ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)

στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

"Internet of Things: Constrained Application Protocol over Information-Centric Networking"

ΓΚΡΕΜΟΣ ΒΑΣΙΛΕΙΟΣ

MM4150002

ΜΠΕΝΕΚΟΣ ΣΠΥΡΙΔΩΝ

MM4150009

ΑΘΗΝΑ, ΙΟΥΝΙΟΣ 2017

ΕΙΣΑΓΩΓΗ – ABSTRACT

Ο όρος Internet of Things (IoT), είναι ένας όρος ο οποίος πριν απο μερικά χρόνια μπορούσε να μοιάζει με σενάριο επιστημονικής φαντασίας που μπορούσε να βρεθεί στις Χολυγουντιανές ταινίες και σε εφαρμογές που "μόνο στις ταινίες" θα μπορούσαν να συμβούν. Να κυκλοφορείς στο σπίτι και καθώς ανοίγεις την πόρτα του δωματίου τα παράθυρα να ρυθμίζονται όπως τα θέλεις, να παίζει η μουσική που σου αρέσει, το φαγητό να ζεσταίνεται στον φούρνο χωρίς να είσαι εκεί να τον ανάψεις, όλα αυτά που τις παλαιότερες εποχές θα χαρακτηρίζονταν ως μαγικά, σήμερα κάθε άλλο παρά στον χώρο του φανταστικού και της μαγείας ανήκουν. Η εξέλιξη της τεχνολογίας και η ευκολία διασύνδεσης στο διαδίκτυο σε όλη σχεδόν την επιφάνεια του γεωγραφικού χάρτη, κατάφεραν να καταστήσουν δυνατή την υλοποίηση του επιστημονικού αυτού σεναρίου που ονομάζεται "Ίντερνετ των πραγμάτων". Ένας απλός και πρακτικός ορισμός θα μπορούσε να περιγράφει τη διασύνδεση συσκευών που χρησιμοποιούνται στην καθημερινή ζωή του ανθρώπου, σε ένα ευρύτερο δίκτυο με στόχο την αύξηση αφενός της αποτελεσματικότητάς τους και αφετέρου της παραγωγικότητας των χρηστών στις διάφορες δραστηριότητές τους.

Παρά την τεχνολογική εξέλιξη τόσο σε επίπεδο Hardware, όσο και σε επίπεδο Software, τα παραδοσιακά δίκτυα και ο τρόπος λειτουργίας τους όπως αυτός έχει εξελιχθεί μέχρι σήμερα είναι πιθανό να μη μπορούν να ανταπεξέλθουν στον ολοένα αυξανόμενο αριθμό συνδεδεμένων συσκευών στο διαδίκτυο. Το γεγονός αυτό, έχει στρέψει το ενδιαφέρον της επιστημονικής κοινότητας προς την κατεύθυνση της βελτιστοποίησης των υπαρχόντων πρωτοκόλλων επικοινωνίας ή και του σχεδιασμού νέων μοντέλων που θα μπορούν να υποστηρίξουν τη διαλειτουργικότητα των συσκευών του Internet of Things. Στις σελίδες που ακολουθούν θα αναλυθεί ο όρος του Internet of Things, οι βασικές τεχνολογίες που χρησιμοποιούνται για να το υποστηρίξουν καθώς και η ιστορική του εξέλιξη από την πρώτη φορά που εμφανίστηκε μέχρι και τα μεγέθη που αναμένεται τα επόμενα χρόνια να φτάσει.

Στη συνέχεια θα αναλυθεί το Constrained Application Protocol (CoAP) ώστε να γίνει κατανοητός ο τρόπος με τον οποίο γίνεται η διασύνδεση και επικοινωνία μεταξύ δύο ή περισσοτέρων «έξυπνων» συσκευών. Θα παρουσιαστούν οι βασικές διαφορές που έχει σε σχέση με το διαδεδομένο πρωτόκολλο HTTP, η μορφή και ο τρόπος που

αποστέλλονται τα διάφορα μηνύματα που υποστηρίζει, ενώ θα αναλυθούν και δυο βασικές επεκτάσεις του πρωτοκόλλου, για παρατήρηση ενός πόρου και για ομαδική επικοινωνία.

Έπειτα, αναλύεται το Information-Centric Networking (ICN) ως ένας τρόπος βελτιστοποίησης της λειτουργίας του CoAP με στόχο την αποτελεσματικότερη και αποδοτικότερη επικοινωνία και ανταλλαγή πληροφοριών μεταξύ των συσκευών που χρησιμοποιούν το Constrained Application Protocol. Περιγράφονται λόγοι που η υιοθέτηση αυτού βοηθά στην υλοποίηση του Internet of Things, οι βασικές επιλογές σχεδιασμού, εξηγούνται τα βασικά πλεονεκτήματα χρήσης αυτού αλλά παράλληλα αναλύονται και οι προκλήσεις της υλοποίησης του ICN.

Τέλος, δεδομένης της τάσης των τελευταίων ετών προς την κατεύθυνση της ασφάλειας των πληροφοριών που μεταδίδονται μέσω του διαδικτύου, κρίθηκε σκόπιμο να υπάρξει αναφορά στα ζητήματα ασφαλείας του Internet of Things. Συγκεκριμένα, αναλύονται οι κίνδυνοι που αντιμετωπίζει το Internet of Things σε επίπεδο συσκευών αλλά και εφαρμογών λόγω της φύσης του, στα ζητήματα ασφαλείας του CoAP και της ICN προσέγγισης απέναντι σε ενδεχόμενες επιθέσεις και απειλές και τέλος προτείνονται ορισμένοι τρόποι που μπορούν αυτές να ξεπεραστούν.

Συνοπτικά, η δομή της εργασίας έχει ως εξής:

ΜΕΡΟΣ ΠΡΩΤΟ: Internet of Things,

Ορισμός του Internet of Things, ιστορική εξέλιξη και μελλοντικές τάσεις καθώς και παρουσίαση των βασικών τεχνολογιών (Sensors, RFID Tags, Bluetooth, NFC) που κάνουν δυνατή την ύπαρξή του σήμερα.

ΜΕΡΟΣ ΔΕΥΤΕΡΟ: Constrained Application Protocol

Ανάλυση και κατανόηση της λειτουργίας του πρωτοκόλλου. Παρουσιάζεται το μοντέλο μεταφοράς μηνυμάτων και η μορφή των μηνυμάτων που αποστέλλονται από και προς τους servers. Στη συνέχεια αναλύεται ο τρόπος με τον οποίο μια συσκευή μπορεί να παρακολουθεί κάποιον πόρο που την ενδιαφέρει όπως επίσης και η συμμετοχή μιας συσκευής σε μια ομάδα συσκευών. Καθ' όλη της διάρκεια της παραπάνω ανάλυσης παραθέτονται και σχετικά παραδείγματα .

ΜΕΡΟΣ ΤΡΙΤΟ: Information-Centric Networking και POINT-Architecture

Στο κεφάλαιο αυτό προτείνεται και αναλύεται το ICN ως ένας τρόπος βελτιστοποίησης της επικοινωνίας συσκευών IoT που χρησιμοποιούν το πρωτόκολλο CoAP, παρουσιάζονται τα πλεονεκτήματα χρήσης αλλά και οι προκλήσεις αυτού, ενώ στη συνέχεια γίνεται μια σε ανάλυση σε βάθος του τρόπου λειτουργίας και σχεδιασμού αυτής της προσέγγισης

ΜΕΡΟΣ ΤΕΤΑΡΤΟ : Προκλήσεις του Internet of things

Οι κυριότερες αδυναμίες ως αποτέλεσμα του επιπέδου ασφαλείας των υπηρεσιών IoT που παρέχονται, προκλήσεις ασφαλείας σε επίπεδο ICN και εν γένει CoAP

Ολοκλήρωση της έρευνας με την παράθεση συμπερασμάτων καθώς και της βιβλιογραφίας που μελετήθηκε.

Περιεχόμενα

ΜΕΡΟΣ ΠΡΩΤΟ

INTERNET OF THINGS

Internet of Things είναι το δίκτυο φυσικών συσκευών που μπορούν να έχουν πρόσβαση στο διαδίκτυο. Οι συσκευές αυτές ενσωματώνουν τεχνολογία και μπορούν να αλληλεπιδρούν με το εξωτερικό περιβάλλον και όταν αυτές οι συσκευές "διαισθάνονται" και επικοινωνούν, επηρεάζεται ο τρόπος που λαμβάνονται οι αποφάσεις. Πρόκειται για μια σύγχρονη, ασύρματη τεχνολογία που μπορεί να εφαρμοστεί σε πολλούς και διαφορετικούς τομείς του πραγματικού κόσμου και αναφέρεται στον ολοένα αυξανόμενο αριθμό συσκευών που έχουν τη δυνατότητα πρόσβασης στο διαδίκτυο, πέραν του προσωπικού υπολογιστή και των κινητών συσκευών. Οι πιο συνηθισμένες εφαρμογές αυτής της τεχνολογίας μέχρι σήμερα, είναι στον τομέα της Ιατρικής με τη δυνατότητα απομακρυσμένης παρακολούθησης της πορείας της υγείας ενός ασθενή και την αποστολή πληροφορίας προς το νοσοκομείο, ώστε να ελέγχεται και να αξιολογείται η πορεία μιας εξέτασης ή πάθησης, αλλά και στη γραμμή παραγωγής για τον προγραμματισμό παραγγελιών, του πλήθους των διαθέσιμων υλών και προϊόντων κλπ. Καθώς όμως η τεχνολογία και τα ασύρματα δίκτυα εξελίσσονται, η τεχνολογία αυτή συναντάται σε περισσότερες συσκευές και τομείς, τόσο του επιχειρηματικού κόσμου, όσο και της ιδιωτικής ζωής του ανθρώπου. Υπάρχουν συσκευές τις οποίες ο απλός άνθρωπος μπορεί να φοράει στο γυμναστήριο και να παρακολουθεί τους παλμούς του, σε ψυγεία για την παρακολούθηση των αποθεμάτων τους, στους διακόπτες των οικιακών συσκευών για λόγους ασφαλείας ή ακόμα και στην αυτοματοποίηση δραστηριοτήτων μέσα στον οικιακό χώρο (έξυπνα παράθυρα, φώτα) που προσφέρουν πλέον στον χρήστη περισσότερες ανέσεις και τον φέρνουν πιο κοντά σε αυτό που ονομάζουμε "έξυπνο σπίτι". Με άλλα λόγια, είναι η τεχνολογία που καθιστά την επικοινωνία του ανθρώπου, του σπιτιού, των συσκευών και ακόμα και των ζώων χωρίς να είναι απαραίτητη η επικοινωνία Ανθρώπου-Μηχανής ή Ανθρώπου-Ανθρώπου.

ΚΕΦΑΛΑΙΟ 1

Εμφάνιση του IoT και βασικές τεχνολογίες

Η αρχική ιδέα του IoT εμφανίστηκε στις αρχές της δεκαετίας του ΄80 όπου και δημιουργήθηκε ο πρώτος αυτόματος πωλητής αναψυκτικών που είχε τη δυνατότητα να παρακολουθεί και να αναφέρει στον προμηθευτή την ποσότητα των αναψυκτικών που βρίσκονταν εκείνη τη στιγμή στο ψυγείο αλλά και τη θερμοκρασία των προϊόντων που βρίσκονταν σε αυτό. Η ονομασία και ο ορισμός του IoT δόθηκε το 1985 από τον Peter T. Lewis σύμφωνα με τον οποίο "IoT είναι η ενσωμάτωση ανθρώπων, διαδικασιών, συσκευών και της τεχνολογίας, σε ένα κοινό δίκτυο, για την απομακρυσμένη παρακολούθηση, χειρισμό και αξιολόγηση των τάσεων των συσκευών".[1]

Ο όρος Internet of Things, έγινε διάσημος το 1999 όταν ο Kevin Ashton οραματίστηκε πως αν όλες οι συσκευές της καθημερινότητας ήταν εξοπλισμένες με τεχνολογίες αναγνωριστικών (RFID, Near Field Communication, Barcodes, QR codes κλπ.) και παράλληλα συνδέονταν μεταξύ τους αλλά και με το διαδίκτυο, οι υπολογιστές θα ήταν σε θέση να παρακολουθούν τη λειτουργία τους. Με αυτό τον τρόπο, και ανάλογα με το πεδίο εφαρμογή της κάθε μιας από αυτές, θα μπορούσαν να εξαχθούν πληροφορίες που θα βελτίωναν την αποδοτικότητα και τη χρηστικότητά τους. Απαραίτητη προϋπόθεση όμως για να γίνει κάτι τέτοιο πραγματικότητα, ήταν η δυνατότητα σύνδεσης όλων των συσκευών στο διαδίκτυο και η διευθυνσιοδότηση όλων των συσκευών. Όταν προτάθηκε αυτό, οι ασύρματες τεχνολογίες ήταν ακόμα σε πρώιμο στάδιο και χρειάστηκαν αρκετά χρόνια ώστε να εξελιχθεί η ιδέα και να φτάσει σήμερα να γίνει σιγά σιγά μέρος της καθημερινότητας του ανθρώπου.[2]

Οι λόγοι για τους οποίους η ύπαρξη του IoT σήμερα είναι δυνατή οφείλεται τόσο σε επιχειρηματικούς όσο και οικονομικούς. Οι κυριότεροι επιχειρηματικοί λόγοι για τους οποίου το IoT μπορεί να γνωρίσει μεγάλη άνθιση στα επόμενα χρόνια είναι οι ακόλουθοι:[3]

- Η ανάπτυξη του Cloud Computing, που παρέχει απομακρυσμένους υπολογιστικούς πόρους για την αποθήκευση, επεξεργασία και διαχείριση

πληροφορίας. Με αυτό τον τρόπο, δίνεται η δυνατότητα σε μικρές απλές συσκευές να αλληλεπιδρούν με μεγάλα συστήματα επεξεργασίας δεδομένων για να μπορούν να παρέχουν ποικίλες πληροφορίες και υπηρεσίες όπου από μόνες τους δε θα μπορούσαν.

- Η εξέλιξη του χώρου των Data Analytics. Ο ολοένα αυξανόμενος σχεδιασμός νέων αλγορίθμων σε συνδυασμό με την εξέλιξη της τεχνολογίας του hardware, της αποθήκευσης δεδομένων και του Cloud Computing, επιτρέπουν τη συσχέτιση και ανάλυση μεγάλου όγκου δεδομένων που ένα απλό τερματικό δε μπορούσε μέχρι πριν μερικά χρόνια να διαχειριστεί μόνο του. Αυτές οι νέες και εξελισσόμενες δυνατότητες δίνουν την ευκαιρία για ευκολότερη, ταχύτερη και αποτελεσματικότερη συλλογή και ανάλυση πληροφορίας και γνώσης.

Πέραν όμως των παραπάνω επιχειρηματικών λόγων, οι οποίοι επιτρέπουν και υποβοηθούν τη λειτουργικότητα του Internet of Things, η εξέλιξη του οράματος δε θα μπορούσε να καταστεί δυνατή αν και από τεχνολογικής άποψης το διαδίκτυο δεν είχε εξελιχθεί σε αυτό που είναι σήμερα. Συγκεκριμένα:

- Η "πανταχού παρών" συνδεσιμότητα, δηλαδή η δυνατότητα ολοένα και περισσότερες συσκευές να έχουν πρόσβαση στο διαδίκτυο χάριν στα φθηνά, πλέον, και γρήγορα δίκτυα.
- Η διαδεδομένη υιοθέτηση των IP-based δικτύων και τεχνολογιών. Η IP πλατφόρμα είναι μια δοκιμασμένη και αποτελεσματική τεχνολογία, η οποία παρέχει εργαλεία και εφαρμογές που μπορούν εύκολα και με χαμηλό κόστος να ενσωματωθούν σε μεγάλο εύρος συσκευών.
- Η σμίκρυνση του Hardware, χάριν στην οποία, πολύ μικρά σε μέγεθος chips μπορούν να τοποθετηθούν σε μικρές συσκευές. Τα μικρά αυτά κυκλώματα δεν έχουν σαφώς την ίδια ικανότητα επεξεργασίας δεδομένων, όμως αν συνδυαστούν με όσα αναφέρθηκαν για το Cloud Computing και την εξέλιξη των Data Analytics, ανοίγουν τις πόρτες σε νέες δυνατότητες παρέχοντας υπηρεσίες στον άνθρωπο που μέχρι πρότινος μπορούσαν να γίνουν μόνο από την υπολογιστική ισχύ ενός προσωπικού υπολογιστή.

Οι παραπάνω λόγοι εξηγούν αφενός την ταχύτητα με την οποία πλέον το IoT εξελίσσεται και γίνεται μέρος της καθημερινότητας και αφετέρου το γιατί μέχρι πρότινος δεν ήταν δυνατό να πραγματοποιηθεί στην πράξη. Θα άξιζε να αναφέρουμε στο σημείο αυτό, πως πέραν των παραπάνω, σημαντικό ρόλο έχει παίξει η έρευνα και η χρηματοδότηση που έχει δοθεί τα τελευταία χρόνια στον τομέα αυτό, επιτρέποντας να έχουμε αύξηση της υπολογιστικής ισχύς με ταυτόχρονη μείωση του κόστους πρόσβασης και κτήσης αυτής.

Τεχνολογίες που εμπλέκονται στο IoT

Έχοντας εξηγήσει εν συντομία την έννοια του IoT, κρίνεται σκόπιμο να αναλυθούν και οι τεχνολογίες από τις οποίες εξαρτάται κατά κύριο λόγο η λειτουργία του. Εκτός από τις "έξυπνες συσκευές" που έχουν τη δυνατότητα να είναι συνδεδεμένες στο διαδίκτυο, είναι απαραίτητη και η ένταξη στο σχεδιασμό της γενικότερης αρχιτεκτονικής, τεχνολογιών οι οποίες θα μπορούν να λαμβάνουν πληροφορίες του περιβάλλοντος, να αναγνωρίζουν τη θέση του αντικειμένου και να συνδυαστούν με βέλτιστο τρόπο ώστε να γίνει δυνατή η υλοποίηση του οράματος "Internet of Things". Οι σημαντικότερες τεχνολογίες οι οποίες μπορούν να παίξουν το ρόλο αυτό σήμερα, θεωρούνται οι εν γένει τεχνολογίες μικρών radio chips, όπως για παράδειγμα οι Sensors, Bluetooth και τα RFID tags. Οι παραπάνω τεχνολογίες, είναι γνωστές και χρησιμοποιούνται σε διάφορους τομείς της ανθρώπινης δραστηριότητας μέχρι και σήμερα, όμως τα ιδιαίτερα χαρακτηριστικά τους όπως για παράδειγμα, το μικρό κόστος κατασκευής και λειτουργικό κόστος, τα καθιστά ιδανικά για την χρήση τους σε συσκευές και υπηρεσίες Internet of Things.

SENSORS

Οι αισθητήρες είναι συσκευές οι οποίες μπορούν να μετρούν τις συνθήκες του περιβάλλοντος στο οποίο τοποθετούνται και στη συνέχεια να μετατρέπουν αυτή την πληροφορία σε ψηφιακή μορφή ώστε να μπορεί να χρησιμοποιηθεί για παρατήρηση, μετρήσεις και αξιολόγηση της ποιότητας του αντικειμένου. Για παράδειγμα, η χρήση αισθητήρων σε γέφυρες μπορεί να δώσει σημαντική πληροφορία για την κατάσταση

της μετά από ένα σεισμό ή μετά μεγάλο χρονικό διάστημα χρήσης της, καθώς μπορεί να δώσει ενδείξεις για μια πιθανή βλάβη που διαφορετικά δε θα γινόταν αντιληπτή. Με αυτό τον τρόπο, μπορεί εγκαίρως να αποφευχθεί κάποια καταστροφή που θα σήμαινε την ύπαρξη θυμάτων. Γενικά, οι αισθητήρες αποτελούν το μέσο με το οποίο γεφυρώνεται η απόσταση μεταξύ του φυσικού κόσμου και του ψηφιακού και συνδυαζόμενοι με άλλες τεχνολογίες μπορούν να βοηθήσουν τον άνθρωπο στην απλοποίηση των καθημερινών δραστηριοτήτων του.

Οι "έξυπνες συσκευές" προκειμένου να λειτουργήσουν όπως σχεδιάζονται, προϋποθέτουν ακριβώς αυτή τη λειτουργικότητα των αισθητήρων. Πρέπει να είναι σε θέση να διαβάζουν και να "αισθάνονται" το περιβάλλον τους ώστε να μπορούν να μεταφράσουν τα ερεθίσματα αυτού σε χρήσιμη πληροφορία και να βοηθούν τον άνθρωπο να λαμβάνει αποφάσεις. Έχοντας πετύχει αυτό και σε συνδυασμό με την τεχνογνωσία των τελευταίων ετών που έχει εξελιχθεί με ταχύτατους ρυθμούς, οι αισθητήρες με το κατάλληλο λογισμικό και υλικό μπορούν να τοποθετηθούν σε καθημερινές οικιακές συσκευές και να χειρίζονται απομακρυσμένα. Ένα παράδειγμα αυτής της λειτουργικότητας είναι οι φούρνοι, οι οποίοι θα μπορούν να λειτουργούν από το κινητό και να δίνουν τη δυνατότητα να μαγειρεύουν το φαγητό χωρίς να είναι παρούσα η νοικοκυρά. Στα ψυγεία, οι αισθητήρες θα μπορούν να δώσουν ανά πάσα στιγμή την πληροφορία για την ποσότητα των διαθέσιμων αγαθών και είτε αυτόματα να πραγματοποιείται μια παραγγελία απο κάποιο σούπερ μάρκετ ή να βοηθούν στα ψώνια που κάνει κάποιος.[2,3,20]

RFID tags

Η τεχνολογία RFID συχνά θεωρείται προαπαιτούμενο για το IoT. Η ετικέτα RFID είναι ένα σύστημα το οποίο τοποθετείται σε ένα αντικείμενο, εκπέμπει και λαμβάνει πληροφορία μέσω ραδιοκυμάτων με σκοπό την αναγνώριση και παρακολούθηση αυτού.

Η λειτουργία των ετικετών προϋποθέτει την ύπαρξη δυο συστατικών μερών, της ετικέτας (tag) και του αναγνώστη (reader) αυτής. Μια ετικέτα περιλαμβάνει ένα ενσωματωμένο κύκλωμα και μια κεραία. Το κύκλωμα χρησιμεύει συνήθως στην

επεξεργασία και αποθήκευση της πληροφορίας, την ανάγνωση του σήματος που έρχεται από το Reader αλλά και την προετοιμασία του σήματος που θα στείλει η ίδια, αλλά παρέχει και άλλες λειτουργίες ανάλογα το αντικείμενο στο οποίο είναι τοποθετημένη. Η κεραία είναι υπεύθυνη για την αποστολή και λήψη του σήματος.

Η λειτουργία του είναι απλή και μπορεί να παρομοιαστεί με αυτή των barcodes, όπου ένα scanner σκανάρει το barcode και διαβάζει την πληροφορία που παρέχει. Η διαφορά τους όμως σε σχέση με τις ετικέτες RFID έγκειται στο γεγονός ότι το scanner, μπορεί να διαβάσει ενα barcode την φορά και απαιτείται η οπτική επαφή μεταξύ τους, ενώ οι RFID ετικέτες μπορούν να αναγνωστούν πολλές ταυτόχρονα χωρίς να μπερδεύονται τα διάφορα σήματα διαφορετικών ετικετών και χάριν στα ραδιοκύματα, η ανάγνωσή τους μπορεί να γίνει απομακρυσμένα. Με αυτή τη δυνατότητα δεδομένη, μια ετικέτα μπορεί να βρίσκεται μέσα σε ένα κουτί, σε ένα ψυγείο, στο κινητό ή στην τσέπη του ανθρώπου.

Έχοντας ως οδηγό τη λειτουργία που προσφέρουν οι ετικέτες RFID καθώς και το γεγονός ότι το IoT είναι ένα δίκτυο συνεχώς συνδεδεμένων συσκευών, στόχος εδώ, είναι να εξοπλίσουμε όσο το δυνατόν μεγαλύτερο αριθμό προϊόντων με αυτή την τεχνολογία. Προϋπόθεση αυτού του στόχου, είναι η ύπαρξη ενός μέσου το οποίο θα είναι φθηνό, απλό και εύκολα προσαρτώμενο στα αντικείμενα. Οι ετικέτες RFID, λύνουν αυτό το πρόβλημα καθώς μπορούν να προστεθούν σε όλα τα προϊόντα με ελάχιστο κόστος και χάριν στο μικρό τους μέγεθος δεν επηρεάζουν την αισθητική και τη λειτουργικότητα αυτών. Επιπλέον, υπάρχουν τύποι παθητικών ετικετών οι οποίες προσθέτουν το πλεονέκτημα ότι δεν απαιτούν κάποια πηγή ενέργειας και λειτουργούν με την ενέργεια που τους παρέχεται από τον reader που στέλνει το σήμα προς αυτές για τη λήψη των πληροφοριών. Αυτό, έχει ως αποτέλεσμα να μην υπάρχει κόστος συντήρησης ή κατανάλωσης ενέργειας που θα επιβάρυνε το προϊόν στο οποίο θα προσαρτηθεί, εξασφαλίζοντας έτσι, έστω θεωρητικά, μια χρησιμότητα εφ' όρου ζωής.

Όλα τα παραπάνω πλεονεκτήματα χρήσης των RFID, αν συνδυαστούν και με τη λειτουργία των αισθητήρων (sensors), η πληροφορία που μπορεί να εξαχθεί ποικίλει ανάλογα το αντικείμενο. Για παράδειγμα, μπορεί να μεταδίδει την θερμοκρασία ενός φούρνου ή ενός θερμοσίφωνα για να ελέγχεται αν λειτουργεί εντός των

προδιαγραφών του και επομένως να αποφευχθεί μια πιθανή βλάβη ή χειρότερα, μια καταστροφή. Άλλο παράδειγμα της χρησιμότητας αυτής της τεχνολογίας είναι η προσθήκη αισθητήρων κραδασμών σε μηχανήματα ενός χημικού εργαστηρίου όπου υπάρχουν επιβλαβείς, για την υγεία του ανθρώπου, ουσίες και επομένως να προειδοποιούνται οι χειριστές αυτών αν κάτι πάει στραβά σε περίπτωση σεισμού ή απλής μεταφοράς αυτών. [2,4,20]

Bluetooth

Μια από τις προκλήσεις που το IoT καλείται να αντιμετωπίσει είναι αυτή της ενέργειας. Μια συσκευή η οποία τροφοδοτείται από το ρεύμα του σπιτιού ή της επιχείρησης και ταυτόχρονα πρέπει να είναι συνδεδεμένη στο διαδίκτυο, δεν αποτελεί πρόβλημα, καθώς μέσω μιας υπάρχουσας σύνδεσης Wi-Fi, η οποία είναι πιο κοστοβόρα από πλευράς ενέργειας, μπορεί να αλληλεπιδρά με το διαδίκτυο. Το πρόβλημα εμφανίζεται στις συσκευές που λειτουργούν με μπαταρία, όπως τα κινητά, tablet, τα ρολόγια. Μια προτεινόμενη εναλλακτική, η οποία ξεπερνά το πρόβλημα αυτό, είναι η εκμετάλλευση της τεχνολογίας Bluetooth.

Το Bluetooth είναι ένα πρότυπο ασύρματης τεχνολογίας για την ανταλλαγή δεδομένων σε μικρές αποστάσεις (χρησιμοποιώντας ακτινοβολία UHF μικρού μήκους κύματος) και μπορεί να εγκατασταθεί σε σταθερές και κινητές συσκευές με σκοπό τη δημιουργία προσωπικών δικτύων (PAN). Εμφανίστηκε το 1994 και έχει χρησιμοποιηθεί στο παρελθόν για πολλές λειτουργίες, μια εκ των οποίων και πιο γνωστή σε όλους είναι η ανταλλαγή αρχείων μεταξύ κινητών τηλεφώνων, τα handsfree και τα ασύρματα ηχεία κινητών για την ακρόαση μουσικής. Από την έκδοση 1.0 πέρασε πολλά στάδια εξέλιξης μέχρι να φτάσει σήμερα στην έκδοση 4.2 με την οποία είναι εξοπλισμένες οι περισσότερες συσκευές σήμερα και την ακόμα νεότερη έκδοση «5.0 BLE (Bluetooth Low-Energy)» η οποία δίνει περισσότερη έμφαση στην εξελισσόμενη τεχνολογία του Internet of Things, με σημαντικότερο πλεονέκτημα τη μείωση της απαιτούμενης ενέργειας λειτουργίας του. Αυτό επιτεύχθηκε κάνοντας το πρωτόκολλο να έχει μεγαλύτερο χρόνο μεταξύ των advertisements των σημάτων και την αποστολή μικρότερων πακέτων δεδομένων. Ο λόγος για τον οποίο η μείωση της απαιτούμενης ενέργειας καθιστά το Bluetooth

ιδανικό για λειτουργίες IoT είναι επειδή η παραδοσιακή τεχνολογία και χρήση του διαδικτύου μπορεί να μειώσει σημαντικά τον χρόνο ζωής της μπαταρίας της συσκευής. Γίνεται επομένως εύκολα κατανοητό πως η χρήση του BLE στις διάφορες συσκευές του IoT θα βοηθήσει στη λειτουργία τους με έναν πιο οικονομικό και αποδοτικό τρόπο. [5]

Η βελτιωμένη λειτουργικότητα του IoT με τη χρήση του BLE υπερβαίνει όμως την απλή εξοικονόμηση ενέργειας. Το BLE έχει τη δυνατότητα να επεκτείνει το φάσμα της σύνδεσης μεταξύ των συσκευών κατά σχεδόν τέσσερις φορές σε σχέση με το δίκτυο Wi-Fi. Αυτό καθιστά μια πιο αξιόπιστη μέθοδο για τη σύνδεση πολλών έξυπνων συσκευών σε ένα περιβάλλον όπως ένα έξυπνο σπίτι. Επιπλέον, οι ταχύτητες επικοινωνίας αναβαθμίζονται σχεδόν στο διπλάσιο από την τρέχουσα έκδοση (σε 2Mbit) και είναι πολύ πιο ικανές να ικανοποιήσουν τις απαιτήσεις της συνεχούς επικοινωνίας που είναι προαπαιτούμενο για συσκευές IoT. Τέλος, ένα ακόμα πλεονέκτημα που προσφέρει η εξέλιξη της τεχνολογίας Bluetooth, είναι ότι μέσα από την αναβάθμιση των πρωτοκόλλων του έχει πλέον διασφαλιστεί πως το σήμα του δε θα μπλέκεται με αυτά άλλων Low Frequency Radios, πράγμα που σε παλαιότερες εκδόσεις του αποτελούσε πρόβλημα.[6]

Near Field Communication

Αποτελεί μια πρότυπη μικρής εμβέλειας ασύρματη τεχνολογία συνδεσιμότητας η οποία μεταφέρει δεδομένα με ρυθμό έως και 424 kbps και έχει γίνει γνωστή κυρίως μέσω της χρήσης της από τα κινητά τελευταίας γενιάς (smartphones). Η λειτουργία της βασίζεται στην επαφή ή την προσέγγιση, σε απόσταση λίγων εκατοστών, της συσκευής που περιέχει το τσιπ NFC, σε κάποια άλλη συσκευή που περιλαμβάνει τον κατάλληλο αισθητήρα. Η τεχνολογία NFC συνδυάζει στοιχεία παλαιότερων τεχνολογιών όπως το Bluetooth και τις RFID-tags που αναφέρθηκαν προηγουμένως.[24] Οι κυριότεροι λόγοι για τους οποίους το Near Field Communication μπορεί να προταθεί για χρήση με το Internet of Things είναι οι ακόλουθοι:[25]

- Επιλύει την πρόκληση των μη ενεργοποιημένων αντικειμένων που δεν έχουν πρόσβαση στο δίκτυο. Οι ενσωματωμένες ετικέτες NFC σε αυτά τα

unpowered αντικείμενα επιτρέπουν την προσθήκη πληροφοριών από οπουδήποτε.

- Οι αλληλεπιδράσεις NFC είναι εύκολες και απλές καθώς δεν χρειάζεται παρά μόνο ένα απλό άγγιγμα
- Παρέχει μεγαλύτερο επίπεδο ασφάλειας, καθώς οι μεταδόσεις είναι μικρής εμβέλειας και δεν μπορεί να γίνει υποκλοπή δεδομένων ασύρματα

Οι υποστηρικτές αυτής της τεχνολογίας έχουν να παραθέσουν και ορισμένα πλεονεκτήματα χρήσης της έναντι του BLE, σημαντικότερα εκ των οποίων είναι τα εξής:

- Η τεχνολογία NFC καταναλώνει μικρότερη ισχύ σε σύγκριση με την τυπική τεχνολογία Bluetooth. Η μόνη περίπτωση στην οποία το NFC χρειάζεται περισσότερη ενέργεια από το Bluetooth, είναι όταν καλείται να τροφοδοτήσει μια παθητική, μη ενεργοποιημένη πηγή.
- Η εγγύτητα που απαιτείται μεταξύ των συσκευών που είναι συνδεδεμένες με το NFC, αποδεικνύεται χρήσιμη προκειμένου να αποτρέπεται η παρεμβολή σημάτων από άλλες συσκευές και προσπαθούν να επικοινωνήσουν, κάτι που το BTLE μπορεί να συναντήσει μεγαλύτερο βαθμό δυσκολίας στο να το αποτρέψει.

Παρόλα αυτά, με τις τελευταίες εκδόσεις του Bluetooth (BLE), η κατεύθυνση στην οποία οι δυο αυτές τεχνολογίες κινούνται είναι προς αυτή της συνεργασίας. Για παράδειγμα, δεδομένου ότι το NFC μπορεί να συνδέσει πιο γρήγορα και με ασφάλεια δυο κοντινές συσκευές (όπως για παράδειγμα ορισμένες συσκευές που βρίσκονται σε μικρή απόσταση σε ένα έξυπνο σπίτι) μπορεί, αφού καταστήσει τη σύνδεση, να τη μετατρέψει σε σύνδεση BLE ώστε να επωφεληθεί τη μεγαλύτερη ταχύτητα μεταφοράς δεδομένων που προσφέρει.

Έχοντας περιγράψει τη βασική ιδέα του Internet of Things καθώς επίσης και τις βασικές τεχνολογίες οι οποίες απαιτούνται για να γίνει εφικτή η υλοποίηση αυτού, στις επόμενες σελίδες θα αναλυθεί σε βάθος η αρχιτεκτονική των πρωτοκόλλων επικοινωνίας που χρησιμοποιούνται σε επίπεδο δικτύου, δίνοντας ιδιαίτερη έμφαση στο πρωτόκολλο CoAP (Constrained Application Protocoll) και του ICN (Information-Centric Networking), το οποίο αποτελεί μια μέθοδο που μπορεί να βελτιστοποιήσει την αποδοτικότητα και αποτελεσματικότητα του CoAP.[26]

ΜΕΡΟΣ ΔΕΥΤΕΡΟ

CONSTRAINED APPLICATION PROTOCOL (CoAP)

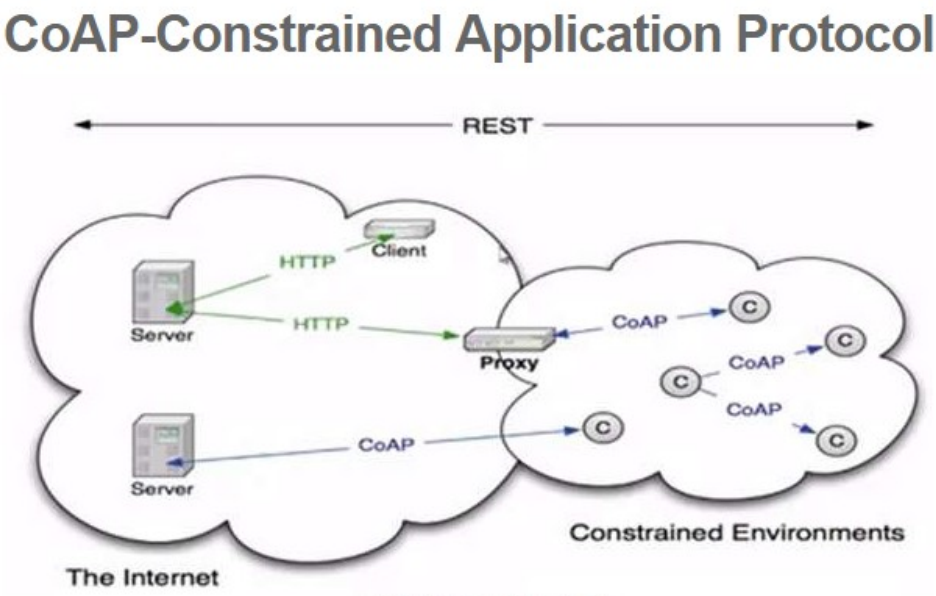
ΚΕΦΑΛΑΙΟ 2

Βασικές έννοιες – Σχέση CoAP και HTTP

Το COAP είναι ένα εξειδικευμένο πρωτόκολλο μεταφοράς το οποίο χρησιμοποιείται με περιορισμένους κόμβους και δίκτυα περιορισμένης εμβέλειας. Είναι σχεδιασμένο για εφαρμογές machine to machine (M2M), όπως είναι αυτές που χρησιμοποιούνται σε περιβάλλοντα IoT. Προορίζεται για την παροχή RESTful υπηρεσιών, όμοιες με αυτές του HTTP, ενώ παράλληλα ελαχιστοποιεί την πολυπλοκότητα και το μέγεθος των πακέτων που αποστέλλονται με σκοπό να είναι λειτουργικές σε περιορισμένα περιβάλλοντα πόρων.[7]

Παρέχει αλληλεπίδραση του τύπου «ερώτηση / απάντηση» μεταξύ των άκρων ενός δικτύου και η φιλοσοφία του μοιάζει με αυτή του Διαδικτύου όσον αφορά τα URIs και τους τύπους των μέσων. Είναι σχεδιασμένο με τέτοιο τρόπο ώστε να καθιστά δυνατή την αλληλεπίδραση με το πρωτόκολλο HTTP που χρησιμοποιείται στο διαδίκτυο και παράλληλα να καλύπτει εξειδικευμένες απαιτήσεις όπως πολλαπλή υποστήριξη (multicast support), μικρό «κόστος» σε θέματα μεγέθους δεδομένων που μεταφέρονται, καθώς επίσης και απλότητα, που είναι αναγκαία σε περιβάλλοντα με περιορισμούς. Ουσιαστικά, αποτελεί μια αναβαθμισμένη έκδοση του HTTP. Έχει σχεδιαστεί για εφαρμογές όπως IoT / WSN / M2M κλπ. και ασίζεται σε UDP. Χρησιμοποιεί μηνύματα ACK έτσι ώστε να γίνει αξιόπιστο όπως το TCP. Έχει χαμηλή λανθάνουσα κατάσταση και καταναλώνει λιγότερη ισχύ σε σύγκριση με το HTTP.

Η αρχιτεκτονική του CoAP θα μπορούσε να περιγραφεί με το παρακάτω σχήμα:



CoAP Architecture

Σύμφωνα με το παραπάνω σχήμα γίνεται άμεσα αντιληπτό πως οι συσκευές που τρέχουν το πρωτόκολλο CoAP δε μπορούν να αλληλεπιδράσουν άμεσα με το πρωτόκολλο HTTP και συχνά μπορεί να απαιτείται η ύπαρξη κάποιου ενδιαμέσου, όπως ενός proxy.[8]

CoAP και HTTP

Σε γενικές γραμμές, το CoAP, έχει πολλές ομοιότητες με το HTTP, υπάρχουν όμως και σημαντικές διαφορές. Οι κόμβοι οι οποίοι χρησιμοποιούν το CoAP είναι συνήθως μεγάλοι σε πλήθος ενώ συχνά συσχετίζονται μεταξύ τους ανά τοποθεσία ή λειτουργικότητα. Για παράδειγμα, μπορεί σε ένα κτίριο να είναι επιθυμητή η μαζική διαχείριση του φωτισμού ή της θερμοκρασίας, ή ακόμα και να επιθυμούμε τη διαχείριση αυτών ανά όροφο ή γραφείο. Απόρροια των παραπάνω είναι η δημιουργία αρκετών ομάδων συσκευών. Οι μηχανισμοί ομαδικής επικοινωνίας (group communication mechanisms), μπορούν να βελτιώσουν την αποδοτικότητα και τον χρόνο απόκρισης μιας τέτοιας εφαρμογής μέσω λειτουργικότητας η οποία όμως, δεν υποστηρίζεται από το HTTP.[7] Οι κυριότερες διαφορές μεταξύ των δυο πρωτοκόλλων αναγράφονται στον επόμενο πίνακα:

Feature	CoAP	HTTP
Protocol	It uses UDP.	It uses TCP.
Network layer	It uses IPv6 along with 6LoWPAN.	It uses IP layer.
Multicast support	It supports.	It does not support.
Architecture model	CoAP uses both client-Server & Publish-Subscribe models.	HTTP uses client and server architecture.
Synchronous communication	CoAP does not need this.	HTTP needs this.
Overhead	Less overhead and it is simple.	More overhead compare to CoAP and it is complex.
Application	Designed for resource constrained networking devices such as WSN/IoT/M2M.	Designed for internet devices where there is no issue of any resources.

Με μια σύντομη ανάγνωση στον παραπάνω πίνακα, βλέπουμε πως το πρωτόκολλο CoAP έχει σημαντικές διαφορές σε σχέση με το HTTP. Υποστηρίζει τη λειτουργία multicast ενώ το HTTP όχι, δεν προαπαιτεί τη συγχρονισμένη επικοινωνία, χρησιμοποιεί τόσο την client-server επικοινωνία όσο και τα μοντέλα Publish-Subscribe που θα εξεταστούν σε επόμενο κεφάλαιο, ενώ φαίνεται καθαρά πως το HTTP έχει σχεδιαστεί χωρίς να λαμβάνει υπόψη το κόστος που μπορεί να έχει ούτε στη μεταφορά δεδομένων ούτε και στην κατανάλωση ενέργειας. Πέραν όμως των παραπάνω διαφορών, υπάρχουν και άλλες διαφορές, σημαντικότερες εκ των οποίων είναι:[8]

- Στη λειτουργία pull, ένα έξυπνο αντικείμενο ενεργεί ως διακομιστής που περιμένει τα αιτήματα από έναν απομακρυσμένο κόμβο και ανταποκρίνεται στα αιτήματα με τις απαιτούμενες πληροφορίες, π.χ. με την παράδοση της στιγμιαίας ανάγνωσης αισθητήρα. Το έξυπνο αντικείμενο δεν «κοιμάται» ή συχνά ξυπνά, καθώς είναι πάντα έτοιμο να απαντήσει άμεσα σε εισερχόμενο αίτημα.
- Στη λειτουργία push, ένα έξυπνο αντικείμενο ενεργεί ως πελάτης και αποστέλλει περιοδικά τις πληροφορίες σε έναν απομακρυσμένο διακομιστή ιστού. Το έξυπνο αντικείμενο κυρίως κοιμάται και ξυπνά μόνο όταν χρειάζεται να μεταδώσει τις πληροφορίες. Εκτός από την περιοδική επικοινωνία, το CoAP παρέχει επίσης την επιλογή Observe που επιτρέπει στα ευφυή αντικείμενα να επικοινωνούν μόνο όταν πληρείται μια συγκεκριμένη συνθήκη.

Το CoAP δεν προορίζεται να αντικαταστήσει το HTTP, ενώ αντίθετα, φαίνεται να το "μιμείται", μόνο επειδή ακολουθεί το RESTful παράδειγμα . Το CoAP προορίζεται ως επίπεδο εφαρμογής για περιορισμένες συσκευές ενώ ένας από τους λόγους που επιλέχθηκε ο σχεδιασμός RESTful είναι προκειμένου να διευκολύνει τη λειτουργία proxying.

Το CoAP χτίζεται έχοντας πάντα ως βασικό κριτήριο τους λίγους πόρους. Η μικρή κεφαλίδα και το διαφορετικό χαρακτηριστικό του CoAP είναι σε θέση να βεβαιώσει ότι η συσκευή περιορισμών δυνατοτήτων μπορεί να επικοινωνεί στο Διαδίκτυο. Επιπλέον, το HTTP και το CoAP έχει το καθένα το δικό τους σκοπό. Το CoAP είναι βελτιστοποιημένο για τα δίκτυα περιορισμένων πόρων και τις συσκευές που είναι τυπικές για εφαρμογές IoT και M2M. Χρησιμοποιεί λιγότερους πόρους από το HTTP και μπορεί να προσφέρει ένα περιβάλλον επικοινωνίας σε WSNs, IoTs και M2M communication. Το HTTP έχει σχεδιαστεί κυρίως για συσκευές στο Διαδίκτυο, όπου η ισχύς και οι άλλοι περιορισμοί δεν αποτελούν σημαντικά ζητήματα. Το HTTP είναι πιο αξιόπιστο από το CoAP καθώς χρησιμοποιεί το TCP.

Επιπλέον, το CoAP έχει εφαρμοστεί για περιβάλλον IoT και M2M, για την αποστολή σύντομων μηνυμάτων χρησιμοποιώντας το UDP. Για παράδειγμα:
Μια τυπική ανταλλαγή CoAP αποτελείται από 2 μηνύματα, δηλ. ένα αίτημα και μια απάντηση. Αντίθετα, ένα αίτημα HTTP απαιτεί πρώτα ο client να δημιουργήσει μια σύνδεση TCP και να τερματίσει αργότερα. Αυτό έχει ως αποτέλεσμα τουλάχιστον 9 μηνύματα για ένα μόνο αίτημα. Το TCP είναι σε θέση να στείλει πολλαπλά πακέτα ταυτόχρονα και να τα αναγνωρίσει όλα με μία μόνο επιβεβαίωση. Η μεταφορά του CoAP ωστόσο απαιτεί επιβεβαίωση για κάθε μπλοκ και οδηγεί σε περισσότερα μηνύματα και υψηλότερο χρόνο μεταφοράς. Εφόσον αναμένουμε ότι η πλειονότητα των μηνυμάτων του CoAP είναι αρκετά μικρά, αυτό είναι λιγότερο σημαντικό. Ο blockwise μηχανισμός του CoAP ωστόσο επιτρέπει σε έναν Server όχι μόνο να λαμβάνει αλλά και να επεξεργάζεται ένα μεγάλο αίτημα μπλοκ-μπλοκ κάτι το οποίο δε θα ήταν εφικτό αν χρησιμοποιούσαμε HTTP και TCP.[10]

Ένα από τα σημαντικότερα πλεονεκτήματα του CoAP όπως περιγράφηκε και προηγουμένως, είναι η το μειωμένο ενεργειακό και δικτυακό κόστος σε σχέση με το

HTTP. Έχουν πραγματοποιηθεί έρευνες που αφορούν το «συνολικό κόστος ιδιοκτησίας» (TCO Total cost of ownership), οι οποίες καταλήγουν στα ακόλουθα:[8]

- Το CoAP είναι γενικά πιο οικονομικό από το HTTP για εφαρμογές με μεγάλο αριθμό έξυπνων αντικειμένων, το καθένα από τα οποία ασχολείται με συχνές συνεδρίες επικοινωνίας, ενώ για σπάνιες αλληλεπιδράσεις η διαφορά κόστους μεταξύ των πρωτοκόλλων είναι ασήμαντη.
- Η χρήση του CoAP επιτρέπει να μειωθεί δραματικά το κόστος των εφαρμογών σε περίπτωση που η χρέωση για τις επικοινωνίες δεδομένων είναι βασισμένη στον όγκο, καθώς η μικρή επιβάρυνση του πρωτοκόλλου και η εξάρτησή του από το UDP επιτρέπουν πολλαπλή μείωση στον όγκο των δεδομένων .
- Τέλος, η χρήση του CoAP θεωρείται οικονομικά πιο επωφελής σε περίπτωση που τα έξυπνα αντικείμενα ενεργοποιούνται μόνο για την περιστασιακή εκκίνηση των επικοινωνιακών συνόδων (push mode of communication), αντίθετα με την περίπτωση όταν το έξυπνο αντικείμενο είναι τακτικά αφυπνισμένο σε κατάσταση αναμονής για εισερχόμενες αιτήσεις επικοινωνίας (pull mode).

Διευρύνοντας περαιτέρω τα οφέλη εφαρμογής του CoAP, αξίζει να αναφερθεί πως χάριν των χαρακτηριστικών του:[10]

- ✓ Μπορεί να προσφέρει μια πιο συμπαγή δυαδική κεφαλίδα 10-20 bytes συνολικά μαζί με τη μεταφορά UDP, μειώνοντας την ποσότητα δεδομένων που χρειάζεται να μεταδίδονται μαζί με το ωφέλιμο φορτίο, επιφέροντας έτσι μείωση στην καθυστέρηση και ελαχιστοποίηση της καταπόνησης της μπαταρίας λόγω δεδομένων μετάδοσης.
- ✓ Η υποστήριξη για την προώθηση ασύγχρονων πληροφοριών (η επιλογή παρακολούθησης) επιτρέπει στα έξυπνα αντικείμενα να στέλνουν πληροφορίες σχετικά με τον πόρο μόνο όταν αλλάζει, επιτρέποντας έτσι στα αντικείμενα να αδρανοποιούνται κατά το μεγαλύτερο διάστημα μειώνοντας περαιτέρω την κατανάλωση ισχύος τους.
- ✓ Η χρήση ενός ελάχιστου υποσυνόλου των αιτημάτων REST επιτρέπει το πρωτόκολλο να είναι λιγότερο περίπλοκο σε σύγκριση με το HTTP,

μειώνοντας έτσι τις απαιτήσεις υλικού για τα έξυπνα αντικείμενα στα οποία εκτελείται.

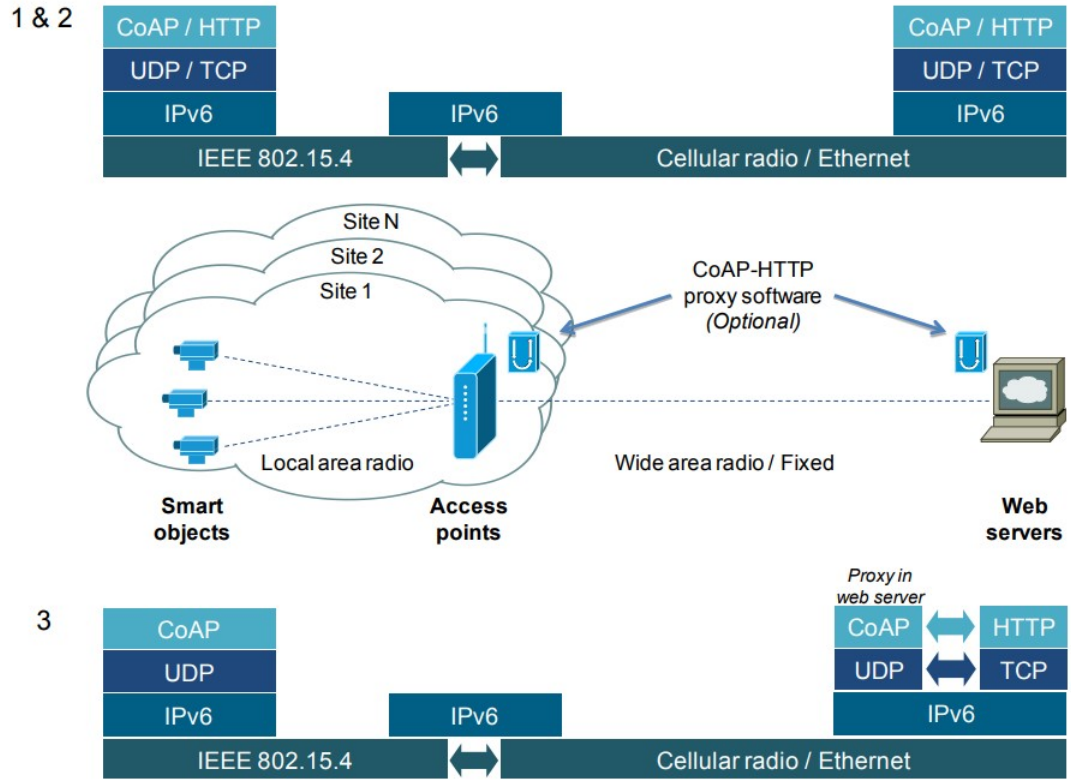
Παρά το γεγονός ότι η λειτουργία client/server στο CoAP μοιάζει πολύ με αυτή του HTTP, μια υλοποίηση CoAP μεταξύ δυο συσκευών, τους δίνει τη δυνατότητα να έχουν ταυτόχρονα και το ρόλο του client και του server. Ένα CoAP request είναι αντίστοιχο με αυτό του HTTP και αποστέλλεται από έναν client ο οποίος αναμένει την απάντηση από έναν «πόρο» ο οποίος αναγνωρίζεται από το URI της. Στη συνέχεια, ο πόρος αποστέλλει την απάντηση (Response Code) στη συσκευή η οποία μπορεί να περιλαμβάνει την «αναπαράσταση» του πόρου. Το πρωτόκολλο CoAP, αντίθετα με το HTTP που είθισται να χρησιμοποιεί για την μεταφορά πακέτων μέσω TCP, μεταφέρει αυτά τα δεδομένα μέσω UDP χρησιμοποιώντας ένα στρώμα μηνυμάτων με προαιρετική αξιοπιστία. Οι τύποι μηνυμάτων που ορίζονται από αυτό το πρωτόκολλο είναι:

- Confirmable,
- Non-confirmable,
- Acknowledgement, αναγνώριση
- Reset, επαναφορά και
- Κωδικούς Απάντησης, οι οποίοι περιλαμβάνονται σε κάποια από τα μηνύματα που μεταφέρουν ερωτήσεις ή απαντήσεις.

Οι ερωτήσεις μπορούν να αποστέλλονται σε confirmable ή non-confirmable μηνύματα, ενώ οι απαντήσεις μπορούν επίσης να μεταφέρονται σε τέτοιου είδους μηνύματα ή να περιλαμβάνονται και στα μηνύματα αναγνώρισης.

Λόγω της μικτής κεφαλίδας και της χρήσης της μεταφοράς UDP, τα γενικά έξοδα επικοινωνίας του CoAP είναι σημαντικά μικρότερα σε σύγκριση με του HTTP. Ως αποτέλεσμα, ανάλογα με το μέγεθος του ωφέλιμου φορτίου και τη ρύθμιση του client-server, η συναλλαγή CoAP / UDP ενδέχεται να απαιτεί μεταφορά 8-10 φορές λιγότερων bytes, σε σύγκριση με την ίδια συναλλαγή που χρησιμοποιεί HTTP / TCP . [8]

Το παρακάτω σχήμα απεικονίζει την αρχιτεκτονική αυτή και αποτελείται από έξυπνα αντικείμενα, σημεία πρόσβασης και servers.



Technical architecture for all of the cases under comparison

Ένας CoAP-HTTP proxy είναι ένα προαιρετικό στοιχείο λογισμικού στην αρχιτεκτονική, το οποίο μπορεί να χρησιμοποιηθεί για μετάφραση μεταξύ CoAP και HTTP αν τα έξυπνα αντικείμενα χρησιμοποιούν το CoAP αλλά ο διακομιστής κατανοεί μόνο το HTTP. Ανάλογα με την αρχιτεκτονική επιλογή, ο διακομιστής μεσολάβησης υλοποιείται είτε στα σημεία πρόσβασης είτε στους διακομιστές ιστού.

Η απεικονιζόμενη αρχιτεκτονική επιτρέπει τρεις εναλλακτικές λύσεις ανάπτυξης με χρήση του CoAP και του HTTP:

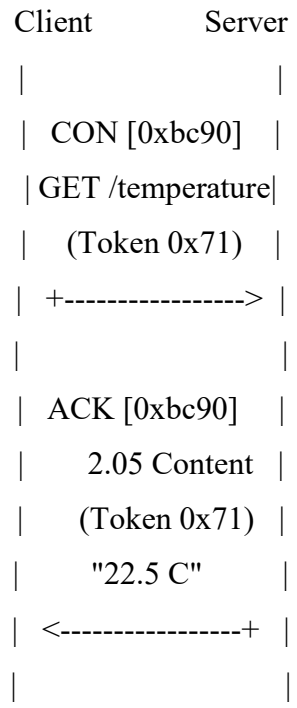
1. CoAP end-to-end (CoAP),
2. HTTP end-to-end (HTTP), και
3. CoAP μεταξύ έξυπνων αντικειμένων και proxy και HTTP μεταξύ proxy και web servers (CoAPproxy).

ΚΕΦΑΛΑΙΟ 3

Μοντέλο Μεταφοράς Μηνυμάτων

Όπως αναφέρθηκε και προηγουμένως, η μεταφορά των μηνυμάτων στο CoAP, γίνεται μέσω σύνδεσης UDP μεταξύ των ακρών. Τα μηνύματα που αποστέλλονται περιλαμβάνουν ένα header σταθερού μήκους (4 Bytes) και μπορεί να ακολουθούνται από κάποιο ωφέλιμο φορτίο, που είναι το ουσιαστικό μήνυμα. Κάθε μήνυμα περιλαμβάνει το Message ID ώστε να αποφεύγονται τα διπλότυπα αλλά παράλληλα να επιτυγχάνεται και κάποιος βαθμός αξιοπιστίας σε επίπεδο απώλειας δεδομένων. Μια επικοινωνία μεταξύ των συσκευών μπορεί να περιλαμβάνει την αποστολή ενός μηνύματος επιβεβαίωσης (CON) μαζί με το request, το οποίο απαντάται από ένα μήνυμα αναγνώρισης (ACK) και ίσως μαζί με το response, εξασφαλίζοντας έτσι ότι το μήνυμα έχει φτάσει τον προορισμό του και από τις δύο πλευρές. Σε περίπτωση που το μήνυμα αποστέλλεται χωρίς αίτημα επιβεβαίωσης, αν τελικά χαθεί, ο client δε θα λάβει την απάντηση που περιμένει, λήγει το timeout που έχει οριστεί και στη συνέχεια αποστέλλει μήνυμα επαναφοράς (RST).[7,11]

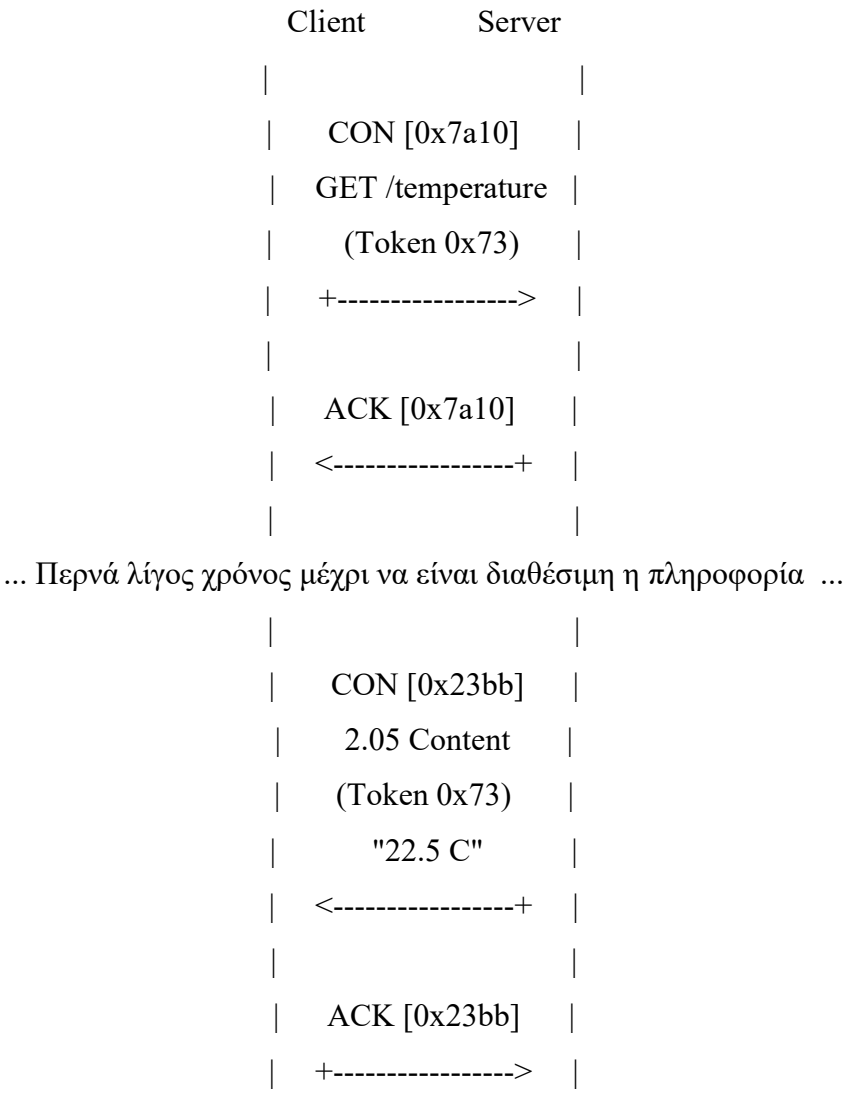
Ένα παράδειγμα του τρόπου επικοινωνίας που περιγράφεται πιο πάνω, είναι αυτό της αποστολής της θερμοκρασίας ενός χώρου. Αν υποθέσουμε πως το ερώτημα που στέλνει μια συσκευή, για παράδειγμα μια εφαρμογή κινητού, σε μια άλλη που έχουμε τοποθετήσει στο τέταρτο όροφο ενός γραφείου που μετρά τη θερμοκρασία, υγρασία κλπ., η επικοινωνία γίνεται όπως περιγράφει το παρακάτω σχήμα:[7]



Το κινητό στέλνει ένα CONfirmable μήνυμα GET προς το θερμόμετρο και στη συνέχεια λαμβάνει την επιβεβαίωση ACK με ενσωματωμένη την πληροφορία που ζητάμε.

Όταν μια συσκευή αποστέλλει ένα ερώτημα GET προς το server, υπάρχουν δυο ενδεχόμενα:

1. Αν ο server μπορεί να απαντήσει άμεσα, η απάντηση φτάνει στη μορφή που περιγράφει το σχήμα 1.
2. Αν όμως για κάποιο λόγο ο server δεν έχει έτοιμη την απάντηση άμεσα, είτε λόγω φόρτου είτε επειδή χρειάζεται χρόνος για να ετοιμαστεί η απάντηση, απαντά προς τον client με ένα απλό μήνυμα ACKnowledgement ώστε να επιβεβαιώσει ότι έλαβε το μήνυμα και να αποφευχθεί η επανάληψη της αποστολής του ερωτήματος, κάτι που μπορεί να επιβαρύνει το δίκτυο, όπως φαίνεται στο παρακάτω σχήμα:



ΜΟΡΦΟΠΟΙΗΣΗ ΜΗΝΥΜΑΤΟΣ

Όπως αναφέρθηκε πιο πάνω, τα μηνύματα που αποστέλλονται κωδικοποιούνται σε απλή δυαδική μορφή και ακολουθούν τη δομή του UDP Datagram. Το μήνυμα ξεκινάει με μια σταθερού μεγέθους κεφαλίδα (Header) 4bytes, η οποία ακολουθείται από ένα μεταβλητού μήκους Token, του οποίου το μέγεθος κυμαίνεται από 0 έως 8 bytes. Μετά το Token, αποστέλλεται μια ακολουθία από μηδέν ή περισσότερες επιλογές (options) που υποστηρίζει το CoAP σε μορφή TLV (Type-Length-Value)

και στη συνέχεια προαιρετικά ακολουθεί το ωφέλιμο φορτίο (payload) το οποίο δύναται να καταλάβει το υπόλοιπο διαθέσιμο datagram. Συγκεκριμένα:

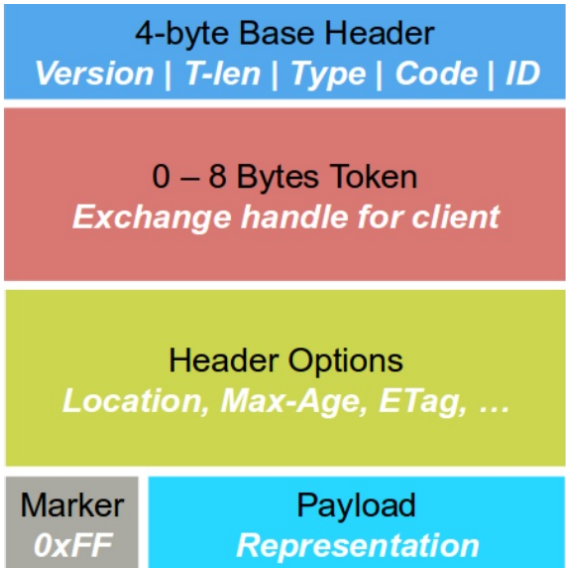
Τα πεδία του Header περιλαμβάνουν:

- Version (VER) 2bit integer: υποδεικνύει την έκδοση του CoAP. Προς το παρόν αναγράφεται η version 01 και ουσιαστικά αφήνει περιθώριο για ύπαρξη μελλοντικών εκδόσεων. Ένα μήνυμα με άγνωστη έκδοση αγνοείται.
- Type (T) 2bit integer: Υποδεικνύει αν το μήνυμα είναι Confirmable (0) ή Non-Confirmable (1), ACKnowledgement(2) ή Reset (3).
- TKL 4bit integer: υποδεικνύει το μεταβλητό μέγεθος του Token (0-8 bytes), ενώ αν είναι μεγαλύτερου μεγέθους αναγνωρίζεται ως "format error".
- Code 8bit integer: το οποίο διασπάται στα πρώτα 3 bit ως κλάση και τα υπόλοιπα ως λεπτομέρειες. Η κλάση μπορεί να πάρει τιμές 0 αν είναι ερώτημα, 2 αν είναι επιτυχημένη απάντηση, 4 ως client error, 5 ως server error.
- MessageID 16bit integer: Χρησιμοποιείται για να αναγνωρίζεται αν υπάρχουν διπλότυπα καθώς και για ταυτοποίηση μηνυμάτων τύπου Acknowledgement/Reset με μηνύματα τύπου Confirmable/non-confirmable.

Στη συνέχεια ακολουθούν οι διάφορες επιλογές (options) οι οποίες μπορεί συνοπτικά να είναι μορφής:

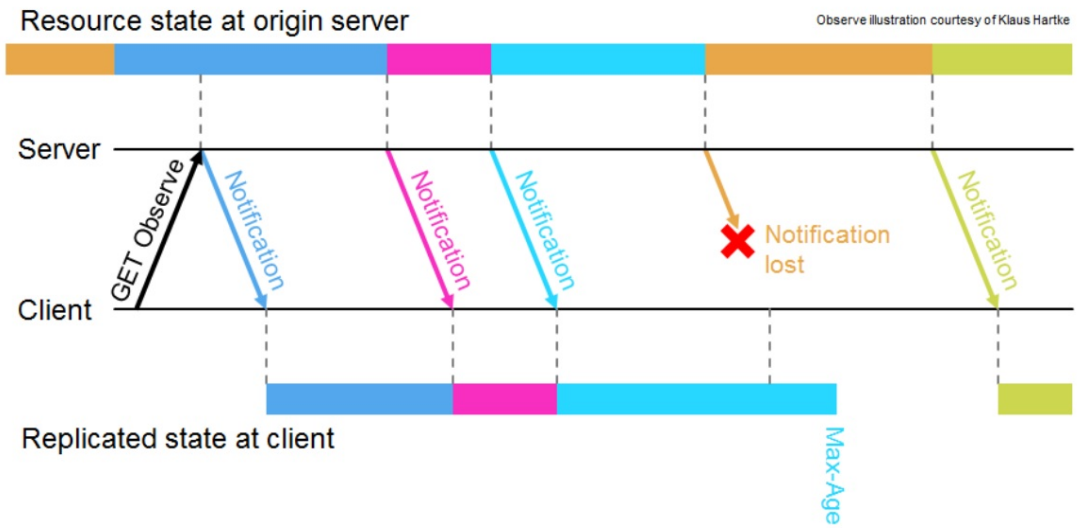
- Empty: Μια ακολουθία μηδενικών bytes
- Opaque: Ακολουθία αδιαφανών bytes
- Uint: Ένας μη αρνητικό integer αριθμός που εκπροσωπείται σε network-byte – order.
- String: Μια συμβολοσειρά string η οποία κωδικοποιείται από (UTF-8) σε Net-Unicode μορφή

Όλα τα παραπάνω μπορούν σχηματικά να γίνουν πιο κατανοητά με το παρακάτω σχήμα:



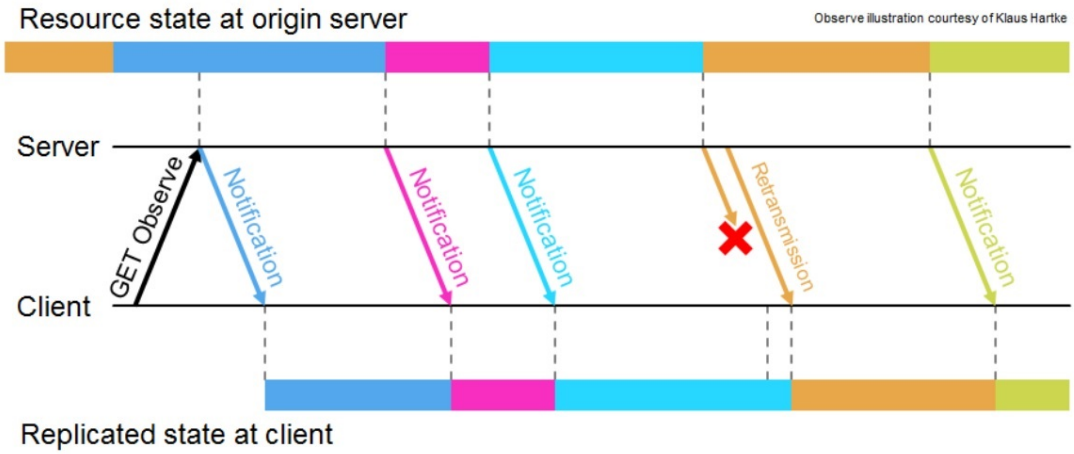
Εικόνα – Hands on CoAP, iot.eclipse org Matthias Kovatsch,Julian Vermillard

ΠΑΡΑΔΕΙΓΜΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΣΥΣΚΕΥΩΝ ΜΕ CoAP:



Εικόνα – Hands on CoAP, iot.eclipse org Matthias Kovatsch,Julian Vermillard

Σύμφωνα με το παραπάνω σχήμα, περιγράφεται μια επικοινωνία Non-Confirmable, η οποία ξεκινάει από την πλευρά του client ο οποίος στέλνει ένα μήνυμα GET observe, που στην ουσία ζητά ανά κάποιο διάστημα να του αποστέλλεται μια κατάσταση. Βλέπουμε πως σε κάποιο σημείο για κάποιο λόγο χάνεται μια παρατήρηση, αλλά δεν αποστέλλεται πάλι και έπειτα, στέλνεται η επόμενη παρατήρηση. Αντίθετα, στο επόμενο σχήμα, το οποίο είναι παράδειγμα επικοινωνίας με Confirmable μηνύματα, όταν χάνεται ένα πακέτο αποστέλλεται εκ νέου από το server.



Εικόνα – Hands on CoAP, iot.eclipse org Matthias Kovatsch,Julian Vermillard

ΚΕΦΑΛΑΙΟ 4

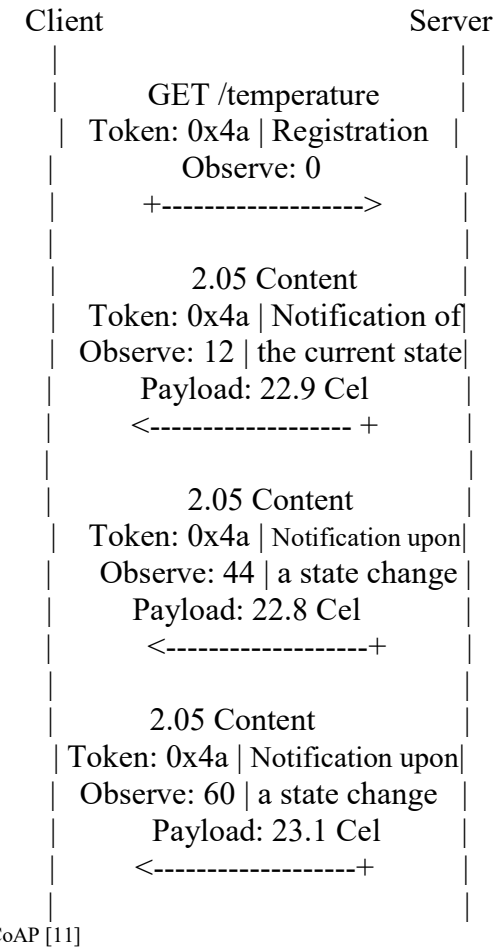
Επεκτάσεις πρωτοκόλλου CoAP

Επέκταση πρωτοκόλλου CoAP observe για παρατήρηση πόρου

Παραπάνω περιγράφθηκε ο βασικός τρόπος λειτουργίας και ανταλλαγής μηνυμάτων μεταξύ δυο συσκευών IoT. Στην ενότητα αυτή, περιγράφεται μια προσέγγιση του βασικού πυρήνα του πρωτοκόλλου CoAP, βάσει της οποίας, δίνεται η δυνατότητα σε μια συσκευή – χρήστη, να παρατηρεί τους πόρους ενός συστήματος ώστε να έχει ενημερωμένη πληροφόρηση για όσο χρονικό διάστημα ενδιαφέρεται. Η διαδικασία αποστολής ερώτησης και απόκρισης που περιγράφθηκε, δε μπορεί να εξυπηρετήσει αυτό το σκοπό, ενώ προσεγγίσεις όπως η HTTP long polling ή repeated polling, προσθέτουν πολυπλοκότητα επιβαρύνοντας δραματικά ένα σύστημα περιορισμένων πόρων. Στη συνέχεια θα αναλυθούν οι απαιτήσεις που χρειάζονται τόσο από την πλευρά του client όσο και από την πλευρά του server προκειμένου να επιτευχθεί η απαιτούμενη λειτουργικότητα.[10]

Στο μοντέλο αυτό υπάρχουν δυο ειδών συμμετέχοντες. Από τη μια πλευρά, βρίσκονται οι συσκευές, observers – clients, οι οποίες ενδιαφέρονται να αποκτούν για

κάποιο χρονικό διάστημα την ενημερωμένη κατάσταση ενός υποκειμένου provider - server, για παράδειγμα την ενημέρωση για αλλαγή των θερμοκρασιών κατά τις νυχτερινές ώρες, ενός γραφείου. Οι παρατηρητές, αρχικά αποστέλλουν ένα μήνυμα με το οποίο γνωστοποιούν ότι επιθυμούν να ενημερώνονται κάθε φορά που αλλάζει κατάσταση ο προμηθευτής (registration). Ο server, με τη σειρά του, έχει την υποχρέωση να διαχειρίζεται τα αιτήματα αυτά, να τα αποθηκεύει σε μια λίστα και στη συνέχεια να τα εξυπηρετεί αποστέλλοντας notifications σε όλους τους ενδιαφερόμενους. Όταν ο client δεν ενδιαφέρεται πλέον να λαμβάνει notifications, απλώς τα απορρίπτει . Η απόρριψη γίνεται αντιληπτή από το server είτε επειδή το notification απορρίπτεται από τον client τόσες φορές ώστε να χαρακτηριστεί ως «not interested», είτε επειδή το notification, μπορεί να αποσταλεί μέσω ενός Acknowledged μηνύματος και επομένως ο server μη λαμβάνοντας επιβεβαίωση διαγράφει το client από τη λίστα ενδιαφερόμενων. [10,14] Σχηματικά:



Σχήμα: Observing a Resource in CoAP [11]

ΠΡΟΔΙΑΓΡΑΦΕΣ ΜΟΝΤΕΛΟΥ

Όσον αφορά τις απαιτήσεις που χρειάζονται από την πλευρά του παρατηρητή – client, οι προδιαγραφές της αρχιτεκτονικής που πρέπει να απαντώνται στα συστήματα είναι οι ακόλουθες:[10]

Αίτημα - Request

Ο client στέλνει αρχικά ένα αίτημα GET στο server με επιλογή «Observe 0». Στη συνέχεια, ο server αποστέλλει μια 2.xx απάντηση αποδοχής δηλώνοντας έτσι ότι έχει καταχωρήσει τη συσκευή στη λίστα με τους ενδιαφερόμενους και επομένως ο παρατηρητής για όσο διάστημα ενδιαφέρεται, θα λαμβάνει ενημερώσεις σχετικά με την κατάσταση του server που τον ενδιαφέρει (πχ. Θερμοκρασία, υγρασία). Έχοντας εγγραφεί ήδη μια φορά στο server, ο παρατηρητής είναι δυνατό να λαμβάνει και πληροφορίες για παραπάνω από μια ενδείξεις που τον ενδιαφέρουν, επομένως θα πρέπει να υπάρχει η λειτουργικότητα να αποκλείονται πολλαπλές εγγραφές προς τον ίδιο provider.

Ειδοποιήσεις – Notifications

Οι ειδοποιήσεις αποτελούν τις αυτοματοποιημένες απαντήσεις – responses που στέλνει η πηγαία συσκευή προς τους καταχωρημένους ενδιαφερόμενους, οι οποίες περιλαμβάνουν την επιθυμητή πληροφορία για την οποία εγγράφηκαν αρχικά. Οι απαντήσεις έχουν τον κωδικό 2.05 που αντιστοιχεί στο περιεχόμενο του μηνύματος που αποστέλλεται. Σε περίπτωση που ο provider αλλάξει κατάσταση με κάποιο τρόπο και δεν είναι δυνατή η αποστολή 2.xx μηνυμάτων απόκρισης, ο server αναλαμβάνει να στείλει κάποιο ανάλογο μήνυμα (για παράδειγμα 4.04 – Not found) και διαγράφει τον παρατηρητή από τη λίστα της πηγής.

Προσωρινή αποθήκευση – Caching

Ο παρατηρητής, έχει τη δυνατότητα αν χρειαστεί να αποθηκεύσει μια ειδοποίηση που θα λάβει από το server στην προσωρινή του μνήμη και να την χρησιμοποιήσει στη

συνέχεια σαν να ήταν μια νέα απάντηση. Για τέτοιες περιπτώσεις, έχουν σχεδιαστεί τα «freshness» και “validation”.

Το freshness model ουσιαστικά, θέτει ένα μέγιστο όριο στο οποίο μια πληροφορία θεωρείται up to date ή όχι. Μια τέτοια αποθηκευμένη πληροφορία, θεωρείται χρήσιμη εφόσον δεν έχει υπερβεί το χρονικό όριο που έχει τεθεί ως max-age. Από την πλευρά του ο server, προσπαθεί να κρατά όσο το δυνατόν πιο ενήμερο μπορεί τον κάθε παρατηρητή, καθώς υπάρχει περίπτωση κάποια στιγμή να μη μπορεί να στέλνει σε όλους τους εγγεγραμμένους παρατηρητές όλες τις μεταβολές που ενδέχεται να συμβούν. Αυτό, μπορεί να συμβεί σε περιπτώσεις όπως, σε ώρα αιχμής, προβληματικό δίκτυο ή σε πολλές συνεχόμενες μεταβολές της ενδιαφερόμενης ένδειξης. Ο τρόπος που το σύστημα χειρίζεται τέτοιες περιπτώσεις είναι, παραλείποντας ορισμένες ενδείξεις λαμβάνοντας υπόψη το μέγιστο δυνατό χρονικό διάστημα που έχει τεθεί από τον κάθε ενδιαφερόμενο ως μέγιστο επιτρεπτό όριο. Αν αυτό δεν είναι δυνατό να επιτευχθεί, τότε ο παρατηρητής θα πρέπει να είναι σε θέση να αντιλαμβάνεται ότι η πληροφορία που διαθέτει για την κατάσταση του Provider, δεν είναι η πραγματική και στη συνέχεια να στέλνει ένα μήνυμα όμοιο με το αρχικό GET, το οποίο όμως θα πρέπει να είναι ρυθμισμένο να στέλνετε μετά από ένα εύλογο χρονικό διάστημα ώστε να μη δημιουργείται συμφόρηση, καθώς είναι πιθανό άλλες συσκευές να κάνουν το ίδιο.

Όσον αφορά το «Validation model», η χρησιμότητά του έγκειται στο γεγονός ότι ένας client είναι δυνατόν να έχει αποθηκεύσει στην προσωρινή του μνήμη παραπάνω από μία τιμή και επομένως, ο client θα πρέπει να μάθει πια από τις πολλαπλές τιμές είναι έγκυρη. Αυτό, επιτυγχάνεται μέσω της αποστολής ενός μηνύματος GET ώστε στη συνέχεια, ο server να στείλει πίσω μια απόκριση με κωδικό 2.03-valid αντί να στείλει εκ νέου μήνυμα 2.05 με πληροφορία, πετυχαίνοντας έτσι και ένα μικρό βαθμό βελτίωση της ταχύτητας και μείωση της συμφόρησης του δικτύου.

Αναδιάταξη – Reordering

Όπως αναφέρθηκε και προηγουμένως, δεδομένου ότι όλη η φιλοσοφία βασίζεται σε μηνύματα που στέλνονται μέσω του internet,υπάρχει περίπτωση η σύνδεση να χαθεί για κάποιο χρονικό διάστημα. Αυτό, μπορεί να δημιουργήσει φαινόμενα, όπως τη λήψη πολλαπλών μηνυμάτων απόκρισης που είχαν αποσταλεί από το server όσο ο παρατηρητής είχε χάσει τη σύνδεσή του στο δίκτυο. Είναι φυσικό επομένως, ο

παρατηρητής να πρέπει να ξεχωρίζει και να θεωρεί ως πιο έγκυρο και κοντά στην πραγματικότητα το μήνυμα εκείνο το οποίο είναι πιο πρόσφατο. Για να επιτευχθεί αυτό, ένα μήνυμα που φτάνει από το server, θέτει τη σειρά των μηνυμάτων που αποστέλλει προς κάθε ενδιαφερόμενο και στέλνει μαζί με την πληροφορία και το ordering που έχει το μήνυμα. Στη συνέχεια, ο παρατηρητής ελέγχει αν η πληροφορία που έλαβε είναι νεότερη από αυτή που ήδη έχει σύμφωνα με μία από τις παρακάτω συνθήκες:

- V1 < V2 AND V2 –V1 < 2^23,
- V1 > V2 AND V1 –V2 > 2^23, όπου:

  V1: είναι η τιμή στο μέχρι τώρα νεότερο μήνυμα

  V2: η τιμή που παρέχεται από την εισερχόμενη ειδοποίηση

Με τη συνθήκη αυτή πιστοποιείται πως η V1 τιμή είναι μικρότερη της V2 σε μορφή 24bit σειριακού αριθμού.

- T2 > T1 +128 sec., όπου:

  T1: τοπική χρονική σήμανση του μέχρι τώρα νεότερου μηνύματος του client

  T2: τοπική χρονική σήμανση του εισερχόμενου μηνύματος.

  Τα 128 δευτερόλεπτα έχουν θεσπιστεί ως επαρκές χρόνος ο οποίος αν έχει ξεπεραστεί, θεωρείται ότι το εισερχόμενο μήνυμα περιλαμβάνει σίγουρα μια πιο ενημερωμένη πληροφορία από όσα μηνύματα έχουν σταλεί μέχρι τώρα.

Μετάδοση – Transmission

Οι ειδοποιήσεις που μεταδίδονται από έναν server, μπορεί να είναι είτε confirmable είτε Non-confirmable. Αν ο παρατηρητής δεν αναγνωρίζει το μήνυμα που λαμβάνει, θα πρέπει να το απορρίπτει και να στέλνει ένα RESET μήνυμα στο server, εναλλακτικά, αν αναγνωρίζει το μήνυμα που έλαβε θα πρέπει να στέλνει acknowledgement. Η αποστολή επιβεβαίωσης είναι ένας τρόπος ένδειξης του ενδιαφέροντος της συσκευής για την παροχή της πληροφορίας. Αν ο provider δε λάβει επιβεβαίωση από τον client, θα θεωρήσει πως πλέον δεν ενδιαφέρεται και θα προβεί στη διαγραφή του από τη λίστα των ενδιαφερομένων.

Ακύρωση – Cancellation

Όταν ένας παρατηρητής παύει να ενδιαφέρεται για την παρεχόμενη πληροφορία, μπορεί απλώς να «αγνοήσει» τα εισερχόμενα μηνύματα από το server. Κάνοντας

αυτό, ο server δε λαμβάνει επιβεβαίωση παράληψης του μηνύματος και επομένως διαγράφει τον παρατηρητή από τον πόρο. Εναλλακτικά, ο παρατηρητής έχει τη δυνατότητα να στείλει ένα μήνυμα GET προς τον πόρο με κωδικό «Observe 1», που σημαίνει την ακύρωση και διαγραφή του από τη λίστα.

Επέκταση πρωτοκόλλου CoAP για ομαδική επικοινωνία (Group Communication)

Μια διαφορετική προσέγγιση του πρωτοκόλλου του CoAP, η οποία όμως είναι πολύ σημαντική και προσθέτει ευελιξία σε περιορισμένα συστήματα, είναι αυτή του Group Communication. Το μοντέλο αυτό χρησιμοποιεί τη λειτουργικότητα του IP Multicast και Unicast. Μια μετάδοση Unicast, στέλνει πακέτα IP από και προς μια συγκεκριμένη διεύθυνση, για παράδειγμα το video streaming μεταξύ δυο συγκεκριμένων υπολογιστών. Αντίθετα, μια multicast μετάδοση, αποστέλλει πακέτα σε μια ομάδα πελατών στο δίκτυο. Το μοντέλο αυτό βασίζεται στη δημιουργία one-to-many σχέσεων μεταξύ των τερματικών συσκευών. Με τη λογική αυτή, ένας CoAP client μπορεί να λαμβάνει ταυτόχρονα πληροφορία από πολλαπλούς server χάριν στη βοήθεια του IP-multicast, όπως για παράδειγμα η μαζική αποστολή ενός μηνύματος που θα σβήσει πολλά φώτα σε έναν χώρο. Μια ομάδα CoAP ορίζεται ως ένα σύνολο τελικών κόμβων του CoAP, όπου ο κάθε τελικός κόμβος έχει ρυθμιστεί ώστε να λαμβάνει αιτήματα επικοινωνίας group-CoAP. Τα αιτήματα αυτά αποστέλλονται στη διεύθυνση IP-multicast που έχει οριστεί για τη συγκεκριμένη ομάδα. Αντίθετα, η απόκριση από τον κάθε δέκτη μιας ομάδας δύναται να αποστέλλεται ως unicast. Τέλος, αξίζει να σημειωθεί πως κάθε κόμβος δύναται να συμμετέχει σε παραπάνω από μία ομάδα.[11]

ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ΜΟΝΤΕΛΟΥ

Πιο αναλυτικά, ένας COAP server, στέλνει ένα μήνυμα το οποίο παραδίδεται σε πολλούς clients, οι οποίοι όμως ανήκουν σε ένα γνωστό, για το server, group. Η γενικότερη φιλοσοφία του μηχανισμού επικοινωνίας μιας ομάδας συσκευών, βασίζεται στο UDP/IP μοντέλο ενώ το Port το οποίο χρησιμοποιείται είθισται να είναι το default port του UDP, δηλαδή το 5683. Παρόλα αυτά, μπορεί να

χρησιμοποιηθούν και άλλα ports, αλλά θα πρέπει να δοθεί προσοχή ώστε όλοι οι συμμετέχοντες να γνωρίζουν το συγκεκριμένο Port επικοινωνίας.

Η ομαδική επικοινωνία, χρησιμοποιεί συνήθως τις εξειδικευμένες μεθόδους του CoAP, GET και PUT, ενώ λιγότερο συχνά μπορεί να χρησιμοποιηθεί και η DELETE. Επιπλέον, υπάρχει πιθανότητα να χρησιμοποιηθεί και η μέθοδος POST, αλλά μόνο σε περιπτώσεις όπου ο κόμβος στον οποίο στέλνεται το μήνυμα POST έχει σχεδιαστεί για να αντιμετωπίσει την πιθανότητα απώλειας σήματος ή σε αναξιόπιστα περιβάλλοντα. Με αυτό τον τρόπο, ένας client μπορεί να στείλει παραπάνω από μία φορές ένα μήνυμα POST στη προσπάθεια επίτευξης μεγαλύτερης αξιοπιστίας. Το μήνυμα αυτό μπορεί να φτάσει σε ορισμένους servers δυο ή παραπάνω φορές, όμως σε κάποιους, λόγω απώλειας επικοινωνίας θα φτάσει μόνο μια. Η διαφορά μεταξύ της μεθόδους αυτής και των προηγούμενων, πιο συνηθισμένων, έγκειται στο γεγονός ότι όσοι server λειτουργούν με τις μεθόδους GET και PUT θα βρίσκονται στην ίδια κατάσταση με την ίδια πληροφορία, ενώ όσοι λειτούργησαν με το POST, δεν είναι βέβαιο πως την ίδια στιγμή θα γνωρίζουν την ίδια πληροφορία και αυτό καθιστά αναγκαίο, όταν χρησιμοποιείται η μέθοδος αυτή, να έχει ληφθεί υπόψη και το ενδεχόμενο απώλειας δεδομένων.

ΑΠΟΣΤΟΛΗ REQUEST ΚΑΙ RESPONSE ΜΗΝΥΜΑΤΩΝ

Σύμφωνα με τον προτεινόμενο σχεδιασμό λειτουργίας του group communication, το MessageID ενός μηνύματος μπορεί να χρησιμοποιηθεί προαιρετικά για την αποφυγή λήψης διπλότυπων αιτημάτων ή απαντήσεων. Δεδομένου ότι όπως αναφέρθηκε, ένας CoAP client μπορεί να είναι μέλος σε περισσότερες από μια ομάδες συσκευών, μπορεί να διακρίνει την προέλευση απαντήσεων από διαφορετικούς server σύμφωνα με τη διεύθυνση IP ή μέσο κάποιου άλλου αναγνωριστικού (όπως π.χ. από το MessageID). Στην περίπτωση που ένας CoAP client έχει στείλει πολλαπλά group requests, οι απαντήσεις που επιστρέφονται συνήθως αντιστοιχίζονται με το Token του μηνύματος. Ανάλογα όμως με το αν το μήνυμα στέλνεται μέσω multicast ή unicast IP, υπάρχουν περαιτέρω περιορισμοί που θα πρέπει να ληφθούν υπόψη. Όταν μια μετάδοση γίνεται με unicast, η τιμή του token η οποία μεταφέρει την απάντηση σε κάποιο αίτημα, μόλις φτάσει στον παραλήπτη αποδεσμεύεται καθώς η πληροφορία

έχει φτάσει πλέον στον ενδιαφερόμενο. Αντίθετα, στην περίπτωση του multicast, κάτι τέτοιο δε μπορεί να ισχύσει καθώς ο παραλήπτης δεν είναι ένας και αποδεσμεύοντας την τιμή Token, μπορεί να προκαλέσει μη αντιστοίχιση αιτήματος/απαντήσεως για κάποιους client.[11]

ΑΝΑΓΝΩΡΙΣΗ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΜΕΛΩΝ ΜΙΑΣ ΟΜΑΔΑΣ

Η συμμετοχή ενός client σε μια ομάδα συσκευών επικοινωνίας μέσω του CoAP, μπορεί να είναι αποτέλεσμα είτε αρχικού προγραμματισμού, όπου ο CoAP client γνωρίζει τη διεύθυνση μιας ομάδας και μπορεί να στείλει απευθείας αίτημα, είτε μέσω «ανακάλυψης» - discovery του κόμβου αποστέλλοντας ένα ερώτημα στο δίκτυο, συνήθως χρησιμοποιώντας τεχνικές DNS-based Discovery Service, ή τέλος, να προταθεί – οριστεί από έναν άλλο κόμβο, ήδη μέλος μιας ομάδας. Η τελευταία περίπτωση διαφέρει από τις προηγούμενες γιατί αναφέρεται συνήθως σε περιπτώσεις όπου κάποια συσκευή έχει τη δυνατότητα να ενεργοποιήσει και να ορίσει μια ομάδα συσκευών, όπως για παράδειγμα να δεσμεύσει σε μια ομάδα όλους τους αισθητήρες φωτιάς ή υγρασίας ενός κτιρίου. Όσον αφορά την περίπτωση αυτή, δεδομένου ότι μια ομάδα συσκευών που είναι εγκατεστημένες σε ένα κτίριο μπορεί να είναι διαφορετικών κατασκευαστών είναι κρίσιμο να επιτευχθεί με κάποιον τρόπο η διαλειτουργικότητα μεταξύ τους. Μια τέτοια προσέγγιση αποτελεί η «Optional CoAP RESTful» διεπαφή. Η φιλοσοφία της μεθόδου αυτής βασίζεται στην διαμόρφωση των πληροφοριών της ομάδας σε κάθε κόμβο ξεχωριστά και προκειμένου μια συσκευή να αποκτήσει πρόσβαση σε αυτή την διεπαφή, χρησιμοποιεί τις unicast μεθόδους (GET/PUT/POST/DELETE). Για να γίνει κάτι τέτοιο οι κόμβοι θα πρέπει να υποστηρίζουν τη διαμόρφωση της ομάδας μέσω RESTful διεπαφών και μεθόδων, και συγκεκριμένα, θα πρέπει να υποστηρίζουν τη διαμόρφωση του περιεχομένου των μηνυμάτων με βάση τη μορφή Javascript Object Notation (JSON). Κάθε κόμβος που συμμετέχει στην ομάδα περιλαμβάνει ένα ζεύγος κλειδιών που ουσιαστικά είναι το όνομα μέλους με την αντίστοιχη αξία του, όπως περιγράφεται πιο κάτω και αντιπροσωπεύει ένα μοναδικό IP membership που κωδικοποιείται ως μέλος του αντικειμένου JSON.

Req: POST /coap-group

Content-Format: application/coap-group+json

{ "n": "All-Devices.floor1.west.bldg6.example.com",

"a": "[ff15::4200:f7fe:ed37:abcd]:4567" }

Res: 2.01 Created

Location-Path: /coap-group/12

{ "n": "coap-test",

"a": "224.0.1.187:56789" }

{ "a": "[ff15::c0a7:15:c001]" }

Όπου:

n: αντιπροσωπεύει το όνομα της ομάδας

a: δείχνει την multicast IP διεύθυνση

Η παραπάνω επικοινωνία αποτελεί ένα παράδειγμα της δημιουργίας μιας ομάδας συσκευών IoT. Στο αρχικό αίτημα που στέλνεται ουσιαστικά ζητείται να απαντήσουν όλες οι συσκευές που βρίσκονται στον δυτικό μέρος του πρώτου ορόφου και μόλις αυτό γίνει δημιουργείται η ομάδα (2.01 created) και στη συνέχεια στέλνεται ένα μήνυμα test ώστε να απαντήσουν οι συμμετέχουσες συσκευές. Όπως φαίνεται και παραπάνω, οι συσκευές κάνουν γνωστή την παρουσία τους δείχνοντας είτε την IPv4 είτε την IPv6 διεύθυνση τους (224.0.1.187:56789 και ff15::c0a7:15:c001 αντίστοιχα). Παρακάτω ακολουθεί ένα παράδειγμα αναγνώρισης - επιβεβαίωσης όλων των μελών μιας ομάδας:

Req: GET /coap-group

Res: 2.05 Content

Content-Format: application/coap-group+json

{ "8" :{ "a": "[ff15::4200:f7fe:ed37:14ca]" },

"11":{ "n": "sensors.floor1.west.bldg6.example.com",

"a": "[ff15::4200:f7fe:ed37:25cb]" },

"12":{ "n": "All-Devices.floor1.west.bldg6.example.com",

"a": "[ff15::4200:f7fe:ed37:abcd]:4567" }

}

Με ανάλογο τρόπο είναι δυνατή και η διαγραφή ενός μέλους μιας ομάδας:

Method: DELETE

URI Template: {+location}

URI Template Variables:

location - The Location-Path returned by the CoAP server

as a result of a successful group creation.

Req: DELETE /coap-group/12

Res: 2.02 Deleted

ΜΕΡΟΣ ΤΡΙΤΟ

INFORMATION-CENTRIC NETWORKING (ICN) – POINT ARCHITECTURE

ΚΕΦΑΛΑΙΟ 5

Παρουσίαση μοντέλου δικτύωσης και πλεονεκτήματα

Όπως έχει αναφερθεί και σε προηγούμενη ενότητα, το IoT πρόκειται στο εγγύς μέλλον να αναπτυχθεί με ταχύτατους ρυθμούς και εκατομμύρια συσκευές να είναι συνδεδεμένες στο διαδίκτυο ανταλλάσσοντας αυτόματα μεγάλο όγκο πληροφοριών. Όντας μια νέα τεχνολογία, μέσα από τις έρευνες για το βέλτιστο τρόπο διασύνδεσης των συσκευών στο διαδίκτυο, έχει προταθεί και αναπτυχθεί μια ποικιλία μεθόδων και τεχνολογιών πρόσβασης. Παρά όμως το γεγονός της τεχνολογικής εξέλιξης, η βασική λογική με την οποία λειτουργούν τα παραδοσιακά δίκτυα ενδέχεται να μην είναι σε θέση να εξυπηρετήσουν έναν τόσο μεγάλο όγκο συνδεδεμένων συσκευών και πληροφοριών. Τέτοιες ανησυχίες, έχουν ωθήσει την επιστημονική κοινότητα στην αναζήτηση λύσεων που θα μπορούσαν να εγγυηθούν την εύρυθμη λειτουργία των

δικτύων στο μέλλον. Μια ενδιαφέρουσα προσέγγιση αποτελεί και η Information Centric δικτύωση (στο εξής ICN).

Πρόκειται για μια προσέγγιση η οποία στοχεύει στο σχεδιασμό μιας αρχιτεκτονικής δικτύου στην οποία το σημείο αναφοράς είναι οι πληροφορίες. Σήμερα, η διανομή περιεχομένου αποτελεί το μεγαλύτερο ποσοστό της κίνησης εντός του διαδικτύου και αν αναλογιστούμε πως σε μερικά χρόνια ακόμα περισσότερες συσκευές θα είναι συνδεδεμένες στο διαδίκτυο λόγω του IoT, η παραδοσιακή δομή του δικτύου «άκρο σε άκρο» (point-to-point) παρουσιάζει αρκετά μειονεκτήματα, κυρίως σε επίπεδο αποδοτικότητας, ασφάλειας, και ιδιωτικότητας.

Παρόλα αυτά, το να αλλάξει όλη η δομή των δικτύων και η αρχιτεκτονική που ακολουθείται τόσα χρόνια και να μεταφερθούμε από IP-based σε ICN-based δικτύωση, αποτελεί μια πολύ δύσκολη, κοστοβόρα και χρονοβόρα διαδικασία, με αποτέλεσμα η κατεύθυνση των ερευνών να έχει στραφεί προς την εύρεση εναλλακτικών τρόπων με τους οποίους το ICN μπορεί να βελτιώσει την υπάρχουσα κατάσταση. Μια τέτοια εναλλακτική, η οποία μπορεί να υποστηρίξει το IoT είναι και η αρχιτεκτονική POINT η οποία έχει ως στόχο να τρέξει το IP πρωτόκολλο πάνω από Information Centric Networking και περιγράφεται σε επόμενες σελίδες[19].

Αρχιτεκτονική POINT

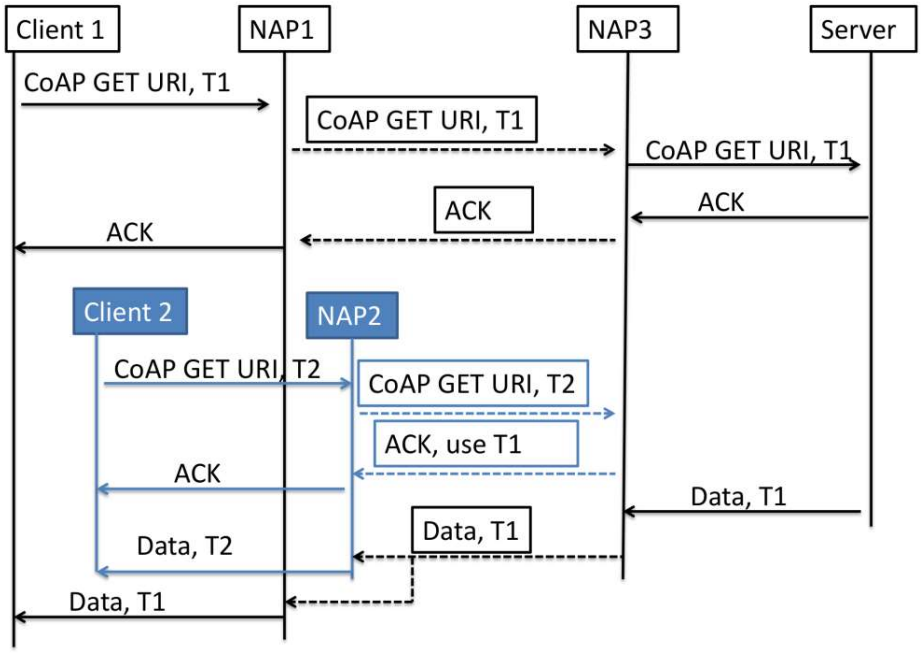
Η αρχιτεκτονική POINT, συνδέει τους τελικούς IP κόμβους κάνοντας χρήση του Publish-Subscribe Internet (PSI). Ως Publish-Subscribe Internet ορίζουμε το πρότυπο σύμφωνα με το οποίο μια συσκευή η οποία ενδιαφέρεται για το περιεχόμενο ενός συγκεκριμένου πόρου, δηλώνει το ενδιαφέρον της κάνοντας μια εγγραφή στην πηγή του περιεχομένου και η οποία με τη σειρά της, όταν θα έχει διαθέσιμη το περιεχόμενο αναλαμβάνει την δημοσιοποίηση του προς όλους τους ενδιαφερόμενους, όπως δηλαδή παρουσιάστηκε στην λειτουργία Observe του CoAP. Στην εικόνα αυτού του μοντέλου εισέρχεται και μια ακόμα νέα έννοια, αυτή των Rendezvous Nodes. Όταν η ενδιαφερόμενη πληροφορία γίνεται διαθέσιμη, αποκτά ένα συγκεκριμένο αναγνωριστικό. Σκοπός αυτού του αναγνωριστικού είναι να δίνει μια ιδέα για το που περίπου αυτή η πληροφορία είναι διαθέσιμη. Τέτοιου είδους πληροφορίες τις διαχειρίζονται τα Rendezvous Nodes, τα οποία ουσιαστικά παρέχουν μια λειτουργία

αναζήτησης και προωθούν ένα αίτημα εγγραφής μιας συσκευής στο κατάλληλο RN αντί στην ίδια καθ' αυτή πηγή της πληροφορίας.

Η σύνδεση των κόμβων – συσκευών με τις άκρες της αρχιτεκτονικής POINT, πραγματοποιείται με τη βοήθεια των NAP (Network Attachment Points), οι οποίοι διαχειρίζονται τα πρωτόκολλα με τα οποία θα πραγματοποιηθούν οι εκάστοτε προωθήσεις μηνυμάτων. Έτσι, όταν σε ένα NAP αποσταλεί η πληροφορία από έναν server με μήνυμα CoAP, οι NAPs αναλαμβάνουν την προώθησή της με λειτουργίες ICN ή και CoAP αν είναι απαραίτητο. Με αυτόν τον τρόπο μειώνεται η κίνηση στο δίκτυο, εξοικονομούνται πόροι που είναι σημαντικό στοιχείο, δεδομένου ότι οι συσκευές είναι περιορισμένων δυνατοτήτων και μπορούν να επιτευχθούν πιο κεντρικοποιημένοι έλεγχοι προς την κατεύθυνση της ασφάλειας[14].

Παράδειγμα Επικοινωνίας με Χρήση Αρχιτεκτονικής POINT

Προκειμένου να γίνει κατανοητή η λειτουργία που μόλις περιγράφηκε, ακολουθεί το παρακάτω σχήμα:



Σύμφωνα με το παραπάνω σχήμα:

- Δύο clients (client 1 και 2) επιθυμούν να ζητήσουν από τον ίδιο κόμβο (server) την ίδια πληροφορία που τους ενδιαφέρει.
- Αρχικά, ο client 1 εκδηλώνει το ενδιαφέρον του για την πληροφορία μέσω ενός μηνύματος CoAP GET, ζητώντας μια πληροφορία, για παράδειγμα την θερμοκρασία T1.
- Το μήνυμα αυτό φθάνει στο NAP1 το οποίο με τη σειρά του, εφόσον αποτελεί το πρώτο αίτημα που ζητά αυτή την πληροφορία, προωθεί εντός του ICN δικτύου το αίτημα στο κατάλληλο σημείο (π.χ. NAP3) απ' όπου τελικά αποστέλλεται στο server.
- Στο συγκεκριμένο παράδειγμα, η πληροφορία δεν είναι έτοιμη, επομένως για αποφυγή διπλοτύπων, αποστέλλεται ένα απλό ACKnowledgement.
- Στο διάστημα που μεσολάβησε μεταξύ της αποστολής του GET και της τελικής απόκρισης του server με την επιθυμητή πληροφορία, εμφανίζεται και μια δεύτερη συσκευή, ο client 2, ο οποίος επιθυμεί να λάβει την ίδια πληροφορία από τον server.
- Ο client 2 αποστέλλει το μήνυμα GET όπως έκανε η πρώτη συσκευή ενώ ο NAP2 αναλαμβάνει με όμοιο τρόπο την προώθησή του στο κατάλληλο NAP3 το οποίο έχει την επικοινωνία με το server.

Στο σημείο αυτό γίνεται εμφανής η συνεισφορά και το πλεονέκτημα που δίνει η πλατφόρμα POINT και γενικότερα η Information Centric Networking. Κάτω από διαφορετικές συνθήκες, χωρίς την ύπαρξη του ICN, το αίτημα του δεύτερου ενδιαφερόμενου θα προωθούταν στον server και στη συνέχεια, όταν θα ήταν έτοιμη η πληροφορία, ο server θα αναλάμβανε την αποστολή της πληροφορίας στους δύο ή και πολύ περισσότερους χρήστες που θα είχαν «Εγγραφεί» για την εν λόγω πληροφορία.

- Αντί αυτού, βάσει της φιλοσοφίας του POINT και του ICN, επειδή έχει προηγηθεί η αποστολή αιτήματος από την πρώτη συσκευή, αποστέλλεται στον δεύτερο κόμβο το ίδιο ACK χωρίς να γίνει κάποια επικοινωνία με το server.
- Τέλος, με την πάροδο του χρόνου, ο server στέλνει τελικά την πληροφορία στο NAP3 το οποίο εν τέλει αναλαμβάνει τη δρομολόγησή του σε όλους τους ενδιαφερόμενους.

Με βάση το παραπάνω παράδειγμα γίνεται αισθητό το κατά πόσο μειώνεται ο φόρτος εργασίας στους τελικούς κόμβους τους συστήματος, οι οποίοι συνήθως είναι μικρές συσκευές συνήθως περιορισμένων υπολογιστικών δυνατοτήτων και συνδέονται στο

διαδίκτυο μέσω κάποιας ασύρματης σύνδεσης, η οποία κάλλιστα μπορεί να χαθεί ή να είναι αρκετά ασθενής, προκαλώντας απώλεια δεδομένων[14].

Πλεονεκτήματα ICN δικτύωσης

Έχοντας περιγράψει σε γενικές γραμμές τον τρόπο με τον οποίο η αρχιτεκτονική POINT μπορεί με τη βοήθεια του ICN να εξυπηρετήσει τα CoAP μηνύματα μεταξύ έξυπνων συσκευών, γίνεται κατανοητό πως η φιλοσοφία του ICN, ουσιαστικά μετασχηματίζει και προτείνει ένα διαφορετικό τρόπο αντιμετώπισης των πληροφοριών. Τα κυριότερα πλεονεκτήματα που εν γένει επιφέρει αυτή η προσέγγιση είναι τα ακόλουθα:

- Η πληροφορία γίνεται προσπελάσιμη από το όνομά της,
- Η προσωρινή αποθήκευση (caching) είναι καθολική σε όλο το δίκτυο.
- Το ICN ταιριάζει περισσότερο με την φιλοσοφία που ακολουθεί πλέον η νόρμα επικοινωνίας, σύμφωνα με την οποία ενδιαφερόμαστε πιο πολύ για την πληροφορία παρά για τις συσκευές, κάνει ευκολότερη την υποστήριξη της κινητικότητας, χωρίς να δίνει έμφαση στο ποιος έστειλε την πληροφορία αλλά μόνο στην ίδια την πληροφορία και κατά πόσο αυτή είναι έγκυρη, επαρκής, ενημερωμένη και άμεση.
- Προσφέρει «αποκέντρωση» του φόρτου εργασίας, καθώς η κίνηση μεταφέρεται από τα άκρα του συστήματος στο cloud
- Παρέχει υψηλότερο επίπεδο ασφάλειας, γεγονός που θα αναλυθεί σε επόμενη ενότητα και τέλος, αποτελεί την ιδανική προτεινόμενη λύση που μπορεί να αντιμετωπίσει τη ραγδαία εξέλιξη του Internet of Things. Με απλά λόγια, το ICN

ακολουθεί την επιταγή του καταναλωτή ο οποίος δεν ενδιαφέρεται από πού έχει έρθει η πληροφορία, αλλά.

- *Συνυφασμένη πολυεκπομπή (Coincidencial Multicast*): Το πλεονέκτημα αυτό είναι το προφανές που περιεγράφηκε στο προηγούμενο παράδειγμα. Σε ένα τυπικό IP-based δίκτυο, η εγγραφή πολλαπλών συσκευών σε έναν πόρο με την επέκταση της «παρατήρησης πόρου» - observe που περιγράφηκε στην ενότητα του CoAP, θα σήμαινε την πολλαπλή αποστολή, από πλευράς του server, μηνυμάτων με την ίδια πληροφορία σε μεγάλο αριθμό συσκευών. Χάριν όμως στην λειτουργικότητα που προσφέρει το ICN, κάτι τέτοιο μπορεί να αποφευχθεί με τη βοήθεια της αρχιτεκτονικής POINT και των ενδιάμεσων NAPs που περιεγράφηκαν.
- *One to many group requests*: Η λειτουργικότητα του group communication που περιεγράφηκε προηγουμένως, έχει επίσης να λαμβάνει πλεονεκτήματα από την προτεινόμενη αρχιτεκτονική. Σε ένα τυπικό δίκτυο CoAP, η επικοινωνία σε επίπεδο ομάδας πραγματοποιείται συνοπτικά ως εξής:
    - Οι servers, συνδέονται σε έναν αριθμό ομάδων μέσω IP Multicast,
    - Το όνομα της ομάδας μαζί με τη διεύθυνσή της καταγράφεται σε έναν DNS server
    - Μια συσκευή που θέλει να στείλει ένα CoAP μήνυμα, μαθαίνει από τους DNS servers τη διεύθυνση της ομάδας συσκευών που την ενδιαφέρει, και
    - Το μήνυμα φθάνει στην επιθυμητή ομάδα όπου και τελικώς αποφασίζεται το αν και το πότε θα σταλεί η απάντηση.

  Η παραπάνω διαδικασία προϋποθέτει τη συμμετοχή διαφορετικών πρωτοκόλλων και λειτουργιών (CoAP, IP_Multicast και DNS) κάτι που επιβαρύνει την αποδοτικότητα του συστήματος. Αντίθετα, με το ICN και του τρόπου λειτουργίας της πλατφόρμας POINT, η παραπάνω διαδικασία γίνεται πιο απλή και εξαιρείται η χρήση των DNS και του multicast καθώς, η POINT προσέγγιση μπορεί απευθείας να μεταφράσει και να προωθήσει τα CoAP μηνύματα στην επιθυμητή ομάδα με τη διαδικασία που περιγράφηκε.
- *Ονομασία συσκευών, δεδομένων και υπηρεσιών*: Η ανομοιογένεια τόσο του εξοπλισμού δικτύου όσο και των υπηρεσιών που προσφέρονται από τα δίκτυα IoT οδηγεί σε μια μεγάλη ποικιλία δεδομένων, υπηρεσιών και συσκευών. Όταν χρησιμοποιείται μια παραδοσιακή αρχιτεκτονική, μόνο οι συσκευές ή οι διεπαφές δικτύου τους ονομάζονται σε επίπεδο δικτύου, αφήνοντας στο επίπεδο εφαρμογής την διαδικασία ονομασίας δεδομένων και υπηρεσιών. Σε πολλές κοινές

εφαρμογές δικτύων IoT, τα δεδομένα και οι υπηρεσίες είναι ο κύριος στόχος και η ειδική επικοινωνία μεταξύ δύο συσκευών είναι δευτερεύουσα. Το δίκτυο διανέμει περιεχόμενο και παρέχει μια υπηρεσία, αντί να δημιουργήσει μια σύνδεση επικοινωνίας μεταξύ δύο συσκευών. Σε αυτό το πλαίσιο, το περιεχόμενο και οι υπηρεσίες δεδομένων μπορούν να παρέχονται από πολλές συσκευές ή από μια ομάδα συσκευών και επομένως η ονομασία δεδομένων και υπηρεσιών είναι συχνά πιο σημαντική από την ονομασία των συσκευών.

- *Κατανεμημένη προσωρινή αποθήκευση και επεξεργασία*: Ενώ οι μηχανισμοί προσωρινής αποθήκευσης χρησιμοποιούνται ήδη από άλλους τύπους δικτύων, τα δίκτυα IoT μπορούν να ωφεληθούν ακόμη περισσότερο από την προσωρινή αποθήκευση και από τα συστήματα επεξεργασίας εντός δικτύου, λόγω των περιορισμών των πόρων τους. Το ασύρματο εύρος ζώνης και η παροχή ρεύματος μπορούν να περιοριστούν για πολλαπλές συσκευές που μοιράζονται ένα κανάλι επικοινωνίας και για μικρές κινητές συσκευές που τροφοδοτούνται με μπαταρίες. Σε αυτήν την περίπτωση, η αποφυγή περιττών μεταδόσεων με συσκευές IoT για ανάκτηση και διανομή δεδομένων IoT σε πολλά σημεία είναι σημαντική, επομένως η επεξεργασία και η αποθήκευση τέτοιου περιεχομένου στο δίκτυο μπορεί να εξοικονομήσει ασύρματο εύρος ζώνης και ισχύ μπαταρίας. Επιπλέον, όπως και για άλλους τύπους δικτύων, οι εφαρμογές για δίκτυα διαδικτύου που απαιτούν μικρότερες καθυστερήσεις μπορούν να επωφεληθούν από τοπικές κρυφές μνήμες και υπηρεσίες για τη μείωση καθυστερήσεων μεταξύ της αίτησης περιεχομένου και της παράδοσης.
- *Αποσύνδεση μεταξύ αποστολέα και δέκτη*: Οι συσκευές IoT κατά κύριο λόγο είναι κινητές και αντιμετωπίζουν διαλείπουσα συνδεσιμότητα δικτύου. Όταν ζητούνται συγκεκριμένα δεδομένα, τα δεδομένα αυτά μπορούν συχνά να παρέχονται από την ICN χωρίς συνεπή άμεση διασύνδεση μεταξύ των συσκευών. Εκτός από τη χρήση δομημένων συστημάτων προσωρινής αποθήκευσης, όπως περιεγράφηκε προηγουμένως, πληροφορίες μπορούν επίσης να διαδοθούν με την προώθηση δεδομένων ευκαιριακά[14].

ΚΕΦΑΛΑΙΟ 6

Προκλήσεις Υλοποίησης I.C.N.

Στην ενότητα αυτή περιγράφονται ορισμένες από τις προκλήσεις του ICN που πρέπει να ληφθούν υπόψη κατά τον καθορισμό ενός πλαισίου IoT πάνω από το ICN και περιγράφει μερικές από τις αντισταθμίσεις που μπορούν να βοηθήσουν στην υπέρβαση αυτών. Το ICN ενσωματώνει αφαίρεση περιεχομένου, υπηρεσίας και κεντρικού υπολογιστή, τη δρομολόγηση με βάση το όνομα, τον υπολογισμό, την προσωρινή αποθήκευση ή την αποθήκευση ως μέρος της δικτυακής υποδομής, συνδέοντας τους καταναλωτές και τις υπηρεσίες που ικανοποιούν τις περισσότερες από τις παραπάνω απαιτήσεις. Ωστόσο, το IoT λόγω της φύσης των συσκευών, απαιτεί ειδικές εκτιμήσεις περιεχομένου για την κάλυψη συγκεκριμένων απαιτήσεων εφαρμογής που προσδιορίζουμε ως προκλήσεις σε αυτή την ενότητα, οι οποίες αναλύονται παρακάτω:

- *Ονοματοδοσία Συσκευών, Δεδομένων και Υπηρεσιών*: Η προσέγγιση ICN των ονομασμένων δεδομένων και υπηρεσιών είναι συνήθως επιθυμητή κατά την ανάκτηση δεδομένων IoT. Οι ονομασίες συσκευών είναι συχνά σημαντικές σε ένα δίκτυο IoT. Η παρουσία ενεργοποιητών απαιτεί από τους πελάτες να δρουν ειδικά σε μια συσκευή, π.χ. για να την ενεργοποιήσουν ή να την απενεργοποιήσουν. Επίσης, η παρακολούθηση των συσκευών για σκοπούς διαχείρισης απαιτεί οι συσκευές να έχουν ένα συγκεκριμένο όνομα που θα τους επιτρέπει να αναγνωρίζονται μοναδικά. Υπάρχουν πολλοί τρόποι επίτευξης της ονοματοδοσίας συσκευών, ακόμη και σε συστήματα που είναι δεδομένο-κεντρικά εκ φύσεως. Για παράδειγμα, σε συστήματα που μπορούν να διευθυνθούν ή να αναζητηθούν βάσει μεταδεδομένων ή περιεχομένου αισθητήρων, το αναγνωριστικό συσκευής μπορεί να συμπεριληφθεί ως ειδικό είδος μεταδεδομένων ή ως αισθητήρας ανάγνωσης.

Συγκεκριμένα, ως επιμέρους προκλήσεις στο επίπεδο της ονοματοδοσίας των συσκευών δημιουργούνται τα ακόλουθα προβλήματα:

- *Μέγεθος του ονόματος δεδομένων / υπηρεσίας*: Για το IoT, για παράδειγμα οι αισθητήρες, είναι πολύ συνηθισμένοι και μπορούν να δημιουργήσουν ή να χρησιμοποιήσουν δεδομένα τόσο μικρά όσο ένας ακέραιος αριθμός, που περιέχει μια τιμή θερμοκρασίας ή μια εντολή ενός byte για να απενεργοποιήσει έναν ενεργοποιητή. Το όνομα του περιεχομένου για κάθε ένα από αυτά τα κομμάτια δεδομένων πρέπει να προσδιοριστεί με μοναδικό τρόπο το περιεχόμενο. Για το λόγο αυτό, πολλά υπάρχοντα συστήματα ονοματοδοσίας έχουν μεγάλα ονόματα που είναι πιθανόν να είναι μεγαλύτερα από το πραγματικό περιεχόμενο δεδομένων για πολλούς τύπους εφαρμογών IoT. Επιπλέον, τα συστήματα ονοματοδοσίας που έχουν ιδιότητες αυτοπιστοποίησης (π.χ. δημιουργώντας το όνομα με βάση το hash του περιεχομένου) υποφέρουν από το πρόβλημα ότι το αντικείμενο μπορεί να ζητηθεί μόνο όταν έχει δημιουργηθεί και το περιεχόμενο είναι ήδη γνωστό, απαιτώντας παράλληλα κάποια μορφή υπηρεσίας ευρετηρίασης. Ενώ αυτό είναι ένα αποδεκτό γενικά για μεγαλύτερα αντικείμενα δεδομένων, είναι ανέφικτο στην χρήση όταν το μέγεθος του αντικειμένου είναι της τάξεως μερικών bytes.
- *Όνομα περιεχομένου με βάση το Hash*: Οι αλγόριθμοι Hashing χρησιμοποιούνται συνήθως για να ονομάσουν περιεχόμενο ώστε να επιβεβαιώσουν ότι το περιεχόμενο είναι αυτό που ζητήθηκε. Αυτό είναι εφικτό μόνο σε περιβάλλοντα όπου το αντικείμενο που ζητήθηκε, ήδη υπάρχει και όπου υπάρχει υπηρεσία καταλόγου για αναζήτηση ονομάτων. Αυτή η προσέγγιση είναι κατάλληλη για συστήματα με μεγάλα αντικείμενα δεδομένων όπου είναι σημαντικό να επαληθευτεί το περιεχόμενο.
- *Όνομα περιεχομένου που βασίζεται σε μεταδεδομένα*: Η εμπιστοσύνη στα μεταδεδομένα επιτρέπει τη δημιουργία ενός ονόματος για ένα αντικείμενο πριν καν δημιουργηθεί. Ωστόσο, αυτός ο μηχανισμός απαιτεί μεταδεδομένα που ταιριάζουν στη σημασιολογία.
- *Ονομασία υπηρεσιών*: Ομοίως με την ονομασία συσκευών ή δεδομένων, οι υπηρεσίες μπορούν να αναφερθούν με ένα μοναδικό αναγνωριστικό, που παρέχεται από μια συγκεκριμένη συσκευή ή από κάποιον που εκχωρείται

από μια κεντρική αρχή ως πάροχος υπηρεσιών. Μπορεί επίσης να είναι μια υπηρεσία που παρέχεται από οποιονδήποτε πληροί συγκεκριμένες συνθήκες μεταδεδομένων. Για παράδειγμα, η ανάκτηση περιεχομένου, η οποία παίρνει ένα όνομα ως είσοδο και επιστρέφει την τιμή αυτού του περιεχομένου, η οποία παίρνει μια εντολή ενεργοποίησης ως είσοδο και ενδεχομένως μετέπειτα επιστρέφει έναν κωδικό κατάστασης.

- *Εμπιστοσύνη*: Πρέπει να διασφαλίσουμε ότι το όνομα ενός δικτυακού στοιχείου δίδεται από έναν αξιόπιστο εκδότη στο πλαίσιο της αίτησης, όπως από έναν για παράδειγμα αξιόπιστο οργανισμό. Περαιτέρω, η εγκυρότητα κάθε τεμαχίου δεδομένων που δημοσιεύεται από μια εξουσιοδοτημένη οντότητα στον χώρο ονομάτων πρέπει να είναι επαληθεύσιμη - π.χ., ακολουθώντας μια ιεραρχική αλυσίδα εμπιστοσύνης σε μια ρίζα που είναι αποδεκτή για την εφαρμογή.
- *Ευελιξία*: Περαιτέρω προκλήσεις προκύπτουν για το σχήμα ιεραρχικής ονομασιολογίας, αναφερόμενοι στις απαιτήσεις σχετικά με τις "κατασκευαστικές ονομασίες" και τις "εκδόσεις κατά παραγγελία". Η πρώτη απαίτηση, συνεπάγεται ότι κάθε χρήστης είναι σε θέση να κατασκευάσει το όνομα ενός επιθυμητού στοιχείου δεδομένων μέσω συγκεκριμένων αλγορίθμων και ότι είναι δυνατή η ανάκτηση πληροφοριών χρησιμοποιώντας επίσης μερικά καθορισμένα ονόματα, ενώ η δεύτερη, αναφέρεται στη δυνατότητα να ζητηθεί ένα περιεχόμενο που δεν έχει ακόμη δημοσιευθεί στο παρελθόν, ενεργοποιώντας έτσι τη δημιουργία του.
- *Έλεγχος και οριοθέτηση*: Ορισμένες πληροφορίες θα μπορούσαν να είναι προσβάσιμες μόνο μέσα σε ένα δεδομένο πεδίο. Αυτή η πρόκληση είναι πολύ σημαντική για τις έξυπνες εφαρμογές σπιτιού και εφαρμογές παρακολούθησης της υγείας, όπου τα ζητήματα ιδιωτικού απορρήτου παίζουν βασικό ρόλο και το τοπικό πεδίο εφαρμογής ενός περιβάλλοντος στο σπίτι ή στο χώρο της υγειονομικής περίθαλψης μπορεί να καθοριστεί καλά. Ωστόσο, ο έλεγχος πρόσβασης βασισμένος σε περιμετρικά κανάλια παραβιάζεται συχνά στα τρέχοντα δίκτυα, επιτρέποντας τις μη-επικαιροποιημένες ενημερώσεις και τις υπηρεσίες που βασίζονται στο cloud, οπότε και αναδύεται η ανάγκη για την ύπαρξη δικλείδων ασφαλείας των δεδομένων που κινούνται στο ICN.
- *Εμπιστευτικότητα*: Καθώς τα ονόματα μπορούν να αποκαλύψουν πληροφορίες σχετικά με τη φύση της επικοινωνίας, θα πρέπει να διατίθενται μηχανισμοί για την εμπιστευτικότητα του ονόματος στην αρχιτεκτονική ICN-IoT.

Οι προκλήσεις που εμφανίζονται στην προσέγγιση του ICN δεν περιορίζονται όμως μόνο σε θέματα εμπιστευτικότητας και ονοματοδοσίας. Υπάρχουν προκλήσεις που περιγράφονται παρακάτω που αφορούν τη δρομολόγηση των δεδομένων μέσα στο δίκτυο. Η δρομολόγηση στο ICN-IoT διαφέρει από τη δρομολόγηση σε παραδοσιακά δίκτυα IP, επειδή η δρομολόγηση ICN βασίζεται σε ονόματα αντί για εντοπιστές. Σε γενικές γραμμές, η δρομολόγηση του ICN μπορεί να κατηγοριοποιηθεί στις ακόλουθες δύο κατηγορίες, κάθε μια από τις οποίες παρουσιάζει επιμέρους προκλήσεις:

- *Απευθείας δρομολόγηση βάσει ονόματος*: Τα πακέτα προωθούνται με το όνομα των δεδομένων ή το όνομα του κόμβου προορισμού. Εδώ, η κύρια πρόκληση είναι να διατηρηθεί σε λογικά επίπεδα η κατάσταση του δρομολογητή ICN που απαιτείται για τη δρομολόγηση / προώθηση δεδομένων. Αυτή η πρόκληση γίνεται πιο σοβαρή όταν χρησιμοποιείται ένα επίπεδο σχήμα ονοματολογίας λόγω της έλλειψης δυνατοτήτων συσσωμάτωσης.
- *Έμμεση δρομολόγηση*: Τα πακέτα προωθούνται με βάση τον εντοπιστή του κόμβου προορισμού και ο εντοπισμός επιτυγχάνεται μέσω της υπηρεσίας ανάλυσης ονομάτων. Συγκεκριμένα, η δέσμευση ονοματοδοσίας μπορεί να γίνει είτε πριν από τη δρομολόγηση (δηλαδή, στατική σύνδεση) είτε κατά τη διάρκεια της δρομολόγησης (δηλ., της δυναμικής σύνδεσης). Για τη στατική σύνδεση, η κατάσταση του δρομολογητή είναι ίδια με αυτή των παραδοσιακών δρομολογητών και η κύρια πρόκληση είναι η ανάγκη για γρήγορη επίλυση ονομάτων, ειδικά όταν οι κόμβοι IoT είναι κινητοί. Για τη δυναμική δέσμευση, οι δρομολογητές ICN πρέπει να διαχειρίζονται έναν πίνακα δρομολόγησης με βάση το όνομα, εξ ου και η πρόκληση να διατηρούνται χαμηλές οι στατικές πληροφορίες. Ταυτόχρονα, η ανάγκη για γρήγορη επίλυση ονομάτων είναι επίσης κρίσιμη.

  Τέλος, μια άλλη πρόκληση είναι η ποσοτικοποίηση του κόστους που σχετίζεται με τη διαχείριση της κινητικότητας, ιδιαίτερα τη στατική δέσμευση έναντι της δυναμικής δέσμευσης. Κατά τη διάρκεια μιας συναλλαγής στο δίκτυο, είτε ο παραγωγός δεδομένων είτε ο καταναλωτής μπορεί να απομακρυνθεί και, συνεπώς, πρέπει να χειριστούμε την κινητικότητα για να αποφύγουμε την απώλεια πληροφοριών. Η ICN δικτύωση, μπορεί να διαφοροποιήσει την κίνηση ενός καταναλωτή δεδομένων από εκείνη ενός παραγωγού. Όταν ένας χρήστης

μετακομίζει σε μια νέα θέση μετά την αποστολή του αιτήματος για δεδομένα, τα δεδομένα μπορεί να χαθούν, πράγμα που απαιτεί από τον χρήστη απλώς να ξαναστείλει το αίτημα, μια τεχνική που χρησιμοποιείται με την προσέγγιση απευθείας δρομολόγησης. Η προσέγγιση έμμεσης δρομολόγησης δεν κάνει διάκριση μεταξύ της κινητικότητας των χρηστών και των server και η προσωρινή αποθήκευση στο δίκτυο μπορεί να βελτιώσει την ανάκτηση δεδομένων για αυτήν την προσέγγιση. Εάν αντίθετα, η ίδια πηγή δεδομένων έχει μετακινηθεί, η πρόκληση είναι να ελέγξει το γενικό έλεγχο κατά την αναζήτηση ενός νέου παραγωγού δεδομένων. Για το σκοπό αυτό, θα μπορούσαν να χρησιμοποιηθούν τεχνικές πλημμύρας, αλλά μόνο ένα επίπεδο εντός του τομέα, διαφορετικά θα εξασθενούσε σοβαρά η σταθερότητα του δικτύου. Για τον χειρισμό της κινητικότητας σε διάφορους τομείς, θα μπορούσαν να χρησιμοποιηθούν πιο εξελιγμένες προσεγγίσεις, συμπεριλαμβανομένης της υιοθέτησης ενός σχεδίου ελέγχου βασισμένου σε SDN[12].

ΚΕΦΑΛΑΙΟ 7

Επιλογές Σχεδιασμού ICN

Έχοντας περιγράψει τον τρόπο λειτουργίας του ICN σε συνδυασμό με την πλατφόρμα POINT, τα πλεονεκτήματα λόγω της χρήσης του καθώς και τις κυριότερες προκλήσεις που καλείται να αντιμετωπίσει, παρακάτω παρατίθενται ορισμένες προτεινόμενες επιλογές σχεδιασμού του οράματος του IoT με χρήση του ICN, οι οποίες επιτρέπουν την αποτελεσματική και αποδοτική διαχείριση των δεδομένων IoT σε ένα δίκτυο ICN. Στόχος αυτού του κεφαλαίου είναι η διευκόλυνση της χρήσης ενός δικτύου ICN χωρίς να απαιτείται προσθήκη ειδικής λειτουργικότητας εφαρμογών IoT στο δίκτυο ICN.

Η σχέση των συσκευών IoT με τα υπάρχοντα πρωτόκολλα

Οι συσκευές IoT μπορούν να παίξουν ρόλο ως γεννήτριες περιεχομένου (π.χ. αισθητήρες), όπου ένα πρότυπο ICN θα πρέπει να είναι αποτελεσματικό για την ανάκτηση και τη διάδοση των δεδομένων. Ωστόσο, οι συσκευές IoT μπορεί επίσης να έχουν ρόλους ως ενεργοποιητές στους οποίους πρέπει να έχουν πρόσβαση οι συσκευές αυτές για σκοπούς ελέγχου. Καθώς τα δίκτυα ICN είναι πιθανό να συνυπάρχουν με τα υπάρχοντα πρωτόκολλα Διαδικτύου στις περισσότερες περιπτώσεις, θα θεωρήσουμε ότι ενδέχεται να υπάρξουν περιπτώσεις όπου μια κεντρική διεύθυνση κεντρικού υπολογιστή είναι πιο κατάλληλη για το IoT. Επιπλέον, για να διευκολυνθεί η υποστήριξη του IoT τόσο για την παραγωγή όσο και για τον έλεγχο και ενεργοποίηση των δεδομένων, υποθέτουμε ότι η δρομολόγηση του ICN πρέπει συνεπώς να λειτουργεί σε συνεννόηση με τα υπάρχοντα πρωτόκολλα Διαδικτύου.

Μορφή, σύνθεση και ονοματοδοσία δεδομένων

Τα δεδομένα που εξυπηρετούνται από το ICN μπορούν να συγκεντρωθούν από μικρότερα στοιχεία. Αν και τα στοιχεία δεδομένων IoT είναι σε πολλές περιπτώσεις μικρά και απλά, μια γενική πρόκληση στον ορισμό των εφαρμογών μέσω ICN είναι να αποφασιστεί το πώς να ομαδοποιήσουμε τα δεδομένα έτσι ώστε να μπορούν να ονομαστούν και να ζητηθούν. Η απαίτηση μερικών δεδομένων μέσα σε μια ομάδα μπορεί να αποτελέσει πρόκληση. Εάν τα δεδομένα που συντάσσονται απαρτίζονται από επιμέρους στοιχεία, τα οποία δεν είναι άμεσα ορατά από τον αιτούντα, η εύρεση ενός τέτοιου υποσυνόλου θα μοιάζει με ένα ερώτημα βάσης δεδομένων το οποίο ενδέχεται να απαιτεί επεξεργασία για να επιλυθεί. Το δίκτυο ICN δεν θα πρέπει να υποστηρίζει τέτοια πολυπλοκότητα.

Επομένως, μια επιλογή σχεδιασμού όσον αφορά τα δεδομένα IoT είναι να διατηρηθεί το δίκτυο ICN ελεύθερο από την υποστήριξη οποιονδήποτε προηγμένων ερωτημάτων και αντ 'αυτού να υποστηρίζει μόνο αντικείμενα με άμεση διεύθυνση. Οποιαδήποτε προηγμένη σύνθεση δεδομένων IoT και σχετική αναζήτηση για υποσυστατικών, θα προτείνεται να γίνεται από τους διακομιστές (endpoints) αντί εντός του δικτύου ICN. Για αποτελεσματική διαλειτουργικότητα του ICN, μόνο η δομή των αντικειμένων δεδομένων με ατομική διεύθυνση πρέπει να συμφωνηθεί και να χαρτογραφηθεί στο υποκείμενο σύστημα ονομασίας ICN, και αυτό, ώστε να αποφευχθούν νέες απαιτήσεις για το ICN και να διασφαλιστεί ότι η ανάγκη για υπολογισμό διατηρείται χαμηλή στο δίκτυο ICN, περιορίζοντάς την μόνο στην απόφαση για το εάν υπάρχει μνήμη cache ή όχι. Παρά το γεγονός ότι σαν σχεδιασμός μοιάζει να διευκολύνει τη λειτουργία της δικτύωσης ICN, δημιουργούνται και ορισμένες επιφυλάξεις:

- Το μέγεθος των άμεσα διευθυνσιοδοτούμενων αντικειμένων θα μπορούσε να παραμείνει αρκετά μικρό για να αποφευχθεί η μετάδοση περιττών δεδομένων μέσω δικτύων με περιορισμένους πόρους και η προσωρινή αποθήκευση στο δίκτυο ICN. Υπάρχει, ωστόσο, ένα εμπόδιο στο ότι τα μικρότερα αντικείμενα δεδομένων οδηγούν σε μεγαλύτερη ονομαστική επιβάρυνση.

- Αυτή η προσέγγιση σημαίνει ότι ένας χώρος διεύθυνσης ICN θα ήταν επαρκής, αλλά για πρακτικούς λόγους ένας ιεραρχικός χώρος διευθύνσεων μπορεί να προσθέσει κάποια οφέλη. Σε κάθε περίπτωση, υπάρχει ευελιξία στη χρήση

διαφορετικών συστημάτων διευθυνσιοδότησης ανάλογα με το τι υποστηρίζεται από το υφιστάμενο πλαίσιο ICN.

Αμετάβλητα αντικείμενα δεδομένων

Ο αριθμός των συσκευών IoT καθώς και η ποσότητα των δεδομένων που παράγονται από αυτές τις συσκευές ενδέχεται να είναι πολύ μεγάλος και τα δεδομένα μπορεί να διαδοθούν σε πολύ μεγάλα δίκτυα ICN. Η πιθανότητα ύπαρξης ασυνεπειών κρυφής μνήμης σε ένα δίκτυο ICN μπορεί ως εκ τούτου να είναι μεγάλη αν επιτρέψουμε τα δεδομένα να είναι μεταβλητά αντικείμενα. Για να υποστηριχθεί η επεκτασιμότητα, είναι σημαντικό να οριστούν ιδιότητες δεδομένων που διευκολύνουν την ανεξαρτησία και τη συνέπεια, ελαχιστοποιώντας ταυτόχρονα την ανάγκη για δυναμικό καθολικό συγχρονισμό. Ως εκ τούτου, μια βασική επιλογή σχεδιασμού είναι η χρήση μόνο αμετάβλητων αντικειμένων δεδομένων. Αυτό υποστηρίζει τη διανομή μεγάλης κλίμακας εξασφαλίζοντας ότι δεν υπάρχουν καθόλου δεδομένα στην περιοχή ICN. Ένας συμβιβασμός από αυτό είναι ότι τα δυναμικά δεδομένα πρέπει να διαμορφώνονται ως ροή αμετάβλητων αντικειμένων δεδομένων, ενδεχομένως καταναλώνοντας περισσότερους πόρους. Ωστόσο, αυτή η πρόκληση μπορεί να επιλυθεί με έξυπνες στρατηγικές προσωρινής αποθήκευσης όπου τα παλιότερα δεδομένα θα απομακρύνονται[12].

Ονοματοδοσία δεδομένων σε ροές αμετάβλητων αντικειμένων δεδομένων

Ως επέκταση των προηγουμένων, αξίζει να αναφερθεί πως πολλές συσκευές IoT παράγουν νέες μετρήσεις αισθητήρων ή άλλες τιμές δεδομένων σε τακτά χρονικά διαστήματα ή κατόπιν ζήτησης. Ένα βασικό πλεονέκτημα της μοντελοποίησης των δεδομένων IoT ως ροής αμετάβλητων αντικειμένων δεδομένων είναι ότι τα ICN

caches δεν θα περιέχουν καθόλου δεδομένα με ένα δοσμένο όνομα. Ωστόσο, δεδομένου ότι τα νέα αντικείμενα δεδομένων που αντιπροσωπεύουν διαφορετικές εκδοχές μιας ένδειξης αισθητήρα μπορεί να εκπέμπονται συχνά, πρέπει να υπάρχει ένας τρόπος με τον οποίο θα διακρίνονται οι διαφορετικές εκδόσεις. Για να υποστηριχθεί αποδοτικά κάτι τέτοιο, συνίσταται τα ονόματα των αντικειμένων να περιλαμβάνουν έναν αριθμό ακολουθίας. Όταν ένα αίτημα, για παράδειγμα observe, δεν περιλαμβάνει κανένα αριθμό στο μήνυμα που αποστέλλεται, θα λαμβάνει ως απόκριση από τη μνήμη cache την όποια πληροφορία έχει αποθηκευμένη εκείνη τη στιγμή. Αντίθετα, αν ένας αριθμός ακολουθίας περιλαμβάνεται στην αίτηση, μόνο μια ακριβής αντιστοίχιση μνήμης cache θα έχει ως αποτέλεσμα μια απάντηση. Ένας πελάτης που θέλει την "τελευταία" ανάγνωση μπορεί σύμφωνα με την προαναφερθείσα επιλογή σχεδιασμού, να μην ζητήσει από το δίκτυο ICN ένα τέτοιο ερώτημα υψηλού επιπέδου, αλλά πρέπει να ζητήσει τη συγκεκριμένη έκδοση πληροφορίας.

Μια άλλη μέθοδος για την απόκτηση της τελευταίας ανάγνωσης ή μιας συγκεκριμένης ανάγνωσης στο παρελθόν από έναν αισθητήρα είναι η πραγματοποίηση προσαρμοστικής ανίχνευσης, για παράδειγμα με τη μείωση του δυαδικού διαστήματος. Εάν ζητηθεί ένας αριθμός ακολουθίας που δεν υπάρχει, θα υπάρξει αρνητική απάντηση από το ICN. Ο client που επιθυμεί πάντα την τελευταία τιμή θα μπορούσε επίσης να συντονίσει δυναμικά τα αιτήματά του για την επόμενη τιμή δεδομένων στη συχνότητα του publisher, προκειμένου να ελαχιστοποιήσει την καθυστέρηση. Το γεγονός ότι ζητούνται μη υπάρχοντα δεδομένα θα μπορούσε εντούτοις να αποτελέσει απειλή για υπερφόρτωση στο ICN, δεδομένου ότι κάθε αίτημα μη υπάρχοντών δεδομένων θα μπορούσε να οδηγήσει σε απώλειες μνήμης cache που κυμαίνονται καθ 'όλη τη διαδρομή προς την πηγή, η οποία πρέπει να απαντήσει ότι τα δεδομένα δεν υπάρχουν. Ωστόσο, η εξυπηρέτηση αιτήσεων για μη υπάρχοντα δεδομένα αποτελεί γενική πρόκληση για την επίλυση του ICN η οποία όμως δεν περιορίζεται μόνο στο φάσμα των συσκευών του Internet of Things.

Μία τρίτη μέθοδος που θα μπορούσε να προταθεί, βρίσκεται μεταξύ των δύο παραπάνω. Εάν τα αιτήματα για ένα αντικείμενο δεδομένων που δεν υπάρχει ακόμα, μπορεί να κρατηθεί για μικρό χρονικό διάστημα μέχρις ότου το αντικείμενο δεδομένων είναι πραγματικά διαθέσιμο, αντί να επιστραφεί αμέσως μήνυμα "not

found". Με άλλα λόγια πραγματοποιείται μια είδους συνδρομή μέχρις ότου η πληροφορία να είναι διαθέσιμη. Εάν το ICN υποστηρίζει τέτοιου είδους αιτήματα, ο χρήστης μπορεί να στείλει αιτήματα για δεδομένα που θα δημοσιευθούν σύντομα. Υπό την προϋπόθεση ότι χρησιμοποιείται η συνάθροιση των αιτήσεων, ο μηχανισμός αυτός θα ήταν αποτελεσματικός και θα ελαχιστοποιούσε την καθυστέρηση[13].

Η σημασία του χρόνου

Ο χρόνος, όπως και σε κάθε είδους σύστημα δικτύου, έτσι και στο ICN, είναι μια πολύ σημαντική ιδιότητα των δεδομένων IoT, και ειδικά για δεδομένα που αλλάζουν με την πάροδο του χρόνου. Είναι σημαντικό να βρεθεί ένας τρόπος ώστε να εκπροσωπήσουμε αυτές τις ροές που σχετίζονται με το χρόνο των αμετάβλητων τιμών δεδομένων στο ICN, καθώς στο παράδειγμα ενός αισθητήρα που μετρά την θερμοκρασία ενός χώρου, η τιμή που αποστέλλεται, την επόμενη χρονική στιγμή μεταβάλλεται. Πρέπει να είναι δυνατόν να ζητηθεί μια τιμή δεδομένων από ένα συγκεκριμένο χρονικό διάστημα και να βρεθεί το όνομα της πιο πρόσφατης τιμής δεδομένων. Το ερώτημα είναι αν οι αριθμοί ακολουθίας είναι αρκετοί για να υποστηρίξουν το χρόνο. Γενικά, οι μέθοδοι που περιεγράφηκαν στην προηγούμενη ενότητα ισχύουν για την εύρεση μιας τιμής δεδομένων IoT από ένα συγκεκριμένο χρονικό σημείο, συμπεριλαμβανομένου του τελευταίου. Το σημείο στο οποίο υστερεί ο σχεδιασμός αυτός είναι η παρακολούθηση και συσχέτιση μεταξύ του αριθμού ακολουθίας και του χρόνου. Ένας τρόπος αντιμετώπισης αυτού, θα μπορούσε να είναι η χρήση αριθμών ακολουθίας που συμφωνούν άμεσα στον χρόνο, για παράδειγμα, ο χρόνος Unix (POSIX). Αυτό όμως θα περιορίσει την χρονική ανάλυση σε δευτερόλεπτα και θα έχει επίσης ως αποτέλεσμα μεγάλα κενά στους αριθμούς ακολουθιών, κάτι που μπορεί να είναι προβληματικό.

Υπάρχουν αρκετές άλλες μέθοδοι για την εύρεση μετρήσεων από μια συγκεκριμένη χρονική στιγμή ή την τελευταία ανάγνωση, για παράδειγμα μέσω ενός αιτήματος υψηλού επιπέδου από ένα διακομιστή ή χρησιμοποιώντας ένα σχήμα ονοματοδοσίας όπου το όνομα μπορεί να συναχθεί απευθείας, οι οποίες δύνανται να χρησιμοποιηθούν ανάλογα την περίπτωση, την ευαισθησία της πληροφορίας και το σύστημα στο οποίο εφαρμόζονται

Αποσύνδεση και ρόλοι client και server

Το δίκτυο ICN παρέχει από μόνο του την αποσύνδεση των αιτούντων (clients) και των ανταποκριτών (servers). Ένα σημαντικό χαρακτηριστικό του ICN είναι ότι επιτρέπει στους ανταποκριτές να είναι περιστασιακά μη διαθέσιμοι (π.χ. λόγω διακοπτόμενης συνδεσιμότητας, χαμηλής στάθμης μπαταρίας, κύκλου λειτουργίας). Ένα άλλο πλεονέκτημα είναι ότι η προσωρινή αποθήκευση στο ICN θα διασφαλίσει ότι τα αντικείμενα δεδομένων παραδίδονται κανονικά μόνο μία φορά από τις συσκευές IoT, ανεξάρτητα από τον αριθμό των άμεσα αιτούντων. Αξίζει να σημειωθεί όμως πως το ICN δεν πρέπει να παρέχει οποιαδήποτε μετατροπή ή συνάθροιση δεδομένων. Επομένως, η αρχιτεκτονική διάδοσης του IoT πρέπει να επιτρέπει οποιονδήποτε αριθμό ενδιάμεσων κόμβων επεξεργασίας. Ένας ενδιάμεσος κόμβος θα είναι ένα endpoint στο δίκτυο ICN που μπορεί να ενεργήσει τόσο ως αιτών όσο και ως ανταποκριτής. Η παράσταση τέτοιων κόμβων μπορεί για παράδειγμα να σχηματίσει ένα κατευθυνόμενο γράφημα μεταξύ servers και clients.

Πρόκειται για επιλογή σχεδίασης για να διατηρηθεί η λειτουργικότητα διάδοσης και συσσωμάτωσης του IoT εκτός του τομέα ICN. Αυτή η αρχιτεκτονική θα είναι μια επικάλυψη που μπορεί να έχει περίπλοκη δομή και να θέσει τη χρήση του ICN σε ένα νέο πλαίσιο, όπου το περιεχόμενο από τους τελικούς αιτούντες έως τους απόλυτους ανταποκριτές μπορεί να περάσει από πολλούς κόμβους επεξεργασίας IoT που συλλέγουν, επεξεργάζονται και επαναδημοσιεύουν δεδομένα μέσω ICN για διάφορους σκοπούς.

Συνδυασμός μοντέλου PULL / PUSH

Μια κρίσιμη απόφαση σχετικά με τα δεδομένα IoT είναι αν θα χρησιμοποιηθεί ένα μοντέλο PULL, ένα μοντέλο PUSH ή και τα δύο. Ορίζουμε ένα μοντέλο PULL ως σύστημα όπου τα δεδομένα αποστέλλονται μόνο όταν ζητείται ρητά, ενώ ένα μοντέλο PUSH υποδεικνύει ότι η μετάδοση δεδομένων ξεκινά από την πηγή με βάση κάποια ενεργοποίηση. Το μοντέλο PULL μπορεί να θεωρηθεί ως περιττό από πλευράς πόρων όταν υπάρχει άφθονη ποσότητα πληροφοριών IoT αλλά προτιμάται όταν οι συσκευές ενδιαφέρονται για κάποια πληροφορία ενίοτε ή σε μη τακτά χρονικά διαστήματα. Το

μοντέλο PUSH από την άλλη πλευρά, είναι αποτελεσματικό όταν υπάρχουν πληροφορίες σε πραγματικό χρόνο και οι πελάτες ενδιαφέρονται συνεχώς για όλες τις πληροφορίες από συγκεκριμένες συσκευές.

Μια απόφαση σχεδιασμού στον τομέα του IoT είναι να υποστηρίζει τόσο το PULL όσο και το PUSH. Το βασικό μοντέλο θα πρέπει να είναι PULL, αφού πρόκειται για τη φυσική λειτουργία του ICN, που σημαίνει ότι οι αιτούντες πρέπει πάντα να ξεκινούν με την αποστολή ενός αιτήματος. Αν το αίτημα αφορά ορισμένα συγκεκριμένα δεδομένα, μπορεί να επιλυθεί επιστρέφοντας τα δεδομένα (αν υπάρχουν). Μία πρόκληση με το μοντέλο PULL σε περιβάλλον ICN, είναι η ανάκτηση νέων δεδομένων που εμφανίζονται σποραδικά ή με βάση συγκεκριμένες συνθήκες. Ως εκ τούτου, αυτό που προτείνεται είναι σε ένα πλαίσιο IoT να μπορεί να υποστηριχθεί η αποτελεσματική ανάκτηση τέτοιων πληροφοριών, χωρίς να χρειάζεται να διερευνηθεί μέσω του ICN. Σύμφωνα με αυτή την πρόταση, ένα αίτημα μπορεί επίσης να περιλαμβάνει ενεργοποιητές, πράγμα που σημαίνει ότι τα δεδομένα θα επιστραφούν (pushed) όταν πληρούνται οι ενεργοποιητές, που μπορεί να είναι αμέσως ή σε αρκετές περιπτώσεις στο μέλλον. Αυτό μπορεί να χρησιμοποιηθεί για παράδειγμα για την αποστολή μηνυμάτων σε συνθήκες «συναγερμού» - triggers. Οι συνθήκες trigger μπορούν να ρυθμιστούν από τον αιτούντα ή να προκαθοριστούν από τον ανταποκριτή. Ο πρώτος θα είναι πιο ευέλικτος αλλά θα έχει και προβλήματα επιδόσεων, δεδομένου ότι ο αριθμός των συνθηκών ενεργοποίησης και η επακόλουθη παραγωγή δεδομένων θα εξαρτηθεί από έναν πιθανό μεγάλο αριθμό αιτούντων. Το τελευταίο είναι πιο κλιμακωτό δεδομένου ότι θα υπάρχει προκαθορισμένος και πεπερασμένος αριθμός συνθηκών ενεργοποίησης. Συνίσταται, τουλάχιστον για την αρχική φάση, να προχωρήσουμε σε μια απλή και κλιμακούμενη λύση και, ως εκ τούτου, να υιοθετήσουμε το μοντέλο όπου οι διαθέσιμες συνθήκες ενεργοποίησης καθορίζονται και δημοσιοποιούνται από τον ανταποκριτή. Το ICN θα ήταν ικανό να υποστηρίξει αυτές τις δημοσιεύσεις δυνατοτήτων, δεδομένου ότι είναι αρκετά στατικές[13].

Μεταδεδομένα, σήμανση και ανίχνευση δεδομένων

Τα δεδομένα του IoT μπορούν να επισημανθούν με μεταδεδομένα για να εντοπιστεί από πού προέρχονται. Η επισήμανση γίνεται σε επίπεδο πάνω από το δίκτυο ICN και μπορεί για παράδειγμα να είναι μια λίστα συμβολοσειρών. Μπορεί να προστεθεί/αλλάξει από τον κόμβο προέλευσης (ή από έναν κόμβο που αντιστοιχεί στο αρχικό αναγνωριστικό) και να προστεθεί/τροποποιηθεί/διαγραφεί από οποιονδήποτε κόμβο που επεξεργάζεται τα δεδομένα. Η ετικέτα μπορεί σε ορισμένες περιπτώσεις να χρησιμοποιηθεί για την ανίχνευση δεδομένων πίσω στις προελεύσεις. Σε ορισμένες περιπτώσεις, δεν έχει νόημα να ζητούνται ή να μεταδίδονται μεταδεδομένα όπου υπάρχουν περιορισμένοι πόροι. Για παράδειγμα όταν ένας ασύρματος κόμβος ζητά δεδομένα που αποθηκεύονται προσωρινά στο δίκτυο ICN, θα ήταν ωφέλιμο εάν αυτός που καλεί να μπορούσε να πει ότι είναι επιθυμητό να μην λάβει μεταδεδομένα[13].

Ο ρόλος των περιορισμένων συσκευών IoT ως κόμβων ICN

Οι τυπικοί κόμβοι ICN, όπως οι δρομολογητές και οι πύλες, θεωρούνται πλούσιοι σε πόρους όπως η ενέργεια, η επεξεργασία, το εύρος ζώνης και η αποθήκευση. Οι συσκευές IoT, από την άλλη πλευρά, είναι αρκετά περιορισμένες σε τέτοιους πόρους. Στις περισσότερες περιπτώσεις, η ενέργεια, η επεξεργασία και το εύρος ζώνης είναι αρκετά δαπανηρές για περιορισμένες συσκευές IoT. Αντίθετα, η αποθήκευση έχει δείξει μια ταχέως μειούμενη τάση των τιμών κατά τα τελευταία χρόνια. Ωστόσο, είναι αμφίβολο αν συσκευές IoT θα πρέπει επίσης να παρέχουν προσωρινή αποθήκευση δεδομένων που παράγονται από άλλες συσκευές IoT. Σε ad-hoc δίκτυα αυτό μπορεί να είναι επιθυμητό, αλλά συχνά υπάρχει η επιθυμία για ασύρματους κόμβους να ελαχιστοποιήσουν την επικοινωνία με το χειρισμό μόνο δεδομένων που τους απασχολούν. Ο βασικός σχεδιασμός είναι να διαχωρίζουμε λογικά τη λειτουργικότητα του διακομιστή IoT (όπως ανίχνευση και μετάδοση δεδομένων IoT) και τη λειτουργικότητα του ICN (όπως δεδομένα δρομολόγησης και προσωρινής αποθήκευσης που παράγονται από άλλες συσκευές). Μία συσκευή περιορισμένης πόρων μπορεί να επιλέξει να εφαρμόζει μόνο λειτουργικότητα IoT και να ενεργεί ως διακομιστής στο ICN, δηλ. να μην ενεργεί ως ενδιάμεσος κόμβος ICN. Ωστόσο,

δεδομένου ότι η αποθήκευση γίνεται φθηνότερη, οι συσκευές IoT θα πρέπει να είναι σε θέση να αποθηκεύουν προσωρινά το δικό τους περιεχόμενο και, ουσιαστικά, να ενεργούν ως πηγές για την ICN[13].

ΜΕΡΟΣ ΤΕΤΑΡΤΟ

ΠΡΟΚΛΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΤΟΥ INTERNET OF THINGS

Λόγω της φύσης της τεχνολογίας του Internet of Things, μια συσκευή ή ένα Πληροφοριακό Σύστημα IoT, απειλείται τόσο από τους κινδύνους των Δικτύων κινητής τηλεφωνίας, τόσο από τους κινδύνους των δικτύων των sensors όσο και από το Ίντερνετ. Η συσχέτιση μιας συσκευής IoT με τις παραπάνω περιοχές δικτύων δεν γίνεται με την πρώτη ματιά αντιληπτή, αρκεί όμως να συλλογιστούμε τα εξής:

Μια συσκευή IoT, για παράδειγμα ένα έξυπνο ρολόι που μετρά την απόσταση που τρέχουμε, τους παλμούς κ.ο.κ., είναι μόνιμα συνδεδεμένο στο διαδίκτυο μέσω κάποιας σύνδεσης. Αυτό σημαίνει ότι πληροφορίες αποστέλλονται και λαμβάνονται συνεχώς, καταγράφεται η διαδρομή που διανύει ο άνθρωπος, καταχωρούνται τα ζωτικά του σημεία και έμμεσα καταγράφεται η καθημερινή του ρουτίνα.

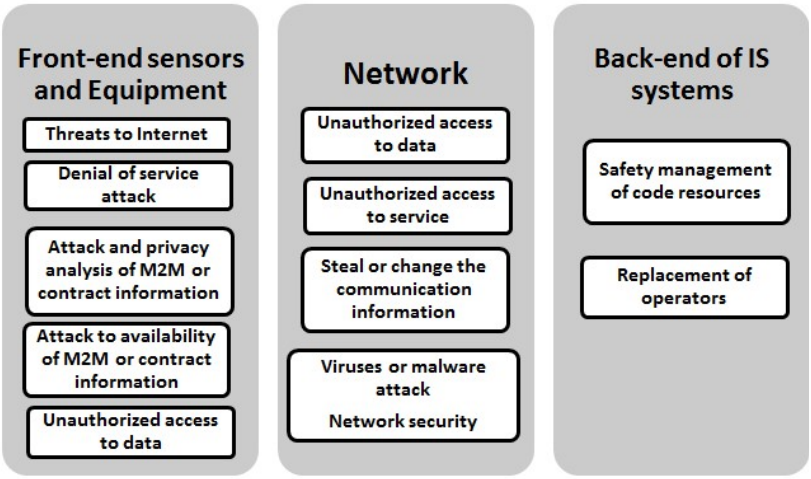
Επιπλέον, η βάση στην οποία στηρίζεται η τεχνολογία του IoT όπως αναφέρθηκε και προηγουμένως, είναι τα RFID tags, οι sensors, το Bluetooth και Near Field Communications. Στην εικόνα αυτή, εισέρχεται ο κίνδυνος της ιδιωτικότητας, της ασφάλειας της πληροφορίας που μεταδίδεται και αποθηκεύεται σε κάποια cloud υπηρεσία. Αν κάποιος έχει τη δυνατότητα να παρέμβει σε οποιοδήποτε κομμάτι της επικοινωνίας μεταξύ του smart watch και του server με τον οποίο επικοινωνεί, μπορεί να εξάγει πληροφορίες όπως, πότε και πόσο ο χρήστης λείπει από το σπίτι, που συχνάζει, τις συνήθειές του κλπ. Τέτοιες πληροφορίες μπορούν να χρησιμοποιηθούν κακόβουλα για να βλάψουν με κάποιον τρόπο τον χρήστη (π.χ. ληστεία) ή και να τον παρακολουθούν.

ΚΕΦΑΛΑΙΟ 8

Αδυναμίες Ασφάλειας Συσκευών και Υπηρεσιών IoT έναντι επιθέσεων

Οι επιθέσεις από hackers, όπως έχει δείξει ως σήμερα η ιστορία, αντί να λιγοστεύουν χάριν στις σουίτες ασφαλείας και τις υπέρογκες χρηματοδοτήσεις προς την Ασφάλεια των Πληροφοριακών Συστημάτων, είναι ολοένα αυξανόμενες και τείνουν να γίνουν πιο προκλητικές και σε αρκετές περιπτώσεις ξεπερνούν τα όρια του απλού hobby ή του hactivism και αγγίζουν τα όρια του εγκλήματος με θύματα όχι τα δεδομένα ή τα χρήματα ενός οργανισμού αλλά τον ίδιο τον άνθρωπο. Η τάση αυτή φαίνεται καθώς ο χρόνος περνά, να γίνεται όλο και πιο έντονη και οι επιθέσεις να είναι ολοένα και πιο επικίνδυνες. Όταν μιλάμε για IoT, οι κίνδυνοι αυτοί δεν περιορίζονται σε επιθέσεις που μπορούν να βλάψουν τα δεδομένα μιας επιχείρησης. Αντίθετα, επειδή οι συσκευές εξοπλισμένες με τεχνολογία IoT , είναι συσκευές που χρησιμοποιεί ο άνθρωπος στην καθημερινότητα του, είτε για το σπίτι του είτε για την παρακολούθηση της υγείας του, οι επιθέσεις μπορούν να προσβάλλουν το ιδιωτικό απόρρητο αλλά και την σωματική του ακεραιότητα. Παράδειγμα, η ερευνητική ομάδα η οποία κατάφερε να παρακάμψει τα πρωτόκολλα ασφαλείας ενός mannequin που είχε βηματοδότη και να το «σκοτώσει». [21]

Αν θα μπορούσαμε να περιγράψουμε πολύ συνοπτικά τις κυριότερες ανησυχίες γύρω από την ασφάλεια ενός περιβάλλοντος Internet of Things θα μπορούσαμε να παρατηρήσουμε την επόμενη εικόνα:



Εικ. (J. Sathish Kumar , Dhiren R. Patel , "A Survey on Internet of Things: Security and Privacy Issues)

Επιπλέον, πηγή των περισσότερων κινδύνων σε περιβάλλοντα IoT είναι η μικρή υπολογιστική ισχύ και το κόστος που οι αλγόριθμοι ασφαλείας μπορούν να επιφέρουν στις επιδόσεις αυτών των απλών συσκευών κάτι που μπορεί να γίνει εύκολα κατανοητό, αντιπαραβάλλοντας ένα σύστημα IoT με ένα κινητό τηλέφωνο ή έναν υπολογιστή. Σε έναν υπολογιστή, ο οποίος είναι συνδεδεμένος με το Ιντερνετ και που έχει σαφώς πολλαπλάσια ικανότητα υπολογιστικής ισχύος, μπορεί να χρησιμοποιηθεί συνδυασμός σουιτών ασφαλείας οι οποίες εξασφαλίζουν ένα αρκετά ικανοποιητικό επίπεδο ασφάλειας και προστασίας της ιδιωτικότητας του χρήστη. Αντίθετα, μια συσκευή IoT, ένα έξυπνο ψυγείο, ένα smart watch, ή αυτόματοι ρυθμιστές θερμοκρασίας ενός χώρου, στερούνται αυτής της ικανότητας. Όπως αναφέρθηκε και προηγουμένως, στόχος ενός συστήματος IoT είναι η παροχή της υπηρεσίας με όσο το δυνατό μικρότερο κόστος, ώστε να μην επιβαρυνθεί η τελική τιμή πώλησης του αντικειμένου, και με όσο το δυνατόν μικρότερο αντίκτυπο στην απόδοση της συσκευής. Με αυτό δεδομένο, γίνεται φανερό πως το περιθώριο ενσωμάτωσης μιας σουίτας ασφαλείας σε μια τέτοια συσκευή σημαίνει μείωση της απόδοσης της και επομένως μείωση της ποιότητας της υπηρεσίας που παρέχει και τελικά να το καθιστούν ευάλωτο σε επιθέσεις, αφήνοντας έτσι περιθώρια, το ζητούμενο της ασφάλειας να ανευρεθεί σε άλλα επίπεδα της λειτουργικότητας, όπως αυτό της μετάδοσης των μηνυμάτων μέσω του δικτύου.

Εκτός από τους κινδύνους που οφείλονται στη φιλοσοφία και τη γενικότερη αρχιτεκτονική του IoT, μερικοί από τους επιμέρους κινδύνους που αφορούν τόσο στη συσκευή αλλά και γενικότερα στην υπηρεσία που παρέχεται, είναι οι ακόλουθοι:

Cloud storage

Τα τελευταία χρόνια ολοένα και περισσότερες επιχειρήσεις στρέφονται προς παρόχους cloud storage καθώς η ποσότητα της πληροφορίας που θέλουν να αποθηκεύουν είναι υπέρογκη. Αποτέλεσμα αυτού, είναι και η στροφή του ενδιαφέροντος και των hacktivists προς τα εκεί και να προσπαθούν να αποκτήσουν πρόσβαση στις πληροφορίες αυτές. Τέτοιες επιχειρήσεις είναι και Ιατρικές, οι οποίες κρατούν και επεξεργάζονται δεδομένα από χιλιάδες ασθενείς. Οι ασθενείς μπορεί να έχουν κάποια συσκευή παρακολούθησης της υγείας τους, της τοποθεσίας τους σε περίπτωση ανάγκης, των ζωτικών τους σημείων ίσως και στο μέλλον εφαρμογές που να ρυθμίζουν κάποιες λειτουργίες πρόσθετων τεχνητών μελών. Πρόσβαση σε αυτές τις υπηρεσίες ή τις πληροφορίες μπορούν να χρησιμοποιηθούν με σκοπό να βλάψουν τον χρήστη.

Μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες

Όπως κάθε παραδοσιακό πληροφοριακό σύστημα, έτσι και στο IoT, υπάρχει ο κίνδυνος της πρόσβασης σε πληροφορία από κακόβουλους τρίτους. Οι συσκευές IoT βασίζονται σε τεχνολογίες Big Data και Cloud, καθώς πολλοί χρήστες στέλνουν αυτόματα δεδομένα, τα οποία καταγράφονται, επεξεργάζονται και στη συνέχεια εξάγουν πληροφορίες τις οποίες διαθέτουν και πάλι στους χρήστες για να χρησιμοποιηθούν. Λαμπρό παράδειγμα μη εξουσιοδοτημένης πρόσβασης αποτελεί η περυσινή επίθεση στο iCloud της Apple που είχε ως αποτέλεσμα να διαρρεύσουν δεκάδες φωτογραφίες και βίντεο διασημοτήτων από προσωπικές τους στιγμές. αυτού. [23]

Υποκλοπή ή αλλαγή πληροφοριών επικοινωνίας

Αποκτώντας πρόσβαση μέσω του δικτύου στην επικοινωνία μεταξύ συσκευής και server, δίνεται η δυνατότητα στον κακόβουλο χρήστη να αλλοιώσει τα στοιχεία που αποστέλλονται. Σε ένα έξυπνο αυτοκίνητο όπως το Tesla, έχει προστεθεί πλέον η δυνατότητα να πλοηγείται αυτόματα προς κάποια κατεύθυνση. Η τεχνολογία αυτή, τα επόμενα χρόνια θα είναι πιο διαδεδομένη. Αν κάποιος επηρεάσει την προκαθορισμένη πορεία του οχήματος μέσω του σήματος GPS, μπορεί να καθοδηγήσει το όχημα κάπου άλλου με σκοπό την απαγωγή του οδηγού ή την κακοποίηση του.

Μη εξουσιοδοτημένη πρόσβαση στην υπηρεσία

Στην ίδια όψη του νομίσματος, εφόσον γίνει δυνατή η πρόσβαση στην υπηρεσία IoT, ο κακόβουλος χρήστης, έχει πλέον τη δυνατότητα να επηρεάσει τις παραμέτρους του συστήματος. Στο προηγούμενο παράδειγμα, τέτοιου είδους πρόσβαση θα σήμαινε ότι κάποιος, απομακρυσμένα μπορεί να ελέγχει την πλοήγηση του αυτοκινήτου και να προκαλέσει άθελα ή ηθελημένα κάποιο ατύχημα.[23]

Denial of service attack

Μια πολύ διαδεδομένη τα τελευταία χρόνια μορφή επίθεσης είναι το DDoS. Με την παραδοσιακή της έννοια, επιτυγχάνεται μέσω της επανάληψης χρήσης της υπηρεσίας σε τέτοιο βαθμό, ώστε η υπηρεσία να μη μπορεί να ανταπεξέλθει στη «ζήτηση» εκείνη τη στιγμή και το σύστημα να «πέφτει». Στον τομέα του IoT, μια συσκευή μπορεί να χρησιμοποιηθεί ως μέσο για να γίνει μια τέτοια επίθεση. Οι hackers, εκμεταλλεύονται το γεγονός ότι πολλές συσκευές δεν έχουν επαρκή πρωτόκολλα ασφαλείας, τις προσβάλλουν με κώδικα ο οποίος ουσιαστικά τις μετατρέπει σε «botnets» και στη συνέχεια, χιλιάδες συσκευές συνδεδεμένες στο διαδίκτυο δημιουργούν ψευδή κίνηση προς κάποιον server με σκοπό τη διακοπή της λειτουργίας του.[22]

Τέλος, οι κίνδυνοι του Internet of Things δεν είναι απαραίτητο να ευθύνονται στην παρέμβαση του ανθρώπου. Παρακάτω ακολουθούν ορισμένοι κίνδυνοι οι οποίοι υπάρχουν λόγω ελλιπούς σχεδιασμού της αρχιτεκτονικής του IoT.

RFID Technology Issues

Η τεχνολογία RFID όπως αναφέρθηκε και προηγουμένως αποτελεί τη ραχοκοκαλιά της τεχνολογίας IoT. Παρόλα αυτά όμως, δεν έχει κατοχυρωθεί ακόμα κάποιο παγκόσμιο πρότυπο επικοινωνίας. Λόγω της μη ύπαρξης ενός προτύπου μπορεί να μην είναι δυνατή η ανάγνωση της πληροφορίας της ετικέτας από έναν δέκτη που έχει διαφορετική αρχιτεκτονική κατασκευής. Αν η συσκευή αυτή, είναι ένας βηματοδότης, είναι προφανής ο κίνδυνος που διατρέχει ο ασθενής. Μπορεί από μια λάθος μέτρηση, να υπάρχουν αποκλίσεις στις μετρήσεις και να δοθεί εντολή για μια λειτουργία η οποία να θέσει σε κίνδυνο τη ζωή του.

Στο ίδιο μήκος κύματος είναι και ο κίνδυνος συμφόρησης των σημάτων. Θα πρέπει να διασφαλίζεται ότι το σήμα που εκπέμπει ένας πομπός φθάνει στον δέκτη που απευθύνεται και αντίστροφα, καθώς και εδώ μπορεί να σταλούν πληροφορίες λανθασμένες και να υπάρξουν προβλήματα.

Επιπλέον, RFIDs φθηνής κατασκευής, μπορεί να είναι κατασκευασμένα με ασθενή πρωτόκολλα ασφαλείας και να μπορούν να παραβιαστούν εύκολα. Μπορεί η πληροφορία που μεταφέρουν οι ετικέτες να μην είναι σημαντική, όμως σε πολλές περιπτώσεις, το να γνωρίζει κάποιος κακόβουλος την ακριβή ή αναμενόμενη τοποθεσία κάποιου αντικείμενου ή του χρήστη του, είναι αρκετό.

Θέματα Wireless sensor networks (WSNs)

Τα WSN δίκτυα, είναι δίκτυα τα οποία αυτό – οργανώνονται με δυναμική τοπολογία και ευρέως κατανεμημένα multi-hops δίκτυα. Τα δίκτυα αυτά, έχουν περιορισμένους πόρους, μικρό χώρο αποθήκευσης, μικρή δυνατότητα υπολογισμών και στενό εύρος ανίχνευσης, χαρακτηριστικά τα οποία οδηγούν σε μια σειρά κινδύνων ασφαλείας του

δικτύου. Κατά τη διαδικασία συλλογής των δεδομένων, το μήνυμα που αποστέλλεται μπορεί να υποπέσει σε κακόβουλη δρομολόγηση, αλλοίωση και γενικότερα κακόβουλη πρόσβαση στο δίκτυο. Τα παραπάνω, θεωρητικά μπορούν να επιλυθούν με προσεγγίσεις κρυπτογραφίας, κάτι τέτοιο όμως τελικά φαίνεται να είναι πολύ δύσκολο εξαιτίας της μικρής υπολογιστικής ισχύος που παρέχεται από τα δίκτυα αυτά και της πληθώρας των διαφορετικών αρχιτεκτονικών που ακολουθούν οι διάφορες συσκευές IoT.[20]

Θεματα ασφαλειας εφαρμογων IoT

Τα θέματα ασφαλείας σε επίπεδο εφαρμογών, είναι προβλήματα που ξεφεύγουν από τον πυρήνα της αρχιτεκτονικής του IoT και αποτελούν μέλημα του δημιουργού της κάθε εφαρμογής. Όπως είναι γνωστό, πλέον ο οποιοσδήποτε έχει τη δυνατότητα να δημιουργήσει μια εφαρμογή και να την παρέχει είτε δωρεάν είτε έναντι κάποιου αντιτίμου. Οι εφαρμογές αυτές επομένως, μπορούν να κατασκευαστούν είτε από μεγάλες εταιρείες είτε από απλούς ιδιώτες που προσπαθούν να αποκτήσουν φήμη στον χώρο του προγραμματισμού. Η διαφορά στις παραπάνω ομάδες software distributors έγκειται στο γεγονός πως οι επιχειρήσεις έχουν τα κεφάλαια, την τεχνογνωσία, την πείρα και το ανθρώπινο δυναμικό ώστε να λάβουν σοβαρά το πρόβλημα της ιδιωτικότητας που εμφανίζεται, σε σχέση με κάποια ομάδα ελεύθερων επαγγελματιών ή και φοιτητών. Άμεσο αποτέλεσμα αυτού, είναι η ύπαρξη μη ασφαλών εφαρμογών που μπορούν εύκολα να παραβιαστούν και να παρέχουν σε μη εξουσιοδοτημένους χρήστες πληροφορίες που αναφέρθηκαν και προηγουμένως σχετικά με τις συνήθειες του χρήστη.

ΚΕΦΑΛΑΙΟ 9

Αδυναμίες Ασφάλειας πρωτοκόλλου CoAP και προσέγγισης ICN

CoAP Security Threats

Παρά το γεγονός ότι η λειτουργικότητα της παρατήρησης των πόρων μπορεί να επιλύει κάποια προβλήματα στις εφαρμογές που χρησιμοποιείται, υπάρχει περίπτωση να αποτελέσει και ένα μέσο που μπορεί να χρησιμοποιηθεί από κακόβολους χρήστες για DDos επιθέσεις. Αυτό μπορεί να συμβεί αφενός μέσω των μηνυμάτων που αποστέλλονται από το server ή από κάποιον κακόβουλο τα οποία δύναται να έχουν μεγαλύτερο μέγεθος, προκαλώντας συμφόρηση και αφετέρου, λόγω της φύσης του πρωτοκόλλου, μπορούν να αποστέλλονται πολλαπλά μηνύματα ως ενημερώσεις της κατάστασης του πόρου. Επομένως, κρίνεται απαραίτητη η ύπαρξη ενός μηχανισμού για αυθεντικοποίηση των μηνυμάτων καθώς και μια συχνότητα αποστολής αυτών, ελεγχόμενη από τον αντίστοιχο αριθμό μηνυμάτων επιβεβαίωσης που στέλνει ο client. Μια άλλη τακτική επίθεσης, είναι αυτή της εξάντλησης των πόρων του server. Αν οι πόροι εξαντληθούν, τότε προκαλείται αστάθεια στο σύστημα και αν επρόκειτο για κάποια ευαίσθητη πληροφορία, για παράδειγμα το επίπεδο θερμοκρασίας εντός ενός πυρηνικού αντιδραστήρα, μπορεί να προκληθούν πολύ σημαντικές ζημίες οι οποίες ενδέχεται να βλάψουν και τους ανθρώπους. Ένας τρόπος αντιμετώπισης αυτού του ενδεχομένου από την πλευρά του server, είναι ο αποκλεισμός αιτημάτων GET που ζητούν την εγγραφή στη λίστα των ενδιαφερομένων, όταν οι πόροι είναι κοντά σε οριακό επίπεδο.[14]

Ασφαλεια και ιδιωτικοτητα σε Information Centric Networking

Η ασφάλεια και η προστασία της ιδιωτικής ζωής είναι ζωτικής σημασίας για όλες τις εφαρμογές IoT. Το πρότυπο ICN όπως έχει αναφερθεί και προηγουμένως, είναι εστιασμένο στις πληροφορίες, σε αντίθεση με το κεντρικοποιημένο διαδίκτυο. Εκτός

από πτυχές όπως η ονομασία, η ανάκτηση περιεχομένου και η προσωρινή αποθήκευση, αυτό έχει επίσης συνέπειες που αφορούν την ασφάλεια.

Το ICN υποστηρίζει το μοντέλο εμπιστοσύνης στο περιεχόμενο και όχι την εμπιστοσύνη στους hosts του δικτύου. Εξαιτίας αυτού, αναδύεται η έννοια της Ασφάλειας Αντικειμένων (Object Security), η οποία έρχεται σε αντίθεση με τους μηχανισμούς ασφαλείας βασισμένους σε συνεδρίες, όπως το TLS-DTLS, το οποίο επικρατεί στο σημερινό κεντρικοποιημένο διαδίκτυο. Η ασφάλεια αντικειμένων βασίζεται στην ιδέα της διασφάλισης πληροφοριών που ανήκουν σε αντικείμενα, σε αντίθεση με τους μηχανισμούς ασφάλειας βασισμένους σε συνεδρίες, οι οποίοι εξασφαλίζουν το κανάλι επικοινωνίας μεταξύ ενός ζεύγους κόμβων. Αυτό ενισχύει ένα χαρακτηριστικό των δικτύων ICN που αναφέρθηκε σε προηγούμενη ενότητα, την αποσύνδεση των αποστολέων από τους δέκτες.

Στο γενικό πλαίσιο του IoT, το μοντέλο Ασφάλειας Αντικειμένων έχει αρκετά συγκεκριμένα πλεονεκτήματα. Πολλές εφαρμογές IoT έχουν ως κύριο στόχο τα δεδομένα και τις υπηρεσίες, ενώ η επικοινωνία μεταξύ δύο συσκευών έρχεται σε δεύτερη προτεραιότητα. Επομένως, είναι πιο λογικό να εξασφαλίζουμε αντικείμενα IoT αντί να εξασφαλίζουμε τη σύνοδο μεταξύ των επικοινωνιακών τελικών σημείων. Παρόλο που το ICN περιλαμβάνει στοιχεία ασφαλείας βασισμένα σε δεδομένα, οι μηχανισμοί πρέπει να είναι αρκετά γενικοί ώστε να ικανοποιούν τις πολλαπλές απαιτήσεις πολιτικής που θέτουν οι διάφορες εφαρμογές. Επιπλέον, οι ανησυχίες σχετικά με την ασφάλεια και την προστασία της ιδιωτικότητας, πρέπει να αντιμετωπιστούν κατά τρόπο συγκεκριμένο όσον αφορά την προοπτική λειτουργίας των δικτύων, η οποία καλύπτει την ονοματολογία, τη δρομολόγηση και την προσωρινή αποθήκευση. Σε γενικές γραμμές, θεωρείται ότι η προστασία της ασφάλειας και της ιδιωτικότητας σε συστήματα IoT, θα πρέπει να επικεντρωθεί κυρίως στις ακόλουθες πτυχές: εμπιστευτικότητα, ακεραιότητα, εξακρίβωση της γνησιότητας και τη διαθεσιμότητα.[15]

Εφαρμόζοντας μεθόδους ασφάλειας και προστασίας της ιδιωτικότητας, αντιμετωπίζουμε διαφορετικές προκλήσεις στο επίπεδο υποδομής του δικτύου. Εξαιτίας της φύσης και της φιλοσοφίας του IoT όσο και των συσκευών, όπως αναφέρθηκε έχουν δημιουργηθεί ανησυχίες σχετικά με θέματα ασφαλείας που

περιγράφηκαν στις προηγούμενες σελίδες. Η πρόταση του ICN ως έναν τρόπο βελτιστοποίησης της λειτουργικότητας, παρά τα πλεονεκτήματα που επιφέρει, δημιουργεί παράλληλα και νέες ενδεχόμενες απειλές στο επίπεδο της υποδομής, κυριότερες από τις οποίες είναι οι ακόλουθες:

- Πρέπει να διασφαλίσουμε ότι το όνομα ενός δικτυακού στοιχείου εκδίδεται από μια αξιόπιστη οντότητα. Καθώς το όνομα δεσμεύεται με ασφάλεια στα δεδομένα του ICN, πρέπει επίσης να ληφθούν υπόψη οι περιορισμοί ασφάλειας του περιεχομένου που δεν έχει ακόμη δημοσιευθεί.
- Ένας εισβολέας μπορεί να αποκτήσει πρόσβαση ή να συλλέξει πληροφορίες από έναν πόρο που δεν έχει το δικαίωμα. Κατά συνέπεια, ένας αντίπαλος μπορεί να εξετάσει, να αφαιρέσει ή και να τροποποιήσει εμπιστευτικές πληροφορίες.
- Ένας εισβολέας μπορεί να μιμείται μια εξουσιοδοτημένη διαδικασία χρήστη ή δικτύου. Ως αποτέλεσμα, ο εισβολέας μπορεί να υποκλέψει τις υπογραφές ή να μιμηθεί μια διεύθυνση πηγής.
- Ένας κακόβουλος χρήστης, μπορεί να χειριστεί τη διαδικασία ανταλλαγής μηνυμάτων μεταξύ οντοτήτων δικτύου. Αυτός ο χειρισμός μπορεί να περιλαμβάνει επανάληψη, εσφαλμένη δρομολόγηση και διαγραφή μηνυμάτων.
- Τέλος, ένας εισβολέας μπορεί να εισάγει ψευδή δεδομένα σε έναν αισθητήρα του δικτύου. Το αποτέλεσμα μπορεί να είναι η αύξηση της καθυστέρησης και υποβάθμιση της απόδοσης για δικτυακές υπηρεσίες και εφαρμογές.[18]

Έχοντας αναλύσει στις προηγούμενες σελίδες τις αδυναμίες τόσο του IoT όσο και του πρωτοκόλλου, παρακάτω, ακολουθούν ορισμένες βασικές προτάσεις ασφάλειας και σχετικές επιλογές σχεδίασης της χρήσης ICN και Object Security οι οποίες μπορούν να συνδράμουν στην αποτελεσματική αντιμετώπιση μεγάλου πλήθους από τις απειλές που συζητήθηκαν.

ΑΝΑΚΤΗΣΗ ΕΜΠΙΣΤΕΥΜΕΝΟΥ ΠΕΡΙΕΧΟΜΕΝΟΥ ΑΠΟ ΜΗ ΑΞΙΟΠΙΣΤΕΣ ΚΡΥΦΕΣ ΜΝΗΜΕΣ (CACHES)

Λειτουργώντας σε ένα δίκτυο ICN, ένας IoT client αναμένεται να βασιστεί στο δίκτυο για να παραδώσει το περιεχόμενο που ζητήθηκε με τον βέλτιστο τρόπο, χωρίς να ασχολείται με το πού βρίσκεται το περιεχόμενο. Αυτό θα μπορούσε ενδεχομένως

να σημαίνει ότι κάθε μεμονωμένο αντικείμενο μέσα σε μια δέσμη αμετάβλητων αντικειμένων ανακτάται από διαφορετική πηγή. Δημιουργείται λοιπόν η ανάγκη ανάκτησης αξιόπιστου περιεχομένου από μη αξιόπιστους κόμβους/κρυφές μνήμες. Μέσω της Ακεραιότητας Ονομάτων-Δεδομένων (Name-Data Integrity), το ICN εγγυάται αυτόματα την ακεραιότητα των δεδομένων στον αιτούντα ανεξάρτητα από την πηγή από την οποία προέρχεται. Επιπλέον, οι υπογραφές που βασίζονται σε αντικείμενα και η κρυπτογράφηση είναι ιδανικές σε τέτοιες περιπτώσεις χρήσης, επειδή ανακουφίζουν μια εφαρμογή πελάτη IoT από την ταλαιπωρία της ανάγκης να δημιουργήσουν εμπιστοσύνη με κάθε κόμβο που μπορεί να αποθηκεύσει προσωρινά ένα αντικείμενο IoT. Αυτό σημαίνει επίσης ότι ένας αιτών πελάτης μπορεί να κάνει χρήση περισσότερων κρυφών μνήμων στο δίκτυο, με αποτέλεσμα την καλύτερη απόδοση και λανθάνουσα κατάσταση.

Επεξεργασια στρωματος εφαρμογων σε μη αξιοπιστους ενδιαμεσους

Η προστασία περιεχομένου σε επίπεδο αντικειμένου παρέχει μεγαλύτερη ευκρίνεια και επομένως περισσότερο έλεγχο. Ένα αντικείμενο δεδομένων ICN μπορεί να περιλαμβάνει διάφορα διακριτά αντικείμενα στρώματος εφαρμογής όπως για παράδειγμα, αντικείμενα XML και JSON. Ένα παράδειγμα αυτού είναι ένα αντικείμενο ICN που αντιστοιχεί σε όλες τις μετρήσεις του αισθητήρα σε ένα συγκεκριμένο χρονικό διάστημα όπου κάθε ανάγνωση αισθητήρα είναι ένα αντικείμενο JSON. Η χρήση της κρυπτογράφησης βάσει αντικειμένων για την παροχή της εμπιστευτικότητας δεδομένων, επιτρέπει τη δυνατότητα κρυπτογράφησης ενός υποσυνόλου αυτών των αντικειμένων επιπέδου εφαρμογής, αφήνοντας άλλα μη κρυπτογραφημένα και διαθέσιμα για επεξεργασία σε μη αξιόπιστους ενδιάμεσους κόμβους (π.χ. διακομιστές μεσολάβησης και προσωρινής αποθήκευσης). Με αυτήν την προσέγγιση, η εφαρμογή IoT έχει περισσότερο έλεγχο των τμημάτων των δεδομένων που θέλει να δημοσιοποιήσει και των τμημάτων των δεδομένων που θέλει να κρατήσει εμπιστευτικά και ορατά μόνο στους ομότιμους κόμβους με τα σωστά κρυπτογραφικά κλειδιά.[15,18]

Ενεργειακη αποδοση κρυπτογραφικων μηχανισμων

Τα πρωτόκολλα ασφαλείας βασισμένα σε περιήγηση βασίζονται στην ανταλλαγή πολλών μηνυμάτων πριν από τη δημιουργία μιας ασφαλούς σύνδεσης μεταξύ ενός ζεύγους κόμβων. Η χρήση τέτοιων πρωτοκόλλων σε περιορισμένες συσκευές IoT μπορεί να έχει σοβαρές συνέπειες όσον αφορά την αποδοτικότητα της ισχύος, διότι στις περισσότερες περιπτώσεις η μετάδοση και λήψη μηνυμάτων είναι πιο δαπανηρή από τις κρυπτογραφικές λειτουργίες. Αυτό ισχύει ιδιαίτερα για ασύρματες συσκευές. Το πρόβλημα ενισχύεται αναλογικά με τον αριθμό των κόμβων με τους οποίους πρέπει να αλληλεπιδρά η περιορισμένη συσκευή, διότι θα πρέπει να δημιουργηθεί μια ασφαλή σύνδεσης με κάθε κόμβο. Εάν μια συσκευή περιορισμένων πόρων ενεργεί ως καταναλωτής δεδομένων, θα σήμαινε τη δημιουργία ασφαλών συνόδων με κάθε κόμβο προσωρινής αποθήκευσης από τον οποίο η συσκευή ανακτά δεδομένα. Όταν ενεργεί ως παραγωγός δεδομένων, η συσκευή θα πρέπει να εγκαταστήσει ασφαλείς συνεδρίες με όλους τους καταναλωτές. Το μοντέλο προστασίας αντικειμένων εξαλείφει αυτό το πρόβλημα επειδή το περιεχόμενο είναι άμεσα διαθέσιμο σε ασφαλή κατάσταση στο δίκτυο. Οι συσκευές IoT που παράγουν δεδομένα μπορούν να το εξασφαλίσουν με όλους τους επιδιωκόμενους καταναλωτές και να αρχίσουν να το μεταδίδουν αμέσως.[15]

Εξουσιοδοτηση ελεγχου προσβασης μεσω Access Control Providers (ACPs)

Ο έλεγχος πρόσβασης αποτελεί αναπόσπαστο στοιχείο οποιασδήποτε αρχιτεκτονικής IoT. Θα πρέπει να είναι δυνατό για τους διαχειριστές να καθορίζουν τις πολιτικές ελέγχου πρόσβασης που διέπουν την πρόσβαση στις πληροφορίες. Όσον αφορά τον έλεγχο πρόσβασης το IoT εισάγονται πολλές νέες προκλήσεις. Αυτές οι προκλήσεις προκύπτουν από το γεγονός ότι μια οντότητα πληροφοριών μπορεί να αποθηκευτεί αφενός σε συσκευές που μπορούν εύκολα να αλλοιωθούν με ή να κλαπούν και αφετέρου, σε τοποθεσίες που δεν ελέγχονται από τον κάτοχο της πληροφορίας, π.χ., κρυφές μνήμες, πύλες. Εκείνοι που δημοσιεύουν την πληροφορία μπορεί να είναι συσκευές με χαμηλές δυνατότητες επεξεργασίας που δεν αλλοιώνονται ή συσκευές

που δεν ανήκουν στη διοικητική περιοχή του ιδιοκτήτη. Στις συνθήκες αυτές ο έλεγχος πρόσβασης είναι μια δύσκολη εργασία.

Οι πολιτικές ελέγχου πρόσβασης μπορούν να εφαρμοστούν είτε από έναν publisher είτε από ένα Rendevous Nodes (RN). Ωστόσο, στους publishers δεν μπορούμε να έχουμε εμπιστοσύνη ώστε να αποθηκεύουν τα στοιχεία πρόσβασης του χρήστη που είναι απαραίτητα για την εξακρίβωση της ταυτότητας του αλλά ούτε και την εξουσιοδότηση να επεξεργάζεται τα διαπιστευτήρια των συνδρομητών. Τα RN, από την άλλη πλευρά, είναι πιο ισχυρά και καλύτερα προστατευμένες συσκευές. Ως εκ τούτου, είναι καλύτεροι υποψήφιοι για επιβολή πολιτικών ελέγχου πρόσβασης. Ωστόσο, μια τέτοια προσέγγιση δεν είναι εύκολη δεδομένου ότι οι RNs είναι συσκευές γενικού σκοπού που συνήθως δεν ανήκουν στο domain του ιδιοκτήτη της πληροφορίας. Αυτό δημιουργεί δύο προκλήσεις.

- Πρώτον, ένα RN πρέπει να είναι αξιόπιστο για την αποθήκευση ενός συστήματος διαχείρισης χρηστών ή / και για τη διεκπεραίωση των διαπιστευτηρίων των συνδρομητών.
- Δεύτερον, ένα RN θα πρέπει να είναι σε θέση να "ερμηνεύει" τις πολιτικές ελέγχου πρόσβασης που ορίζονται από διαφορετικούς ιδιοκτήτες με διαφορετικές απαιτήσεις.

Για να ξεπεραστούν αυτά τα προβλήματα, χρησιμοποιούμε τον έλεγχο πρόσβασης εισάγοντας μια νέα οντότητα, την Access Control Provider (ACP). Τα ACPs είναι αξιόπιστες οντότητες δικτύου που μπορεί να ανήκουν σε κάτοχο ή μπορεί να παρέχονται ως υπηρεσία από ένα τρίτο μέρος όπως για παράδειγμα από host ACPs όπου η κάθε πολιτική ελέγχου πρόσβασης που φιλοξενείται σε ένα ACP προσδιορίζεται από ένα URI, το οποίο λαμβάνει ένας host αφού δημιουργήσει και αποθηκεύσει ένα στοιχείο ελέγχου πρόσβασης στο ACP. Στη συνέχεια, όταν μια συσκευή – συνδρομητής προσπαθήσει να αποκτήσει πρόσβαση στο προστατευόμενο αυτό στοιχείο, το RN παράγει έναν τυχαίο αριθμό (token) και το μεταδίδει με ασφάλεια στον συνδρομητή μαζί με το URI της πολιτικής ελέγχου πρόσβασης. Στη συνέχεια, ο συνδρομητής εντοπίζει το ACP, μεταδίδει το διακριτικό, και ζητά άδεια για τη συγκεκριμένη πολιτική. Αν ο συνδρομητής είναι εξουσιοδοτημένος, τότε ο ACP δημιουργεί και υπογράφει ψηφιακά μια έγκριση που περιλαμβάνει το διακριτικό και το URI της πολιτικής και το στέλνει στο RN. Τέλος, ο RN ειδοποιεί τον publisher σχετικά με την επιτυχημένη συνδρομή.[15]

NAME-BASED TRUST

Η εμπιστοσύνη στο PSI (και στο ICN γενικά) πρέπει να οικοδομηθεί γύρω από αναγνωριστικά στοιχεία και πληροφορίες, δηλ. ονόματα, παρά σε (ασφαλή) κανάλια επικοινωνίας και αποθήκευσης (και επεξεργασίας) κόμβων. Ως εκ τούτου, οι συνδρομητές πρέπει να είναι σε θέση να επαληθεύουν την ακεραιότητα και την αυθεντικότητα των πληροφοριών που λαμβάνουν, ανεξάρτητα από τον publisher και/ή το κανάλι επικοινωνίας. Η ακεραιότητα ενός στοιχείου πληροφοριών εγγυάται ότι το στοιχείο αυτό δεν έχει αλλοιωθεί κατά τη διάρκεια της μετάδοσης. Η αυθεντικότητα διαβεβαιώνει ότι ένα στοιχείο είναι αυτό που ο συνδρομητής πραγματικά ζήτησε, δηλαδή δεσμεύει το όνομα του στοιχείου με τα στοιχεία του στοιχείου. Αξίζει να σημειωθεί στο σημείο αυτό ότι οι έννοιες της ακεραιότητας και της αυθεντικότητας δεν είναι ίδιες ούτε η μια υποδεικνύει την ύπαρξη της άλλης.
Ένα στοιχείο μπορεί να μην έχει αλλοιωθεί (με αποτέλεσμα να μπορεί να επαληθευτεί η ακεραιότητά του) αλλά μπορεί να μην είναι αυθεντικό.

Η εμπιστοσύνη που βασίζεται στην πληροφορία έχει ιδιαίτερη σημασία για την αξιοπιστία της αρχιτεκτονικής, καθώς διευκολύνει την προσωρινή αποθήκευση και την αναπαραγωγή πληροφοριών. Εφόσον η εμπιστοσύνη δεν βασίζεται σε κεντρικούς υπολογιστές, οι πληροφορίες μπορούν να αποθηκευτούν προσωρινά ακόμη και σε αναξιόπιστους κόμβους. Σε αυτό το επίπεδο, η εμπιστοσύνη που βασίζεται στην πληροφορία μπορεί να επιτευχθεί χρησιμοποιώντας την ιεραρχική κρυπτογράφηση με βάση την ταυτότητα (HIBE).

Ένα σύστημα κρυπτογράφησης βάσει ταυτότητας (IBE) είναι ένα δημόσιο σχήμα κλειδιού. Το HIBE είναι μια γενίκευση του IBE που αντικατοπτρίζει την οργανωτική ιεραρχία. Ένα σχήμα IBE καθορίζεται από τέσσερις αλγορίθμους, επονομαζόμενοι Setup, Extract, Encrypt and Decrypt, οι οποίοι αναλύονται παρακάτω:

- Setup: λαμβάνει ως είσοδο μια παράμετρο ασφαλείας k και επιστρέφει ένα κύριο μυστικό κλειδί (MSK) και κάποιες συστημικές παραμέτρους (SP). Το MSK κρατείται μυστικό σε ένα αξιόπιστο διακομιστή ενώ το SP είναι διαθέσιμο στο κοινό.

- Extract: παίρνει ως είσοδο SP, MSK, και αυθαίρετη συμβολοσειρά ως ID και επιστρέφει ένα μυστικό κλειδί KID. Το ID μπορεί να χρησιμοποιηθεί ως δημόσιο κλειδί και το KID είναι το αντίστοιχο ιδιωτικό κλειδί αποκρυπτογράφησης.
- Extract: παίρνει ως είσοδο SP, MSK, και αυθαίρετη συμβολοσειρά ως ID και επιστρέφει ένα μυστικό κλειδί KID. Το ID μπορεί να χρησιμοποιηθεί ως δημόσιο κλειδί και το KID είναι το αντίστοιχο ιδιωτικό κλειδί αποκρυπτογράφησης
- Encrypt: λαμβάνει ως είσοδο ένα αυθαίρετο αναγνωριστικό συμβολοσειράς, ένα μήνυμα M, και SP, και επιστρέφει ένα CID κειμένου Ciphertext.
- Decrypt: λαμβάνει ως εισροή ένα CIDtext CID, το αντίστοιχο ιδιωτικό κλειδί αποκρυπτογράφησης KID και επιστρέφει το M.

Οι αλγόριθμοι εγκατάστασης (Setup) και εξαγωγής (Extract) μπορούν να εκτελεστούν μόνο από τον κεντρικό διακομιστή, ο αλγόριθμος κρυπτογράφησης μπορεί (Encrypt) να εκτελεστεί από οποιαδήποτε οντότητα που γνωρίζει SP, και ο αλγόριθμος αποκρυπτογράφησης (Decrypt) εκτελείται μόνο από την οντότητα που κατέχει την αντίστοιχη K.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η τεχνολογία του Internet of Things είναι μια νέα ιδέα και ένα όραμα το οποίο τα επόμενα χρόνια αναμένεται να γνωρίσει ιδιαίτερη άνθηση σε όλους τους τομείς της ανθρώπινης δραστηριότητας. Υπάρχουν πολλές προσεγγίσεις οι οποίες μπορούν να εξυπηρετήσουν το σκοπό της πανταχού συνδεσιμότητας με όσο το δυνατόν μικρότερα λειτουργικά και οικονομικά κόστη να επιβαρύνουν τον χρήστη. Στα προηγούμενα κεφάλαια αναλύθηκαν δυο πολύ βασικές προσεγγίσεις οι οποίες δεν αντικρούουν η μια την άλλη, αλλά αντίθετα, η μια έρχεται να επωφεληθεί στοιχεία της άλλης. Έχοντας μελετήσει τη βιβλιογραφία και τα πολυάριθμα άρθρα που έχουν δημοσιευτεί από αξιόλογους επιστήμονες, το συμπέρασμα που μπορεί να βγάλει κάποιος είναι πως το όραμα του Internet of Things, δεν είναι σενάριο επιστημονικής φαντασίας και η τεχνογνωσία και η μεθοδολογία για να γίνει πραγματικότητα, υπάρχει ήδη. Το hardware υπήρχε δεκαετίες διαθέσιμο, ενώ από πλευράς υλοποίησης, το πρωτόκολλο CoAP συνιστά τον τρόπο με τον οποίο γίνεται εφικτή η επικοινωνία μεταξύ δυο ή περισσότερων «έξυπνων» συσκευών. Η δικτύωση ICN έρχεται να υποβοηθήσει τον τρόπο λειτουργίας του CoAP, προσθέτοντας στοιχεία που αυξάνουν την αποδοτικότητα, τη λειτουργικότητα αλλά και το βαθμό ασφάλειάς του.

Παρόλα αυτά, δεν παύει να παραμένει μια νέα προσέγγιση στην οποία κανείς δεν μπορεί να δηλώσει πως έχει ουσιαστική πείρα και όπως σε κάθε νέα μορφή τεχνολογίας που εμφανίζεται, έτσι και με την περίπτωση του IoT οι κίνδυνοι που ελλοχεύουν, ακόμα παραμένουν σχετικά άγνωστοι. Σε κάθε συμβατικό πληροφοριακό σύστημα εμφανίζονται καθημερινά νέοι κίνδυνοι, οι οποίοι όμως αντιμετωπίζονται άμεσα, καθώς η βιβλιογραφία και η εμπειρία δείχνει τις καλύτερες πρακτικές που μπορούν να ακολουθηθούν. Στο διαδίκτυο των πραγμάτων, οι κίνδυνοι αλλάζουν μορφή καθώς τα συστήματα αυτά αλληλεπιδρούν με το φυσικό περιβάλλον, κάτι που ανατρέπει τα ως τώρα δεδομένα στις στρατηγικές ασφάλειας.

Συνοψίζοντας όλα τα παραπάνω, όσον αφορά τους απλούς αναγνώστες και χρήστες του IoT, είναι αναγκαίο να είναι πλήρως ενημερωμένοι σχετικά με τις δυνατότητες, τη συνδεσιμότητα αλλά και τους κινδύνους του. Ένας προσωπικός υπολογιστής θέτει

σε κίνδυνο έναν χρήστη μόνο διαδικτυακά, όμως πρέπει να γίνει κατανοητό πως τα προϊόντα που θα ανήκουν στο περιβάλλον του IoT, κρύβουν πολλούς και πιο πολυσύνθετους κινδύνους που μπορούν εύκολα να θέσουν σε κίνδυνο τη ζωή του ανθρώπου. Αντίστοιχα, οι επιστήμονες οι οποίοι ασχολούνται με το αντικείμενο αυτό, μελετώντας τη βιβλιογραφία, γίνεται αντιληπτό πως αναγνωρίζουν τους κινδύνους που υπάρχουν στο νέο αυτό περιβάλλον και οι προτάσεις που κάνουν, σε έναν βαθμό γίνονται και με γνώμονα αυτό, χτίζοντας σταδιακά ένα μέλλον με ριζικό επαναπροσδιορισμό της πληροφορίας και των αλληλεπιδράσεων όπως μέχρι σήμερα είναι γνωστή.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Mattern, Friedemann; Floerkemeier, Christian (2010), "From the Internet of Computers to the Internet of Things"

2. Paolo Magrassi (2001), "A World Of Smart Objects: The Role Of Auto Identification Technologies"

3. Karen Rose, Scott Eldridge, Lyman Chapin (2015), "Internet of Things –An overview"

4. Daiwat A. Vyas, Dvijesh Bhatt, Dhaval Jha (2012), "IoT: Trends, Challenges and Future Scope"

5. Lee Badman (2017), "Bluetooth 4.1 aims for Internet of Things", Ανακτήθηκε από: *"http://digitaledition.networkcomputing.com/wireless/bluetooth-41 aims-for-internet-of-things/240164838*"

6. Nathan Rockerhousen (2016), "The internet of things and Bluetooth". Ανακτήθηκε από: *"http://gridconnect.com/blog/general/the-internet-of things-and-bluetooth/"*

7. Z.Shelb y, K.Hartke, C.Bormann (June 2014) - "The Constrained Application Protocol (CoAP)", [IETF-RFC7252]

8. Tapio Leva, Oleksiy Mazhelis, Henna Suomi (2013) - "Comparing the cost efficiency of CoAP and HTTP in Web of Things applications"

9. Matthias Kovatsch, Julien Vermillard - "Hands on with CoAP". Ανακτήθηκε από*: "https://www.slideshare.net/jvermillard/hands-on-with-coap 36793005"*

10. K. Hartkle (September 2015), “Observing Resources in the Constrained Application Protocol (CoAP)” [IETF-RFC7641]

11. A. Rahman (October 2014), “Group Communication for the Constrained Application Protocol (CoAP)” [IETF-RFC7390]

12. ICN Research Group, D. Raychadhuri, E.Bacelli, O. Schelen, A. Lindren. B.Ahlgren, G. Wang, R.Ravidran (April 2016) “Requirements and Challenges for IoT over ICN”. Ανακτήθηκε από: *“https://datatracker.ietf.org/doc/draft-zhang-icnrg-icniot-requirements/”*

13. F. Ben Abdesslem (November 2015), “Proposed Design Choices for IoT over Information Centric Networking”. Ανακτήθηκε από: “*https://tools.ietf.org/html/draft-lindgren-icnrg-designchoices-00”*

14. N. Fotiou, H.Islam, D. Lagutin, T. Hakala, G.C. Polyzos (November 2016), “CoAP over ICN”. Ανακτήθηκε από: *“https://www.researchgate.net/publication/311894649_CoAP_over_ICN”*

15. George C. - Polyzos- Nikos Fotiou (July 2015) “Building a reliable Internet of Things using Information-Centric Networking”. Ανακτήθηκε από: *“https://link.springer.com/article/10.1007/s40860-015-0003-5#Sec2”*

16. Harald Sundmaeker Patrick Guillemin Peter Friess Sylvie Woelfflé (March 2010), “Vision and Challenges for Realising the Internet of Things”

17. Govinda K. , Saravanaguru R.A.K (2016) “Review on IOT Technologies”. Ανακτήθηκε από: *“https://www.ripublication.com/ijaer16/ijaerv11n4_115.pdf”*

18. Teemu Koponen, Barath Raghavan, Scott Shenker, Ankit Singla, James Wilcox “Information-Centric Networking: Seeing the Forest for the Trees”

19. Liang Wang, “Information-Centric Networking From Point-to-Point Communication To Content Distribution”. Ανακτήθηκε από: “https://www.cl.cam.ac.uk/~lw525/publications/icn-basics.pdf”

20. Mark Roberti (October 2013), “RFID, Sensors and the Internet of Things”

21. Darlen Storm, Researchers kill a pacemaker, kill a man(nequin). Ανακτήθηκε από: *“http://www.comp uterworld.com/article/2981527/cybercrime hacking/researchers-hack-a-pacemaker-kill-a-man-nequin.html”*

22. Arbor Networks, “Some perspective on IoT devices an DDoS Attacks” (October 2016). Ανακτήθηκε από: *“https://www.arbornetworks.com/blog/insight/perspective-iot-devices-ddos attacks/”*

23. Qi Jing, Athanasios Vasilakos, Jiafu Wan, Jingwei Lu, Dechao Qiu (November 2014) “Security of the Internet of Things: perspectives and challenges”

24. Cameron Faulkner (May 2017), "What is NFC? Everything you need to know" Ανακτήθηκε από: *“http://www.techradar.com/news/what-is-nfc/2”*

25. NFC site, “Near Field Communication vs Bluetooth” (May2017). Ανακτήθηκε από: *“http://nearfieldcommunication.org/bluetooth.html”*

26. Paula Hunter (August 2016) “IoT and NFC: 4 reasons why IoT needs NFC”. Ανακτήθηκε από: *“http://internetofthingsagenda.techtarget.com/blog/IoT Agenda/IoT-NFC-Four-reasons-why-IoT-needs-NFC”*