρίς να περιλαμβάνει άλλα δεδομένα που μπορεί να είναι επαναλαμβανόμενα, άσχετα ή ακόμη και ευαίσθητα.

- Επιστάτης δεδομένων

Ο θυρωρός δεδομένων είναι ένα άτομο που λαμβάνει μεγάλο όγκο δεδομένων και τα συμπυκνώνει σε πληροφορίες στις οποίες μπορούν να ενεργήσουν οι επιχειρήσεις. DDDM

- Λήψη αποφάσεων βάσει δεδομένων

Μια προσέγγιση στην επιχειρηματική διακυβέρνηση που εκτιμά τις αποφάσεις που μπορούν να υποστηριχθούν με επαληθεύσιμα δεδομένα.

- Hadoop

Ένα κατανεμημένο πλαίσιο επεξεργασίας ανοιχτού κώδικα που διαχειρίζεται την επεξεργασία και την αποθήκευση δεδομένων για εφαρμογές μεγάλων δεδομένων που εκτελούνται σε συστήματα συμπλέγματος. Διάχυτος υπολογισμός, που ονομάζεται επίσης πανταχού παρόν υπολογισμός Η ενσωμάτωση της υπολογιστικής ικανότητας σε καθημερινά αντικείμενα για να τα κάνει να επικοινωνούν αποτελεσματικά και να εκτελούν χρήσιμες εργασίες με τρόπο που ελαχιστοποιεί την ανάγκη του τελικού χρήστη να αλληλεπιδρά με υπολογιστές.

- SCADA - Εποπτικός Έλεγχος και Απόκτηση Δεδομένων

Ένα σύστημα υπολογιστή για τη συλλογή, ανάλυση και έλεγχο δεδομένων σε πραγματικό χρόνο. TCP/IP Η σουίτα πρωτοκόλλου Διαδικτύου είναι το μοντέλο δικτύωσης υπολογιστών και το σύνολο πρωτοκόλλων επικοινωνίας που χρησιμοποιούνται στο Διαδίκτυο και σε παρόμοια δίκτυα υπολογιστών.

Βιβλιογραφία

[1] Cisco. 2012. The Internet of Everything: How More Relevant and Valuable Connections Will Change the World. Cisco IBSG, 2012. Ανακτήθηκε 19/05/2022 από: https://www.cisco.com/c/dam/global/en_my/assets/ciscoinnovate/pdfs/IoE.pdf.

[2] Gartner. 2017. Gartner Says 8.4 Billion Connected "Things" Will be in Use in 2017, Up 31 Percent from 2016. Ανακτήθηκε 19/05/2022 από: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

[3] Whitmore, Andrew, Anurag Agarwal, and Li Da Xu. 2015. The Internet of Things—A Survey of Topics and Trends. Information Systems Frontiers 17 (2): 261–274.

[4] Weyrich, Michael, and Christof Ebert. 2016. Reference Architectures for the Internet of Things. IEEE Software 33, no. 1: 112–116. . Ανακτήθηκε 24/05/2022 από: https://doi.org/10.1109/MS.2016.20.

[5] Tarkoma, Sasu, and Artem Katasonov. 2011. Internet of Things Strategic Research Agenda (IoT–SRA). Finnish Strategic Centre for Science, Technology, and Innovation: For Information and Communications (ICT) Services, Businesses, and Technologies, Finland.

[6] Haller, S., S. Karnouskos, and C. Schroth. 2009. The Internet of Things in an Enterprise Context. In Future Internet Symposium, 14–28. Berlin, Heidelberg: Springer.

[7] Shin, Donghee. 2014. A Socio-technical Framework for Internet-of-Things Design: A Human-Centered Design for the Internet of Things. Telematics and Informatics 31 (4): 519–531.

[8] Lynn, Theodore, Philip Healy, Steven Kilroy, Graham Hunt, Lisa van der Werff, Shankar Venkatagiri, and John Morrison. 2015. Towards a general research framework for social media research using big data. In 2015 IEEE International Professional Communication Conference (IPCC), 1–8. IEEE.

[9] Cavalcante, Everton, Marcelo P. Alves, Thais Batista, Flavia C. Delicato, and Paulo F. Pires. 2015. An Analysis of Reference Architectures for the Internet of Things. International Workshop on Exploring Component-based Techniques for Constructing Reference Architectures (CobRA).

[10] Breivold, Hongyu Pei. 2017. A Survey and Analysis of Reference Architectures for the Internet-of-Things. ICSEA 2017, 143.

[11] Bauer, Martin, Mathieu Boussard, Nicola Bui, Jourik De Loof, Carsten Magerkurth, Stefan Meissner, Andreas Nettsträter, Julinda Stefa, Matthias Thoma, and Joachim W. Walewski. 2013. IoT Reference Architecture. In Enabling Things to Talk, 163–211. Berlin, Heidelberg: Springer.

[12] L. Columbus. (2017, November) Internet of things (iot) intelligence update 2017. Accessed:2019-05-09. [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2017/11/12/2017-internet-of-things-iot-intelligence-updat

[13] E. Ramos, R. Morabito, and J.-P. Kainulainen, "Distributing intelligence to the edge and beyond," IEEE Computational Intelligence Magazine, In Press, pre-print: https://www.researchgate.net/publication/ 329183219 Distributing Intelligence to the Edge and Beyon

[14] J. Eder, G. Kappel, and M. Schrefl. (1994) Coupling and cohesion in object-oriented systems. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.55.5819

[15] C. Szegedy, Wei Liu, Yangqing Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich, "Going deeper with convolutions," in 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), June 2015, pp. 1–9

[16] A. A. Awan, H. Subramoni, and D. K. Panda, "An in-depth performance characterization of cpu- and gpu-based dnn training on modern architectures," in Proceedings of the Machine Learning on HPC Environments, ser. MLHPC'17. New York, NY, USA: ACM, 2017, pp. 8:1–8:8. [Online]. Available: http://doi.acm.org/10.1145/3146347.3146356

[17] R. C. Geyer, T. Klein, and M. Nabi, "Differentially private federated learning: A client level perspective," arXiv preprint arXiv:1712.07557, 2017.

[18] S. J. Russell and P. Norvig, Artificial Intelligence: A Modern Approach. Malaysia; Pearson Education Limited, 2016.

[19] Accenture and General Electric. 2014. Industrial Internet Insights Report for 2015. Accessed April 2020. https://www.accenture.com/us-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Industrial-Internet-Changing-Competitive-Landscape-Industries.pdf.

[20] Boyes, Hugh, Bil Hallaq, Joe Cunningham, and Tim Watson. 2018. The Industrial Internet of Things (IIoT): An Analysis Framework. Computers in Industry 101: 1–12.

[21] Lin, Shi-Wan, Brandford Miller, Jacques Durand, Graham Bleakley, Amine Chigani, Robert Martin, Brett Murphy, and Mark Crawford. 2019. The Industrial Internet of Things Volume G1: Reference Architecture V1.90. Industrial Internet Consortium, June. Accessed December 2019. https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf.

[22] Fremantle, Paul. 2015. A Reference Architecture for the Internet of Things. WSO2 White paper.

[23] Microsoft. 2018. Microsoft Azure IoT Reference Architecture, Version 2.1. Accessed December 2019.

http://download.microsoft.com/download/A/4/D/A4DAD253-BC21-41D3-B9D9-87D2AE6F0719/Microsoft_Azure_IoT_Reference_Architecture.pdf.

[24] Peña, Miguel Angel López, and Isabel Muñoz Fernández. 2019. SAT-IoT: An Architectural Model for a High-Performance Fog/Edge/Cloud IoT Platform. IEEE World Forum on Internet of Things (WF-IoT), 633–638. IEEE.

[25] Bradley, E.: Reliability Engineering: A Life Cycle Approach, 1st edn. CRC Press, Boca Raton (2016)

[26] Xie, M., Dai, Y.-S., Poh, K.-L.: Computing system reliability: models and analysis. Springer Science & Business Media (2004)

[27] Fries, R.C.: Reliable Design of Medical Devices, 2nd edn, 3rd edn, Number 2. Taylor and Francis Group/CRC Press, London (2006)

[28] Mavrogiorgou, A., Kiourtis, A., Symvoulidis, C., Kyriazis, D.: Capturing the reliability of unknown devices in the IoT world. In: 2018 5th International Conference on Internet of Things: Systems, Management and Security, IoTSMS 2018, pp. 62–69 (2018)

[29] ISO, P., 9000: 2015 Ouality management systems-Fundamentals and vocabulary. International Organization for Standardization (ISO), Geneva: ISO (2015)

[30] Atzori, L., Iera, A., Morabito, G.: Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. Ad Hoc Netw. 56, 122–140 (2017)

[31] Rayes, A., Salam, S.: Internet of Things-from Hype to Reality: The Road to Digitization, 1st edn. Springer, Cham (2016)

[32] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of Things: a survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutor. 17(4), 2347–2376 (2015)

[33] Kouicem, D.E., Bouabdallah, A., Lakhlef, H.: Internet of Things security: a top-down survey. Comput. Netw. 141, 199–221 (2018)

[34] Shi, W., Cao, J., Zhang, Q., Li, Y., Lanyu, X.: Edge computing: vision and challenges. IEEE Internet Things J. 3(5), 637–646 (2016)

[35] Alaba, F.A., Othman, M., Hashem, I.A.T., Alotaibi, F.: Internet of Things security: a survey. J. Netw. Comput. Appl. 88(March), 10–28 (2017)

[36] Yaqoob, I., Ahmed, E., Hashem, I.A.T., Ahmed, A.I.A., Gani, A., Imran, M., Guizani, M.: Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. IEEE wireless commun. 24(3), 10–16 (2017)

[37] Karkouch, A., Mousannif, H., Al Moatassime, H., Noel, T.: A model-driven architecture-based data quality management framework for the Internet of Things. In:

Proceedings of 2016 International Conference on Cloud Computing Technologies and Applications, CloudTech 2016, pp. 252–259 (2017)
[38] Al-Masri, E.: QoS-aware IIoT microservices architecture. In: 2018 IEEE International Conference on Industrial Internet (ICII), pp. 171–172 (2018)

[39] Rafferty, J., Synnott, J., Nugent, C.D., Ennis, A., Catherwood, P.A., Mcchesney, I., Cleland, I., Mcclean, S.: A scalable, research oriented, generic, sensor data platform. IEEE Access 6, 45473–45484 (2018)

[40] Tsai, C.W., Lai, C.F., Vasilakos, A.V.: Future Internet of Things: open issues and challenges. Wirel. Netw. 20(8), 2201–2217 (2014)

[41] Evans, D.: The Internet of Things—how the next evolution of the internet is changing everything. CISCO white paper, pp 1–11 (2011)

[42] Kushalnagar N., Gabriel M., Christian S.: "IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals." 1–11 (2007)

[43] Fekade, B., Maksymyuk, T., Kyryk, M., Jo, M.: Probabilistic recovery of incomplete sensed data in IoT. IEEE Internet Things J. 5(4), 2282–2292 (2017)

[44] Abeshu, A., Chilamkurti, N.: Deep learning: the Frontier for distributed attack detection in fog-to-things computing. IEEE Commun. Mag. 56(2), 169–175 (2018)

[45] Moore, S.J., Nugent, C.D., Cleland, I., Zhang, S.: Impact analysis of erroneous data on IoT reliability. In: Proceedings of the 2019 IEEE SmartWorld Smart City Innovation Conference, pp. 1908–1915 (2019)

[46] Allhoff, F., Henschke, A.: The Internet of Things: foundational ethical issues. Internet Things 1–2, 55–66 (2018)

[47] Zin, T.T., Tin, P., Hama, H.: Reliability and availability measures for Internet of Things consumer world perspectives. In: 2016 IEEE 5th Global Conference on Consumer Electronics, GCCE 2016, pp. 1–2 (2016)

[48] Ahmed, I., Saleel, A.P., Beheshti, B., Khan, Z.A., Ahmad, I.: Security in the Internet of Things (IoT). In: 2017 Fourth HCT Information Technology Trends (ITT), pp. 84–90. IEEE, New York (2017)

[49] Li, F., Nastic, S., Dustdar, S.: Data quality observation in pervasive environments. In: Proceedings—15th IEEE International Conference on Computational Science and Engineering, CSE 2012 and 10th IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, EUC 2012, pp. 602–609 (2012)

[50] Alam, T.: A reliable communication framework and its use in Internet of Things (IoT). Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. 5(10), 450–456 (2018)

[51] Behera, R.K., Reddy, K.H.K., Roy, D.S.: Reliability modelling of service oriented Internet of Things. In: 2015 4th International Conference on Reliability,

Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2015, pp. 1–6 (2015)
[51] Brogi, A., Forti, S.: QoS-aware deployment of IoT applications through the fog. IEEE Internet Things J. 4(5), 1–8 (2017)

[52] Cook, A., Misirli, G., Fan, Z.: Anomaly detection for IoT time-series data: a survey. IEEE Internet Things J. l, 7(7), 6481–6494 (2020)

[53] da Costa, K.A.P., Papa, J.P., Lisboa, C.O., Munoz, R., de Albuquerque, V.H.C.: Internet of Things: a survey on machine learning-based intrusion detection approaches. Comput. Netw. 151, 147–157 (2019)

[54] Da Li, X., He, W., Li, S.: Internet of Things in industries: a survey. IEEE Trans. Ind. Inform. 10(4), 2233–2243 (2014)

[55] DDCMS: Code of practice for consumer IoT security (2018). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

[56] Desnitsky, V.A., Kotenko, I.V., Nogin, S.B.: Detection of anomalies in data for monitoring of security components in the Internet of Things. In: Proceedings of International Conference on Soft Computing and Measurements, SCM 2015, pp. 189–192 (2015)

[57] Ghorbani, H.R., Ahmadzadegan, M.H.: Security challenges in Internet of Things: survey. In: 2017 IEEE Conference on Wireless Sensors (ICWiSe), pp. 1–6. IEEE, New York (2017)

[58] Gonzalez-Vidal, A., Cuenca-Jara, J., Skarmeta, A.F.: IoT for water management: towards intelligent anomaly detection. In: IEEE 5th World Forum on Internet of Things, WF-IoT 2019—Conference Proceedings, pp. 858–863 (2019)

[59] Kamyod, C.: End-to-end reliability analysis of an IoT based smart agriculture. In: 3rd International Conference on Digital Arts, Media and Technology, ICDAMT 2018, pp. 258–261 (2018)

[60] Karkouch, A., Mousannif, H., Al Moatassime, H., Noel, T.: Data quality in Internet of Things: a state-of-the-art survey. J. Netw. Comput. Appl. 73, 57–81 (2016)

[61] Kharchenko, V., Kolisnyk, M., Piskachova, I., Bardis, N.: Reliability and security issues for IoT-based smart business center: architecture and Markov model. In: Proceedings—2016 3rd International Conference on Mathematics and Computers in Sciences and in Industry, MCSI 2016, pp. 313–318 (2017)

[62] Kim, M.: A quality model for evaluating IoT applications. Int. J. Comput. Electr. Eng. 8(1), 66–76 (2016)

[63] Li, S., Huang, J.: GSPN-based reliability-aware performance evaluation of IoT services. In: Proceedings—2017 IEEE 14th International Conference on Services Computing, SCC 2017, pp. 483–486 (2017)
[64] Maalel, N., Natalizio, E., Bouabdallah, A., Roux, P., Kellil, M.: Reliability for emergency applications in Internet of Things. In: Proceedings—IEEE International Conference on Distributed Computing in Sensor Systems, DCoSS 2013, pp. 361–366 (2013)

[65] Moustafa, N., Hu, J., Slay, J.: A holistic review of Network Anomaly Detection Systems: a comprehensive survey. J. Netw. Comput. Appl. 128(October 2018), 33–55 (2019)

[66] Nomm, S., Bahsi, H.: Unsupervised anomaly based botnet detection in IoT networks. In: Proceedings—17th IEEE International Conference on Machine Learning and Applications, ICMLA 2018, pp. 1048–1053 (2019)

[67] Rizzardi, A., Miorandi, D., Sicari, S., Cappiello, C., Coen-Porisini, A.: Networked smart objects: moving data processing closer to the source. Lect. Notes Inst. Comput. Sci. Soc. Inform. Telecommun. Eng. LNICST 170, 28–35 (2016)

[68] Saini, N.K.: Trust factor and reliability-over-a-period-of-time as key differentiators in IoT enabled services. In: 2016 International Conference on Internet of Things and Applications, IOTA 2016, pp. 411–414 (2016)

[69] Sato, H., Kanai, A., Tanimoto, S., Kobayashi, T.: Establishing trust in the emerging era of IoT. In: Proceedings—2016 IEEE Symposium on Service-Oriented System Engineering, SOSE 2016, pp. 398–406 (2016)

[70] Sedjelmaci, H., Senouci, S.M., Al-Bahri, M.: A lightweight anomaly detection technique for low-resource IoT devices: a game-theoretic methodology. In: 2016 IEEE International Conference on Communications, ICC 2016, pp. 1–6 (2016)

[71] Sicari, S., Cappiello, C., De Pellegrini, F., Miorandi, D., Coen-Porisini, A.: A security-and quality-aware system architecture for Internet of Things. Inf Syst Front. 18(4) 665–677 (2014)

[72] Sicari, S., Rizzardi, A., Miorandi, D., Cappiello, C., Coen-Porisini, A.: A secure and quality-aware prototypical architecture for the Internet of Things. Inf. Syst. 58, 43–55 (2016)

[73] Sinche, S., Polo, O., Raposo, D., Femandes, M., Boavida, F., Rodrigues, A., Pereira, V., Sa Silva, J.: Assessing redundancy models for IoT reliability. In: 19th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2018, pp. 14–15 (2018)

[74] Singh, D., Tripathi, G., Jara, A.J.: A survey of Internet-of-Things: future vision, architecture, challenges and services. In: 2014 IEEE World Forum on Internet of Things, WF-IoT 2014, pp. 287–292 (2014)

[75] Spanos, G., Giannoutakis, K.M., Votis, K., Tzovaras, D.: Combining statistical and machine learning techniques in IoT anomaly detection for smart homes. In: IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD, 2019 Sept., pp. 1–6 (2019)
[76] Stankovic, J.A.: Research directions for the Internet of Things. IEEE Internet Things J. 1(c), 3–9 (2014)

[77] Stiawan, D., Idris, M.Y., Malik, R.F., Nurmaini, S., Budiarto, R.: Anomaly detection and monitoring in Internet of Things communication. In: Proceedings of 2016 8th International Conference on Information Technology and Electrical Engineering: Empowering Technology for Better Future, ICITEE 2016, pp. 1–4 (2017)

[78] Su, M.Y.: Real-time anomaly detection systems for Denial-of-Service attacks by weighted k-nearest-neighbor classifiers. Expert Syst. Appl. 38(4), 3492–3498 (2011)

[79] Thanigaivelan, N.K., Nigussie, E., Kanth, R.K., Virtanen, S., Isoaho, J.: Distributed internal anomaly detection system for Internet-of-Things. In: 2016 13th IEEE Annual Consumer Communications and Networking Conference, CCNC 2016, pp. 319–320 (2016)

[80] Chiang, M., Zhang, T.: Fog and IoT: an overview of research opportunities. IEEE Internet Things J. 3(6), 854–864 (2016)

[81] S. Sudevalayam, P. Kulkarni, Energy harvesting sensor nodes: survey and implications. IEEE Commun. Surv. Tuts. 13(3), 443–461 (2011)
[82] A. N. Parks, A. P. Sample, Y. Zhao, J. R. Smith, in 2013 IEEE Topical Conference on Biomedical Wireless Technologies,Networks, and Sensing Systems. A wireless sensing platform utilizing ambient RF energy (IEEE, 2013), pp. 154–56
[83] R. Vyas, H. Nishimoto, M. Tentzeris, Y. Kawahara, T. Asami, in 2012 IEEE/MTT-s International Microwave Symposium Digest. A battery-less, energy harvesting device for long range scavenging of wireless power from terrestrial TV broadcasts (IEEE, 2012), pp. 1–3
[84] K. Huang, X. Zhou, Cutting the last wires for mobile communications by microwave power transfer. IEEE Communications Magazine. 53(6), 86–93 (2015)
[85] C. Boyer, S. Roy, Backscatter communication and RFID: coding, energy, and MIMO analysis. IEEE Transactions on Communications. 62(3), 770–785 (2014)
[86] U. Karthaus, M. Fischer, Fully integrated passive UHF RFID transponder IC with 16.7-μw minimum RF input power. IEEE Journal of solid-state circuits. 38(10), 1602–08 (2003)
[87] W. Liu, K. Huang, X. Zhou, S. Durrani, Full-duplex backscatter interference

networks based on time-hopping spreading spectrum. IEEE Transactions on Wireless Communications. 16(7), 4361–4377 (2017)
[88] N. V. Huynh, D. T. Hoang, X. Lu, D. Niyato, P. Wang, D. I. Kim, Ambient backscatter communications: a contemporary survey. IEEE Communications Surveys & Tutorials. 20(4), 2889–2922 (2018)
[89] A. Bletsas, S. Siachalou, J. N. Sahalos, Anti-collision backscatter sensor networks. IEEE Trans. Wireless Commun. 8(10), 5018–5029 (2009)
[90] J. Wang, H. Hassanieh, D. Katabi, P. Indyk, in Proceedings of the ACM SIGCOMM 2012 conference on Applications,technologies,architectures, and protocols for computer communication. Efficient and reliable low-power backscatter networks (ACM, 2012), pp. 61–72
[91] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, J. R. Smith, Ambient backscatter: wireless communication out of thin air. ACM SIGCOMM Comput. Commun. Rev. 43(4), 39–50 (2013
[92] W. Liu, Y. C. Liang, Y. Li, B. Vucetic, Backscatter multiplicative multiple-access systems: fundamental limits and practical design. IEEE Trans. Wirel. Commun. 17(9), 5713–5728 (2018
[93] V. Iyer, V. Talla, B. Kellogg, S. Gollakota, J. Smith, in Proceedings of the 2016 ACM SIGCOMM Conference. Inter-technology backscatter: Towards internet connectivity for implanted devices (ACM, 2016), pp. 356–369
[94] G. Yang, C. K. Ho, Y. L. Guan, Multi-antenna wireless energy transfer for backscatter communication systems. IEEE Journal on Selected Areas in Communications. 33(12), 2974–2987 (2015)
[95] B. Clerckx, E. Bayguzina, Waveform design for wireless power transfer. IEEE Transactions on Signal Processing. 64(23), 6313–6328 (2016)
[96] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, R. Wichman, In-band full-duplex wireless: Challenges and opportunities. IEEE J. Sel. Areas Commun. 32(9), 1637–1652 (2014)
[97] J. J. Pomárico-Franquiz, Y. S. Shmaliy, Accurate self-localization in RFID tag information grids using FIR filtering. IEEE Trans. Ind. Informat. 10(2), 1317–1326 (2014
[98] Y. Zeng, R. Zhang, T. J. Lim, Wireless communications with unmanned aerial vehicles: Opportunities and challenges. IEEE Communications Magazine. 54(5), 36–42 (2016
[99] J. Sanchez-Gomez, R. Sanchez-Iborra, and A. Skarmeta, “Transmission technologies comparison for IoT communications in smart-cities,” in GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Dec 2017, pp. 1–6
[100] J. P. S. Sundaram, W. Du, and Z. Zhao, “A survey on LoRa networking: Research problems, current solutions and open issues,” IEEE Communications Surveys Tutorials, pp. 1–1, 2019.

[101] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of things: A survey on enabling technologies, protocols, and applications,” IEEE Communications Surveys Tutorials, vol. 17, no. 4, pp. 2347–2376, Fourthquarter 2015.
[102] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, “Understanding the limits of LoRaWAN,” IEEE Communications Magazine, vol. 55, no. 9, pp. 34–40, Sep. 2017
[103] R. Fernandes, R. Oliveira, M. Lu´ıs, and S. Sargento, “On the real capacity of LoRa networks: The impact of non-destructive communications,” IEEE Communications Letters, vol. 23, no. 12, pp. 2437–2441, Dec 2019
[104] J. Gubbi et al., “Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions,” Future Generation Computer Systems, vol. 29, no. 7, Sept. 2013
[105] D. Miorandi et al., “Internet of Things,” Ad Hoc Networks, vol. 10, no. 7, Sept. 2012
[106] A. Zanella et al., “Internet of Things for Smart Cities,” IEEE Internet of Things J., vol. 1, no. 1, Feb. 2014, pp. 22–32
[107] A. Biral et al., “The Challenges of M2M Massive Access in Wireless Cellular Networks,” Digital Communications and Networks, vol. 1, no. 1, Feb. 2015
[108] S.-Y. Lien,K.-C. Chen, and Y.Lin, “Toward Ubiquitous Massive Accesses in 3GPP Machine-to-Machine Communications” IEEE Commun. Mag., vol. 49, no. 4, Apr. 2011, pp. 66–74
[109] K. Zheng et al., “The Analysis and Implementation of AllJoyn Based Thin Client Communication System with Heartbeat Function,” Int'l. Conf. Cyberspace Technology, Nov. 2014, pp. 1–4
[110] H. Cha, W. Lee, and J. Jeon, “Standardization Strategy for the Internet of Wearable Things,” Int'l. Conf. Information and Commun. Technology Convergence, Oct. 2015, pp. 1138–42
[111] G. Gardasevic et al., “On the Performance of 6LoWPAN through Experimentation,” Int'l. Wireless Commun. and Mobile Computing Conf., Aug. 2015, pp. 696–701
[112] G. Gardasevic et al., “On the Performance of 6LoWPAN through Experimentation,” Int'l. Wireless Commun. and Mobile Computing Conf., Aug. 2015, pp. 696–701
[113] On-Ramp Wireless Inc., “Light Monitoring System Using A Random Phase Multiple Access System,” July 2013, U.S. Patent 8,477,830
[114] A. J. Berni and W. Gregg, “On the Utility of Chirp Modulation for Digital Signaling,” IEEE Trans. Commun., vol. 21, no. 6, June 1973 pp. 748–51
[115] C. Anton-Haro and M. Dohler, Machine-to- Machine (M2M) Communications: Architecture, Performance and Applications, 1st ed., Woodhead Publishing Ltd., Jan. 2015.
[116] C. Pielli et al., “Platforms and Protocols for the Internet of Things,” Endorsed Transactions on Internet of Things, vol. 15, no. 1, Oct. 2015.

[117] Baker, T., et al., A secure fog-based platform for SCADA-based IoT critical infrastructure. Software: Practice and Experience, 2019.
[118] Aloi, G., et al., Enabling IoT interoperability through opportunistic smartphone-based mobile gateways. Journal of Network and Computer Applications, 2017. 81: p. 74-84
[119] Noura, M., M. Atiquzzaman, and M. Gaedke, Interoperability in Internet of Things: Taxonomies and Open Challenges. Mobile Networks and Applications, 2019. 24(3): p. 796-809
[120] Campolo, C., A. Molinaro, and A. Iera, A reference framework for social-enhanced Vehicle-to-Everything communications in 5G scenarios. Computer Networks, 2018. 143: p. 140-152
[121] Chen, R., J. Guo, and F. Bao, Trust management for SOA-based IoT and its application to service composition. IEEE Transactions on Services Computing, 2014. 9(3): p. 482-495
[122] Amadeo, M., et al., IoT Services Allocation at the Edge via Named Data Networking: From Optimal Bounds to Practical Design. IEEE Transactions on Network and Service Management, 2019
[123] Abbassi, I.H., et al. TrojanZero: Switching Activity-Aware Design of Undetectable Hardware Trojans with Zero Power and Area Footprint. in 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE). 2019. IEEE.
[124] Zhou, K., T. Liu, and L. Zhou. Industry 4.0: Towards future industrial opportunities and challenges. in 2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD). 2015. IEEE.
[125] Pace, P., et al., An edge-based architecture to support efficient applications for healthcare industry 4.0. IEEE Transactions on Industrial Informatics, 2019. 15(1): p. 481-489.
[126] Dizdarević, J., et al., A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration. ACM Computing Surveys (CSUR), 2019. 51(6): p. 116
[127] Luo, Y., et al., A novel mobile and hierarchical data transmission architecture for smart factories. IEEE Transactions on Industrial Informatics, 2018. 14(8): p. 3534-3546.
[128] Al-khafajiy, M., et al., Towards fog driven IoT healthcare: challenges and framework of fog computing in healthcare, in Proceedings of the 2nd International Conference on Future Networks and Distributed Systems. 2018, ACM: Amman, Jordan. p. 1-7.

[129] Çorak, B.H., et al. Comparative Analysis of IoT Communication Protocols. in 2018 International Symposium on Networks, Computers and Communications (ISNCC). 2018. IEEE
[130] Badawy, M.M., Z.H. Ali, and H.A. Ali, QoS provisioning framework for service-oriented internet of things (IoT). Cluster Computing, 2019.
[131] Asghari, P., A.M. Rahmani, and H.H.S. Javadi, Service composition approaches in IoT: A systematic review. Journal of Network and Computer Applications, 2018. 120: p. 61-77.
[132] Tayeb, S., S. Latifi, and Y. Kim. A survey on IoT communication and computation frameworks: An industrial perspective. in 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC). 2017. IEEE
[133] Zaidan, A.A., et al., A survey on communication components for IoT-based technologies in smart homes. Telecommunication Systems, 2018. 69(1): p. 1-25.
[134] Akpakwu, G.A., et al., A survey on 5G networks for the Internet of Things: Communication technologies and challenges. IEEE Access, 2017. 6: p. 3619-3647.
[135] Montori, F., et al., Machine-to-machine wireless communication technologies for the Internet of Things: Taxonomy, comparison and open issues. Pervasive and Mobile Computing, 2018
[136] Al-Sarawi, S., et al. Internet of Things (IoT) communication protocols. in 2017 8th International Conference on Information Technology (ICIT). 2017. IEEE.
[137] Siboni, S., et al., Security Testbed for Internet-of-Things Devices. IEEE Transactions on Reliability, 2018. 68(1): p. 23-44.
[138] Asghari, P., A.M. Rahmani, and H.H.S. Javadi, Internet of Things applications: A systematic review. Computer Networks, 2019. 148: p. 241-261.
[139] Matthieu, C. and G. Ramleth, Security and rights management in a machine-to-machine messaging system. 2015, Google Patents.
[140] Jo, M., et al., Device-to-device-based heterogeneous radio access network architecture for mobile cloud computing. IEEE Wireless Communications, 2015. 22(3): p. 50-58.
[141] Yang, G., et al., IoT-based remote pain monitoring system: From device to cloud platform. IEEE journal of biomedical and health informatics, 2018. 22(6): p. 1711-1719.
[142] Le, M., S. Clyde, and Y.-W. Kwon, Enabling multi-hop remote method invocation in device-to-device networks. Human-centric Computing and Information Sciences, 2019. 9(1): p. 20

[143] Da Xu, L., W. He, and S. Li, Internet of things in industries: A survey. IEEE Transactions on industrial informatics, 2014. 10(4): p. 2233-2243.
[144] Shelby, Z., K. Hartke, and C. Bormann, The constrained application protocol (CoAP). 2014.
[145] Javed, R.H., et al. ApproxCT: Approximate Clustering Techniques for Energy Efficient Computer Vision in Cyber-Physical Systems. in 2018 12th International Conference on Open Source Systems and Technologies (ICOSST). 2018.
[146] Zhou, Z., et al., Potential risk of IoT device supporting IR remote control. Computer Networks, 2018
[147] Kertesz, A., T. Pflanzner, and T. Gyimothy, A Mobile IoT Device Simulator for IoT-Fog-Cloud Systems. Journal of Grid Computing, 2018
[148] Wang, J., et al., A self-adaptive load-dispatching control framework for device data accessing in IoT-based systems. International Journal of Communication Systems, 2017. 30(12): p. e3260
[149] Mukherjee, S. and G.P. Biswas, Networking for IoT and applications using existing communication technology. Egyptian Informatics Journal, 2018. 19(2): p. 107-127.

[150] [150] Sampoulatidis , I., Ververidis, D., Tsarchopoulos, P., Nikolopoulos, S., Kompatsiaris, I.,
[151] Komninos, N.: ImproveMyCity: an open source platform for direct citizen-government com munication. In Proceedings of the 21st ACM international conference on Multimedia, 839–842 ACM 2013, October
[152] [151] Choi, C., Esposito, C., Wang, H., Liu, Z., Choi, J.: Intelligent power equipment management based on distributed context-aware inference in smart cities. IEEE 2018
[153] [152] Pace, P., Aloi, G., Caliciuri, G., Gravina, R., Savaglio, C., Fortino, G., Corona, M.:INTERHealth: An interoperable IoT solution for active and assisted living healthcare services. In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT) 81–86 IEEE (2019, April)
[154] [153] Adel, E., El-Sappagh, S., Barakat, S., Elmogy, M.: A unified fuzzy ontology for distributed electronic health record semantic interoperability. In U-Healthcare Monitoring Systems, 353- 395, Academic Press (2019)

https://www.researchgate.net/figure/Industrial-Internet-Integrated-Reference-Model-I3RM_fig8_336693486

https://www.arm.com/solutions/iot/iot-technology
https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/12310/Pelekanos_MDE1633.pdf?sequence=1&isAllowed=y

https://dspace.lib.ntua.gr/xmlui/bitstream/handle/123456789/52409/Athanasopoulos%20Athanasios%20Diploma%20Thesis.pdf?sequence=1

https://docs.wso2.com/display/IoTS100COPY/WSO2+IoT+Server+Architecture

http://users.sch.gr/jabatzo/files/yliko/live%20ebooks/diktya_ypolog_G_2018_final/_2.html

http://telematics.upatras.gr/telematics/system/files/bouras_site/ergasies_foithtwn/Babatsikou_thlematiki.pdf

http://artemis.cslab.ece.ntua.gr:8080/jspui/bitstream/123456789/14546/1/DT2006-0063.pdf

https://eclass.uth.gr/modules/document/file.php/DS_U_129/%CE%94%CE%B9%CE%B1%CF%86%CE%AC%CE%BD%CE%B5%CE%B9%CE%B5%CF%82%20%CE%BC%CE%B1%CE%B8%CE%AE%CE%BC%CE%B1%CF%84%CE%BF%CF%82/dspTopics.pdf

http://artemis.cslab.ece.ntua.gr:8080/jspui/bitstream/123456789/17494/1/%CE%B4%CE%B9%CF%80%CE%BB%CF%89%CE%BC%CE%B1%CF%84%CE%B9%CE%BA%CE%AE%20%CE%94%CE%AE%CE%BC%CE%BF%CF%82%20%CE%9A%CF%89%CE%BD%CF%83%CF%84%CE%B1%CE%BD%CF%84%CE%AF%CE%BD%CE%BF%CF%82%20%20%CE%9F%CE%BA%CF%84%CF%8E%CE%B2%CF%81%CE%B9%CE%BF%CF%82%202019.pdf

http://gr.feasyblue.com/ble-module/bluetooth-5-ble-module/bluetooth-low-energy-chip.html

https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/9207/Tzanidakis_Marios.pdf?sequence=1&isAllowed=y

https://www.semanticscholar.org/paper/A-protection-strategy-for-fault-detection-and-for-Monadi-Koch-Ciobotaru/6b5f260942d42532f6bf9e945e53963e9058d62b