ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Μελέτη των ζητημάτων ασφαλείας για δίκτυα LPWAN

Του φοιτητή,

Ιωάννη – Όμηρου Κούλογλου

Αρ. Μητρώου: 09 / 3535

Επιβλέπων μέλος ΔΕΠ

Δρ. Περικλής Χατζημίσιος
Καθηγητής
Τμήμα Μηχανικών Πληροφορικής ΑΤΕΙΘ

Φεβρουάριος 2019

Θεσσαλονίκη

ΠΕΡΙΛΗΨΗ

Το Διαδίκτυο των πραγμάτων (Internet of Things) αποτελεί μία έννοια που έχει σαν στόχο τη διασύνδεση ενός μεγάλου αριθμού καθημερινών συσκευών για την ανάπτυξη και τη διευκόλυνση των καινοτόμων συστημάτων που αρχίζουν να εμφανίζονται στην αγορά. Με τη διασύνδεση των καθημερινών συσκευών, προκύπτουν κάποιες ανάγκες για τα καινοτόμα συστήματα IoT όπως είναι το ύψος του κόστους διαχείρισης του έργου, η κατάλληλη διαχείριση των δεδομένων που ανταλλάσσονται μεταξύ των συσκευών, η ενέργεια που καταναλώνεται για την επικοινωνία αλλά και για τις λειτουργίες καθώς και η μέγιστη απόσταση που θα επιτρέπει τη σωστή επικοινωνία των συσκευών με το σύστημα. Για να καλυφθούν τα παραπάνω, η ύπαρξη ενός δικτύου επικοινωνίας σε συνεργασία με την κατασκευή κατάλληλων συσκευών ήταν απαραίτητο για τις ανάγκες της αγοράς. Τα Low Power Wide Area Network σε συντομογραφία LPWAN, δημιουργήθηκαν για αυτό το λόγο και αποτελούν αναπόσπαστο κομμάτι των IoT. Με τη μεγάλη απήχηση που έχουν τα δίκτυα LPWAN στην αγορά και το γεγονός ότι είναι ασύρματα δίκτυα, τα τοποθετεί αυτομάτως στο στόχαστρο επιθέσεων από κακόβουλες οντότητες. Στην εργασία αυτή, αναφέρονται τα βασικά χαρακτηριστικά, οι μηχανισμοί ασφαλείας αλλά και οι επιθέσεις δικτύου που μπορούν να δεχθούν τα τρία βασικά πρότυπα των δικτύων LPWAN, που είναι τα πρωτόκολλα LoRaWAN, Sigfox και NorthBand-IoT.

ABSTRACT

The Internet of Things is a concept that aims to connect a large number of everyday devices to develop and facilitate innovative systems that are emerging on the market. With the interconnection of everyday devices, there are some needs for innovative IoT systems such as the amount of project management costs, proper management of the data exchanged between the devices, the energy used for communication and functions as well as the maximum distance that will allow the devices to communicate correctly with the system. To meet the above, the existence of a communication network in cooperation with the construction of suitable devices was necessary for the needs of the market. The Low Power Wide Area Network, abbreviated to LPWAN, was created for this purpose and is an integral part of IoT. With the high impact of LPWAN networks on the market and the fact that they are wireless networks, they automatically target them for attacks by malicious entities. In this paper, the key features, security mechanisms and network attacks that the three basic standards of LPWAN networks, such as LoRaWAN, Sigfox and NorthBand-IoT, can be addressed.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να εκφράσω τις ευχαριστίες μου στον καθηγητή του τμήματος Μηχανικών Πληροφορικής ΑΤΕΙΘ κ. Δρ. Περικλή Χατζημίσιο για το πολύτιμο χρόνο, τις σημαντικές υποδείξεις και συμβουλές που διέθεσε για τη περάτωση της παρούσας πτυχιακής εργασίας.

Ακόμα, θα ήθελα να ευχαριστήσω όλους τους καθηγητές του τμήματος Μηχανικών Πληροφορικής ΑΤΕΙΘ, για τις πολύτιμες γνώσεις που μου προσέφεραν όλα αυτά τα χρόνια .

Τέλος, θέλω να εκφράσω ένα τεράστιο ευχαριστώ στα αγαπημένα μου πρόσωπα, για την στήριξη και την εμπιστοσύνη που μου έδειξαν κατά τη διάρκεια των σπουδών μου.

ΠΕΡΙΕΧΟΜΕΝΑ

Ευρετήριο εικόνων

Ευρετήριο πινάκων

ΚΕΦΑΛΑΙΟ 1–Εισαγωγή

1.1 – Εισαγωγή στα δίκτυα LPWAN και στα ζητήματα ασφαλείας τους

Τα ήδη υπάρχοντα ασύρματα δίκτυα τηλεπικοινωνιών δεν είναι σχεδιασμένα για να καλύπτουν και να εξυπηρετούν χρήστες καινοτόμων συστημάτων IoT. Οι μεγάλες αποστάσεις, η μεταφορά μικρού όγκου δεδομένων, η κατάλληλη κατανάλωση ενέργειας και το συνολικό κόστος των παραπάνω αποτελούν ένα σημαντικό πρόβλημα στην αγορά. Για παράδειγμα, μία τεχνολογία έξυπνης πόλης (smart city) όπως είναι η περίπτωση χρήσης της έξυπνης τηλεμέτρησης νερού, οι συσκευές που έχει στη διάθεση της (ηλεκτροβάνα/ έξυπνα υδρόμετρα) έχουν μια πολύ απλή δουλειά, να στέλνουν ανά μικρά τακτά διαστήματα τις μετρήσεις τους σε έναν εξυπηρετητή του συστήματος, με το μικρότερο δυνατόν κόστος, και μέγιστο κύκλο ζωής. Δίκτυα τρίτης και τέταρτης γενιάς δεν μπορούν να θεωρηθούν κατάλληλα για τέτοια συστήματα.

Οργανισμοί και εταιρείες όπως για παράδειγμα 3GPP, LoRa Alliance προσπάθησαν επιτυχώς να δημιουργήσουν τις κατάλληλες τεχνολογίες για την επίλυση των παραπάνω προβλημάτων. Στην εργασία αυτή αναφέρονται οι τεχνολογίες των πρωτοκόλλων LoRaWAN, NB-IoT και Sigfox. Οι τεχνολογίες αυτές αποτελούν πρότυπα των δικτύων Low Power Wide Area Network που αποδεδειγμένα με το χαμηλό κόστος υλικού, τη μικρή κατανάλωση που επιφέρει πάνω από 10 χρόνια διάρκεια ζωής, και με τα αρκετά χιλιόμετρα κάλυψης επικοινωνίας με τους εξυπηρετητές του συστήματός τους, έχουν αρχίσει να πραγματοποιούν τα σενάρια των έξυπνων πόλεων.

Με τη μεγάλη απήχηση που έχουν τα δίκτυα LPWAN στην αγορά και το γεγονός ότι είναι ασύρματα δίκτυα, τα τοποθετεί αυτομάτως στο στόχαστρο επιθέσεων από κακόβουλες οντότητες. Για την αντιμετώπιση αυτού του προβλήματος οι τεχνολογίες των δικτύων LPWAN έχουν εμπλουτίσει τα συστήματα τους με διάφορους μηχανισμούς ασφαλείας για τη διασφάλιση της αυθεντικοποίησης των συσκευών δικτύου, την ακεραιότητα των μηνυμάτων που στέλνονται από τις τελικές συσκευές αλλά και την εμπιστευτικότητα των χρηστών του συστήματος

μεταξύ τους (όπως είναι οι τελικοί χρήστες και οι πάροχοι συστήματος), οι κύριοι μηχανισμοί ασφαλείας των πρωτοκόλλων LoRaWAN, NB-IoT και Sigfox αναφέρονται παρακάτω. Ένας πάροχος συστήματος IoT που έχει στη διάθεση του μία τεχνολογία δικτύου LPWAN, οφείλει πέρα από τους μηχανισμούς ασφαλείας που του παρέχει η εκάστοτε τεχνολογία, να υλοποιήσει και να εφαρμόσει τα δικά του μέτρα ασφαλείας για τη διασφάλιση του συστήματος του απέναντι στις κακόβουλες επιθέσεις που επίσης αναφέρονται στην εργασία.

Τέλος, για κάθε τεχνολογία δικτύων Low Power Wide Area Network που αναλύονται στην εργασία αυτή, αντιστοιχεί και μία περίπτωση χρήσης συστήματος έξυπνης πόλης αναφέροντας τις επιθέσεις ασφαλείας που μπορούν να δεχθούν τα συστήματα τους. Για την τεχνολογία του NB-IoT πρωτοκόλλου αναφέρεται η περίπτωση χρήσης του συστήματος έξυπνης τηλεμέτρησης κατανάλωσης νερού [58], από την εταιρεία επικοινωνίας Vodafone και τον πάροχο νερού Aguas de Valencia. Για την τεχνολογία του LoRaWAN, η περίπτωση χρήσης του συστήματος έξυπνου οδικού φωτισμού Streetlight InteliLIGHT® [60] με πάροχο την εταιρία Flashnet SRL, και τέλος με την τεχνολογία του Sigfox αναφέρεται η περίπτωση χρήσης του συστήματος SMOCKEO [63] με πάροχο τη εταιρεία Cobject SAS.

1.2 – Στόχος της πτυχιακής εργασίας

Ο στόχος της πτυχιακής εργασίας είναι η συγκέντρωση των επιθέσεων ασφαλείας που δέχονται τα έξυπνα συστήματα IoT, που για την κατάλληλη λειτουργία τους εμπλουτίζουν το σύστημα τους με την χρησιμοποίηση δικτύων LPWAN. Για να μπορέσει να επιτευχθεί ο στόχος αυτός, θα πρέπει αρχικά να αναφερθούν τα βασικά πρότυπα των LPWAN, όπως είναι οι τεχνολογίες πρωτοκόλλων LoRaWAN, Sigfox, NB-IoT, οι μηχανισμοί ασφαλείας που διαθέτουν για την διασφάλιση της λειτουργίας των συστημάτων, καθώς και οι επιθέσεις ασφαλείας που πραγματοποιούνται από κακόβουλες οντότητες.

1.3 – Δομή της πτυχιακής εργασίας

Στο κεφάλαιο δεύτερο αναφέρονται οι βασικοί μηχανισμοί των δικτύων LPWAN, στα επόμενα υποκεφάλαια αναφέρονται τα βασικά χαρακτηριστικά των τεχνολογιών LoRaWAN, Sigfox και NB-IoT όπως είναι η αρχιτεκτονική δικτύου που χρησιμοποιούν, η διαμόρφωση συχνότητας για την επικοινωνία των συσκευών τους, το είδος των συσκευών που διαθέτουν αλλά και μία εισαγωγή για τους μηχανισμούς ασφαλείας τους. Στο κεφάλαιο τρία, αναλύονται σε τεχνικό επίπεδο οι μηχανισμοί ασφαλείας των παραπάνω πρωτοκόλλων, όπως είναι τα κλειδιά που αποτελούν διαπιστευτήρια για την ταυτότητα της κάθε συσκευής, τους τρόπους ενεργοποίησης τους καθώς και οι μηχανισμοί κρυπτογράφησης που διαθέτουν για την ακεραιότητα των μηνυμάτων. Στο τέταρτο κεφάλαιο αναφέρονται οι βασικές επιθέσεις ασφαλείας που δέχονται τα δίκτυα LPWAN καθώς και οι πιθανοί τρόποι αντιμετώπισης τους και στα επόμενα υποκεφάλαια οι επιθέσεις ασφαλείας που δέχεται η κάθε τεχνολογία ξεχωριστά, ανάλογα την αρχιτεκτονική τους. Τέλος, στο κεφάλαιο πέντε γίνεται αναφορά της εφαρμογής των τεχνολογιών σε μια περίπτωση χρήσης έξυπνων συστημάτων αντίστοιχα, καθώς και η ανάλυση των επιθέσεων που δέχονται από κακόβουλες οντότητες στο σύστημά τους.

ΚΕΦΑΛΑΙΟ 2 – ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΠΡΩΤΟΚΟΛΛΩΝ LPWAN

2.1 – Εισαγωγή

Το κεφάλαιο αυτό περιγράφει τα βασικά χαρακτηριστικά που διέπουν τα δίκτυα Low Power Wide Area Network (LPWAN). Ακόμα, περιγράφονται τα βασικά πρότυπα LPWAN που έχουν κυριαρχήσει στην αγορά, τα πρωτόκολλα LongRange (LoRa), Sigfox και NorthBand-IoT (NB-IoT).

Αρχικά σε ένα πιο γενικό πλαίσιο, περιγράφεται η χρησιμότητα των δικτύων LPWAN, παραδείγματα περιπτώσεων χρήσης τους, η βασική αρχιτεκτονική που ακολουθούν όλα τα πρωτόκολλα αυτών των δικτύων καθώς γίνεται και μία βασική αναφορά στους μηχανισμούς ασφαλείας που υλοποιούνται.

Επιπλέον, για κάθε ένα από τα πρωτόκολλα που αναφέρθηκαν παραπάνω γίνεται μία ανάλυση της αρχιτεκτονικής δικτύου που χρησιμοποιούν καθώς και για το υλικό (τελικές συσκευές/συγκεντρωτές/εξυπηρετητές) που έχουν στη διάθεση τους. Ακόμα, αναφέρεται η διαμόρφωση συχνότητας και ο τύπος που χρησιμοποιούν ανάλογα τη τεχνολογία και τέλος, γίνεται μία αναφορά στους μηχανισμούς ασφαλείας που έχουν στη διάθεση τους.

2.2 – Βασικά Χαρακτηριστικά LPWAN

Τα πολυαναφερόμενα δίκτυα ευρείας περιοχής και χαμηλής ισχύος Low Power Wide Area Networks (LPWAN) αποτελούν την τελευταία εξέλιξη στην ασύρματη επικοινωνία επιτρέποντας σε τελικές συσκευές IoT (end-device) να συνδέονται με τους συγκεντρωτές-πύλες (Gateways) σε αποστάσεις χιλιομέτρων. Οι πύλες διαβιβάζουν τα δεδομένα που λαμβάνουν από τις τελικές συσκευές σε έναν εξυπηρετητή δικτύου (server) μέσω Ethernet ή 3G / 4G / 5G, ο οποίος διαχειρίζεται όλη την αποκρυπτογράφηση των δεδομένων. Τα LPWAN θεωρούνται υποσχόμενοι υποψήφιοι για εφαρμογές IoT.

Το Διαδίκτυο των Πραγμάτων (IoT) αποτελείται από έξυπνες τεχνολογίες και συστήματα τα οποία συνδέονται σε ένα παγκόσμιο δίκτυο και επικοινωνούν μεταξύ τους στέλνοντας δεδομένα και πληροφορίες. Τα συστήματα LPWAN δίνουν τη

δυνατότητα με τις λειτουργίες τους, σε παρόχους “έξυπνων” υποδομών να σχεδιάζουν συστήματα IoT για περιπτώσεις χρήσης που απαιτούν από τις συσκευές να στέλνουν περιοδικώς μικρά ποσά δεδομένων σε απομακρυσμένα δίκτυα που εκτείνονται σε μεγάλη απόσταση και χρησιμοποιούν συσκευές που τροφοδοτούνται από μπαταρίες οι οποίες διατηρούν την ισχύ τους για πολλά χρόνια. Με την εμφάνιση και την ανάπτυξη καινούργιων τεχνολογιών LPWAN, υπάρχει πλέον μεγαλύτερη ευελιξία στον ορισμό της "χαμηλής ισχύος" και της "ευρείας περιοχής" [1].

Τα LPWAN είναι οι κατάλληλες λύσεις για περιπτώσεις χρήσης που απαιτούν τη περιοδική μεταφορά δεδομένων σε μεγάλες αποστάσεις. Έξυπνες περιπτώσεις χρήσης όπως βλέπουμε στην εικόνα 1, εξαρτώνται από την ευελιξία των τεχνολογιών LPWAN είναι για παράδειγμα η τηλεμέτρηση κατανάλωσης νερού, οι έξυπνοι ανιχνευτές καπνού, οι έξυπνοι αισθητήρες φωτισμού που αναλύονται μαζί με την τεχνολογία που χρησιμοποιούν σε παρακάτω κεφάλαιο. Δεδομένης της εμβέλειας, του μικρού φορτίου δεδομένων των πακέτων και της διεισδυτικότητας των LPWAN, οι αισθητήρες που χρησιμοποιούν οι έξυπνες συσκευές μπορούν να στέλνουν τα πακέτα τους ακόμα και από δύσκολες τοποθεσίες όπως είναι ένα υπόγειο, σε δύσκολα κλίματα και μακριά από τους συγκεντρωτές (Gateways).

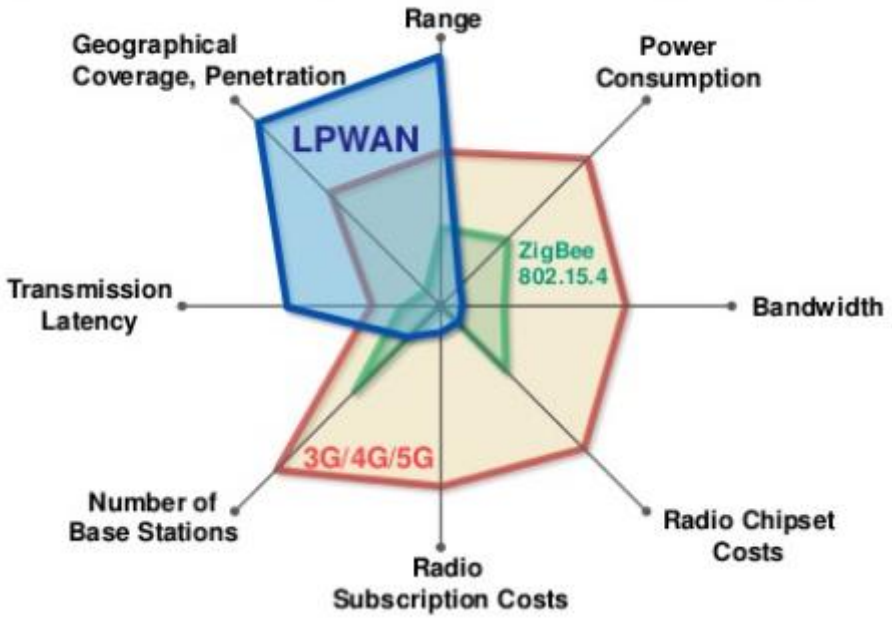
Εικόνα 1 Περιπτώσεις χρήσεων των LPWAN δικτύων σε διαφορετικούς τομείς[2]

2.1.1 – Ιδιότητες των τεχνολογιών

Η επιτυχία των τεχνολογιών LPWAN έγκειται στην ικανότητά τους να προσφέρουν τη κατάλληλη συνδεσιμότητα χαμηλής κατανάλωσης ενέργειας σε μεγάλο αριθμό συσκευών που διανέμονται ταυτόχρονα σε μεγάλες γεωγραφικές περιοχές με μικρό κόστος. Οι στόχοι των τεχνολογιών LPWAN για την επιτυχημένη λειτουργία τους είναι επίτευξη των παρακάτω λειτουργιών που φαίνονται και στην εικόνα 2 [3]:

- **Μεγάλη εμβέλεια**: Οι τεχνολογίες LPWAN είναι σχεδιασμένες για να διαθέτουν ευρεία κάλυψη μιας περιοχής και ταυτόχρονα την άριστη διάδοση σημάτων σε δύσκολα εσωτερικά σημεία όπως υπόγεια.
- **Λειτουργία εξαιρετικά χαμηλής ισχύος:** Η λειτουργία χαμηλής κατανάλωσης ενέργειας αποτελεί βασική προϋπόθεση για τις LPWAN τεχνολογίες, για να το πετύχουν αυτό χρησιμοποιούν ειδικά διαμορφωμένες συσκευές IoT, κερδίζοντας την αυτονομία τους με χρήση μπαταριών. Στις πρόσφατα ανεπτυγμένες τεχνολογίες LPWAN η διάρκεια ζωής της μπαταρίας αγγίζει τα 10 έτη.

- **Μικρό κόστος:** Η εμπορική επιτυχία των τεχνολογιών LPWAN συνδέεται με τη πετυχημένη επικοινωνία και σύνδεση μεγάλου αριθμού τελικών συσκευών, διατηρώντας ταυτόχρονα χαμηλό το κόστος του υλικού τους.
- **Επεκτασιμότητα:** Η κατάλληλη υποστήριξη του τεράστιου αριθμού συσκευών που αποστέλλουν συνεχώς πληροφορίες και δεδομένα, είναι μία από τις βασικές απαιτήσεις για τις τεχνολογίες LPWAN. Αυτές οι τεχνολογίες θα πρέπει να λειτουργούν καλά με τον αυξανόμενο αριθμό και την πυκνότητα των συνδεδεμένων συσκευών.
- **Ποιότητα εξυπηρέτησης (Quality of Service QoS):** Οι τεχνολογίες LPWAN έχουν ως στόχο τη δημιουργία διαφόρων συσκευών με μια πληθώρα σημαντικών απαιτήσεων. Μία περίπτωση απαίτησης είναι η δημιουργία των «έξυπνων» συσκευών για τη συνεχή μέτρηση π.χ. τηλεμέτρησης κατανάλωσης νερού, αλλά και η δημιουργία των «έξυπνων» συσκευών που θα πρέπει να μεταδίδουν τους συναγερμούς που παράγονται από εφαρμογές οικιακής ασφάλειας σε ελάχιστο χρόνο π.χ. Έξυπνοι ανιχνευτές καπνού. Επομένως, οι τεχνολογίες είναι σημαντικό να παρέχουν ποιότητα υπηρεσίας (QoS).

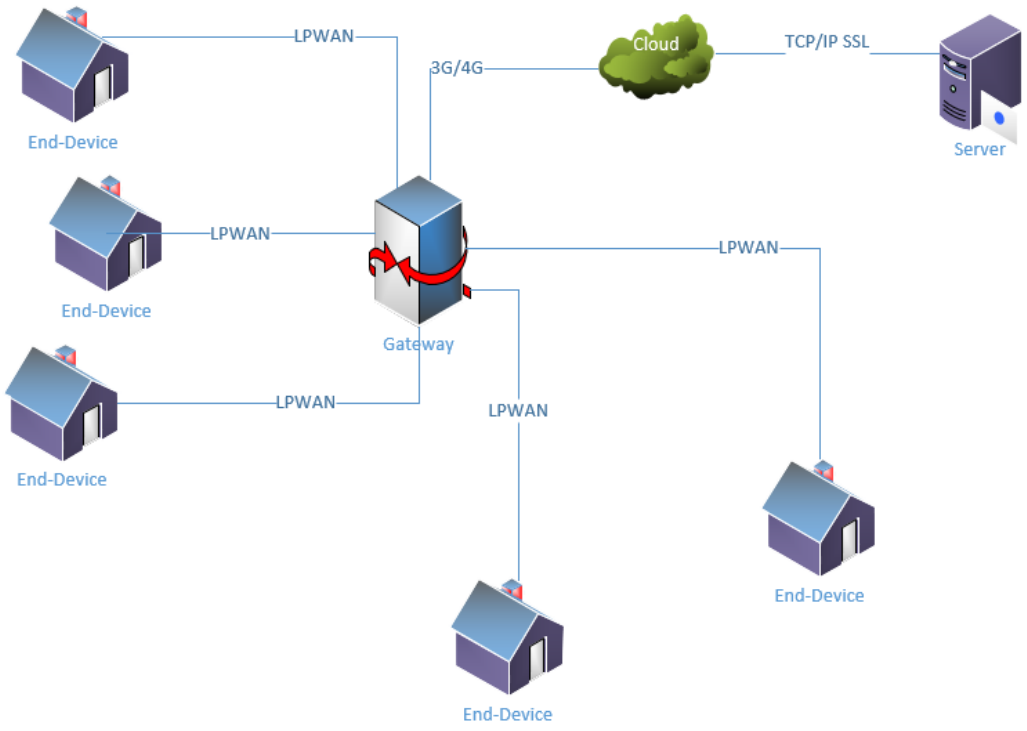


Εικόνα 2 Χαρακτηριστικά LPWAN σε σχέση με άλλα δίκτυα. [4]

2.1.2 – Τοπολογία LPWAN

Οι συσκευές LPWAN, οι οποίες χαρακτηρίζονται από την υψηλή ευαισθησία τους λόγο αισθητήρων και όχι από υψηλούς χρόνους μετάδοσης των πακέτων, χρησιμοποιούν για την επικοινωνία και την σύνδεση τους την τοπολογία αστέρα, όπου όλες οι τελικές συσκευές (End-device) έχουν άμεση σύνδεση με έναν συγκεντρωτή (Gateway).

Όπως βλέπουμε και στην εικόνα 3 ο συγκεντρωτής λειτουργεί ως μετατροπέας πρωτοκόλλου και κατευθύνει τα πακέτα που αποστέλλονται από τις τελικές συσκευές στο νέφος μέσω 3G / 4G / LTE, όπου ο εξυπηρετητής διαχειρίζεται όλη την αποκρυπτογράφηση των δεδομένων και χειρίζεται την εσωτερική διανομή και αποθήκευση τους.



Εικόνα 3 Τοπολογία LPWAN

2.2 – Πρωτόκολλο επικοινωνίας LoRaWAN

Το LoRa και LoRaWAN, αποτελούν αν όχι την πιο διαδεδομένη μία από τις πιο διαδεδομένες τεχνολογίες LPWAN, το LoRa αποτελεί το φυσικό επίπεδο του LoRaWAN. Όντας LPWAN το LoRaWAN είναι τεχνολογία χαμηλής κατανάλωσης ενέργειας με περίπου 10 χρόνια ζωής, χαμηλό ρυθμό μετάδοσης δεδομένων στα 27 kbps σε κανάλι των 500 kHz ή 50 kbps με χρήση διαμόρφωσης μετατόπισης συχνότητας (Frequency-shift Keying - FSK) και μεγάλο εύρος επικοινωνίας 2-5 χιλιόμετρα σε αστικές περιοχές και 15 χλμ. σε προαστιακές περιοχές. Η τεχνολογία LoRaWAN αναπτύχθηκε αρχικά από την Cycleo που μετέπειτα η εταιρεία αυτή πουλήθηκε στην Semtech η οποία πήρε τα ηνία του LoRaWAN. Όπως και όλα τα LPWAN το δίκτυο LoRaWAN είναι οργανωμένο σε τοπολογία αστέρα, όπου οι συγκεντρωτές (Gateways) στέλνουν και λαμβάνουν πακέτα από τις συσκευές και τα αντίστοιχα πακέτα τα στέλνουν στους εξυπερετητές δικτύου που με τη σειρά τους στέλνουν εντολές στους συγκεντρωτές και στις συσκευές, οπότε η παραπάνω επικοινωνία θεωρείται αμφίδρομη. Οι τελικές συσκευές στέλνουν δεδομένα στους συγκεντρωτές μέσω της τεχνολογίας LoRaWAN και οι συγκεντρωτές συνδέονται με το εξυπηρετητή δικτύου μέσω IP/TCP(3G/4G) [5].

2.2.1 – Αρχιτεκτονική Δικτύου

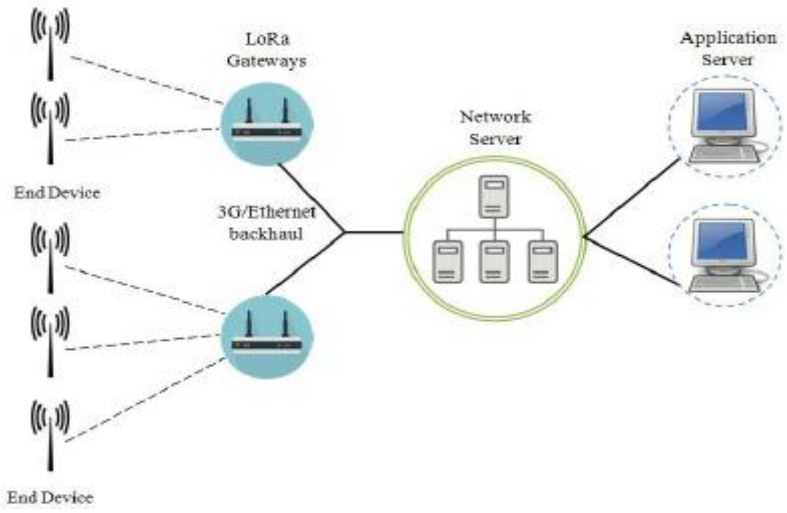
Όπως αναφέραμε παραπάνω ένα δίκτυο διαμορφωμένο στην τεχνολογία LoRaWAN παρέχει ένα μεγάλο εύρος περιοχής για την επικοινωνία του συστήματος, το οποίο είναι οργανωμένο με τοπολογία αστέρα. Τα στοιχεία που χρησιμοποιούνται στο δίκτυο του LoRa και LoRaWAN για την λειτουργία των συστημάτων σύμφωνα και με την εικόνα 4 είναι τα εξής [6]:

Τελικές Συσκευές LoRa (End Device)- Οι συσκευές που χρησιμοποιεί η τεχνολογία του LoRa αποτελούν ουσιαστικά μετατροπείς οι οποίοι έχουν είτε τη δυνατότητα να ανιχνεύουν τα σήματα που απευθύνονται σε αυτές είτε έναν καλοσχεδιασμένο μηχανισμό λειτουργίας για να λαμβάνουν τα αντίστοιχα σήματα ή και τα δύο, έχοντας πάντα σαν ιδιότητα την μεγάλη ευκολία να επικοινωνούν με απόσταση. Με την χρήση μιας λειτουργικής μονάδας (module) μπορούν να έχουν ταυτόχρονα τις παραπάνω δυνατότητες, μερικά παραδείγματα «έξυπνων» συστημάτων που χρησιμοποιούν τις συσκευές αυτές είναι η έξυπνη μέτρηση νερού, ανίχνευσης καπνού και έξυπνου οδικού φωτισμού.

LoRa Συγκεντρωτές (Gateways) - Η ιδιότητα των συγκεντρωτών LoRa περιλαμβάνει την διαχείριση των πακέτων LoRaWAN που προέρχονται από τις τελικές συσκευές και τα οποία προωθεί στους συγκεντρωτές του δικτύου. Η επικοινωνία όντας LPWAN είναι αμφίδρομη και η επικοινωνία με τους εξυπηρετητές πετυχαίνεται με τη χρήση IP/TCP δικτύων. Με βάση το παραπάνω, σαν συμπέρασμα έχουμε ότι η διασύνδεση back-haul μεταξύ των συγκεντρωτών και των εξυπηρετητών δικτύου πετυχαίνεται μέσω Ethernet ή 3G / 4G αναλόγως τις ανάγκες. Οι συγκεντρωτές όπως είδαμε και στην τεχνολογία του Sigfox καλούνται επίσης σταθμοί βάσης.

Εξυπηρετητής Δικτύου (Network Server) - Έχοντας σαν παράμετρο τη τοπολογία αστέρα ο εξυπηρετητής δικτύου αποκωδικοποιεί τα πακέτα που προέρχονται από τις τελικές συσκευές και παράγει ταυτοχρόνως τα πακέτα τα οποία προορίζονται για τις τελικές συσκευές. Ακόμα, διατηρεί χρονοδιάγραμμα αποστολής και λήψης πακέτων, προσαρμόζει το ρυθμό μετάδοσης τους ανάλογα με τη διευκόλυνση των πόρων του συστήματος, συνδέει και αποσυνδέει τελικές συσκευές του συστήματος, σε περιπτώσεις προβλημάτων ασφαλείας απορρίπτει αν χρειαστεί τα κακόβουλα πακέτα και έχει τον πλήρη έλεγχο των στοιχείων του συστήματος.

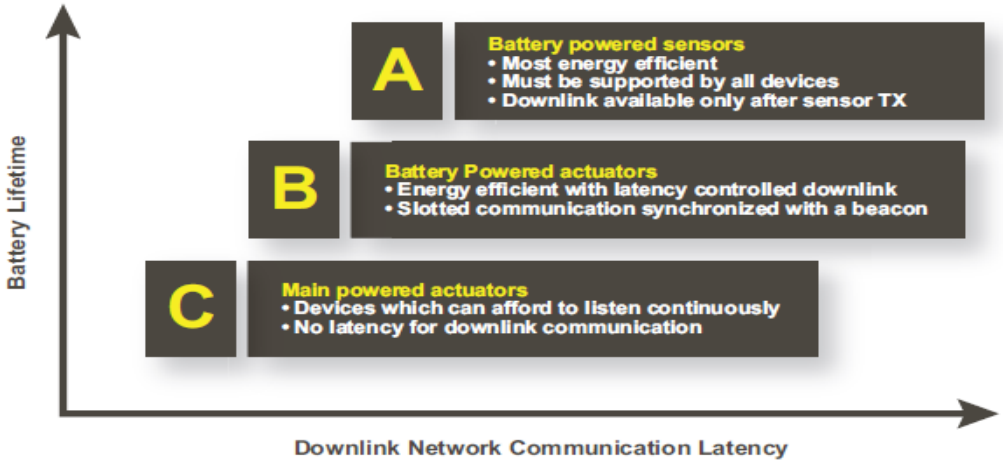
Εξυπηρετητής Εφαρμογής (Application Server) - Για το λεγόμενο front-end ή αλλιώς τις εφαρμογές οι οποίες μέσω διεπαφών εμφανίζουν τα μετρικά δεδομένα στους τελικούς χρήστες, είναι απαραίτητη η ύπαρξη του εξυπηρετητή εφαρμογής που συγκεντρώνει τα δεδομένα και είτε τα διαχειρίζεται και τα οπτικοποιεί είτε τα στέλνει όπως τα αποθήκευσε στους τελικούς χρήστες.



Εικόνα 4 Αρχιτεκτονική δικτύου LoRaWAN[6]

2.2.2 – Συσκευές LoRa

Όπως είδαμε και παραπάνω οι τελικές συσκευές εξυπηρετούν διαφορετικά συστήματα με διαφορετικές απαιτήσεις. Επομένως η τεχνολογία LoRaWAN για να βελτιστοποιήσει την εφαρμογή της στα συστήματα αυτά χρησιμοποιεί διαφορετικές κατηγορίες συσκευών όπως θα δούμε και θα αναλύσουμε βάση της εικόνας 5. Οι κατηγορίες κλάσεων των συσκευών διαχειρίζονται την ισορροπία μεταξύ της κατερχόμενης ζεύξης (downlink) και τον χρόνο ζωής της μπαταρίας[7].



Εικόνα 5 Διαφοροποίηση κλάσεων των συσκευών LoRa[7].

Αμφίδρομη τελική συσκευή Α κλάσης (**Class A**)- Οι τελικές συσκευές της κλάσης Α διαθέτουν αμφίδρομη επικοινωνία όπου σύμφωνα με αυτό, κάθε μετάδοση ανερχόμενης ζεύξης των τελικών συσκευών ακολουθείται από δύο σύντομα σήματα κατερχόμενης ζεύξης. Ο χρόνος μετάδοσης των πακέτων που είναι προγραμματισμένος για τις τελικές συσκευές, βασίζεται στις ανάγκες επικοινωνίας του συστήματος με μια μικρή παραλλαγή που βασίζεται σε τυχαία χρονική βάση με τη χρησιμοποίηση πρωτοκόλλου τύπου ALOHA. Η λειτουργία κλάσης Α των τελικών συσκευών για το σύστημα, αποτελεί τη λειτουργία με τη χαμηλότερη ισχύ για εφαρμογές που απαιτούν μόνο επικοινωνία κατερχόμενης ζεύξης από τον εξυπηρετητή αμέσως σχεδόν μετά την αποστολή της μετάδοσης μιας ανερχόμενης ζεύξης. Οι επικοινωνίες κατερχόμενης ζεύξης από το διακομιστή σε οποιαδήποτε άλλη στιγμή θα πρέπει να περιμένουν μέχρι την επόμενη προγραμματισμένη ανερχόμενης ζεύξη.

Αμφίδρομη τελική συσκευή με προγραμματισμένες λήψεις Β κλάσης (**Class B**) - Μία σημαντική διαφορά της κλάσης Β από την Α, είναι η προγραμματισμένη ώρα λήψης. Για να το πετύχει αυτό, οι συσκευές λαμβάνουν ένα συγχρονισμένο σήμα μέσω του φάσματος από τους συγκεντρωτές. Αυτό επιτρέπει στον εξυπηρετητή να γνωρίζει πότε ακούει η τελική συσκευή.

Αμφίδρομη τελική συσκευή με συνεχή λήψη Γ κλάσης (**Class C**) - Οι τελικές συσκευές της κλάσης C έχουν διαρκώς ανοικτά τα παράθυρα λήψης και μένουν κλειστά μόνο κατά τη διαδικασία μετάδοσης.

2.2.3 – Διαμόρφωση Συχνότητας

Το δίκτυο του LoRaWAN λειτουργεί σε ελεύθερο φάσμα και τα οι συχνότητες LoRaWAN χρησιμοποιούν ζώνες ISM όπως είναι οι 433MHz και 868MHz που είναι διαδεδομένες στην Ευρώπη, η 915MHz σε Ηνωμένες Πολιτείες και 430MHz στην Ασία, οι συχνότητες αυτές θέτουν περιορισμούς οι οποίοι συχνά είναι συγκεκριμένοι για κάθε χώρα. Η λειτουργία των πρωτοκόλλων LoRa διατίθεται σε δύο ξεχωριστά επίπεδα. Αυτό του Φυσικού επιπέδου που χρησιμοποιεί μια τεχνική εξάπλωσης του φάσματος (Chirp Spread Spectrum CSS) στην οποία τα δεδομένα κωδικοποιούνται χρησιμοποιώντας την τεχνική αύξησης / μείωσης συχνότητας που έχει σχεδιαστεί για να επιτυγχάνει υψηλή ευαισθησία. Και του MAC επιπέδου το οποίο ως ανοιχτό πρότυπο, διαθέτει έλεγχο του μέσου πρόσβασης για να

επιτρέπει σε αρκετές τελικές συσκευές να επικοινωνούν με το συγκεντρωτή χρησιμοποιώντας το δίκτυο LoRaWAN.

2.2.4 – Ασφάλεια

Ένα βασικό χαρακτηριστικό των LPWAN είναι η συνεχής αναζήτηση μηχανισμών ασφαλείας. Η τεχνολογία του LoRaWAN χρησιμοποιεί δύο επίπεδα ασφάλειας: ένα για το δίκτυο και ένα για την εφαρμογή. Η ασφάλεια δικτύου διασφαλίζει την αυθεντικότητα της επικοινωνίας των τελικών συσκευών στο δίκτυο ενώ το επίπεδο εφαρμογής διασφαλίζει ότι ο χειριστής του δικτύου δεν μπορεί να αποκτήσει πρόσβαση στα προσωπικά δεδομένα της εφαρμογής του τελικού χρήστη. Η μέθοδος κρυπτογράφησης AES χρησιμοποιείται για την ασφαλή ανταλλαγή των βασικών στοιχείων όπως είναι τα κλειδιά του δικτύου.

Η τεχνολογία LoRaWAN λόγο της συνεχώς αναβάθμισης στην αρχιτεκτονική δικτύου, στις κλάσεις συσκευών και γενικά στη βελτιστοποίηση των στοιχείων που συντελείται το σύστημα της, αυξάνει σταδιακά τους μηχανισμούς ασφαλείας της και αποτελεί μία βασική τεχνολογία για κάθε “έξυπνη” υποδομή συστημάτων.

Περισσότερα για τα χαρακτηριστικά ασφαλείας της τεχνολογίας LoRaWAN αναλύουμε παρακάτω στο κεφάλαιο, αλλά και τις επιθέσεις που μπορεί να δεχθεί το δίκτυο.

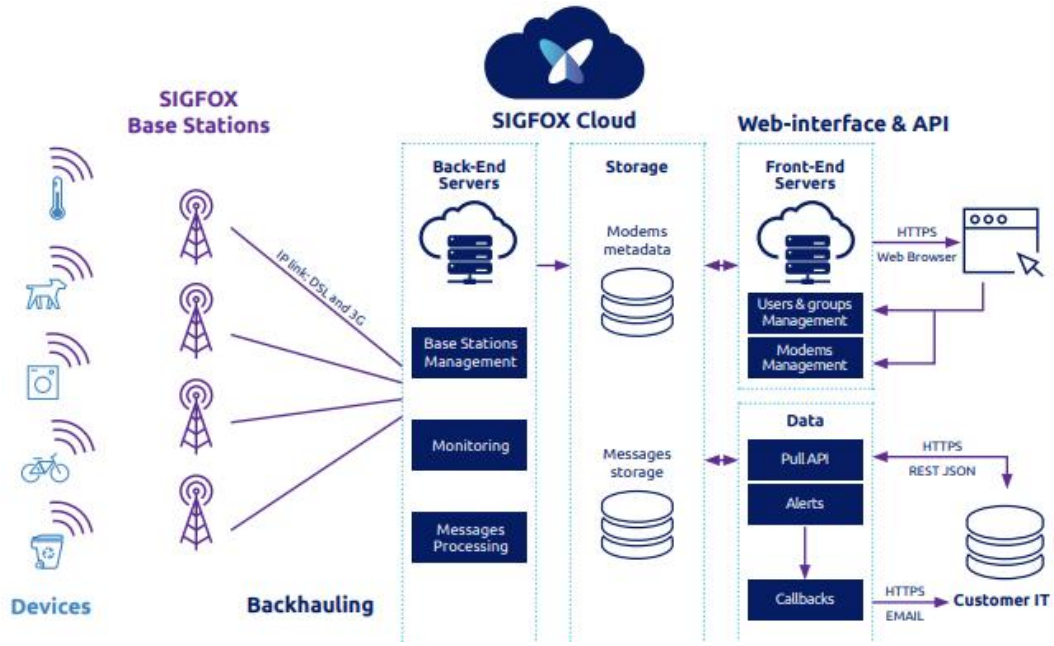
2.3 – Πρωτόκολλο επικοινωνίας Sigfox

Το Sigfox αποτελεί μία από τις βασικές τεχνολογίες LPWAN η οποία εγγυάται συσκευές χαμηλής κατανάλωσης ενέργειας, χαμηλού κόστους και μικρού μεγέθους αποστολή δεδομένων ανά πακέτο. Λειτουργεί σε παγκόσμιο δίκτυο και χρησιμοποιείται για συστήματα IoT. Η τεχνολογία του Sigfox είναι αποδεδειγμένα μια πολύ καλή λύση αν επιλέξει κάποιος μια οικονομική λύση στη σύνδεση και στη διάρκεια ζωής των συσκευών. Το Sigfox επεκτείνει και συμμετέχει σε νέα συστήματα IoT και παρέχει μια εφεδρική συνδεσιμότητα για τις συσκευές με υψηλό εύρος ζώνης (bandwidth). Οι συσκευές σε ένα δίκτυο όπως του Sigfox επικοινωνούν με το δίκτυο όταν ανιχνευτεί ένα συμβάν (όπως καπνός) ή μετρηθεί κάτι (στιγμιαία μέτρηση κατανάλωσης νερού), τότε θα ενεργοποιηθεί η μονάδα επικοινωνίας των συσκευών και θα στείλει το μήνυμα. Μετέπειτα, το μήνυμα που στέλνει η μονάδα θα ληφθεί από το δίκτυο και τα δεδομένα που

συμπεριλαμβάνονται μέσα σε αυτό θα αποθηκευτούν στον εξυπηρετητή του Sigfox. Το Sigfox είναι σχεδιασμένο για να μεγιστοποιεί την ενεργειακή απόδοση του δικτύου του, με αποτέλεσμα να επιλέγεται η χρήση του για τον λόγο αυτό. Το πετυχαίνει αυτό, διότι καταναλώνει πολύ χαμηλή ισχύ όταν μεταδίδει δεδομένα. Ανάλογα με την τοπολογία και το γεωγραφικό περιβάλλον που βρίσκονται οι συσκευές του δικτύου, το Sigfox έχει τη δυνατότητα να παρέχει σύνδεση μεγάλης εμβέλειας μέχρι και δεκάδες χιλιόμετρα. Πιο συγκεκριμένα χρησιμοποιεί μη αδειοδοτημένες ζώνες ISM και οι συχνότητες που χρησιμοποιεί είναι 868 MHz στην Ευρώπη και 915 MHz στις Η.Π.Α. Το μέγεθος του πακέτου που στέλνει στην ανερχόμενη ζεύξη είναι 12-bytes ενώ στη κατερχόμενη ζεύξη είναι 8 bytes και ο ρυθμός δεδομένων είναι 100 bps[8].

2.3.1 – Αρχιτεκτονική δικτύου

Σύμφωνα με την εικόνα 6, χωρίζουμε την αρχιτεκτονική δικτύου του Sigfox στις παρακάτω παραγράφους [9].



Εικόνα 6 Αρχιτεκτονική δικτύου Sigfox [8].

Τα πακέτα αποστέλλονται από τις τελικές συσκευές και μέσω του αέρα φθάνουν στους συγκεντρωτές του Sigfox και στη συνέχεια περνούν στο οπισθοζευκτικό κύκλωμα (backhaul). Το κύκλωμα αυτό, σαν κύριο πρωτόκολλο επικοινωνίας χρησιμοποιεί το DSL για συνδεσιμότητα και 3G ή 4G ως εναλλακτικά. Στην περίπτωση που δεν υπάρχει η δυνατότητα χρησιμοποίησης των δύο παραπάνω πρωτοκόλλων, η δορυφορική συνδεσιμότητα μπορεί να χρησιμοποιηθεί ως εναλλακτική τεχνολογία.

Το σύστημα υποστήριξης (back-end) χειρίζεται την επεξεργασία πακέτων που έρχονται από τους συγκεντρωτές. Στο κεντρικό δίκτυο αποστέλλονται και αρκετά πακέτα που περιέχουν το ίδιο μήνυμα αλλά θα πρέπει μόνο ένα να αποθηκευτεί. Το κεντρικό δίκτυο παράλληλα παρακολουθεί την κατάσταση του δικτύου και διαχειρίζεται τους συγκεντρωτές όπως προς την λειτουργία τους.

Η υποδομή δικτύου του Sigfox αποθηκεύει επίσης τα πακέτα σε δύο διαθέσιμα μέρη του συστήματος. Στην αποθήκευση των μεταδεδομένων υπάρχει η δυνατότητα να επαναχρησιμοποιηθούν για την κατασκευή υπηρεσιών και στην αποθήκευση των μηνυμάτων των πελατών ώστε οι πελάτες να έχουν τη δυνατότητα να τα ανακτήσουν αργότερα για να τα εκμεταλλευτούν.

Τέλος, μέσω ειδικών ιστοσελίδων και διεπαφών (API) το Sigfox επιτρέπει στους πελάτες να έχουν πρόσβαση στα μηνύματά τους. Μπορούν είτε να αποκτήσουν πρόσβαση στην πλατφόρμα μέσω του προγράμματος περιήγησης ιστού τους είτε να χρησιμοποιούν ένα REST API και χρησιμοποιώντας κατάλληλα ερωτήματα (Queries) να συγχρονίσουν το σύστημα τους και να δέχονται τα μηνύματα στη συσκευή τους.

2.3.2 – Διαμόρφωση Συχνότητας

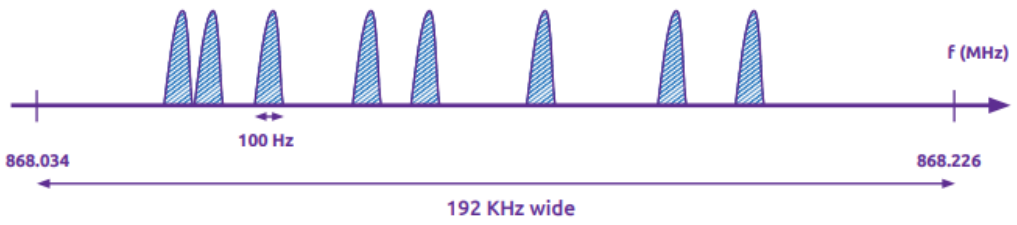
Το Sigfox αποτελεί μία τεχνολογία εξαιρετικά στενής ζώνης (ultra-narrowband) που σημαίνει ότι λειτουργεί σε ένα αρκετά μικρό εύρος ζώνης. Χρησιμοποιεί μια τυποποιημένη μέθοδο μετάδοσης ραδιοσυχνοτήτων που ονομάζεται δυαδική διαμόρφωση μετατόπισης φάσης (Binary Phase-Shift Keying - BPSK) και χρησιμοποιεί πολύ μικρά κομμάτια φάσματος και μετατρέπει τη λειτουργία ενός φορέα ραδιοκύματος πραγματοποιώντας τη κωδικοποίηση των δεδομένων. Αυτό

δίνει τη δυνατότητα στον δέκτη να ακούει μόνο σε ένα μικρό μήκος φάσματος, μετριάζοντας την επιρροή του θορύβου. Η παραπάνω μέθοδος αποτελεί ραδιοεξοπλισμό ακραίου σημείου (end point radio) και μια πιο εξελιγμένη βάση για τη διαχείριση του δικτύου[10].

Το Sigfox εκπέμπει σε 192KHz του ελεύθερου φάσματος για την ανταλλαγή μηνυμάτων μέσω του αέρα. Όπως αναφέραμε παραπάνω αποτελεί μία τεχνολογία εξαιρετικά στενής ζώνης όπως την βλέπουμε και στην εικόνα 7. Τα μηνύματα που στέλνει έχουν πλάτος 100 Hz και ο ρυθμός μετάδοσής τους είναι 100 ή 600 bit ανά δευτερόλεπτο, ανάλογα με την περιοχή[9].

Το Sigfox επικοινωνεί με τους συγκεντρωτές σε μεγάλες αποστάσεις χωρίς να τους επηρεάζει ο θόρυβος, μέσω ζώνες φάσματος. Οι ζώνες που χρησιμοποιεί εξαρτώνται από την τοποθεσία:

- Για την Ευρώπη, η ζώνη που χρησιμοποιείται είναι μεταξύ 868 και 868.2 MHz,
- για τον υπόλοιπο κόσμο, είναι μεταξύ 902 και 928 MHz με διάφορους περιορισμούς σύμφωνα με τους τοπικούς κανονισμούς.



Εικόνα 7 Η λειτουργία του Sigfoxμε ultra-narrowband[9].

2.3.3 – Ασφάλεια

Το Sigfox για να αντιμετωπίσει τις προκλήσεις ασφαλείας που χρησιμοποιεί διαθέτει συστηματικές διαδικασίες. Αποτελεί μία από τις πιο ασφαλείς τεχνολογίες LPWAN λόγο του μοναδικού του σχεδιασμού. Οι συσκευές Sigfox λειτουργούν κυρίως εκτός σύνδεσης με τις εντολές για την λειτουργία τους να υπάρχουν ήδη μέσα στη συσκευή. Όταν χρειάζεται να μεταδίδουν ή να λαμβάνουν δεδομένα από το δίκτυο του Sigfox, εκπέμπουν ένα ραδιοφωνικό μήνυμα με τη κατάλληλη οδηγία. Αυτό το μήνυμα το λαμβάνουν οι συγκεντρωτές οι οποίοι με τη σειρά τους το εκπέμπουν στον εξυπηρετητή του Sigfox, όπου οι χρήστες μπορούν μέσω διαφόρων διεπαφών ή queries να λάβουν τα δεδομένα του. Αυτή η αρχιτεκτονική δικτύου του Sigfox παρέχει μια σημαντική τεχνική αντιμετώπισης των προκλήσεων ασφαλείας που μπορεί να διατρέχει ένα ασύρματο δίκτυο LPWAN.

Ακόμα, στην τεχνολογία του Sigfox κάθε συσκευή αντιπροσωπεύεται από ένα μοναδικό συμμετρικό κλειδί ελέγχου ταυτότητας για την διάρκεια ζωής της ή αν χρειαστεί αντικατάσταση κατά τον έλεγχο της. Η τεχνική του μοναδικού κλειδιού για κάθε συσκευή είναι μια σημαντική ιδιότητα του Sigfox, διότι αν μια συσκευή πέσει στα χέρια μίας κακόβουλης οντότητας δεν θα κινδυνέψουν τα κλειδιά των υπόλοιπων. Ένα κρυπτογραφικό διακριτικό υπολογίζεται χρησιμοποιώντας αυτό το κλειδί ελέγχου ταυτότητας για κάθε μήνυμα αποστολής ή λήψης. Αυτό το διακριτικό χρησιμοποιείται για τον έλεγχο ταυτότητας του αποστολέα και την ακεραιότητα του μηνύματος. Για την αντιμετώπιση τον επαναλαμβανομένων μηνυμάτων (Replay Attacks) το Sigfox χρησιμοποιεί έναν μετρητή που περιέχεται σε κάθε μήνυμα ώστε να γνωρίζει το σύστημα τον αριθμό που θα έπρεπε να είναι το κάθε μήνυμα. Μία ακόμα ευελιξία που προσφέρει η ασφάλεια του Sigfox, είναι η δυνατότητα είτε να επιτρέπεται στους χρήστες να χρησιμοποιούν τις δικές τους μεθόδους κρυπτογράφησης εάν είναι απαραίτητο, είτε να χρησιμοποιούν τις μεθόδους κρυπτογράφησης της τεχνολογίας του Sigfox[11].

Ποιο αναλυτικά τα χαρακτηριστικά ασφαλείας του Sigfox θα αναλυθούν σε παρακάτω κεφάλαιο, μαζί με τις επιθέσεις ασφαλείας που μπορεί να δεχθεί αλλά και τους πιθανούς τρόπους αντιμετώπισης τους.

2.4 – Πρωτόκολλο επικοινωνίας NB - IoT

Μέσω της συνεργασίας που έχει επιτευχθεί από τους οργανισμούς προτυποποίησης του 3GPP (3rd Generation Partnership Project) [12], έχει διασφαλιστεί η συνδεσιμότητα των τεχνολογιών και των χρηστών που τις χρησιμοποιούν. Το παραπάνω το πέτυχαν με την συνεχή αναβάθμιση των τεχνολογιών ασύρματης πρόσβασης στις κινητές ευρυζωνικές συνδέσεις. Μέσω της συνεχής αναβάθμισης των τεχνολογιών, ήρθε να προστεθεί και ένα πρότυπο ραδιοφωνικής τεχνολογίας για εφαρμογές επικοινωνιών τύπου μηχανής (Machine Type Communication-MTC) το NorthBand–IoT (NB-IoT). Στόχος του προτύπου είναι να προσφέρει την καλύτερη σε ποιότητα συνδεσιμότητα σε οικονομικά πλαίσια, συνδέοντας πληθώρα συσκευών IoT και υποστηρίζοντας παράλληλα χαμηλή κατανάλωση ισχύος.

Το 3GPP ξεκίνησε τη διαδικασία της έρευνα και προτυποποίησης της τεχνολογίας του NB-IoT το 2014. Η κατευθυντήρια αρχή της έρευνας του NB-IoT ήταν για τον προσδιορισμό των απαιτήσεων στις επικοινωνίες των συσκευών, η επιλογή μεθοδολογίας και αξιολόγησης της αλλά και ταυτόχρονα η εξασφάλιση ότι προηγούμενα προτεινόμενα πρότυπα παρομοίων τεχνολογιών και φιλοσοφίας δεν θα μπορούσαν να ικανοποιήσουν τις καθορισμένες απαιτήσεις.

2.4.1 – Αρχιτεκτονική δικτύου

Χαρακτηριστικό των προτύπων 3GPPείναι η αρχιτεκτονική που ακολουθούν. Παρακάτω βλέπουμε τη δομή της τεχνολογίας NB-IoT που ακολουθεί τα πρότυπα δικτύων LTE-M[13].

2.4.1.1 – Συγκεντρωτής - Κεραία

Ο συγκεντρωτής αποτελεί μία κεραία, συνήθως κάποιας τηλεφωνικής υπηρεσίας και για κάθε περίπτωση χρήσης του NB-IoT είναι απαραίτητη η συνεργασία του παρόχου με τις υπηρεσίες τους. Οι κεραίες των τηλεφωνικών υπηρεσιών λειτουργούν σε ένα προκαθορισμένο φάσμα, οπότε η τεχνολογία του NB-IoT λειτουργεί στο φάσμα αυτό. Υπάρχουν περιπτώσεις κεραιών που λειτουργούν και σαν συγκεντρωτές σε τεχνολογίες NB-IoT ταυτόχρονα με την κανονική τους χρήση. Οι περιπτώσεις αυτές για λόγους οικονομικούς κυρίως είναι πολύ συχνές, καθώς έχουν τη δυνατότητα λειτουργίας σε διάφορες συχνότητες

συμπεριλαμβανομένων και του NB-IoT. Η συνηθέστερη περίπτωση είναι μία τεχνολογία NB-IoT να εμπίπτει σε μια συχνότητα GSM ή LTE που σημαίνει ότι δύνεται η δυνατότητα χρησιμοποίησης μιας κανονικής κεραίας.

Για να μπορέσει ένας πάροχος να χρησιμοποιήσει κάποια συγκεκριμένη συχνότητα που επιθυμεί σύμφωνα με το σύστημα του, χρειάζεται να ακολουθεί ένα συνδυασμό παραγόντων. Όπως για παράδειγμα τους περιορισμούς και την δομή των συχνοτήτων που διαθέτει η περιοχή που θα εφαρμοστεί η τεχνολογία NB-IoT, η τεχνολογία που χρησιμοποιεί η εκάστοτε υπηρεσία αλλά και η δυνατότητα του παρόχου δικτύου καθώς το NB-IoT δεν λειτουργεί σε ελεύθερο φάσμα όπως η τεχνολογία του LoRa.

2.4.1.2 – Τελική συσκευή

Οι τελικές συσκευές αποτελούν τους τρόπους μέτρησης, ειδοποίησης, κίνησης και πολλών ειδών περιπτώσεων χρήσης των αισθητήρων που διαθέτουν. Η σημαντικότερη λειτουργία τους όμως είναι ότι διαθέτουν ένα μικροελεγκτή ή μικροεπεξεργαστή που μπορεί να επικοινωνεί με το δίκτυο και να διαχειρίζεται τις ραδιοσυχνότητες ανάλογα με την εντολή που δέχονται.

2.4.1.3 – Δίκτυα επικοινωνίας

Η επικοινωνία μεταξύ των συγκεντρωτών και των εξυπηρετητών στην τεχνολογία του NB-IoT μπορεί να επιτευχτεί με δύο τρόπους. Αρχικά, η εύκολη είναι η απλή χρησιμοποίηση του πρωτόκολλο TCP / IP. Αλλιώς δίνει τη δυνατότητα σχεδίασης ενός ξεχωριστού πρωτοκόλλου από τον πάροχο. Για την επιλογή δύο, είναι απαραίτητη η δρομολόγηση του ιδιωτικού δικτύου εντός κυτταρικού δικτύου, καθώς και τη διάθεση εξυπηρετητή διαχείρισης συσκευών που υποστηρίζει αυτό το εναλλακτικό πρωτόκολλο.

2.4.2 – Διαμόρφωση Συχνότητας

Σε αντίθεση με τα πρωτόκολλα Sigfox και LoRaWAN που λειτουργούν σε ελεύθερο φάσμα, για τη μέγιστη αποδοτικότητα της συχνότητας η τεχνολογία του NB-IoT έχει σχεδιαστεί με πολλές λειτουργίες προτύπων διαμόρφωσης συχνοτήτων του 3GPP όπως είναι τα GSM (Global System for Mobile communications) και LTE(Long-Term Evolution). Όπως βλέπουμε και στην εικόνα 8 οι λειτουργίες αυτές είναι του standalone (αυτόνομου) όπου συμβαίνει η

εναλλαγή ενός από τους φορείς GSM σε φορέα NB-IoT. Η επιλογή του in-band (εντός του φάσματος) όπου λειτουργεί μέσα στο φάσμα ενός φορέα LTE, και τέλος υπάρχει η guardband (ενδιάμεσο φάσμα) όπου λειτουργεί ενδιάμεσα από φορείς LTE.

2.4.2.1 – Αυτόνομη λειτουργία

Η λειτουργία του αυτόνομου προτύπου είναι μια καλή επιλογή για τεχνολογίες που λειτουργούν με LTE. Μέσω της χρησιμοποίησης του GSM, ένα δίκτυο LTE έχει στη διάθεση του ένα ή περισσότερους φορείς GSM. Καθώς το GSM λειτουργεί κυρίως στις συχνότητες 900MHz και 1.800MHz που αποτελούν τις βασικότερες συχνότητες στην αγορά, που συνεπάγεται η αύξηση του χρόνου μετάδοσης και μεγιστοποιεί τα οφέλη των συστημάτων που τις χρησιμοποιούν[14].

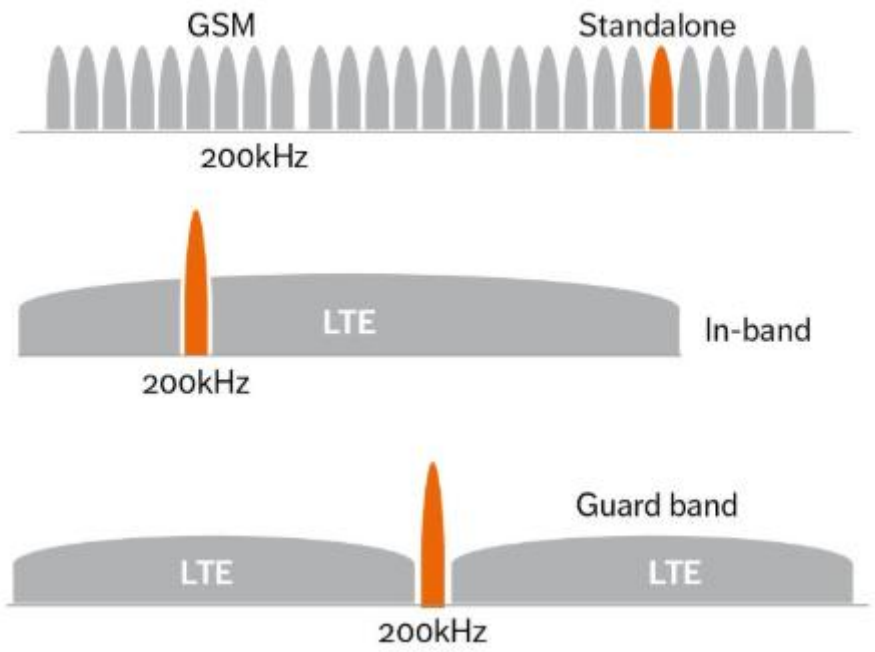
2.4.2.2 – Εντός του φάσματος λειτουργία

Η εντός του φάσματος είναι μία λειτουργία ανάπτυξης των συχνοτήτων στο οποίο οι φορείς του NB-IoT χρησιμοποιούν υπάρχοντα μπλοκ φορέων LTE για την επικοινωνία του συστήματος [15].

Για τους παρόχους που λειτουργούν κυρίως με δίκτυα LTE, η εντός του φάσματος λειτουργία αποτελεί μία ποιοτική λύση για τη διαμόρφωση συχνότητας του συστήματος και ταυτοχρόνως και την πιο οικονομική λύση.

2.4.2.3 – Ενδιάμεσα του φάσματος λειτουργία

Η τρίτη και τελευταία λειτουργία είναι η ανάπτυξη του NB-IoT μέσα σε μια ζώνη φάσματος LTE. Για την διασφάλιση της λειτουργίας χωρίς παρεμβολές η τεχνολογία του NB-IoT και LTE είναι απαραίτητο να συνυπάρχουν. Για να επιτευχθεί αυτό, το φυσικό επίπεδο του NB-IoT σε αντίθεση με άλλες τεχνολογίες LPWA, έχει σχεδιαστεί με την απαίτηση της συνύπαρξης στη ζώνη φάσματος LTE[14].



Εικόνα 8 Επιλογές χρήσης του φάσματος στο NB-IoT[16].

2.4.3 – Ασφάλεια

Το NB-IoT έχει σαν γνώμονα για τον έλεγχο ταυτότητας και την κρυπτογράφηση του, το LTE όπου και κληρονομεί τις ιδιότητες του. Όπως αναφέρουμε και παρακάτω στα θέματα ασφαλείας, το NB-IoT διαθέτει τρία επίπεδα, το κατώτερο επίπεδο είναι το «επίπεδο Αντίληψης» (Perception Layer), το «επίπεδο Δικτύου» (Network Layer) και το «επίπεδο Εφαρμογών» (ApplicationLayer). Οι απαιτήσεις ασφαλείας του πρωτοκόλλου NB-IoT προέρχονται απο την αρχιτεκτονική των τριών επιπέδων που αναφέρουμε και σε παρακάτω κεφάλαιο. Το κατώτερο επίπεδο είναι ευαίσθητο τόσο στις ενεργές όσο και στις παθητικές επιθέσεις. Σε μία παθητική επίθεση, ο επιτιθέμενος θα παρακολουθεί απλά το δικτύου προσαρμόζοντας τις τεχνικές του στις πληροφορίες που ανταλλάσσονται ενώ με τις ενεργές επιθέσεις επηρεάζει την ακεραιότητα των πακέτων μέσω της πλαστογράφησής των δεδομένων τους. Για να διασφαλιστεί η πιστοποίηση της ταυτότητας και η επαλήθευση της ακεραιότητας των δεδομένων, η ύπαρξη κρυπτογραφικών αλγορίθμων είναι απαραίτητη.

Στο επίπεδο αντίληψης, κάθε τελική συσκευή έχει την δυνατότητα απευθείας επικοινωνίας με τους συγκεντρωτές οπότε η διαδρομή αυτή πρέπει να διασφαλιστεί με τον παραπάνω μηχανισμό κρυπτογράφησης. Στο επίπεδο δικτύου το NB-IoT οι συγκεντρωτές συλλέγουν τα πακέτα με τα δεδομένα τους και στη συνέχεια τα τροφοδοτούν πίσω στον εξυπηρετητή, οπότε σύμφωνα με την τεχνική αυτή μπορούν να εμφανιστούν επιθέσεις δικτύου που επιλύονται σε κάποιο βαθμό μέσω της κληρονομικότητας των μηχανισμών LTE. Στο επίπεδο εφαρμογής η τεχνολογία NB-IoT διαχειρίζεται τα δεδομένα αποτελεσματικά. Ως εκ τούτου, οι βασικές απαιτήσεις ασφάλειας για το επίπεδο αυτό είναι ο έλεγχος ταυτότητας και η επεξεργασία αυτών των τεράστιων ετερογενών δεδομένων[11].

2.5 – Επίλογος κεφαλαίου

Στο κεφάλαιο αυτό πραγματοποιήθηκε μία βασική αναφορά στα δίκτυα LPWAN. Αρχικά για τα βασικά χαρακτηριστικά τους που αποτελούν τον λόγο της μεγάλης ζήτησής τους στα συστήματα των IoT. Έπειτα, αναφέρθηκε η τοπολογία που επιλέχθηκε για να τηρηθούν τα χαρακτηριστικά αυτά και τέλος, τα βασικά πρότυπα δικτύων LPWAN στα οποία βασίζονται τα σημερινά IoT συστήματα.

Στο τελευταίο υποκεφάλαιο των πρωτοκόλλων που αναφέρθηκαν παραπάνω, γίνεται μία βασική αναφορά των χαρακτηριστικών ασφαλείας τους, τα οποία θα αναφερθούν ενδελεχώς στο επόμενο κεφάλαιο για τη κάθε μία τεχνολογία.

ΚΕΦΑΛΑΙΟ 3 – ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΑΣΦΑΛΕΙΑΣ LPWAN

3.1 – Εισαγωγή

Το κεφάλαιο αυτό περιγράφει αρχικά, τα βασικά χαρακτηριστικά ασφαλείας που διέπουν τα δίκτυα Low Power Wide Area Network (LPWAN). Στη συνέχεια, περιγράφονται τα χαρακτηριστικά ασφαλείας των βασικών προτύπων LPWAN που έχουν κυριαρχήσει στην αγορά όπως είναι τα πρωτόκολλα LongRage (LoRa),Sigfox και NorthBand-IoT (NB-IoT).

Στο υποκεφάλαιο του κάθε πρωτοκόλλου αναλύονται οι μηχανισμοί ασφαλείας που διαθέτει. Οι μηχανισμοί έχουν κατηγοριοποιηθεί ανάλογα την ιδιότητα τους, όπως είναι η διασφάλιση της αυθεντικότητας, ακεραιότητας και της εμπιστευτικότητας.

Για να διασφαλιστούν οι ιδιότητες των μηχανισμών ασφαλείας των LPWAN σε ένα σύστημα, έχουν αναπτυχθεί αλγόριθμοι κρυπτογράφησης και ταυτοποίησης πακέτων που στέλνονται στο δίκτυο του συστήματος, κατάλληλα πιστοποιητικά όπως κλειδιά συνόδου που χρησιμοποιούνται για την αυθεντικοποίηση και τη κρυπτογράφηση αλλά και μηχανισμοί ενεργοποίησης των συσκευών του συστήματος που συνεισφέρουν κατάλληλα στη διασφάλιση του.

3.2 – Βασικοί μηχανισμοί ασφαλείας LPWAN

Στις τρέχουσες τεχνολογίες LPWAN, η κύρια μέθοδος αντιμετώπισης των βασικών επιθέσεων των δικτύων τους αποτελεί η αποτελεσματική κρυπτογράφηση από άκρο σε άκρο των πακέτων και των δεδομένων που αποστέλλουν οι συσκευές και οι συγκεντρωτές μεταξύ τους. Υπάρχουν όμως όπως είναι λογικό, συγκεκριμένα ζητήματα ασφάλειας που προκύπτουν λόγω της αρχιτεκτονικής των επιπέδων (layer) του πρωτοκόλλου. Βασικοί μηχανισμοί των τεχνολογιών LPWAN που διασφαλίζουν την ομαλή λειτουργία των συστημάτων τους [17]:

- Τα κλειδιά κρυπτογράφησης για τους εξυπηρετητές δικτύου και εφαρμογής (Network - Application Server) πρέπει να προφυλάσσονται με μηχανισμούς ασφαλείας όπως ειδοποιήσεις παραβίασης (tamperalert) από τις ίδιες τις

τελικές συσκευές. Το παραπάνω είναι πολύ σημαντικό για τα δίκτυα LPWAN, καθώς οι συσκευές IoT τοποθετούνται κυρίως σε ένα εξωτερικό περιβάλλον για το μεγαλύτερο χρονικό διάστημα της ζωής τους όπου δεν υπάρχει προστασία. Το να αυξηθεί το επίπεδο φυσικής ασφάλειας των συσκευών IoT είναι αρκετά δαπανηρό αλλά και μη πρακτικό.

- Έλεγχος ταυτότητας διακομιστή (Authentication Network Server AES) αποτελεί τη συνηθέστερη μέθοδο κρυπτογράφησης στα LPWAN και για μεγαλύτερη αποτελεσματικότητα χρησιμοποιεί τη λειτουργία μετρητή (countermode CTR). Σε αυτόν τον τρόπο λειτουργίας, οι συσκευές IoT παράγουν ένα κρυπτογραφημένο μήνυμα που παράγεται μέσω της διαδικασίας XOR στα μηνύματα που περιλαμβάνουν έναν μετρητή, όπως το κλειδί συνόδου εφαρμογής (Application Session Key – AppSkey) και το απλό κείμενο. Ως αποτέλεσμα, οι κρυπτογραφήσεις είναι ευάλωτες στις επιθέσεις κρυπτογράφησης (cyphertext attacks), καθώς αν κάποια κακόβουλη οντότητα αλλάξει τα δεδομένα του πακέτου, έχει τη δυνατότητα να αντιληφθεί σε ποια θέση bit στο κρυπτογραφημένο πακέτο αντιστοιχεί στην ίδια θέση bit στα δεδομένα που διαθέτει που αποτελεί ίσως το πιο σημαντικό ελάττωμα ασφαλείας.
- Ενδιάμεσα της αυθεντικοποίησης του εξυπηρετητή δικτύου και του συγκεντρωτή, η ύπαρξη ενός εισβολέα στο ενδιάμεσο δίκτυο τον φέρνει σε θέση να τροποποιήσει το κρυπτογραφημένο πακέτο χωρίς να μπορεί ο εξυπηρετητής εφαρμογής να παρατηρήσει την αλλαγή. Αυτό συμβαίνει εάν ο εισβολέας αυτός μπορεί να υποκλέψει τα κλειδιά συνόδου (session keys – AppSkey/NwkSKey) , τότε μπορεί να δημιουργήσει ένα μήνυμα που θα περάσει τη διαδικασία ελέγχου του εξυπηρετητή δικτύου. Η υποκλοπή των παραπάνω κλειδιών μπορεί να γίνει με την έκθεση των τελικών συσκευών των δικτύων LPWAN. Είναι πολύ συχνό φαινόμενο να πραγματοποιηθεί μία φυσική επίθεση στις τελικές συσκευές των τεχνολογιών LPWAN καθώς λειτουργούν με μπαταρίες και παραμένουν για μεγάλες χρονικές περιόδους (πάνω από 5-10 χρόνια σύμφωνα με τις καινούργιες τεχνολογίες) σε ημι-ελεγχόμενα περιβάλλοντα ή ακόμη και σε μη ελεγχόμενες περιοχές. Για την περίπτωση αυτή είναι δύσκολο να δημιουργηθεί κάποιος αυτοματοποιημένος μηχανισμός ασφαλείας, εκτός του μηχανισμού που

αναφέρθηκε παραπάνω της αποστολής ειδοποιήσεων παραβίασης (tamperalert) από τις ίδιες τις τελικές.

3.3 – Μηχανισμοί Ασφαλείας LoRaWAN

Αυτή η ενότητα παρέχει μια επισκόπηση των χαρακτηριστικών ασφαλείας του πρωτοκόλλου LoRaWAN v1.1 που κυκλοφόρησε τον Οκτώβριο του 2017. Ακολουθώντας τον κλασικό ορισμό της ασφάλειας, η τεχνολογία του LoRaWAN έχει σαν βασικό στόχο την διασφάλιση της **εμπιστευτικότητας** (confidentiality), της **ακεραιότητας** (integrity) και της **αυθεντικότητας** (Authenticity Validation) ενός συστήματος. Δεδομένου ότι το κανάλι επικοινωνίας είναι ασύρματο και έτσι είναι διαθέσιμο σε οποιονδήποτε έχει τεχνικές γνώσεις ώστε να το επιτεθεί και να παραποιήσει τα δεδομένα που αποστέλνονται μέσω αυτού, είναι απαραίτητη η αυθεντικότητα της επικοινωνίας - με άλλα λόγια αν τα πακέτα που στέλνονται προέρχονται από την σωστή πηγή.

3.3.1 – Πιστοποίηση Εμπιστευτικότητας

Η χρήση των κλειδιών δικτύου (Network Session key) και του κλειδιού εφαρμογής (Application Session Key) εφαρμόζεται από την έκδοση του LoRaWANv1.0.2 και αποτελούν το καθένα ένα ζευγάρι ξεχωριστών κλειδιών. Ο λόγος πίσω από αυτό είναι ότι το LoRaWAN σχεδιάστηκε με την επιχειρηματική προοπτική χρήσης ενός φορέα εκμετάλλευσης δικτύου ή τηλεπικοινωνιών, ο οποίος λειτουργεί με τα πρωτόκολλα LPWAN, ενώ οι ιδιοκτήτες των τελικών συσκευών IoT και οι πάροχοι των έξυπνων συστημάτων IoT μπορούν να χρησιμοποιήσουν την υποδομή του εκάστοτε LPWAN για να δημιουργήσουν συνδεσιμότητα μεταξύ τους. Δεδομένου ότι απαιτείται έλεγχος εμπιστευτικότητας και ακεραιότητας μεταξύ της τελικής συσκευής και του δικτύου (συγκεντρωτές και εξυπηρετητές) και μεταξύ της συσκευής και ενός παροχέα εφαρμογών στη μονάδα στήριξης (backend), το κλειδί δικτύου εξασφαλίζει την πρώτη, ενώ η σύνδεση από άκρο σε άκρο προστατεύεται από το κλειδί εφαρμογής. Παρακάτω στον πίνακα 1 βλέπουμε την χρησιμότητα των κλειδιών εφαρμογής και δικτύου και τα βασικά χαρακτηριστικά τους, όπου χρησιμοποιούνται για την κρυπτογράφηση και την ακεραιότητα των δεδομένων.

3.3.1.1 – Κλειδιά Ασφαλείας δικτύου και εφαρμογής

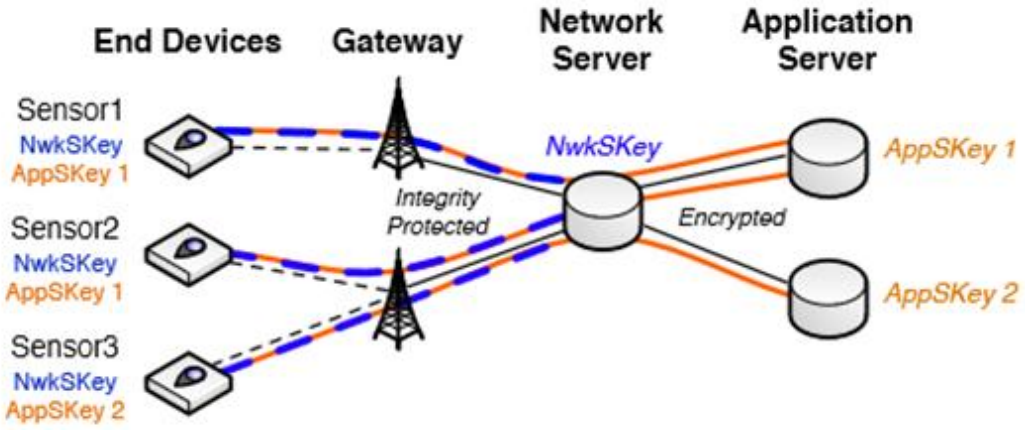
Τα κλειδιά που αναφέρθηκαν παραπάνω, είναι μοναδικά για κάθε τελική συσκευή και είτε είναι προκαθορισμένα μέσω της διαδικασίας σύνδεσης ενεργοποίησης από το προσωπικό (Activation By Personalisation - ABP) είτε μέσω της ενεργοποίησης μέσω του αέρα (Over The Air Activation – OTAA) από το κλειδί εφαρμογής και πιο συγκεκριμένα όπως φαίνεται και στο πίνακα 1 και στην εικόνα 9, για τα κλειδιά ασφαλείας στο LoRaWAN έχουμε [49]

- **Κλειδί συνόδου Εφαρμογής** (Application session key AppSKey) - Το κλειδί συνόδου(session) εφαρμογής είναι ένα μοναδικό κλειδί για κάθε τελική συσκευή με μέγεθος 128-bit, το οποίο δεν μεταδίδεται στο δίκτυο και διαμοιράζεται μέσω των τελικών συσκευών και του εξυπηρετητή εφαρμογής. Χρησιμοποιείται για την κρυπτογράφηση και την αποκωδικοποίηση των πακέτων που προορίζονται με σκοπό να διασφαλιστεί η ακεραιότητα των δεδομένων που προέρχονται από τις συσκευές στους τελικού χρήστες
- **Κλειδί συνόδου Δικτύου** (Network session key NwkSKey) - Το κλειδί συνόδου δικτύου όπως και το παραπάνω, είναι ένα μοναδικό κλειδί για κάθε τελική συσκευή με μέγεθος 128-bit, το οποίο δεν μεταδίδεται στο δίκτυο και διαμοιράζεται μέσω των τελικών συσκευών και του εξυπηρετητή δικτύου. Χρησιμοποιείται για την διασφάλιση της ακεραιότητας των δεδομένων που προορίζονται για τους τελικούς χρήστες.
- **Κλειδί Εφαρμογής** (Application Key AppKey) - Το κλειδί εφαρμογής αποτελεί ένα μοναδικό κλειδί για κάθε τελική συσκευή με μέγεθος 128-bit, το οποίο είναι καθορισμένο κλειδί από τον διαχειριστή του δικτύου για τις τελικές συσκευές. Το κλειδί αυτό δεν μεταδίδεται στο δίκτυο αλλά μοιράζεται μέσω των συσκευών και του εξυπηρετητή εφαρμογής. Χρησιμοποιείται για τον υπολογισμό και την επαλήθευση του κώδικα ακεραιότητας μηνύματος (message integrity code MIC) κάθε μηνύματος.
- **Διεύθυνση τελικής συσκευής** (End-device address DevAddr) – Η διεύθυνση της τελικής συσκευής έχει στόχο όπως είναι λογικό να καθορίζει και τη θέση της τελικής συσκευής στο δίκτυο, είναι 32-bitμέγεθος και καθορίζεται από τον εξυπηρετητή δικτύου.

- **Κλειδί ακεραιότητας και προώθησης του Κλειδιού συνόδου Δικτύου** (Forwarding Network session integrity key FNwkSIntKey) - Το κλειδί αυτό είναι ένα κλειδί συνόδου δικτύου καθορισμένο μόνο για μία συγκεκριμένη τελική συσκευή. Χρησιμοποιείται από την τελική συσκευή για τον υπολογισμό του κώδικα ακεραιότητας μηνύματος ή μέρους του κώδικα ακεραιότητας μηνύματος (MIC) για τα μηνύματα ανερχόμενης ζεύξης με σκοπό εξασφάλιση της ακεραιότητας των δεδομένων τους. Το κλειδί αυτό αποθηκεύεται με τρόπο που να διασφαλίζει την αποτροπή της υποκλοπής και της επαναχρησιμοποίησης από κακόβουλες οντότητες [18].
- **Κλειδί ακεραιότητας και εξυπηρέτησης του Κλειδιού συνόδου Δικτύου** (Serving Network session integrity keySNwkSIntKey) - Το κλειδί αυτό έχει ακριβώς τις ίδιες ιδιότητες με το κλειδί προώθησης του δικτύου (FNwkSIntKey), η μοναδική διαφορά είναι ότι χρησιμοποιείται από την τελική συσκευή για τον υπολογισμό του κώδικα ακεραιότητας μηνύματος για τα μηνύματα κατερχόμενης ζεύξης.
- **Κλειδί αποκρυπτογράφησης συνόδου Δικτύου (**Network session encryption key NwkSEncKey) – Το κλειδί αυτό είναι ένα κλειδί δικτύου οριστικοποιημένο για τις τελικές συσκευές. Χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση των εντολών του κώδικα επαλήθευσης μηνυμάτων (MAC) κατερχόμενης και ανερχόμενης ζεύξης και των δεδομένων τους.

Πίνακας 1 Τα βασικά κλειδιά των τελικών συσκευών για την ασφαλή επικοινωνία με το δίκτυο και το σύστημα [18].

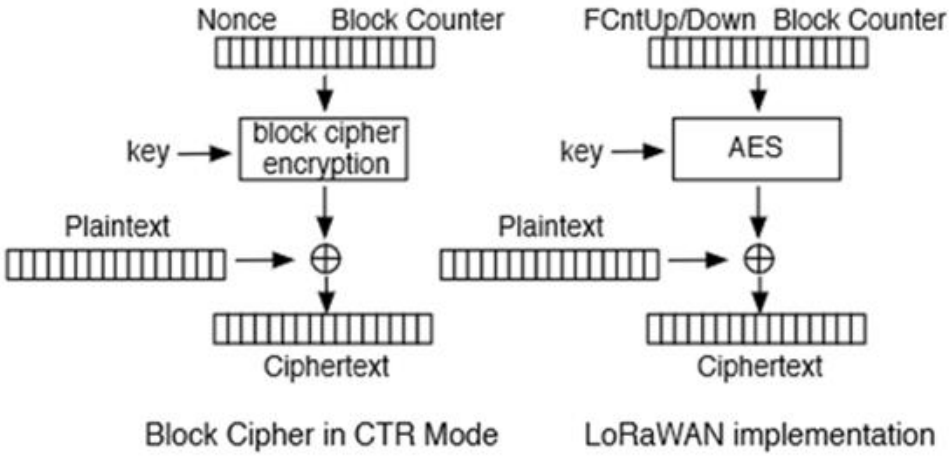
Key name	Key type	Length/bits	Generation	Usage
AppKey	Symmetric	128	By application	MIC for join request and accept Encrypt join accept Generate session keys
AppSkey	Symmetric	128	By AppKey	Encrypt data messages
NwkSKey	Symmetric	128	By AppKey	MIC for messages Encrypt command-only messages



Εικόνα 9 Τα κλειδιά και η χρησιμότητα τους στο δίκτυο LoRaWAN [49]

Ακόμα, όσον αφορά την εμπιστευτικότητα του καναλιού, όταν αποστέλλεται ένα μήνυμα στον εξυπηρετητή δικτύου, τα δεδομένα που υπάρχουν στα πακέτα κρυπτογραφούνται αρχικά με την χρησιμοποίηση του κλειδιού συνόδου εφαρμογής. Η εμπιστευτικότητα των δεδομένων διασφαλίζεται με την χρησιμοποίηση του πιο γνωστού μηχανισμού κρυπτογράφησης (AES) που λειτουργεί σε λειτουργία μετρητή (CTR), την χρησιμότητα και τον τρόπο λειτουργίας την βλέπουμε παρακάτω.

Η μέθοδος κρυπτογράφησης που παρουσιάζεται στην εικόνα 10, παράγει ένα ρεύμα (stream) τυχαίων ψηφίων χρησιμοποιώντας την τυχαία μετάθεση (pseudo-random) που παρέχεται στη μέθοδο. Το ρεύμα που αναφέραμε, στη συνέχεια χρησιμοποιείται ως κύρια ρεύμα (mainstream) για την κρυπτογράφηση των πακέτων με χρήση της μεθόδου XOR. Καθώς ο μετρητής είναι ουσιαστικά μια λειτουργία για την κρυπτογράφηση ρεύματος, το ακριβές ρεύμα δεν μπορεί ποτέ να χρησιμοποιηθεί δύο φορές. Το LoRaWAN ακολουθεί το σχεδιασμό μετρητή (CTR) στο γράμμα και επιλέγει το AES ως μηχανισμό κρυπτογράφησης και χρησιμοποιεί τον μετρητή μηνυμάτων LoRa (μετρητή ανερχόμενων πακέτων FCntUp ή μετρητή κατερχόμενων πακέτων FCntDown) ως τρέχων τυχαίο αριθμό, ο οποίος αυξάνεται συνεχώς για κάθε μήνυμα [49].



Εικόνα 10 Λειτουργία μετρητή (CTR) για την μέθοδο κρυπτογράφησης [49]

3.3.1.2 – Πρωτόκολλα σύνδεσης των τελικών συσκευών

Δεδομένου ότι για την αποστολή πακέτων προς τον εξυπηρετητή δικτύου και εφαρμογών χρειάζονται δύο κλειδιά συνόδου αποτελεί βασική προϋπόθεση η αποθήκευση τους για να ενεργοποιηθούν και να χρησιμοποιηθούν από τις τελικές συσκευές που συμμετέχουν στο σύστημα. Η τεχνολογία του LoRaWAN ορίζει δύο μηχανισμούς για αυτή τη διαδικασία ενεργοποίησης, την Ενεργοποίηση με Προσωποποίηση (Activation by Personalisation ABP) και Ενεργοποίηση μέσω αέρα(Over-the-Air Activation OTAA) [42].

3.3.1.2.1 – Ενεργοποίηση μέσω αέρα

Η μέθοδος ενεργοποίησης μέσω αέρα χρησιμοποιεί ένα αναγνωριστικό των τελικών συσκευών (DevEUI) το οποίο είναι μια μοναδική διεύθυνση επιπέδου MAC με μέγεθος 64bit για κάθε τελική συσκευή, ένα αναγνωριστικό εφαρμογής (JoinEUI) που και αυτό είναι μία μοναδική 64-bit διεύθυνση για την αναγνώριση της εφαρμογή, και το κλειδί εφαρμογής που αναφέρθηκε παραπάνω. Η μέθοδος αυτή διασφαλίζει την σύνδεση των τελικών συσκευών, για να το πετύχει αυτό για κάθε συσκευή (είτε για πρώτη φορά είτε λόγω επανασύνδεσης π.χ. επανεκκίνησης) δημιουργείται για αυτήν ένα ξεχωριστό κλειδί συνόδου δικτύου. Ακόμα, με την χρησιμοποίηση των διαφορετικών κλειδιών αυξάνεται η προστασία εναντίον της αλλοίωσης (tampering) των πακέτων ακόμα και αν ένα από αυτά κλαπεί. Σε κάθε συσκευή για να αρχίσει η διαδικασία ενεργοποίησης μέσω αέρα

στέλνει ένα αίτημα εγγραφής (join-request). Το αίτημα αυτό περιέχει τα παραπάνω αναγνωριστικά, αλλά και μία τιμή συσκευής (DevNonce). Η τιμή αυτή, είναι μια τυχαία τιμή που παρακολουθείται από τον εξυπηρετητή δικτύου και χρησιμοποιείται για να απορρίπτει αιτήματα εγγραφής που έχουν λάθος τιμές συσκευής, με τον μηχανισμό αυτό διασφαλίζεται και η αντιμετώπιση της επίθεσης επανάληψης. Στη περίπτωση που ο εξυπηρετητής δεχτεί το αίτημα εγγραφής, θα στείλει με τη σειρά του μέσω του δικτύου ένα αίτημα αποδοχής (join- accept)

Στην εφαρμογή της μεθόδου ενεργοποίησης μέσω αέρα για την σύνδεση στο δίκτυο, το κλειδί εφαρμογής (AppKey) χρησιμοποιείται για την δημιουργία των δύο νέων: του κλειδιού συνόδου εφαρμογής και κλειδιού συνόδου δικτύου που αναφέρθηκαν παραπάνω και είναι μοναδικά για κάθε τελική συσκευή. Αν κάποιος καταφέρει να υποκλέψει το κλειδί εφαρμογής, τότε η συσκευή που εκτέθηκε και το χρησιμοποιεί θεωρείται μη αξιόπιστη διότι αποτελεί τη βάση για την δημιουργία των κλειδιών συνόδου. Παρόλα αυτά οι υπόλοιπες συσκευές δεν έχουν πρόβλημα αξιοπιστίας.

3.3.1.2.2 – Ενεργοποίηση με Προσωποποίηση

Η μέθοδος ενεργοποίησης με προσωποποίηση συνδέει άμεσα μια τελική συσκευή με ένα συγκεκριμένο δίκτυο παρακάμπτοντας τη διαδικασία αιτήματος που είδαμε με τη παραπάνω μέθοδο. Χρησιμοποιώντας τη μέθοδο αυτή, η κάθε τελική συσκευή θα έχει απευθείας αποθηκευμένα από τους παρόχους των υπηρεσιών τα κλειδιά συνόδου, χωρίς την διαδικασία δημιουργίας κλειδιών από το κλειδί εφαρμογής και των αναγνωριστικών. Η συσκευή θα ενεργοποιηθεί και θα μπορέσει να χρησιμοποιηθεί από τη τεχνολογία LoRa μετά την τοποθέτηση της. Κάθε συσκευή θα διαθέτει τα δικά της μοναδικά κλειδιά συνόδου, που σημαίνει ότι στην περίπτωση που κάποια συσκευή εκτεθεί δεν θα εκθέσει και τη λειτουργία των άλλων τελικών συσκευών. Για την διασφάλιση της εμπιστευτικότητας των κλειδιών είναι ασφαλές να ειπωθεί ότι τα κλειδιά δεν μπορούν να προκύψουν με κανέναν τρόπο από τις διαθέσιμες στο κοινό πληροφορίες. Κάθε φορά που μία συσκευή ενεργοποιείται για τη χρησιμοποίηση της από τα δίκτυο ή όταν επανεγκατασταθεί, εκπέμπει μία αίτηση για επανεκκίνηση σαν μία εκπομπή ανερχόμενης ζεύξης και περιμένει για την ενεργοποίηση της μέχρι να λάβει αίτημα αποδοχής από το

δίκτυο. Μετά την εκ νέου αρχικοποίηση της συσκευής, χρησιμοποιεί την προεπιλεγμένη διαμόρφωση της [18].

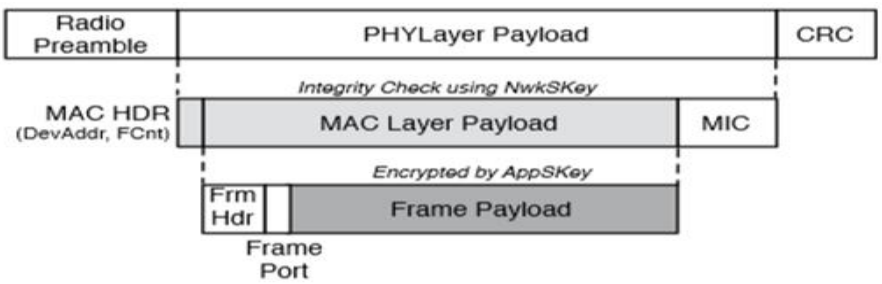
3.3.2 – Πιστοποίηση Ακεραιότητας

Η πιστοποίηση της ακεραιότητας των δεδομένων που αποστέλλονται στην τεχνολογία LoRaWAN πετυχαίνεται με τους παρακάτω μηχανισμούς.

3.2.2.1 – Κωδικός ακεραιότητας μηνύματος (Message integrity code MIC)

Ο κωδικός ακεραιότητας για τα μηνύματα που στέλνονται, χρησιμοποιείται από την τεχνολογία LoRaWAN για να παρέχει έναν έλεγχο ακεραιότητας στα πακέτα που στέλνονται και στα δεδομένα που περιλαμβάνονται στα πακέτα. Ο κωδικός αυτός μπορεί να δημιουργηθεί χρησιμοποιώντας το κλειδί συνόδου δικτύου σαν παράμετρο στην μέθοδο κρυπτογράφησης AES-CMAC. Όταν τα πακέτα ανερχόμενης ζεύξης φθάνουν στον εξυπηρετητή, ο εξυπηρετητής θα ελέγξει πρώτα την ακεραιότητα του πακέτου και στην περίπτωση που περάσει τον έλεγχο θα μεταφερθεί στον εξυπηρετητή εφαρμογής. Για τα αιτήματα εγγραφής (join-request) που χρησιμοποιούνται στην μέθοδο ενεργοποίησης μέσω αέρα, το κωδικός ακεραιότητας παράγεται χρησιμοποιώντας σαν παράμετρο το κλειδί εφαρμογής (AppKey) αντί για το κλειδί συνόδου δικτύου. Στη παρακάτω εικόνα η φωτεινή σκιασμένη περιοχή προστατεύεται από τον κωδικό ακεραιότητας που παράγεται από το κλειδί συνόδου δικτύου ενώ η σκοτεινή σκιασμένη περιοχή κρυπτογραφείται από το κλειδί συνόδου εφαρμογής [18].

Με βάση τη παρακάτω εικόνα 11 μπορούμε να συμπεράνουμε ότι: Το πακέτο αποτελείται από το MACHDR (MAC κεφαλίδα), FRMHDR (Κεφαλίδα πακέτου), FramePort (Θύρα πακέτου), FramePayload (Δεδομένα πακέτου)



Εικόνα 11 Η εφαρμογή του κωδικού ακεραιότητας μηνύματος σε ένα πακέτο.[49]

3.2.2.2 – Μέθοδος Κρυπτογράφησης AES – 128

Η τεχνολογία του LoRaWAN όπως και τα περισσότερα πρωτόκολλα LPWAN χρησιμοποιούν μηχανισμό κρυπτογράφησης. Χαρακτηριστικά στην συγκεκριμένη τεχνολογία, χρησιμοποιείται η μέθοδος κρυπτογράφησης του Προηγμένου Προτύπου Κρυπτογράφησης (Advanced Encryption Standard – AES), το οποίο αποτελεί πρότυπο κρυπτογράφησης και είναι καθορισμένο από το National Institute of Standards and Technology (NIST). Η μέθοδος AES είναι ένας αλγόριθμος συμμετρικού κλειδιού, που σημαίνει ότι το ίδιο κλειδί ασφαλείας χρησιμοποιείται τόσο για κρυπτογράφηση όσο και για την αποκρυπτογράφηση δεδομένων. Η τεχνολογία του LoRaWAN χρησιμοποιεί AES για τη διασφάλιση της ακεραιότητας και της εμπιστευτικότητας. Χρησιμοποιούνται τρεις λειτουργίες AES, η κρυπτογράφηση βασισμένη στον κωδικό ελέγχου γνησιότητας μηνύματος (Cipher-based Message Authentication Code CMAC) που χρησιμοποιείται για την ακεραιότητα, και οι επόμενες δύο για την εμπιστευτικότητα που είναι η λειτουργία της AES μετρητή κρυπτογράφησης και της AES λειτουργίας Κωδικού Ηλεκτρονικού Βιβλίου (Electronic Book Code ECB) αποκρυπτογράφησης. Οι τρείς λειτουργίες του AES χρησιμοποιούν κλειδί μεγέθους 128bit[19].

3.2.2.2.1 – AES CMAC

Η λειτουργία της κρυπτογράφησης βασισμένης στον κωδικό ελέγχου γνησιότητας μηνύματος (Cipher-based Message Authentication Code CMAC) χρησιμοποιείται για τον υπολογισμό μίας τιμής κατακερματισμού για μια συγκεκριμένη είσοδο μηνύματος όπως βλέπουμε και στην εικόνα 12. Μια συνάρτηση κατακερματισμού παρέχει σαν έξοδο μια μοναδική σειρά κειμένου με παραμέτρους τα δεδομένα εισόδου. Το αποτέλεσμα της λειτουργίας θα πρέπει να είναι τελείως διαφορετική συμβολοσειρά και μέγεθος από τα δεδομένα που πήρε σαν παράμετρο. Τα αποτελέσματα από τον κατακερματισμό χρησιμοποιούνται κυρίως για τη διασφάλιση της ακεραιότητας. Αυτή η μέθοδος βασίζεται στο RFC4493. Το RFC4493 καθορίζει τη λειτουργία αυτή, που βασίζεται σε ένα συμμετρικό κλειδί κρυπτογράφησης κλειδιού (AES σε αυτή την περίπτωση). Η λειτουργία αυτή παρέχει έλεγχο ακεραιότητας της προέλευσης δεδομένων για τα πακέτα. Στις προδιαγραφές ασφαλείας της τεχνολογίας του LoRaWAN αυτή η λειτουργία

χρησιμοποιείται για την παραγωγή του κωδικού ακεραιότητας μηνύματος από τα δεδομένα των πακέτων και τα αιτήματα εγγραφής και αποδοχής.

Input	K	[NwkSKey ǀ AppKey]
	M	message to be authenticated
	len	length of the message in octets
Output	A	message authentication code

Εικόνα 12 Στην εικόνα βλέπουμε της παραμέτρους και τα αποτελέσματα της λειτουργίας CMAC [46].

3.2.2.2.2 – AES Μετρητή Κρυπτογράφησης (CTR)

Η AES κρυπτογράφησης, χρησιμοποιώντας τη λειτουργία μετρητή, χρησιμοποιείται για την παραγωγή ενός κρυπτογραφημένου αποτελέσματος με παραμέτρους το κλειδί κρυπτογράφησης και το μήνυμα εισόδου όπως εμφανίζεται και στην εικόνα 13. Η λειτουργία αυτή βασίζεται στον γενικό αλγόριθμο που περιγράφεται από το Institute of Electrical and Electronics Engineers (IEEE) 6 802.15.4/2006 Annex B [IEEE 802154]. Στις προδιαγραφές ασφαλείας της τεχνολογίας του LoRaWAN αυτή η λειτουργία χρησιμοποιείται για την παραγωγή του κλειδιού συνόδου δικτύου και του κλειδιού συνόδου εφαρμογής με παραμέτρους τα αιτήματα αποδοχής και για τη κρυπτογράφηση των δεδομένων των πακέτων.

Στην λειτουργία αυτή, για την κρυπτογράφηση των αιτημάτων αποδοχής χρησιμοποιείται η λειτουργία Κωδικού Ηλεκτρονικού Βιβλίου (Electronic Book Code ECB). Τόσο η λειτουργία μετρητή όσο και η ECB είναι τρόποι διασφάλισης της εμπιστευτικότητας. Χαρακτηριστικά στη λειτουργία Κωδικού Ηλεκτρονικού Βιβλίου τα δεδομένα ενός πακέτου κρυπτογραφούνται ξεχωριστά και αντιστοίχως αποκρυπτογραφούνται ξεχωριστά. Συνεπάγεται ότι η κρυπτογράφηση και η αποκρυπτογράφηση δεδομένων ενός πακέτου είναι εντελώς ανεξάρτητη από τους τα δεδομένα άλλων πακέτων [20].

Input	K	[NwkSKey | AppSKey | AppKey | 16 x 0x00]
	M	message to be encrypted
Output	C	cipher (encrypted) text

Εικόνα 13 Στην εικόνα βλέπουμε τις παραμέτρους και τα αποτελέσματα της λειτουργίας κρυπτογράφησης μετρητή [46]

3.2.2.2.3 – AES αποκρυπτογράφησης (ECB)

Η μέθοδος AES σε λειτουργία ECB χρησιμοποιείται από τον εξυπηρετητή δικτύου για να κρυπτογραφήσει το αίτημα αποδοχής που συνεπάγεται την αποδοχή των τελικών συσκευών ώστε να είναι στην διάθεση τους η αποκρυπτογράφηση των δεδομένων που λαμβάνουν. Στις προδιαγραφές ασφαλείας της τεχνολογίας του LoRaWAN αυτή η λειτουργία χρησιμοποιείται όπως είδαμε και παραπάνω μόνο για την κρυπτογράφηση ενός αιτήματος αποδοχής από το εξυπηρετητή δικτύου.

3.3.3 – Πιστοποίηση Αυθεντικότητας

Η πιστοποίηση Αυθεντικότητας στην τεχνολογία του LoRaWAN αποτελεί ένα βασικό κομμάτι των συστημάτων που χρησιμοποιούν τα πρωτόκολλα των LPWAN και για να επιτευχθεί αυτό βασικός στόχος είναι η προστασία από τα κακόβουλα πακέτα.

3.3.3.1 – Προστασία από επαναληπτικά πακέτα (Replay Attack)

Το πρωτόκολλο του LoRaWAN διαθέτει το μηχανισμό μετρητή πακέτων (FrameCounter - FCnt), όπου κάθε τελική συσκευή έχει στη διάθεση της τρεις μετρητές για την παρακολούθηση του αριθμού των πακέτων που αποστέλλονται. Ο πρώτος μετρητής μετράει τα πακέτα που στέλνονται μέσω ανερχόμενης ζεύξης στον εξυπηρετητή δικτύου (FCntUp) και ο δεύτερος μέσω κατερχόμενης ζεύξης από το διακομιστή δικτύου στη συσκευή (FCntDown) και ο τρίτος είναι η διαφορά τους [18].

Όταν εκτελείται μία κατερχόμενη ζεύξη, εμφανίζονται δύο είδους μετρητές πακέτων. Ο ένας μετρητής σύμφωνα με το LoRaWAN v1.0, όπου όλες οι θύρες μοιράζονται την τιμή του μετρητή κατερχόμενης ζεύξης (FCntDown), και ένα είδος μετρητή σύμφωνα με το LoRaWAN1.1 που αποτελείται από δύο τιμές. Η πρώτη

τιμή χρησιμοποιεί ξεχωριστά τη θύρα 0 για την MAC επικοινωνία (network NFCntDown) και η δεύτερη χρησιμοποιεί όλες τις πύλες όταν δεν υπάρχει πληροφορία για κάποια συγκεκριμένη πύλη (Application AFCntDown). Στην περίπτωση ενεργοποίησης μέσω αέρα (OTAA), κάθε φορά που μια συσκευή επεξεργάζεται επιτυχώς ένα αίτημα αποδοχής, μηδενίζονται οι μετρητές πακέτων από την πλευρά της τελικής συσκευής (FCntUp) αλλά και οι μετρητές πακέτων από τη πλευρά του δικτύου (NFCntDown & AFCntDown). Από την άλλη πλευρά, οι συσκευές που έχουν ενεργοποιηθεί μέσω της διαδικασίας ενεργοποίησης από προσωποποίηση έχουν τους μετρητές πακέτων μηδενισμένους από τη κατασκευή τους. Υπάρχει ένας σοβαρός κανόνας ασφαλείας για τις συσκευές αυτές, ότι δεν πρέπει να επαναφέρονται οι μετρητές καθ 'όλη τη διάρκεια ζωής τους. Στην περίπτωση που η τελική συσκευή κατά τη διάρκεια του χρόνου ζωής της χρειαστεί αλλαγή μπαταρίας λόγω μικρής ισχύος, οι μετρητές πλαισίων είναι πολύ σημαντικό να παραμένουν ίδιοι.

Όταν εκτελείται μία ανερχόμενη ζεύξη, ο μετρητής πακέτων (FCntUp) αυξάνεται με κάθε μήνυμα. Οι μετρητές δικτύου και εφαρμογής (NFCntDown - AFCntDown) αυξάνονται επίσης με κάθε κατερχόμενη ζεύξη, ο μετρητής δικτύου μέσω της πύλης 0 (αν λείπει η πληροφορία της πύλης τότε μέσω μίας άλλης) και ο μετρητής εφαρμογής μέσω μίας άλλης πύλης διαφορετικής από τη πύλη 0. Ο μετρητής από την πλευρά του δέκτη συγχρονίζεται με την ληφθείσα τιμή, έπειτα η τιμή αυτή αυξάνεται και σε σύγκριση με την τρέχουσα τιμή μετρητή και το πεδίο MIC του μηνύματος υπολογίζεται τοπικά χρησιμοποιώντας το κατάλληλο κλειδί συνόδου δικτύου. Στις περιπτώσεις επανάληψης πακέτων, είτε είναι επιβεβαιωμένα είτε όχι ο μετρητής δεν αυξάνεται. Ο εξυπηρετητής δικτύου λειτούργει σαν ελεγκτής των επαναληπτικών πακέτων και δέχεται τα δεδομένα μόνο από το πρώτο επιβεβαιωμένο ίδιο πακέτο. Το μέγεθος των μετρητών είναι 32bit, και το πεδίο που υπάρχει ο μετρητής στο πακέτο, αντιστοιχεί στα λιγότερο σημαντικά 16 bits.

Η επαναχρησιμοποίηση της ίδιας τιμής του μετρητή ανερχόμενης ζεύξης (FCntUpFCntUp) δεν πραγματοποιείται από τη τελική συσκευή με τη χρήση των ίδιων κλειδιών συνόδου, εκτός από την αναμετάδοση του ίδιου επιβεβαιωμένου ή μη επιβεβαιωμένου πλαισίου. Επίσης δεν επεξεργάζονται ποτέ οποιαδήποτε

αναμετάδοση του ίδιου πακέτου κατερχόμενης ζεύξης και οι επόμενες μεταδόσεις αγνοούνται χωρίς επεξεργασία.

3.3.3.3 – Μήνυμα επιβεβαίωσης (Message acknowledge bit ACK)

Για τη καλύτερη και ασφαλέστερη λειτουργία του συστήματος, υπάρχει ο μηχανισμός δημιουργίας μηνυμάτων επιβεβαίωσης, τα οποία όπως λέει και το όνομα τους επιβεβαιώνουν τη λήψη των πακέτων από μία συσκευή στην άλλη. Χαρακτηριστικά στη τεχνολογία του LoRaWAN, ο δέκτης πρέπει να αποκρίνεται με ένα πλαίσιο δεδομένων που έχει στα περιεχόμενα του το μήνυμα επιβεβαίωσης (ACK) που έχει οριστεί. Εάν ο αποστολέας είναι μία τελική συσκευή και ζητάει επιβεβαίωση λήψης για ένα πακέτο που έστειλε, το δίκτυο θα προωθήσει το μήνυμα επιβεβαίωσης μέσω μίας κατερχόμενης ζεύξης. Εάν ο αποστολέας είναι ένας συγκεντρωτής, η συσκευή μέσω μίας ανερχόμενης ζεύξης αποστέλλει το μήνυμα επιβεβαίωσης. Ένα μήνυμα επιβεβαίωσης (ACK) αποστέλλεται μόνο για το τελευταίο μήνυμα που ελήφθη και αναμεταδόθηκε.

3.4 – Μηχανισμοί Ασφαλείας Sigfox

Η τεχνολογία του Sigfox διαθέτει τα παρακάτω χαρακτηριστικά ασφαλείας που είναι απαραίτητα για τη διασφάλιση της σωστής και ασφαλής λειτουργίας των συστημάτων. Η έρευνα των μηχανισμών ασφαλείας που διαθέτει έγινε με βάση την έκθεση για την τεχνική ανάλυση του πρωτοκόλλου [21].

Ένα από τα βασικά χαρακτηριστικά ασφαλείας της τεχνολογίας αυτής, αποτελεί η επαλήθευση του μηνύματος που στέλνεται από κάποια συσκευή. Η συσκευή αυτή αναγνωρίζεται μέσω μιας μοναδικής ταυτότητας (ID συσκευής) που υπάρχει στο μήνυμα. Με την ταυτότητα αυτή, διασφαλίζεται ότι το μήνυμα έχει δημιουργηθεί και αποστέλλεται από τη συσκευή με την αναγνωρισμένη ταυτότητα του μηνύματος, η ταυτότητα αυτή ελέγχεται από το σύστημα αν αντιπροσωπεύει τη συσκευή από όπου στάλθηκε και επιτρέπεται αν πληροί τα χαρακτηριστικά η σύνδεση στο δίκτυο.

Ακόμα, ένα πολύ σημαντικό χαρακτηριστικό είναι η διασφάλιση της ακεραιότητας του μηνύματος που στέλνεται από κάποια συσκευή. Προστατεύει δηλαδή την περίπτωση υποκλοπής μηνύματος από έναν εισβολέα και βεβαιώνει ότι οποιαδήποτε τροποποίηση μπορεί να ανιχνευθεί και να απορριφθεί από το δίκτυο.

Επιπλέον χαρακτηριστικό αποτελεί η δυνατότητα προστασίας από επαναλαμβανόμενα μηνύματα, την περίπτωση όπου ένας εισβολέας έχει υποκλέψει ένα ή περισσότερα μηνύματα και τα επαναλαμβάνει διαρκώς ώστε να επιφέρει πρόβλημα στο σύστημα, το Sigfox έχει τη δυνατότητα να τα απορρίψει. Το βασικότερο χαρακτηριστικό των LPWAN αλλά και του Sigfox είναι η δυνατότητα κρυπτογράφησης του μηνύματος από τη συσκευή μέχρι τον εξυπηρετητή του Sigfox.

3.4.1 – Βασικά χαρακτηριστικά

Η τεχνολογία του Sigfox έχει διαμορφώσει όλα τα στοιχεία του συστήματος να διαθέτουν βασικά χαρακτηριστικά ασφαλείας από προεπιλογή, στους χρήστες του Sigfox, στους χειριστές του Sigfox και στους κατασκευαστές συσκευών.

Τα χαρακτηριστικά της προεπιλεγμένης ασφαλείας για το σύστημα, είναι όπως αναφέραμε και παραπάνω η ακεραιότητα, η επαλήθευση και η προστασία από τα επαναλαμβανόμενα μηνύματα για τα δεδομένα που ταξιδεύουν στο δίκτυο. Είναι η κρυπτογράφηση για να διασφαλιστεί η εμπιστευτικότητα των δεδομένων και αυτό πετυχαίνεται με τη βοήθεια της μεθόδου κρυπτογράφησης Advanced Encryption Standard (AES). Ακόμα ένα πολύ βασικό χαρακτηριστικό είναι ότι κάθε συσκευή είναι μεμονωμένη και επικοινωνεί αυτόνομα με το δίκτυο, πράγμα που σημαίνει ότι αν μια συσκευή δεχθεί κάποιου είδους ασύρματης επίθεσης δεν θα επηρεαστεί το σύστημα του Sigfox.

Από την πλευρά της κατασκευής των συσκευών, το Sigfox είχε ορίσει τρία διαφορετικά επίπεδα ασφαλείας. Έχοντας ως γνώμονα τις περίπτωσης χρήσης των συστημάτων και τι χρειάζεται, τότε ο πάροχος του συστήματος θα αποφασίσει ποιο επίπεδο θα εφαρμόσει:

- Μεσαίου επιπέδου όπου τα διαπιστευτήρια ασφαλείας θα είναι αποθηκευμένα στις συσκευές.
- Υψηλού επιπέδου όπου τα διαπιστευτήρια ασφαλείας θα είναι αποθηκευμένα σε προστατευμένη περιοχή βασισμένη σε Software.
- Πολύ υψηλού επιπέδου όπου τα διαπιστευτήρια ασφαλείας θα είναι αποθηκευμένα σε ένα ασφαλές στοιχείο.

Το παραπάνω ασφαλές στοιχείο χρησιμοποιείται ακόμα για τη κρυπτογράφηση των δεδομένων που μεταφέρονται μέσω του δικτύου. Μόνο μια συγκεκριμένη συσκευή και ο χρήστης γνωρίζουν το μυστικό κλειδί. Ο αλγόριθμος αυτός δεν επηρεάζει το μέγεθος του πακέτου, δηλαδή αφού κρυπτογραφηθούν τα δεδομένα το μέγεθος θα παραμείνει στα 12 byte.

Καθόλη τη διαδρομή που διανύουν τα πακέτα όπως βλέπουμε και στην εικόνα 14, για να φτάσουν στον εξυπηρετητή, το δίκτυο του Sigfox διασφαλίζει ότι η ταυτότητα του πακέτου δεν θα μπορέσει κάποια κακόβουλη οντότητα να την υποκλέψει. Στην περίπτωση που μία συσκευή εκτεθεί, θα εισαχθεί στον μηχανισμό της «μαύρης λίστας» και ταυτόχρονα δεν θα μπορεί να επικοινωνεί με το δίκτυο.

Εικόνα 14 Η διαδρομή που διανεύει ένα πακέτο μέχρι το τελικό χρήστη[21].

3.4.2 – Ασφάλεια κατά τη σχεδίαση

3.4.2.1 – Λειτουργία Τοίχος - Ασφαλείας

Συνήθως οι συσκευές IoT χρησιμοποιούν το Διαδίκτυο για τη λειτουργία τους, όμως στην περίπτωση της τεχνολογίας του Sigfox δεν είναι απευθείας συνδεδεμένα στο Διαδίκτυο και δεν επικοινωνούν μαζί του. Χαρακτηριστικά, οι συσκευές του Sigfox δεν είναι συνδεδεμένες σε κανένα δίκτυο ή σε κάποιο σταθμό βάσης και η λειτουργία τους εξαρτάται από ένα ραδιοφωνικό μήνυμα. Πιο συγκεκριμένα, διαθέτει μια εσωτερική λειτουργία, όπου όταν χρειαστεί να διαβιβάσει ή να δεχθεί δεδομένα από το Διαδίκτυο, η συσκευή θα εκπέμψει το ραδιοφωνικό μήνυμα. Αυτό το μήνυμα λαμβάνεται στη συνέχεια από τον κοντινότερο συγκεντρωτή και μεταφέρεται στους εξυπηρετητές του Sigfox, το οποίο με τη σειρά του μεταφέρεται σε έναν προκαθορισμένο προορισμό ενός τελικού χρήστη.

Στην περίπτωση που η συσκευή χρειάζεται απάντηση από το σύστημα, υπάρχει λύση. Κατά τη διάρκεια ενός περιορισμένου χρονικού παραθύρου που είναι προκαθορισμένο από την αρχή της λειτουργίας στη συσκευή, το σύστημα μέσω των σταθμών βάσης έχει τη δυνατότητα να στείλει στη συσκευή αυτά που απαιτεί. Αυτός ο σχεδιασμός ασφαλείας φροντίζει να μην υπάρχει τρόπος οι συσκευές με αυθαίρετο τρόπο να στέλνουν δεδομένα μέσω του Διαδικτύου. Επομένως, προστατεύονται από επιθέσεις που προέρχονται από το Διαδίκτυο μέσω ενός πολύ αυστηρού τείχους προστασίας.

3.4.2.2 – Αποστολή - Λήψη δεδομένων και ασφάλεια

Τα μέτρα ασφάλειας για την αυθεντικοποίηση και την προστασία της ακεραιότητας των δεδομένων κατά την αποστολή τους και τη λήψη τους, είναι κρίσιμα για την απόκτηση εμπιστοσύνης ολόκληρου του συστήματος. Ο σχεδιασμός του πρωτοκόλλου Sigfox παρέχει αυτές τις λειτουργίες στα βασικά του χαρακτηριστικά. Σε αυτά δύνεται η δυνατότητα να συμπεριληφθεί ένα προαιρετικό μέτρο κατά της υποκλοπής των δεδομένων.

3.4.2.2.1 – Αυθεντικοποίηση

Κάθε πιστοποιημένη συσκευή της τεχνολογίας Sigfox, διαθέτει ένα μοναδικό συμμετρικό κλειδί ελέγχου ταυτότητας που τοποθετείται κατά τη πιστοποίηση της.

Κάθε μήνυμα που αποστέλλεται ή λαμβάνεται από μία συσκευή περιέχει ένα κρυπτογραφικό διακριτικό που υπολογίζεται με βάση το κλειδί ελέγχου ταυτότητας. Η επαλήθευση του διακριτικού διασφαλίζει τον έλεγχο ταυτότητας του αποστολέα στα μηνύματα ανερχόμενης (uplink) και κατερχόμενης (downlink) ζεύξης από το δίκτυο αλλά και την ακεραιότητα των δεδομένων.

Ακόμα, εκτός του δικτύου Sigfox, στο επικοινωνιακό σύστημα μεταξύ των τελικών χρηστών και των διεπαφών η αυθεντικοποίηση διασφαλίζεται με τους βασικούς τρόπους προστασίας όπως του VPN ή του HTTPS.

3.4.3 – Ασφάλεια στην αρχιτεκτονική δικτύου

3.4.3.1 – Πιστοποιημένες συσκευές Sigfox

Όπως αναφέραμε και παραπάνω, οι συσκευές που χρησιμοποιεί το Sigfox, αποθηκεύουν ένα μοναδικό κλειδί ελέγχου ταυτότητας. Η μοναδικότητα του κλειδιού αποτελεί μια πού σημαντική ιδιότητα που ακόμα και στη περίπτωση που μία συσκευή εκτεθεί από κάποια κακόβουλη οντότητα δεν θα υπάρξει κάποιο σημαντικό αντίκτυπο στο σύστημα. Παρόλα αυτά, πρακτικές ασφαλείας έχουν αναπτυχθεί και η ασφαλής αποθήκευση του κλειδιού είναι απαραίτητη από τον σχεδιαστή συσκευών. Η εταιρεία Sigfox συνεργάζεται με τα συστήματα της για να αυξήσει το επίπεδο ασφάλειας των συσκευών μέσω της υιοθέτησης βέλτιστων πρακτικών ασφαλείας. Η δημιουργία νέων συσκευών αποτελεί βασικό στόχο της Sigfox για την παροχή ασφάλειας στο επίπεδο των συσκευών.

3.4.3.2 – Σταθμοί βάσης

Οι συγκεντρωτές (Gateways) ή αλλιώς σταθμοί βάσης (Base stations) διαθέτουν στο σύστημα τους διαπιστευτήρια για να επικοινωνούν με τους εξυπηρετητές και γενικά με το δίκτυο. Οι πλέον σύγχρονες προσεγγίσεις βασίζονται στη Μονάδα αξιόπιστης πλατφόρμας (Trusted Platform Module - TPM) και εξασφαλίζοντας την ασφαλή επικοινωνία.

3.4.3.3 – Εξυπηρετητές συστήματος Sigfox

Οι εξυπηρετητές που αποτελούν τον βασικό πύρινα του δικτύου Sigfox αποθηκεύουν τα κλειδιά ελέγχου ταυτότητας των συσκευών Sigfox καθώς και τα μεταδεδομένα που αποστέλλονται μεταξύ των συσκευών και του δικτύου. Έχουν αναπτυχθεί λύσεις ώστε να υπάρχει όσο το δυνατόν μεγαλύτερη εξασφάλιση της

ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητας αυτών των μεταδεδομένων. Το Sigfox για να μπορέσει να είναι ανταγωνιστικό, έχει δημιουργήσει μια διαδικασία συνεχούς βελτίωσης για να διασφαλιστεί ότι το ο βασικός πυρήνας του δικτύου συμμορφώνεται με τους τοπικούς κανονισμούς.

3.4.4 – Ασφάλεια πακέτων

3.4.4. – Αριθμός ακολουθίας

Ο αριθμός ακολουθίας αποτελεί ένα μηχανισμό του Sigfox που σε συνεργασία με τον κωδικό ελέγχου γνησιότητας μηνύματος (Message Authentication Code - MAC) χρησιμοποιούνται για την αντιμετώπιση επιθέσεων επαναλαμβανόμενων πακέτων. Πρόκειται για έναν απλό μετρητή μηνυμάτων που ξεκινά από το μηδέν μέχρι έναν ακέραιο αριθμό που είναι ο αριθμός μηνυμάτων που έχουν σταλθεί.

Ο βασικός πυρήνας του Sigfox και οι συγκεντρωτές του επαληθεύουν τον αριθμό ακολουθίας, και ανάλογα το αποτέλεσμα επιτρέπουν το πακέτο να περάσει στους συγκεντρωτές ή το απορρίπτουν. Η ακεραιότητα του μετρητή διασφαλίζεται από το ελέγχου ταυτότητας μηνύματος.

Υπάρχει ένα εύρος αριθμών που μπορεί να έχει ο αριθμός ακολουθίας για να επικυρωθεί. Αυτό το εύρος είναι μεταξύ του αρχικού επικυρωμένου αριθμού ακολουθίας προσθέτοντας τον αριθμό ένα (1) και του τελευταίου επικυρωμένου αριθμού ακολουθίας προσθέτοντας πέρα από τον αριθμό ένα (1) το επίπεδο συνδρομής επί τρία (3), το επίπεδο αυτό αντιστοιχεί στο μέγιστο αριθμό μηνυμάτων που παράγονται από τη συσκευή την ημέρα με ελάχιστη τιμή το είκοσι.

Για παράδειγμα, εάν ο τελευταίος επικυρωμένος αριθμός ακολουθίας ήταν 5, το εύρος αριθμών για τον επόμενο αριθμό ακολουθίας θα είναι σύμφωνα με το επίπεδο συνδρομής, όπου εάν το επίπεδο συνδρομής διαθέτει 140 μηνύματα την ημέρα, ο αριθμός ακολουθίας πρέπει να είναι μεταξύ 6 και 426 (6 + 3 x 140), ενώ αν διαθέτει ένα μήνυμα την ημέρα θα είναι μεταξύ 6 και 26 γιατί παράγονται λιγότερο από είκοσι την ημέρα.

3.4.4.2 – Κωδικός ελέγχου γνησιότητας μηνύματος – MAC

Για να μπορέσει το σύστημα του Sigfox να διασφαλίσει ότι το μήνυμα έχει αποσταλεί από μία συγκεκριμένη συσκευή, χρησιμοποιείται ο κωδικός ελέγχου

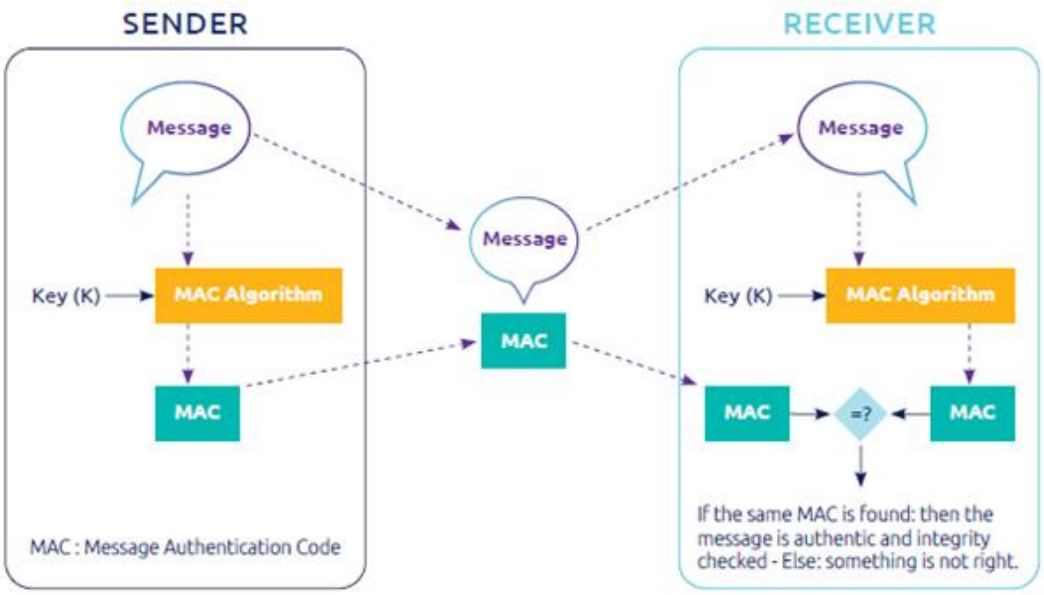
γνησιότητας μηνύματος ή αλλιώς MAC (Message Authentication Code). Ο κωδικός αυτός, παρέχει στους συγκεντρωτές τα στοιχεία ταυτότητας και ακεραιότητας. Ο αλγόριθμός με τον οποίο παράγεται ο κωδικός αυτός, έχει σαν παραμέτρους[22]:

- Το μήνυμα που θα αποστέλλεται και πρέπει να γίνει ο έλεγχος ταυτότητας (ή μέρος αυτού).
- Το Κλειδί ελέγχου ταυτότητας δικτύου ή αλλιώς NAK (Network Authentication Key) που είναι ένα κλειδί που υπάρχει στις συσκευές.

Μέσω των παραπάνω παραμέτρων ο αλγόριθμος παράγει ένα διακριτικό σε κρυπτογραφική μορφή. Ακόμα θα πρέπει για να είναι επιτυχημένος ο αλγόριθμος να είναι σε θέση να δημιουργήσει ένα έγκυρο ζεύγος μηνυμάτων-ετικετών όπου η ετικέτα δεν έχει παραχθεί από τον αποστολέα. Δηλαδή η τιμή δεν πρέπει να είναι προβλέψιμη. Το κυριότερο είναι να αποφευχθεί η αμελητέα πιθανότητα ότι δύο διαφορετικά μηνύματα θα παράγουν την ίδια ετικέτα.

Κάθε συσκευή διαθέτει ένα μοναδικό συμμετρικό κλειδί ελέγχου ταυτότητας δικτύου (NAK) κατά τη διάρκεια της κατασκευής. Με βάση αυτό το κλειδί ελέγχου ταυτότητας δημιουργείται ένα κρυπτογραφικό διακριτικό σε κάθε μήνυμα που αποστέλλεται ή λαμβάνεται από τη συσκευή. Η επαλήθευση του διακριτικού εξασφαλίζει τον έλεγχο ταυτότητας του αποστολέα που εφαρμόζεται για κάποιο μήνυμα ανερχόμενης ή κατερχόμενης ζεύξης. Στο επικοινωνιακό σύστημα μεταξύ των τελικών χρηστών και τον διεπαφών η αυθεντικοποίηση διασφαλίζεται με τους βασικούς τρόπους προστασίας όπως το VPN ή το HTTPS.

Σαν συμπέρασμα μπορούμε να πούμε ότι κωδικός ελέγχου γνησιότητας μηνύματος – MAC διασφαλίζει την ακεραιότητα ενός μηνύματος και την αυθεντικοποίηση του αποστολέα. Η διαδικασία του αλγορίθμου φαίνεται και στην εικόνα 15



Εικόνα 15 Η διαδικασία του αλγορίθμου MAC[22].

3.4.4.2.1 – Κρυπτογράφηση πακέτων

Όπως αναφέραμε παραπάνω, στο Sigfox από προεπιλογή τα δεδομένα μεταφέρονται στον αέρα χωρίς κρυπτογράφηση. Ωστόσο, ανάλογα με την εφαρμογή, τα δεδομένα αυτά μπορεί να είναι πολύ ευαίσθητα και πρέπει να διασφαλίζεται η ιδιωτικότητα τους.

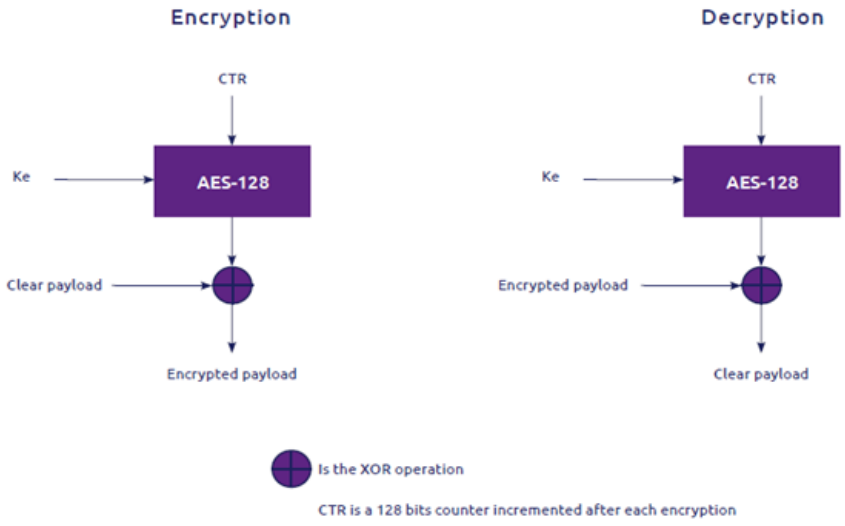
Ωστόσο, η τεχνολογία του Sigfox παρέχει στους πελάτες τη δυνατότητα είτε να εφαρμόσουν τις δικές τους λύσεις κρυπτογράφησης από άκρο σε άκρο είτε να βασιστούν σε μια λύση κρυπτογράφησης που παρέχεται από το πρωτόκολλο Sigfox. Η λύση κρυπτογράφησης του πρωτοκόλλου σχεδιάστηκε ειδικά για τα πακέτα που παράγει σε συνεργασία με την CEA-LETI, όπου το κλειδί κρυπτογράφησης προέρχεται από το κλειδί της συσκευής. Η κρυπτογράφηση θα χρησιμοποιεί NAK που είναι ουσιαστικά το κλειδί της συσκευής, τον μετρητή ακολουθίας και τον μετρητή ανατροπής (roll-over counter - ROC).

3.4.4.2.2 – Κρυπτογράφηση των δεδομένων

Η υπηρεσία κρυπτογράφησης των δεδομένων προσφέρεται από τον πάροχο του συστήματος. Σε αυτή την περίπτωση, ο τελικός χρήστης εμπιστεύεται τη τεχνολογία Sigfox για τη κρυπτογράφηση των δεδομένων. Για να το πετύχει αυτό η κρυπτογράφηση των δεδομένων πραγματοποιείται μέσω του πρωτοκόλλου Sigfox

στη συσκευή, που από την κατασκευή της έχει τις κατάλληλες εντολές για να το πραγματοποιήσει. Η αποκρυπτογράφηση γίνεται στον βασικό πυρήνα του δικτύου Sigfox, και η αποκρυπτογραφημένη πληροφορία παραδίδεται με τη χρησιμοποίηση ασφαλών χειρισμών των διεπαφών στον τελικό χρήστη.

Ο αλγόριθμος κρυπτογράφησης που χρησιμοποιείται είναι ο AES-128 σε λειτουργία μετρητή (CTR), που μπορούμε να δούμε στην εικόνα 16.



Εικόνα 16: Η μέθοδος αποκρυπτογράφησης AES-128 CTR. [21]

3.5 – Μηχανισμοί Ασφαλείας NB-IoT

3.5.1 – Πρότυπα 3GPP -Έκδοση 13η

Όπως αναφέρθηκε και στο παραπάνω κεφάλαιο η τεχνολογία του NB-IoT βασίστηκε στην έρευνα του οργανισμού 3GPP *(Third Generation Partnership Project)* και συγκεκριμένα στο εγκεκριμένο πρότυπο της έκδοσης 13 [23] έχοντας σαν γνώμονα την Long-Term Evolution (LTE) 4G τεχνολογία. Ο μηχανισμός ασφαλείας είναι παράγωγο της Μονάδας Ταυτότητας Συνδρομητή (Subscriber Identity Module - SIM) που χρησιμοποιείται στις συσκευές IoT. Η τεχνολογία NB-IoT με την χρήση της SIM βασίζεται στην ασφάλεια από το σχεδιασμό και εξαλείφει την ανάγκη για κάθε σύστημα να διαθέτει ατομικούς και ανεξάρτητους μηχανισμούς ασφάλειας. Αυτό επιτυγχάνεται με τους παρακάτω μηχανισμούς ασφαλείας στο μέγιστο βαθμό ώστε τα δεδομένα που μεταδίδονται μέσω της τεχνολογίας NB-IoT να θεωρούνται απαραβίαστα.

3.5.2 – Πρότυπα 3GPP Έκδοση 14η

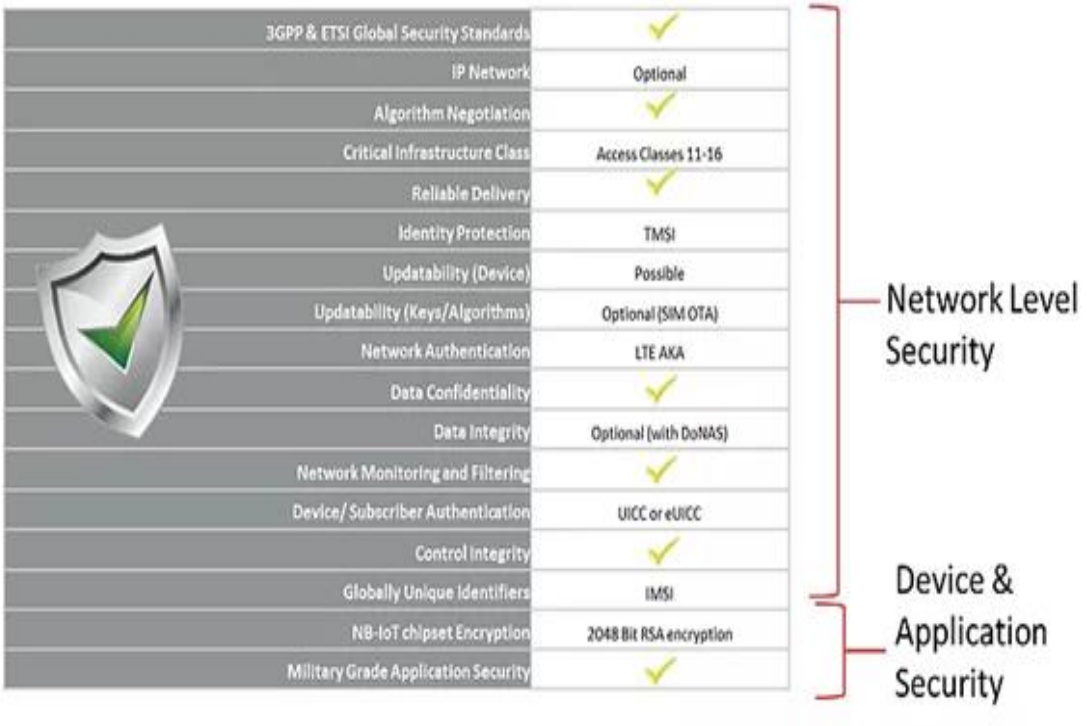
Η πιο πρόσφατη έρευνα και έκδοση του NB-IoT είναι το εγκεκριμένο πρότυπο 14 [24] όπου αναπτύσσει σε μεγαλύτερο βαθμό την ακρίβεια τοποθέτησης και το ρυθμό μετάδοσης δεδομένων. Η έκδοση 14 δεν έχει ακόμα εφαρμοστεί στις περιπτώσεις χρήσης του NB-IoT. Αποτελεί το πρώτο πρότυπο που συνδυάζει την τεχνολογία 4G LTE και 5G που στοχεύει στις εφαρμογές IoT και όταν εφαρμοστεί, θα παρέχει προηγμένα χαρακτηριστικά για δίκτυα Low Power Wide Area Network (LPWAN). Το πιο συμαντικό από τα χαρακτηριστικά αυτά είναι η αύξηση της ασφάλειας του δικτύου με την υλοποίηση της τεχνολογίας «ενσωματωμένης» SIM (eSIM), επιτρέποντας την παροχή διαπιστευτηρίων και των κλειδιών κρυπτογράφησης μέσω του αέρα (over-the-air OTA). Ακόμα ένα χαρακτηριστικό είναι η υλοποίηση των υπηρεσιών εντοπισμού χωρίς την χρήση του Παγκόσμιου Συστήματος Τοποθεσίας (Global Positioning System GPS) καθώς οι συσκευές του NB-IoT δικτύου παρέχουν ακρίβεια τοποθέτησης 50 μέτρων χωρίς την ενσωμάτωση GPS. Επιπλέον, ο μέγιστος ρυθμός μετάδοσης της ανερχόμενης και κατερχόμενης ζεύξης θα αυξηθεί σε 157 Kbit/s και 102 Kbit/s αντιστοίχως το οποίο

είναι κατά πολύ μεγαλύτερο από της προηγούμενες εκδόσεις. Η υποστήριξη αυτής της τεχνολογίας της ενσωματωμένης SIM είναι απαραίτητη για την ασφάλεια σε IoT δίκτυα. Συνεπώς η έκδοση 14 αποτελεί μία απαραίτητη προϋπόθεση για την ασφάλεια στο δίκτυο NB-IoT. Παρακάτω βλέπουμε τον πίνακα 2 με τα χαρακτηριστικά που αναφέρθηκαν στην παράγραφο.

Πίνακας 2 Χαρακτηριστικά της έκδοσης 14 [25]

NB-IoT Release 14 enhancements	
Position Tracking	Positioning support (E-CID, UTDOA or OTDOA)
Firmware and software updates, group message delivery	Multicast Support
Better service continuity	Enhanced connected mode mobility for service continuity
Competitive wearables support	Lower device Tx power (~14 dBm) for power and cost optimized wearables (at cost of coverage)
Capacity Enhancements	Optimized multicarrier NB-IoT operations

Σύμφωνα με την εικόνα 17, μπορούμε να ξεχωρίσουμε σε υποενότητες την συγκεκριμένη ενότητα των χαρακτηριστικών ασφαλείας του NB-IoT. Για την αυθεντικοποίηση των συσκευών του NB-IoT αναφέρονται τα βασικά χαρακτηριστικά των ενσωματωμένων Μονάδων Ταυτότητας Συνδρομητή (eUICC). Για την αυθεντικοποίηση του δικτύου αναλύεται η λειτουργία αυθεντικοποίησης AKA των δικτύων LTE. Τέλος για την προστασία της ταυτότητας αναφέρεται η λειτουργία TMSI.



Εικόνα 17 Αρχιτεκτονική των χαρακτηριστικών ασφαλείας του NB-IoT [26].

3.5.3 – Αυθεντικοποίηση των συσκευών

Η τεχνολογία του NB-IoT όπως αναφέραμε παραπάνω κληρονομεί την ασφάλεια που διαθέτει ο οργανισμός 3GPP, η οποία μέσω κάρτας SIM (ή αλλιώς όπως θα βλέπουμε παρακάτω universal integrated circuit card -UICC) που είναι τοποθετημένη στις συσκευές εξασφαλίζει την αυθεντικότητα μέσω της πιστοποίησης ταυτότητας, την προστασία σημάτων και την κρυπτογράφηση πακέτων [27].

3.5.3.1 – Μονάδα Ταυτότητα Συνδρομητή(SIM-UICC)

Η SIM χειρίζεται την αυθεντικότητα της συσκευής στο δίκτυο. Διασφαλίζει δηλαδή τον έλεγχο ταυτότητας και την ασφάλεια σε ένα δίκτυο κινητής τηλεφωνίας, η συσκευή που έχει τοποθετημένη μια κάρτα SIM λειτουργεί αποτελεσματικά ως ένας αξιόπιστος συγκεντρωτής και διασφαλίζει την ασφαλή πρόσβαση του δικτύου για κάθε πακέτο.

3.5.3.2 – Ενσωματωμένη Μονάδα Ταυτότητας Συνδρομητή (eSIM - eUICC)

Η τεχνολογία της ενσωματωμένης SIM, είναι τοποθετημένη στο κύριο κύκλωμα μίας τελικής συσκευή. Η κάρτα - μονάδα αυτή δεν διαθέτει συγκεκριμένα διαπιστευτήρια αλλά μέσω της διαδικασίας ενεργοποίησης μέσω αέρα μπορούν να της δοθούν. Ένα ακόμα βασικό χαρακτηριστικό της τεχνολογίας αυτής είναι ότι οι ενσωματωμένες κάρτες δεν μπορούν να αφαιρεθούν από τη συσκευή.

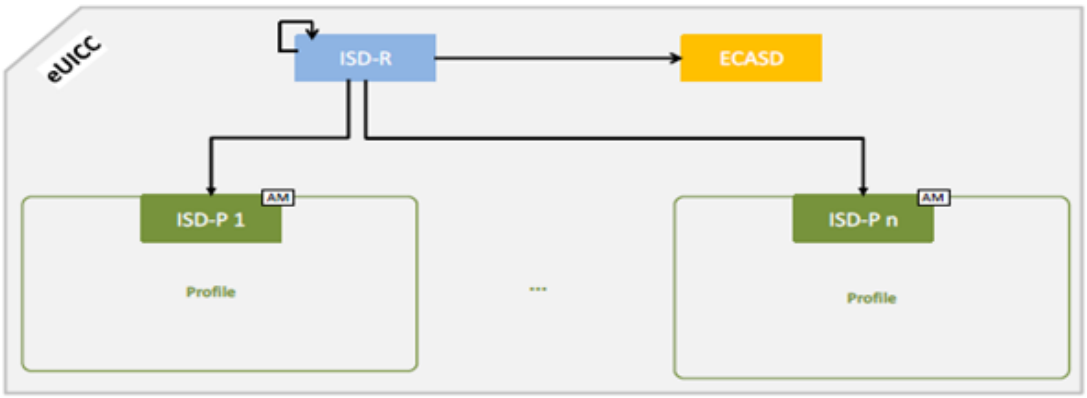
3.5.3.3 – Απομακρυσμένη ενεργοποίηση της ενσωματωμένης SIM (eUICC)

Η απομακρυσμένη ενεργοποίηση είναι μια προδιαγραφή που έχει δημιουργηθεί και εφαρμοστεί μέσω της GSMA (Global System for Mobile Communications association), η οποία επιτρέπει στους παρόχους των συστημάτων που χρησιμοποιούν την τεχνολογία NB-IoT, να ενεργοποιούν εξ αποστάσεως την μονάδα ταυτότητας συνδρομητή που είναι ενσωματωμένη σε μια τελική συσκευή όπως για την περίπτωση χρήση της έξυπνης τηλεμέτρησης νερού στην ηλεκτροβάνα και στο υδρόμετρο.

3.5.3.4 – Αρχιτεκτονική μηχανισμών της eUICC

Στην έκθεση της GSMA [28] μπορούμε να δούμε την αρχιτεκτονική μηχανισμών της ενσωματωμένης μονάδας ταυτότητας συνδρομητή (eUICC), όπου παραθέτονται παρακάτω και αποτελούν τον βασικό πυρήνα του μηχανισμού ταυτοποίησης χρήστη και αυθεντικότητας του δικτύου για την τεχνολογία NB-IoT.

Η αρχιτεκτονική της eUICC περιλαμβάνει συγκεκριμένους μηχανισμούς διαχείρισης των διαδρομών και των προφίλ όπως μπορούμε να τα δούμε και στη εικόνα 18 για την διαχείριση του συστήματος. Αρχικά βλέπουμε τον μηχανισμό του εκδότη ασφαλέστερης διαδρομής (Issuer Security Domain Root - ISD-R) που αντιπροσωπεύεται από τον διαχειριστή της ασφαλής δρομολόγησης (Subscription Manager Secure Routing - SM-SR). Ακόμα διαθέτει την αρχή ελέγχου της eUICC (eUICC Controlling Authority Security Domain – ECASD) που αντιπροσωπεύεται από τον εξουσιοδοτημένο εκδότη-πάροχο (Certificate Issuer - CI). Τέλος διαθέτει τον μηχανισμό του προφίλ εκδότη (Issuer Security Domain Profile - ISD-P) που με τη σειρά του αντιπροσωπεύεται από τον διαχειριστή προετοιμασίας δεδομένων (Subscription Manager Data Preparation SM-DP), μία ενσωματωμένη κάρτα ταυτότητας συνδρομητή μπορεί να διαθέτει παραπάνω από ένα προφίλ εκδότη.



Εικόνα 18 Αρχιτεκτονική μηχανισμών της eUICC[28]

3.5.3.4.1 – Εκδότης ασφαλέστερης διαδρομής - ISD-R

Στην ενσωματωμένη κάρτα ταυτότητας συνδρομητή μπορεί να υπάρξει όπως είναι λογικό, μόνο ένα ISD-R. Ο μηχανισμός αυτός ενεργοποιείται και εγκαθιστάτε στην κάρτα από τον κατασκευαστή της (eUICC Manufacturer – EUM) κατά τη παραγωγή της. Μετά τη διαδικασία αυτή, ο μηχανισμός όπως ορίζεται στα χαρακτηριστικά που μπορούμε να βρούμε στην ενότητα 5.3 στο [29], ενεργοποιείται και αρχίζει ο κύκλος ζωής της διαδρομής που έχει δημιουργηθεί. Ο μηχανισμός αυτός είναι σε θέση να διαχειρίζεται μόνο τις λειτουργίες της πλατφόρμας για το μηχανισμό ασφαλείας των προφίλ εκδότη (ISD-Ps)

3.5.3.4.2 – Αρχή ελέγχου της eUICC – ECASD

Όπως και για το ISD-R, για κάθε μία ενσωματωμένη κάρτα ταυτότητας συνδρομητή μπορεί να υπάρξει μόνο μία αρχή ελέγχου eUICC, όπου επίσης ενεργοποιείται και εγκαθιστάται στην κάρτα από τον κατασκευαστή της κατά τη παραγωγή της και ορίζεται στα χαρακτηριστικά που μπορούμε να βρούμε στην επίσης στην ενότητα 5.3 στο [29] και τέλος ενεργοποιείται και αρχίζει ο κύκλος ζωής της.

Η αρχή ελέγχου συμμετέχει ενεργά με τις λειτουργίες του διαχειριστή της ασφαλής δρομολόγησης όπου και εγκαθιστά το προσωπικό κλειδί για την πιθανότητα αλλαγής της. Αλλά και με του διαχειριστή προετοιμασίας δεδομένων όπου και εγκαθιστά το προσωπικό κλειδί για την λήψη και την εγκατάσταση.

Στην διαδικασία παραγωγής της ενσωματωμένης κάρτας ταυτότητας συνδρομητή, η αρχή ελέγχου μέσω του κατασκευαστή της κάρτας, διαθέτει ένα δημόσιο κλειδί του εξουσιοδοτημένου παρόχου για την επαλήθευση πιστοποιημένων υπογραφών (PK.CI.ECDSA – Public Key of the CI in the ECASD for verifying certificate signatures), ένα ιδιωτικό κλειδί της αρχής ελέγχου που χρησιμοποιεί ο αλγόριθμος κρυπτογράφησης ECKA (Elliptic Curve cryptography Key Agreement algorithm), μία πιστοποίηση για την αυθεντικοποίηση και την δημιουργία κλειδιών της κάρτας eUICC(CERT.ECASD.ECKA for eUICC Authentication and key establishment) και τέλος τη ταυτότητα της κάρτας eUICC (eUICC-IDEID).

3.5.3.4.3 – Προφίλ Εκδότη - ISD-P

Ένας μηχανισμός όπως είναι το προφίλ εκδότη μπορεί να υποστηρίξει μόνο ένα προφίλ. Για κάθε ενσωματωμένη κάρτα ταυτότητας μπορεί να υπάρχουν παραπάνω από ένα ISD-P αλλά μόνο ένα ενεργοποιημένο.

Το προφίλ εκδότη εγκαθίσταται μέσω του εκδότη ασφαλέστερης διαδρομής και στη συνέχεια εξατομικεύεται από το διαχειριστή προετοιμασίας δεδομένων. Τουλάχιστον ένας μηχανισμός προφίλ εκδότη με ένα ενεργοποιημένο προφίλ έχει εγκατασταθεί τη πρώτη φορά από τον κατασκευαστή κατά τη διάρκεια της κατασκευής της κάρτας ώστε να καταστεί δυνατή η μελλοντική σύνδεση της eUICC. Ένας μηχανισμός προφίλ εκδότη παραμένει συνδεδεμένο για όλο τον κύκλο ζωής του με το μηχανισμό εκδότη ασφαλέστερης διαδρομής.

3.5.3.4.4 – Ταυτότητα της ενσωματωμένης μονάδας ταυτότητας eUICC - EID

Η ταυτότητα EID της κάρτας eUICC αποτελεί τη μονάδα ταυτοποίησης της και χρησιμοποιείται για την απομακρυσμένη ενεργοποίηση και διαχείριση της. Είναι αποθηκευμένη όπως αναφέρθηκε παραπάνω στον μηχανισμό Αρχής ελέγχου της eUICC. Παρέχεται η δυνατότητα να ανακτηθεί από οποιαδήποτε συσκευή έχει την δυνατότητα να στείλει μια εντολή GET DATA προς τον μηχανισμό της αρχής ελέγχου.

3.5.3.5 – Χαρακτηριστικά ασφαλείας της eUICC

Η ενότητα αυτή παρέχει μια γενική εικόνα των χαρακτηριστικών ασφάλειας των τεχνολογιών όπως το NB-IoT που χρησιμοποιούν τον μηχανισμό eUICC. Αρχικός στόχος της ενσωματωμένης ταυτότητας είναι να διασφαλίσει το επίπεδο ασφαλείας που προσφέρει η τρέχουσα μονάδα ταυτότητας (SIM-UICC) ώστε σύμφωνα με την αρχιτεκτονική της να αναπτυχθεί περαιτέρω καθώς οι ανάγκες για ασφάλεια αυξάνονται διαρκώς.

Οι μηχανισμοί ασφαλείας που διαθέτει η eUICC εφαρμόζονται στους διάφορους φορείς και ρόλους όπως είναι ο τελικός χρήστης, ο κατασκευαστής (EUM), ο

διαχειριστής προετοιμασίας δεδομένων (SM-DP), ο διαχειριστής της ασφαλής δρομολόγησης (SM-SR) αλλά και του εξουσιοδοτημένου παρόχου (CI). Κάθε ρόλος θεωρείται ως στοιχείο που ανήκει σε έναν κρίσιμο τομέα για το σύστημα και πρέπει να πληροί τα κατάλληλα κριτήρια πιστοποίησης του συστήματος.

Σύμφωνα πάντα με την έκθεση [28] κάθε διαχειριστής πιστοποιείται σύμφωνα με ένα σύστημα πιστοποίησης που έχει συμφωνηθεί από την GSMA, η ενσωματωμένη κάρτα πρέπει επίσης να πιστοποιείται σύμφωνα με το σύστημα προστασίας προφίλ της GSMA αλλά και ο κατασκευαστής να είναι πιστοποιημένος από την SAS. Η προστασία των πακέτων και των δεδομένων των οντοτήτων που αναφέρθηκαν πρέπει να διασφαλίζεται, που συνεπάγεται ότι η επικοινωνία μεταξύ των οντοτήτων και του συστήματος πρέπει να διασφαλίζει την αυθεντικοποίηση και την ακεραιότητα τους. Για να επιτευχθεί αυτό για όλες τις διαδικασίες που περιγράφονται, τα πεδία ασφαλείας είναι ταυτοποιημένα και έχουν εφαρμόσει τους βασικούς αλγορίθμους κρυπτογράφησης τουλάχιστον.

3.5.3.5.1 – Εξουσιοδοτημένος χρήστης (Certificate Issuer CI)

Ο εξουσιοδοτημένος χρήστης (CI) που αναφέρθηκε παραπάνω, διαθέτει έναν συγκεκριμένο ρόλο. Ο ρόλος αυτός είναι η έκδοση των πιστοποιητικών για τις λειτουργίες της απομακρυσμένης ενεργοποίησης της eUICC και ταυτόχρονα βοηθάει στην ταυτοποίηση των διαφόρων οντοτήτων του συστήματος. Παρέχει πιστοποιητικά ρίζας (Root Certificate) που χρησιμοποιούνται για την ταυτοποίηση των πιστοποιητικών που έχουν εκδοθεί από τον ίδιο, παρέχει επίσης ένα δημόσιο κλειδί που είναι κομμάτι του πιστοποιητικού ρίζας και χρησιμοποιείται στην eUICC για την ταυτοποίηση των πιστοποιητικών. Ακόμα διαθέτει ένα πιστοποιητικό (CERT.DP.ECDSA) για την αυθεντικοποίηση του διαχειριστή προετοιμασίας δεδομένων (SM-DP) όπου χρησιμοποιείται για την διαδικασία φόρτωσης και εγκατάστασης προφίλ. Άλλα δύο πιστοποιητικά διατίθενται μέσω του CI, το πρώτο (CERT.SR.ECDSA) είναι για την αυθεντικοποίησης του διαχειριστή ασφαλής δρομολόγησης (SM-DR) και χρησιμοποιείται για την διαδικασία “SM-SR change”, και το δεύτερο για την αυθεντικοποίηση του κατασκευαστή (EUM), όπου και χρησιμοποιείται για την διαδικασία λήψης και εγκατάστασης προφίλ.

3.5.3.5.2 – Αλγόριθμοι και μεγέθη κλειδιών

Η μονάδα ταυτοποίησης χρήστη χρησιμοποιεί δύο αλγορίθμους κρυπτογράφησης για την διαδικασία διασφάλισης της ακεραιότητας των δεδομένων. Οι αλγόριθμοι αυτοί αποτελούν αποτελέσματα έρευνας διαφόρων οργανισμών ασφαλείας όπως για παράδειγμα του NIST: SP 800-57 Μέρος 1: Recommendation for Key Management [30] και του BSI: TR-02102: Kryptographische Verfahren: Empfehlungenund Schlüssellängen[31].

Οι πιο γνωστοί αλγόριθμοι που υλοποιούνται στη eUICC και ταυτόχρονα και στο πρωτόκολλο του NB-IoT είναι η συμμετρική λειτουργία της μεθόδου AES που είδαμε και στο πρωτόκολλο LoRaWAN με μέγεθος κλειδιού 128bits αλλά και της ασύμμετρης μεθόδου RSA (Rivest – Shamir – Adleman) που είναι ένα από τα πρώτα συστήματα κρυπτογράφησης δημόσιου κλειδιού και χρησιμοποιείται ευρέως για ασφαλή μετάδοση δεδομένων με μέγεθος κλειδιού 2048bits

3.5.4 – Αυθεντικοποίηση Δικτύου

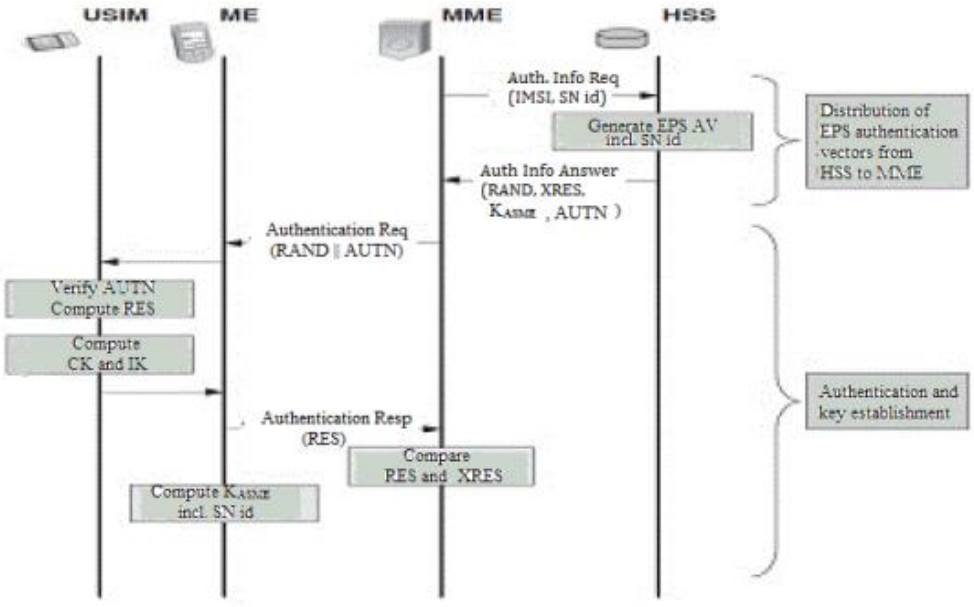
Όπως αναφέρθηκε και παραπάνω η τεχνολογία του NB-IoT αποτελεί πρότυπο του 3GPP που συνδέεται στενά με το LTE και κληρονομεί όλες τους μηχανισμούς ασφαλείας που συνδέονται με αυτό. Η χρησιμοποίηση ενός ιδιωτικού κλειδιού το οποίο είναι τοποθετημένο στην κάρτα που διαθέτουν οι συσκευές του NB-IoT κατά τη διάρκεια κατασκευής τους, χρησιμοποιείται για την ταυτόχρονη πιστοποίηση του δικτύου και της συσκευής. Μία εξίσου σημαντική λειτουργία του κλειδιού αυτού, είναι η δημιουργία συχνά ενημερωμένων κλειδιών συνόδου για την κρυπτογράφηση των δεδομένων μεταξύ της συσκευής και του βασικού πυρήνα δικτύου της τεχνολογίας NB-IoT[32].

3.5.4.1 – Έλεγχος ταυτότητας και συμφωνία κλειδιού AKA LTE

Το πρωτόκολλο επεκτάσιμης ελέγχου ταυτότητας (EAP) είναι ένας μηχανισμός ελέγχου ταυτότητας των πακέτων που χρησιμοποιείται σε δίκτυα LTE. Ο έλεγχος ταυτότητας και συμφωνίας κλειδιού (Authentication and Key Agreement - AKA) είναι μία από τις λειτουργίες του EAP. Το πρωτόκολλο χρησιμοποιεί τον μηχανισμό ελέγχου ταυτότητας και κλειδιού που στηρίζεται σε μηχανισμούς πρόκλησης-απόκρισης (Challenge /response), το EAP-AKA για να μπορέσει να

χρησιμοποιηθεί από δίκτυα κινητής τηλεφωνίας τέταρτης γενιάς (LTE-4G) τροποποιείται και κληρονομείται από τρίτης γενιάς LTE ως εξελιγμένο σύστημα πακέτων (Evolved Packet System Authentication and Key Agreement EPS-AKA)και χρησιμοποιείται όταν ο χρήστης έχει πρόσβαση στο δίκτυο[33].

Ο μηχανισμός εξελιγμένου συστήματος πακέτων (EPS AKA) που φαίνεται και στην εικόνα 19 υλοποιείται με τη βοήθεια και τη συνεργασία τριών διεργασιών. Αρχικά η πρώτη διεργασία δημιουργεί διανύσματα αυθεντικοποίησης εξελιγμένου συστήματος πακέτων (EPS) στον εξυπηρετητή συνδρομητών (Home Subscriber Server - HSS) κατόπιν αιτήματος από την Οντότητα Διαχείρισης της Κινητικότητας (Entity Management Mobility - MME) όπου και τα διανέμει. Στην δεύτερη διεργασία αυθεντικοποιείται και καθιερώνεται ένα νέο κλειδί όπου διαμοιράζεται μεταξύ του δικτύου εξυπηρέτησης και του εξοπλισμού του χρήστη (user equipment UE). Στη τελευταία διεργασία εφαρμόζεται ο μηχανισμός για την διανομή των δεδομένων ελέγχου ταυτότητας στη λειτουργία τους αλλά και ανάμεσα των δικτύων εξυπηρέτησης[34].



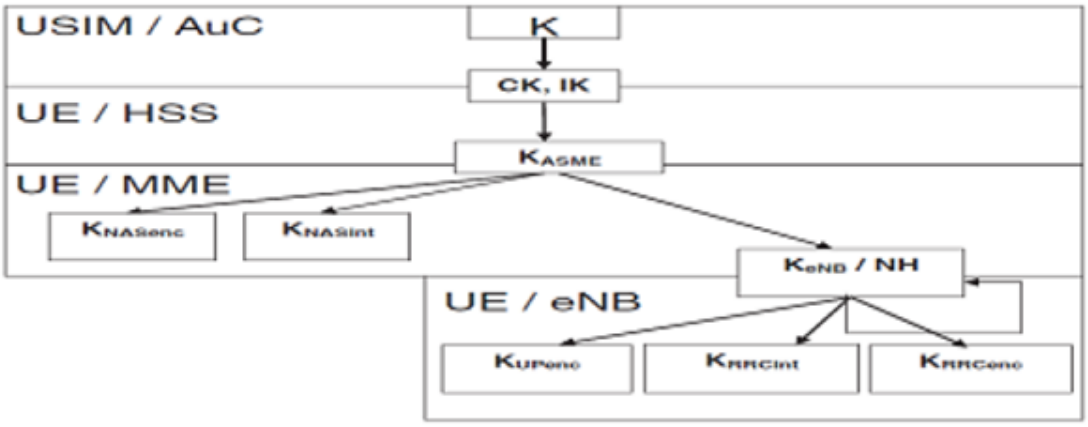
Εικόνα 19 Πρωτόκολλο EPS AKA [34].

3.5.4.1.1– Κλειδιά και η ιεράρχηση τους

Το ενδιάμεσο κλειδί βασικής διοικητικής οντότητας ασφαλούς πρόσβασης KASME (Key access security management entity), είναι το κύριο κλειδί από το οποίο προέρχονται όλα τα κλειδιά που απαιτούνται για διάφορους μηχανισμούς ασφαλείας στο πρωτόκολλο EPS AKA, το KASME αποτελεί επίσης και το κύριο τοπικό κλειδί για τον συνδρομητή. Στο δίκτυο, το παραπάνω κλειδί είναι αποθηκευμένο στην οντότητα διαχείρισης της κινητικότητας MME ενώ το μόνιμο κύριο κλειδί (MasterKey – K) αποθηκεύεται στο κέντρο ελέγχου ταυτότητας (AuC). Σύμφωνα με τα παραπάνω εμφανίζονται κάποια πλεονεκτήματα, όπως ότι είναι εφικτός ο διαχωρισμός του κρυπτογραφικού κλειδιού, όπου η χρήση κάθε κλειδιού για τη κρυπτογράφηση ενός πακέτου και η γνώση ενός κλειδιού δεν συνεπάγεται τη δεύτερη. Επίσης το σύστημα βελτιώνεται με τη συνεχή δημιουργία καινούργιων κλειδιών δηλαδή βοηθάει στην ανανέωση των κλειδιών που χρησιμοποιούνται στον μηχανισμό ασφαλείας. Στην περίπτωση που κάποιο κλειδί ανανεωθεί, το EPS AKA δεν χρειάζεται να εκτελείται κάθε φορά για τη διασφάλιση των ραδιοσυχνοτήτων [34].

Στον εξελιγμένο κόμβο B (Evolved Node B - eNB) αποθηκεύεται ακόμα ένα κλειδί το K(eNB) που με τη χρήση του, δύνεται η δυνατότητα ανανέωσης νέων κλειδιών για την προστασία της πρόσβασης των ραδιοσυχνοτήτων χωρίς να εμπλέκεται η οντότητα διαχείρισης της κινητικότητας.

Στην εικόνα 20 παρουσιάζεται η ιεράρχηση των κλειδιών που χρησιμοποιεί το EPS. Υπάρχει ένα κλειδί ρίζας K το οποίο είναι μια συμβολοσειρά τυχαίων δυαδικών ψηφίων και αποτελεί το κύριο κλειδί ενός συνδρομητή το οποίο είναι αποθηκευμένο στην SIM και στο AuC. Παρακάτω υπάρχουν τα ενδιάμεσα κλειδιά CK, IK 128-bit μεγέθους και προέρχονται από το K χρησιμοποιώντας πρόσθετες παραμέτρους εισόδου, από τα κλειδιά αυτά προέρχεται και το Kasme όπου χρησιμοποιείται ως τοπικό βασικό κλειδί που αναφέρθηκε παραπάνω. Το K(eNB) που προέρχεται με τη σειρά του από το Kasme και είδαμε παραπάνω, το NH που επίσης προέρχεται από το Kasme και χρησιμοποιείται για καταστάσεις παράδοσης. Τέλος τα KRRCenc, KRRCint, KUPenc χρησιμοποιούνται για την κρυπτογράφηση και ταυτόχρονα για την διασφάλιση της ακεραιότητας του ελέγχου πόρων ραδιοσυχνοτήτων (Radio Resource Control – RRC).



Εικόνα 20 Ιεράρχηση κλειδιών EPS AKA [34].

3.4.5 – Προστασία Ταυτότητας

Η πιστοποίηση και εμπιστευτικότητα ταυτότητας συνδρομητή, αλλά και η εμπιστευτικότητα των δεδομένων του χρηστών είναι οι βασικές πτυχές ασφάλειας στο GSM. Μέσω της ταυτότητας συνδρομητή κινητής τηλεφωνίας (IMSI) διασφαλίζεται η ταυτοποίηση του χρήστη. Αναλόγως του ηλεκτρονικού σειριακού αριθμού (Electronic serial number. – ESN) των συστημάτων όπως είναι το Προηγμένο Σύστημα Κινητών Τηλεφώνων (Advanced Mobile Phone System - AMPS) και το συνολικό σύστημα ελέγχου πρόσβασης (Total Access Communication System - TACS) οι παραπάνω πτυχές και η χρήση του μεμονωμένου κλειδιού πιστοποίησης Ki, αποτελούν ευαίσθητα διαπιστευτήρια αναγνώρισης. Οι ευαίσθητες αυτές πληροφορίες δεν μεταδίδονται ποτέ μέσω ραδιοσυχνοτήτων και για αυτό ευθύνεται ο σχεδιασμός των συστημάτων ελέγχου ταυτότητας και κρυπτογράφησης του GSM. Για την επίτευξη της αυθεντικοποίησης χρησιμοποιείται ένας μηχανισμός πρόκλησης-απόκρισης (challenge/response). Με την χρήση ενός προσωρινού κλειδιού κρυπτογράφησης Kc που δημιουργείται με τυχαίο μηχανισμό, η επικοινωνία διασφαλίζεται μέσω της κρυπτογράφησης. Για την πραγματοποίηση της ταυτοποίησης ενός κινητού σταθμού (mobile Moving Station – MS) χρησιμοποιείται ο μηχανισμός προσωρινής κινητής ταυτότητας συνδρομητή (Temporary Mobile Subscriber Identity - TMSI) η οποία εκδίδεται από το δίκτυο και μπορεί να αλλάζει περιοδικά για πρόσθετη ασφάλεια [35].

3.4.5.1 – TMSI

Το NB-IoT χρησιμοποιεί την τεχνολογία του TMSI για την προστασία της ταυτότητας των τελικών συσκευών και του διακομιστή. Πρωτόκολλα όπως είναι η τεχνολογία των IoT και συγκεκριμένα των LPWAN τα οποία διαχειρίζονται ευαίσθητες πληροφορίες των τελικών χρηστών, είναι απαραίτητο να περιλαμβάνουν μηχανισμούς διασφάλισης μέσω πιστοποιητικών της ιδιωτικής ζωής. Στη τεχνολογία του NB-IoT χρησιμοποιείται ο μηχανισμός TMSI, ο οποίος χρησιμοποιήθηκε από τον οργανισμό 3GPP για να απευθύνονται οι τεχνολογίες στις κινητές συσκευές αντί του μηχανισμού διεθνούς ταυτότητας συνδρομητή κινητής τηλεφωνίας (International Mobile Subscriber Identity - IMSI) ο οποίος χρησιμοποιείται μόνο μία φορά κατά την ενεργοποίηση της συσκευής [26].

3.3 – Επίλογος κεφαλαίου

Στο κεφάλαιο αυτό, αναφέρθηκαν τα βασικά χαρακτηριστικά ασφαλείας των LPWAN. Στη συνέχεια πραγματοποιήθηκε μία τεχνική αναφορά των μηχανισμών ασφαλείας των πρωτοκόλλων LoRa, Sigfox, NB-IoT.

Η αποτελεσματική λειτουργία των συστημάτων αλλά και η διασφάλιση των προσωπικών δεδομένων των τελικών χρηστών, αποτελεί βασικό στόχο των LPWAN. Για την επίτευξη των στόχων τους, έχουν υλοποιηθεί και εμπλουτιστεί στο σύστημα τους, οι παραπάνω μηχανισμοί ασφαλείας.

Έχοντας εδραιωθεί στην αγορά, τα βασικά πρότυπα που αναφέρονται στην εργασία, αποτελούν πόλο έλξης επιθέσεων από κακόβουλες οντότητες. Οι επιθέσεις αυτές στοχεύουν στους μηχανισμούς ασφαλείας κάθε τεχνολογίας LPWAN με κύριο στόχο τη μείωση της λειτουργίας του συστήματος και την υποκλοπή των προσωπικών δεδομένων των τελικών χρηστών. Στο παρακάτω κεφάλαιο αναλύονται οι επιθέσεις που πραγματοποιούνται στα βασικά πρότυπα των LPWAN.

ΚΕΦΑΛΑΙΟ 4 – ΕΠΙΘΕΣΕΙΣ ΑΣΦΑΛΕΙΑΣ LPWAN

4.1 – Εισαγωγή

Στο αυτό το κεφάλαιο γίνεται μία αναφορά των επιθέσεων ασφαλείας που δέχονται τα δίκτυα LPWAN. Στη συνέχεια αναφέρονται οι επιθέσεις που δέχονται τα πρωτόκολλα όπως αναλύονται στην εργασία καθώς και παραδείγματα πειραμάτων τα οποία έχουν διεξαχθεί από έρευνες για την αποτελεσματική αντιμετώπιση τους.

Οι επιθέσεις, πραγματοποιούνται στους μηχανισμούς ασφαλείας που διαθέτει κάθε πρωτόκολλο και στα επίπεδα που υλοποιούνται. Τα δίκτυα LPWAN, διαθέτουν αποτελεσματικούς μηχανισμούς ασφαλείας. Παρόλα αυτά η κακόβουλη οντότητα που εκτελεί τις επιθέσεις έχει τις κατάλληλες γνώσεις αλλά και το κατάλληλο υλικό για να τις πραγματοποιήσει.

Στο τέλος κάθε υποκεφαλαίου, αναφέρεται μία επίθεση ασφαλείας, και παραθέτονται πιθανοί τρόποι αντιμετώπισης αυτών των απειλών που είτε πρόκειται για ενέργειες των διαχειριστών του δικτύου είτε για μηχανισμούς που έχουν αναπτυχθεί για κάθε σύστημα.

4.2 – Θέματα Ασφαλείας LPWAN

Τις επιθέσεις που δέχονται τα δίκτυα LPWAN τις διαχωρίζουμε σε δύο κατηγορίες σε φυσικές επιθέσεις και επιθέσεις δικτύου. Οι επιθέσεις αυτές μπορούν να εφαρμοστούν στα LPWAN πρωτόκολλα αναλόγως τον βαθμού ασφαλείας που διαθέτουν.

4.2.1 – Φυσικές Επιθέσεις

Οι επιθέσεις στη φυσική παρουσία των τελικών συσκευών γίνεται με κύριο σκοπό την έκθεση των κλειδιών του δικτύου τους. Ακόμα, η φυσική καταστροφή των συσκευών και η αποσύνδεσή τους από το δίκτυο αποτελεί ένα πρόβλημα για τη λειτουργία του συστήματος χωρίς να επηρεάσει όμως τις υπόλοιπες συσκευές.

4.2.1 – Έκθεση τελικών συσκευών και των κλειδιών τους

Μία κακόβουλη οντότητα με φυσική πρόσβαση στο χώρο των τελικών συσκευών ενδέχεται να τα θέσει σε κίνδυνο. Εάν η οντότητα αυτή αποκτήσει πρόσβαση σε μια συσκευή δικτύου, μπορεί να αποσπάσει τα κλειδιά της. Οι τελικές συσκευές διαθέτουν από τον κατασκευαστή τους, μία μονάδα ραδιοσυχνοτήτων και ένα μικροελεγκτή (micro controller unit MCU) για την λειτουργία και την επικοινωνία τους με το δίκτυο των LPWAN. Η μονάδα ραδιοσυχνοτήτων επικοινωνεί με τον μικροελεγκτή (MCU) μέσω μίας διασύνδεσης UART ή SPI. Οι εντολές και οι ανταλλαγές δεδομένων μεταξύ της μονάδας και του μικροελεγκτή μπορούν να παρεμποδιστούν και να υποκλαπούν χρησιμοποιώντας κατάλληλο υλικό.

Ακόμα, σε μια πιο απλή εκδοχή της επίθεσης αυτής, είναι η φυσική καταστροφή των συσκευών. Η φυσική επίθεση δεν θα προκαλέσει βλάβη στο δίκτυο αφού δεν επηρεάζει τις άλλες συσκευές που είναι συνδεδεμένες με τον συγκεντρωτή και τον εξυπηρετητή, καθώς δεν ανταλλάσουν μεταξύ τους πληροφορίες σε αντίθεση με τα δίκτυα πλέγματος (mesh networks). Σκοπός της επίθεσης αυτής, είναι να θέσει εκτός λειτουργίας την συσκευή, με αποτέλεσμα να μην στέλνει μηνύματα χρέωσης στον πάροχο. Ο πάροχος θα αντιληφθεί την καταστροφή της συσκευής διότι θα σταματήσει να δέχεται δεδομένα.

4.2.2 – Επιθέσεις Δικτύου

4.2.2.1 – Ενεργές επιθέσεις

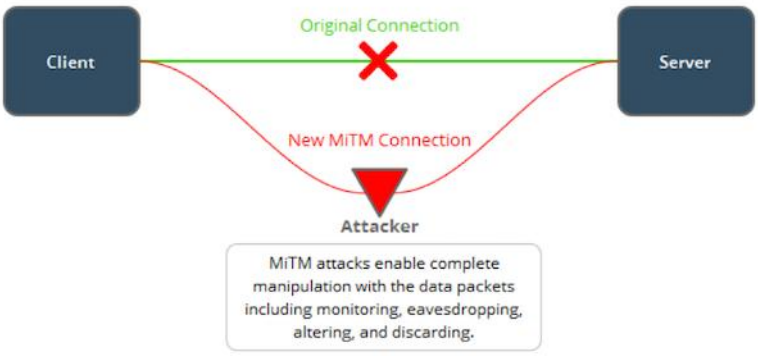
Μια ενεργή επίθεση (Active attack) είναι η ενέργεια που συνήθως πραγματοποιείται από μία κακόβουλη οντότητα όταν αναφερόμαστε στον όρο του "hacking". Κατά τη διάρκεια μιας ενεργής επίθεσης, μια κακόβουλη οντότητα έχει την δυνατότητα να εισάγει δικά της δεδομένα στο σύστημα καθώς και να μεταβάλει τα δεδομένα στο εσωτερικό των πακέτων που στέλνονται στο δίκτυο. Παρακάτω αναφέρονται διάφοροι τύποι των επιθέσεων αυτών:

4.2.2.1.1 – Επίθεση ενδιάμεσου ανθρώπου – Man in The Middle

Οι επιθέσεις ενδιάμεσου ανθρώπου είναι ένας κοινός τύπος επίθεσης στην ασφάλεια των δικτύων στον κυβερνοχώρο, μέσω της οποίας δίνεται η δυνατότητα

παρακολούθησης της επικοινωνίας μεταξύ δύο κόμβων από τον επιτιθέμενο. Όπως βλέπουμε και στην εικόνα 21, η επίθεση λαμβάνει χώρα ανάμεσα σε δύο νόμιμα επικοινωνούντες συσκευές-κόμβους, επιτρέποντας στον εισβολέα να παρακολουθεί μια συνομιλία που δεν επιτρέπεται να συμμετέχει, εξ ου και το όνομα ενδιάμεσος άνθρωπος «man-in-the-middle» [36].

Μια σοβαρή επίθεση που προκύπτει από την επίθεση ενδιάμεσου ανθρώπου είναι η επίθεση Μετατροπής Χαρακτήρα (Bit-Flipping Attack)**.** Η επίθεση αυτή έχει ως στόχο τη μέθοδο κρυπτογράφησης και το κείμενο που κρυπτογραφείται μέσω αυτής. Πετυχαίνοντας αυτό, ο εισβολέας μπορεί να αλλάξει το κείμενο με τέτοιο τρόπο ώστε να γνωρίζει τις αλλαγές που έκανε. Αντιθέτως, ανάλογα τον βαθμό δυσκολίας της κρυπτογραφικής μεθόδου ο εισβολέας μπορέι να μην γνωρίζει τον βαθμό που μετέτρεψε τον κείμενο. Αυτός ο τύπος επίθεσης δεν είναι απευθείας εναντίον της ίδιας της κρυπτογραφικής μεθόδου, αλλά εναντίον ενός συγκεκριμένου μηνύματος ή σειράς μηνυμάτων.



Εικόνα 21 Αναπαράσταση επιθέσεων ενδιάμεσου ανθρώπου[37].

4.2.2.1.2 – Τεχνικές Παρεμβολών - Jamming Techniques

Οι επιθέσεις παρεμβολών ή αλλιώς Jamming attacks, εκμεταλλεύονται τα κανάλια εκπομπής σήματος ενός δικτύου όταν αυτά συγχρονίζονται ή κατά τη διάρκεια της αυθεντικοποίησης, αναγκάζοντας τις συσκευές να χάσουν τη διασύνδεση τους με τα κανάλια, δηλαδή την επικοινωνία τους με το δίκτυο.

Η πιο γνωστή και ταυτοχρόνως πιο σοβαρή τεχνική επίθεσης παρεμβολής είναι η Άρνηση Παροχής Υπηρεσιών (Denial of Service). Σκοπός αυτών των επιθέσεων είναι να μειώσουν ή και να αχρηστεύσουν το δίκτυο που συνδέει τις τελικές συσκευές.

Για να καταφέρει μια κακόβουλη οντότητα την πραγματοποίηση μιας επίθεσης άρνησης υπηρεσιών σε δίκτυα LPWAN, χρειάζεται να εξαντλήσει τους πόρους που διαθέτει ένα δίκτυο με βασικό στόχο τους κόμβους αναμετάδοσης των σημάτων. Μια τέτοια επίθεση διευκολύνεται με το γεγονός ότι η αρχική επικοινωνία μεταξύ μίας τελικής συσκευής και του δικτύου εκτελείται πριν από τον έλεγχο ταυτότητας. Οπότε, στην περίπτωση της επίθεσης η συσκευή επαναλαμβάνει τα αντίστοιχα βήματα του πρωτοκόλλου για να επιτευχθεί η επικοινωνία, ζητώντας παράλληλα έγκριση από άλλα πρόσθετα κανάλια, χωρίς να καταφέρει να ολοκληρώσει τον κύκλο επικοινωνίας με το πρωτόκολλο και να απελευθερώσει τα κανάλια που χρησιμοποιούνται [38].

4.2.2.1.3 – Επίθεση Επανάληψης – Replay Attack

Η επίθεση επανάληψης ή αλλιώς Replay attack, είναι μια κατηγορία επίθεσης δικτύου κατά την οποία μία κακόβουλη οντότητα καταφέρνει μέσω άλλων επιθέσεων, όπως για παράδειγμα του ενδιάμεσου ανθρώπου, να υποκλέψει μια μετάδοση δεδομένων και να καθυστερήσει τη μετάδοση τους είτε να την επαναλαμβάνει με τον ρυθμό που επιθυμεί. Η καθυστέρηση ή η επανάληψη της διαβίβασης δεδομένων μπορεί να πραγματοποιηθεί από τον αποστολέα άθελα του είτε από τη κακόβουλη οντότητα, η οποία παρακολουθεί τα δεδομένα και τα αναμεταδίδει με δόλιο σκοπό. Οπότε, μια επίθεση επανάληψης είναι μια επίθεση στο πρωτόκολλο ασφαλείας επαναλαμβάνοντας δεδομένα από τον επιτιθέμενο

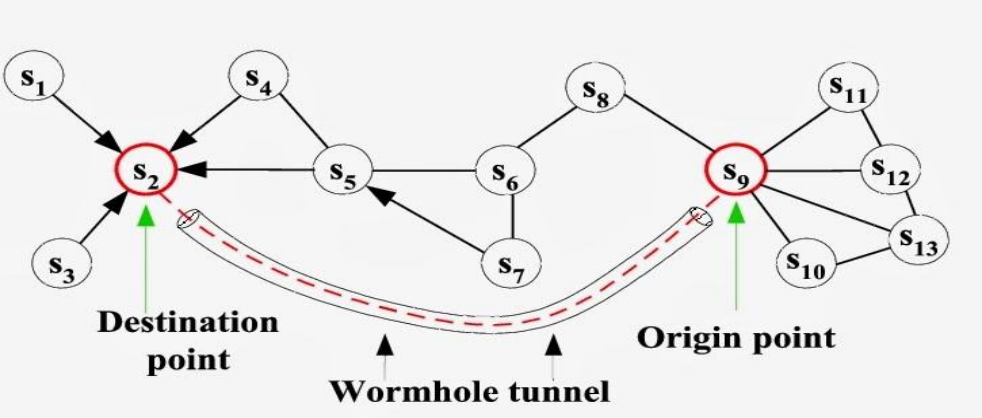
στο προοριζόμενο κόμβο. Με αυτό τον τρόπο εξαπατώνται οι συμμετέχοντες ώστε να πιστεύουν ότι έχουν ολοκληρώσει επιτυχώς τη μετάδοση δεδομένων ή ότι υπήρξε πρόβλημα στην επικοινωνία με αποτέλεσμα οι ίδιοι να επαναλαμβάνουν την αποστολή δεδομένων και να πραγματοποιούν άθελα τους επίθεση επανάληψης. Οι επιθέσεις επανάληψης βοηθούν τους επιτιθέμενους είτε να αποκτήσουν πρόσβαση σε ένα δίκτυο υποκλέπτοντας πληροφορίες που δεν θα ήταν εύκολα προσβάσιμες είτε να δημιουργήσουν σημαντικό πρόβλημα στο δίκτυο [39].

4.2.2.2 – Παθητικές επιθέσεις

Οι παθητικές επιθέσεις δηλώνουν την παθητική παρακολούθηση του δικτύου από τους επιτιθέμενους. Αυτό σε σύγκριση με μια ενεργή επίθεση που είδαμε παραπάνω, όπου ο εισβολέας προσπαθεί να εισέλθει στο σύστημα για να αποκτήσει πρόσβαση ή να αλλάξει δεδομένα. Παρόλο που μια τέτοιου είδους επίθεση ακούγεται λιγότερο επιβλαβής, η ζημιά στο τέλος μπορεί να είναι εξίσου σοβαρή. Παρακάτω αναφέρονται διάφοροι τύποι τέτοιων επιθέσεων:

4.2.2.2.1 – Επίθεση Σκουληκότρυπας –Wormhole Attack

Σε αυτόν τον τύπο επίθεσης, μία κακόβουλη οντότητα αντιγράφει ολόκληρο το πακέτο που στέλνεται μέσω δύο κόμβων, διοχετεύοντάς το στο ειδικά διαμορφωμένο δίκτυο της και ταυτόχρονα στη διάθεση της. Στη συνέχεια, ο εισβολέας μεταδίδει το πακέτο που έχει ήδη χρησιμοποιήσει στον κόμβο προορισμού και στον χρόνο που επιθυμεί. Για να πετύχει το τελευταίο, ο εισβολέας μεταδίδει τα αντιγραμμένα πακέτα στον κόμβο που προοριζόταν να σταλούν εξ αρχής κατά τέτοιο τρόπο ώστε να φτάσουν στον κόμβο προορισμού την στιγμή που θα έφταναν τα αρχικά πακέτα ή και νωρίτερα. Όπως βλέπουμε στην εικόνα 22, ο εισβολέας χρησιμοποιεί μία «σήραγγα σκουληκότρυπας» αποφεύγοντας τους κόμβους που εμπλέκονται, η διαδικασία αυτή είναι μη ανιχνεύσιμη [40].



Εικόνα 22 Παράδειγμα επίθεσης σκουληκότρυπας[40]

4.2.2.2.2 – Κρυφάκουσμα - Eavesdropping

Το κρυφάκουσμα αποτελεί την πιο γνωστή επίθεση σε ασύρματα δίκτυα. Είναι παρόμοια με την επίθεση ενδιάμεσου ανθρώπου την οποία αναφέραμε παραπάνω.

Η επίθεση αυτή αποτελεί μια σημαντική απειλή για το περιεχόμενο ενός μηνύματος που μεταδίδεται στο δίκτυο. Κατά τη διάρκεια της αποστολής ενός μηνύματος ένα τρίτο άτομο, που δεν είναι εξουσιοδοτημένος αποδέκτης του μηνύματος, καταφέρνει και «κρυφακούει» τα περιεχόμενα του. Πρόκειται για μια επίθεση κατά της εμπιστευτικότητας της επικοινωνίας.

Αυτό μπορεί να προκληθεί είτε με την μή χρήση κρυπτογράφησης, όπου τα μηνύματα αποστέλλονται σαν μη κρυπτογραφημένο κείμενο και μπορούν να διαβαστούν από οποιονδήποτε έχει τη δυνατότητα παρακολούθησης τους είτε εναλλακτικά από μια ευάλωτη μέθοδο κρυπτογράφησης εκθέτοντας το μεγαλύτερο μέρος της επικοινωνίας του δικτύου. Η απειλή έχει ως κύριο στόχο τη παρακολούθηση των κλειδιών κρυπτογράφησης που χρησιμοποιούνται για την αποκρυπτογράφηση των μηνυμάτων. Ο σκοπός του επιτηθόμενου είναι να καταλάβει τη λειτουργία της μεθόδου και να χρησιμοποιήσει τα αντίστοιχα κλειδιά για τα επόμενα μηνύματα. Το αποτέλεσμα της επίθεσης αυτής οδηγεί σε διαρροή ευαίσθητων πληροφοριών των χρηστών δικτύου, οι οποίες μπορεί να

περιλαμβάνουν δεδομένα που σχετίζονται με την προστασία της ιδιωτικής τους ζωής[41].

4.3 – Επιθέσεις Ασφαλείας LoRaWAN

4.3.1 – Έκθεση τελικών συσκευών και των κλειδιών τους

Η τεχνολογία του LoRaWAN διασφαλίζει την ασφάλεια από άκρο σε άκρο όπως είδαμε στο κεφάλαιο με τα χαρακτηριστικά ασφαλείας, μέσω των κλειδιών εφαρμογής και δικτύου. Ωστόσο, οι τελικές συσκευές LoRa στη περίπτωση όπου μία κακόβουλη οντότητα αποκτήσει φυσική πρόσβαση στο χώρο που βρίσκονται τότε ενδέχεται να τις θέσει σε κίνδυνο. Εάν η οντότητα αυτή αποκτήσει πρόσβαση στον χώρο που βρίσκεται μια συσκευή, έχει τη δυνατότητα με συγκεκριμένους τρόπους να αποσπάσει κλειδιά που χρησιμοποιεί η συσκευή. Οι τελικές συσκευές διαθέτουν από την κατασκευή τους μια μονάδα ραδιοεπικοινωνίας LoRa (radio module) και μια ένα μικροελεγκτή (MCU). Η μονάδα ραδιοσυχνοτήτων επικοινωνεί με τον μικροελεγκτή (MCU) μέσω μίας διασύνδεσης UART ή SPI. Οι εντολές και οι ανταλλαγές δεδομένων μεταξύ της μονάδας και του μικροελεγκτή μπορούν να παρεμποδιστούν και να υποκλαπούν χρησιμοποιώντας κατάλληλο υλικό. Οι παραπάνω μονάδες δεν διαθέτουν μεθόδους κρυπτογράφησης για να διασφαλιστεί η επικοινωνία μεταξύ του μικροελεγκτή και της μονάδας ραδιοσυχνοτήτων. Σε αυτή την περίπτωση στοχεύει η κακόβουλη οντότητα, διότι δεν υπάρχει κανένας τρόπος να καταλάβει το σύστημα ότι οι εντολές που αποστέλλονται στη μονάδα ραδιοεπικοινωνίας στάλθηκαν από τον μικροελεγκτή ή από την κακόβουλη οντότητα. Επίσης, μέσω διαφόρων μηχανισμών μια κακόβουλη οντότητα θα μπορούσε να παρακολουθήσει όλες τις ανταλλαγές πακέτων στην επικοινωνία του μικροελεγκτή και της μονάδας ραδιοσυχνοτήτων και να χρησιμοποιήσει τα δεδομένα που υπόκλεψε για να δημιουργήσει μια συσκευή με τα ίδια κλειδιά, επικοινωνώντας στο δίκτυο σαν μια αυθεντική τελική συσκευή. Οπότε μέσω αυτής της επίθεσης το σύστημα κινδυνεύει να εκθέσει κρίσιμες πληροφορίες σε κακόβουλες οντότητες[42].

Για να αποδειχθεί μια τέτοια επίθεση πραγματοποιήθηκε ένα πείραμα, το «Xignal mousetrap[43]». Στο πείραμα αυτό η συσκευή παραβιάστηκε για να εκτεθεί η διασύνδεση UART μεταξύ του μικροελεγκτή MCU και της μονάδας ραδιοεπικοινωνίας LoRa. Ένα τσιπ τεχνολογίας του FTDI συνδέθηκε με τη διασύνδεση με σκοπό να κρυφακούει την επικοινωνία και τα δεδομένα που ανταλλάσσονται μεταξύ τους. Η παγίδα που ουσιαστικά στήθηκε, προκαλούσε την επανεκκίνηση του συστήματος, οπότε ο μικροελεγκτή έστελνε σε κάθε επανεκκίνηση εντολές δημιουργίας καινούργιων κλειδιών. Οπότε με την χρησιμοποίηση των κλειδιών που υποκλαπήκαν δημιουργήθηκε μία συσκευή με τα ίδια διαπιστευτήρια και εκτελούσε επιτυχώς το κακόβουλο έργο της.

4.3.2.1 – Πιθανοί Τρόποι Αντιμετώπισης

Σαν βασικούς τρόπους αντιμετώπισης της φυσικής προστασίας των τελικών συσκευών, ο πάροχος ενός συστήματος τεχνολογίας LoRaWAN μπορεί να υιοθετήσει:

- Τελικές συσκευές με τοποθετημένους μηχανισμούς κατά την κατασκευή τους που έχουν την δυνατότητα να στείλουν μηνύματα προειδοποίησης κατά την φυσική επίθεση που δέχονται (tamper-proof).
- Διαφορετικά κλειδιά για κάθε τελική συσκευή, ώστε να μην επηρεαστεί όλο το σύστημα αν εκτεθεί μια συσκευή

4.3.2 – Τεχνικές επιθέσεων Παρεμβολών

Η επίθεση δικτύου μέσω τεχνικών επιθέσεων παρεμβολών είναι ένα από τα σοβαρά προβλήματα συστημάτων IoT. Μέσω αυτών των τεχνικών οι κακόβουλες οντότητες μεταδίδουν ένα ισχυρό ραδιοφωνικό σήμα κοντά στις συσκευές του συστήματος (κυρίως στους συγκεντρωτές) και διακόπτουν τη λειτουργία τους. Οι επιθέσεις αυτές απαιτούν τη χρησιμοποίηση ειδικού υλικού(hardware) για την πραγματοποίηση τους, αλλά και εξειδικευμένους μηχανισμούς αντιμετώπισης για την ελαχιστοποίηση των συνεπειών τους. Ωστόσο, σύμφωνα με το αποτέλεσμα του παρακάτω πειράματος, αναφέρεται ότι είναι δυνατή η επιρροή των παρεμβολών στη τεχνολογία LoRaWAN με μια απλή χρήση υλικού τύπου LoRa που υπάρχει στην αγορά (commercial off the self – COTS).

Όπως αναφέρθηκε και στο κεφάλαιο με τα χαρακτηριστικά ασφαλείας η τεχνολογία LoRaWAN χρησιμοποιεί τη διαμόρφωση εξάπλωσης φάσματος CSS (Chirp Spread Spectrum) η οποία είναι γνωστή για την ανθεκτικότητα της κατά των παρεμβολών. Στο πείραμα των [44] βγήκε το πόρισμα ότι οι συσκευές φυσικού επιπέδου LoRa υποφέρουν από ζητήματα συνύπαρξης. Επίσης, ένα ακόμα αρνητικό αποτέλεσμα της συνύπαρξης των συσκευών LoRa, είναι όταν οι συσκευές αυτές εκτελούν ταυτόχρονες εκπομπές χρησιμοποιώντας την ίδια συχνότητα και διαμόρφωση εξάπλωσης φάσματος, υπάρχει η περίπτωση να παρεμβαίνουν μεταξύ τους. Οπότε, οι κακόβουλες οντότητες με τη χρησιμοποίηση συσκευών LoRa που υπάρχουν στην αγορά, τους δίνεται η δυνατότητα να εμποδίσουν τη λειτουργία των δικτύων LoRa.

4.3.2.1 – Πιθανοί Τρόποι Αντιμετώπισης

Οι διαχειριστές του συστήματος είναι εύκολο να αντιληφθούν τις επιθέσεις παρεμβολής, αλλά χρειάζονται ειδικούς μηχανισμούς και κινήσεις αντιμετώπισης για να είναι το σύστημα τους ασφαλές, για παράδειγμα:

- Οι διαχειριστές δικτύου μπορούν να αποτρέψουν την επίθεση αλλάζοντας την συχνότητα εκπομπής.
- Η έρευνα [45] προτείνει μια νέα στρατηγική αντιμετώπισης των παρεμβολων για IoT συστήματα, η οποία επιτρέπει σε ένα διαχειριστή του συστήματος να προστατεύει τις συσκευές IoT από μια επίθεση τεχνικής παρεμβολών. Η αλληλεπίδραση μεταξύ του διαχειριστή του συστήματος και του επιτιθέμενου (Jammer) διαμορφώνεται ως παιχνίδι “Colonel Blotto” στο οποίο ο διαχειριστής ενεργώντας ως υπερασπιστής, επιδιώκει να αναχαιτίσει την επίθεση από παρεμβολές διανέμοντας τη δύναμη του με έξυπνο τρόπο για να μειώσει το ποσοστό λάθους ανά bit (bit error rate - BER) που προκαλείται από τον επιτιθέμενο. Ο επιτιθέμενος από την άλλη πλευρά, στοχεύει στη διακοπή της απόδοσης του συστήματος, κατανέμοντας την ισχύ παρεμβολής σε διαφορετικές ζώνες συχνοτήτων. Για την επίλυση του παιχνιδιού προτείνεται ένας εξελικτικός αλγόριθμος ο οποίος μπορεί να βρει μια λύση μέσω Nash-equilibrium στο Blotto παιχνίδι. Τα αποτελέσματα προσομοίωσης δείχνουν ότι ο προτεινόμενος αλγόριθμος επιτρέπει στον διαχειριστή του συστήματος να διατηρεί το BER πάνω από

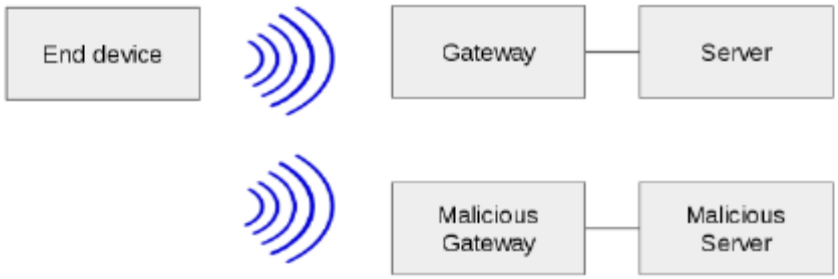
ένα αποδεκτό όριο διατηρώντας έτσι την απόδοση του δικτύου IoT παρουσία επίθεσης παρεμβολής.

4.3.3 – Κρυφάκουσμα

Η επίθεση του κρυφακούσματος ή αλλιώς Eavesdropping, έχει ως στόχο την υποκλοπή πακέτων που αποστέλλονται κατά την επικοινωνία των τελικών συσκευών και του συγκεντρωτή. Για να το πετύχει αυτό μια κακόβουλη οντότητα πρέπει να βρει τρόπο να «σπάσει» τον μηχανισμό κρυπτογράφησης του LoRaWAN.

Για τη πραγματοποίηση της επίθεσης αυτής, ο επιτιθέμενος είναι απαραίτητο να έχει στη κατοχή του ένα ασύρματο «ανιχνευτικό» (sniffer) τύπου LoRaWAN, να διαθέτει βασικές γνώσεις για τις τελικές συσκευές και τα πακέτα που στέλνει αλλά και την δυνατότητα να μπορεί να εκτελέσει επανεκκινήσεις στις συσκευές. Δύο αδυναμίες του πρωτοκόλλου LoRa, που ευνοούν την πραγματοποίηση της επίθεσης κρυφακούσματος, είναι η ενεργοποίηση των τελικών συσκευών μέσω διαδικασίας ABP και η λανθασμένη χρησιμοποίηση της λειτουργίας μετρητών. Αν η κακόβουλη οντότητα καταφέρει να έχει την ιδιότητα επανεκκίνησης των τελικών συσκευών στη διάθεση της έχει και ταυτόχρονα την δυνατότητα να μηδενίζει τους μετρητές. Με τη πραγματοποίηση της επανεκκίνησης, οι μετρητές θα ξεκινήσουν από το 0. Στην διαδικασία ABP το κλειδί δεν αλλάζει διότι είναι από την κατασκευή του τοποθετημένο στη συσκευή, με αυτό τον τρόπο η κακόβουλη οντότητα θα έχει στη διάθεση του και την τιμή του μετρητή αλλά και το κλειδί που κρυπτογραφούνται τα πακέτα. Σαν αποτέλεσμα τον κινήσεων αυτών είναι η έκθεση του αλγορίθμου κρυπτογράφησης[46].

Η εικόνα 23 δείχνει τη προσομοίωση της επίθεσης κρυφακούσματος. Η επίθεση στον αλγόριθμο κρυπτογράφησης και της υποκλοπής των διαπιστευτηρίων, δίνει τη δυνατότητα στην κακόβουλη οντότητα να δημιουργήσει ένα ψεύτικο συγκεντρωτή και εξυπηρετητή για τη λήψη ασύρματων πακέτων από το δίκτυο.



Εικόνα 23 Προσομοίωση του κρυφακούσματος [46].

Για να μπορέσει μια κακόβουλη οντότητα να πραγματοποιήσει την επίθεση κρυφακούσματος χρειάζεται να έχει μία ακολουθία γεγονότων. Αρχικά, υποκλέπτει πακέτα που αποστέλλονται στο δίκτυο LoRaWAN και τα αποθηκεύει με σκοπό να αναλύσει το περιεχόμενο τους. Έπειτα, υποκλέπτει και αποθηκεύει πακέτα μετά την επανεκκίνηση της συσκευής και τα οποία τα συγκρίνει με τα πακέτα προ επανεκκίνησης με σκοπό να τα τοποθετήσει κατάλληλα ανάλογα με την τιμή του μετρητή. Τέλος, χρησιμοποιώντας τη μέθοδο «crib dragging» (μέθοδος που μπορεί να αποκαλύψει το απλό κείμενο δύο μηνυμάτων που έχουν κρυπτογραφηθεί με το ίδιο κλειδί, χωρίς καν να γνωρίζουν το κλειδί [47]) κωδικοποιεί τα δεδομένα τους.

4.3.3.1 – Πιθανοί Τρόποι Αντιμετώπισης

Για να μπορέσει να επιτευχθεί η διασφάλιση του συστήματος απέναντι σε επιθέσεις κρυφακούσματος, θα πρέπει να στις περιπτώσεις κυρίως επανεκκίνησης να ληφθούν καλύτερα μέτρα δημιουργίας διαπιστευτηρίων. Για παράδειγμα:

- Αντικατάσταση των τιμών των μετρητών με τη χρήση της ιδιότητας “nonce number” (ένας αριθμός που χρησιμοποιείται μόνο μια φορά)
- Στην περίπτωση της υπερχείλισης (Overflow) των μετρητών ή σε κάθε επανεκκίνηση (reset) θα πρέπει ταυτόχρονα να αλλάζουν τα κλειδιά. Στην διαδικασία ενεργοποίησης των τελικών συσκευών μέσω αέρα θα πρέπει να πραγματοποιηθεί ξανά η διαδικασία ενεργοποίησης για την απόκτηση καινούργιων κλειδιών. Αν η ενεργοποίηση των συσκευών γίνει μέσω προσωπικού πρέπει να ρυθμιστούν ξανά και τα κλειδιά να αλλάξουν.

4.3.4 – Επίθεση Επανάληψης

Η επίθεση επανάληψης μπορεί να χρησιμοποιηθεί και σαν τεχνική παρεμβολής της λειτουργίας του συστήματος αλλά και για τη πλαστογράφηση δεδομένων. Όπως είδαμε και στην επίθεση του κρυφακούσματος, στην ενεργοποίηση των συσκευών με τη διαδικασία ABP συνεπάγεται και η «εύκολη» έκθεση τους σε επιθέσεις δικτύου. Τα στατικά κλειδιά που τοποθετούνται στη συσκευή στην περίπτωση επανεκκίνησης δεν αλλάζουν, ενώ δεν υπάρχουν μηχανισμοί ταυτοποίησης όπως για παράδειγμα τα αιτήματα ζήτησης και αποδοχής που υπάρχουν στη διαδικασία ενεργοποίησης μέσω αέρα. Σαν αποτέλεσμα είναι πολύ πιο πιθανή η περίπτωση εμφάνισης κακόβουλων πακέτων στους εξυπηρετητές δικτύου τα οποία όμως πρέπει να διαθέτουν τα κατάλληλα χαρακτηριστικά για να γίνουν αποδεκτά από τον εξυπηρετητή. Τα κλειδιά συνόδου πρέπει να ταυτίζονται με τα κλειδιά συνόδου κάποιας ενεργοποιημένης τελικής συσκευής. Η διεύθυνση της συσκευής που στέλνει τα κακόβουλα πακέτα πρέπει επίσης να ταυτίζεται με την κατάλληλη τιμή του μετρητή είτε πριν είτε μετά την επανεκκίνηση[48].

Οπότε αν η κακόβουλη οντότητα έχει στη διάθεση της την τιμή του μετρητή και τα κλειδιά συνόδου, έχε τη δυνατότητα να ξαναστείλει προηγούμενα μηνύματα με τα κατάλληλα διαπιστευτήρια στο δίκτυο μεταξύ τελικών συσκευών και εξυπηρετητή. Ο στόχος της επίθεσης επανάληψης των πακέτων είναι η επίτευξη της επανάληψης της τιμής του μετρητή. Στην περίπτωση της ενεργοποίησης των συσκευών μέσω αέρα, η οντότητα πρέπει να περιμένει την επίτευξη της υπερχείλισης των τιμών του μετρητή που συνεπάγεται με την επανεκκίνηση του. Στην περίπτωση της ενεργοποίησης από προσωποποίηση (ABP) μπορεί επίσης να περιμένει την υπερχείλιση ή αν έχει τη δυνατότητα να εκτελέσει την επανεκκίνηση μέσω μιας φυσικής επίθεσης, κίνηση που θέλει πολύ λιγότερο χρόνο.

Όπως αναφέρθηκε παραπάνω ο σκοπός των επιθέσεων επανάληψης είναι η πλαστογράφηση των δεδομένων αλλά και η δυνατότητα της επίθεσης άρνησης παροχής υπηρεσιών (Denial of Service) που αποτελεί μία τεχνική παρεμβολής. Στη δεύτερη περίπτωση, ο στόχος της άρνησης παροχής υπηρεσιών είναι η συνεχής επανάληψη των μηνυμάτων με τα σωστά διαπιστευτήρια προς τον συγκεντρωτή και τον εξυπηρετητή με σκοπό την μείωση της λειτουργίας τους και

σαν αποτέλεσμα οι τελικές συσκευές να μην επικοινωνούν με το σύστημα [48]. Για την επίτευξη της δεύτερης περίπτωσης η κακόβουλη οντότητα θα πρέπει να γνωρίζει τη μορφή της φυσικής αναπαράστασης δεδομένων στα πακέτων του LoRaWAN, τη συχνότητα που χρησιμοποιεί ο πάροχος υπηρεσιών και το σύστημα, να έχει υποκλέψει μηνύματα από μία τελική συσκευή προς το δίκτυο αλλά και τη δυνατότητα αποκρυπτογράφηση των δεδομένων τους.

4.3.4.1 – Πιθανοί Τρόποι Αντιμετώπισης

Για τη καλύτερη διασφάλιση του συστήματος από την επίθεση επανάληψης, ο πάροχος υπηρεσιών που χρησιμοποιεί την τεχνολογία LoRaWAN θα πρέπει να υλοποιήσει τις ασφαλέστερες τεχνικές που του διαθέτει η τεχνολογία, αλλά και να διαθέτει κατάλληλους μηχανισμούς για τη προστασία των διαπιστευτηρίων, για παράδειγμα:

- Με τη προστασία των κλειδιών συνόδου, επιλύει την επίθεση επανάληψης διότι δεν γίνεται να αποκρυπτογραφηθούν και να υποκλαπούν τα πακέτα που αποστέλλονται μεταξύ των τελικών συσκευών και του συγκεντρωτή.
- Η διασφάλιση των μετρητών είναι πολύ σημαντικό κομμάτι της προστασίας του LoRa εναντίων της επίθεσης επανάληψης, καθώς χρησιμοποιούνται για την δημιουργία των κλειδιών που αναφέρθηκαν παραπάνω (AppSKey, NwkSKey).
- Η ενεργοποίηση των τελικών συσκευών μέσω αέρα είναι ένας καλός τρόπος αντιμετώπισης της επίθεσης, χωρίς όμως να τον καθιστά 100% ασφαλές τρόπο λόγο της περίπτωσης υπερχείλισης των μετρητών [49].
- Όπως αναφέρθηκε και στην επίθεση του κρυφακούσματος, στην περίπτωση υπερχείλισης (Overflow) των μετρητών θα πρέπει ταυτόχρονα να αλλάζουν τα κλειδιά. Στην περίπτωση ενεργοποίησης μέσω αέρα θα πρέπει να γίνει η διαδικασία ενεργοποίησης ξανά για την απόκτηση καινούργιων κλειδιών. Αν η ενεργοποίηση των συσκευών γίνει μέσω ABP πρέπει να ρυθμιστούν ξανά και τα κλειδιά να αλλάξουν [49].
- Η χρησιμοποίηση τυχαίων τιμών «Nonce numbers» για τις τιμές των μετρητών στη περίπτωση επανεκκίνησης αποτελεί μια πολύ καλή λύση των επιθέσων επανάληψης.

4.3.5 – Επίθεση Σκουληκότρυπας

Όπως αναφέρθηκε και παραπάνω στις επιθέσεις ασφαλείας των LPWAN σε αυτόν τον τύπο επίθεσης, μια κακόβουλη οντότητα διαθέτει μία συσκευή για την υποκλοπή πακέτων που αποστέλλονται από μια αυθεντική συσκευή στο δίκτυο και αφού τα αποθηκεύσει ή τα αντιγράψει μόνο, τα διοχετεύει στο ειδικά διαμορφωμένο δίκτυο του σε άλλη συσκευή που βρίσκεται σε απόσταση. Η κακόβουλη οντότητα δεν χρειάζεται να γνωρίζει για να επιτεθεί τη μέθοδο κρυπτογράφησης.

Συγκεκριμένα σε ένα LoRaWAN δίκτυο, με την χρήση μιας συσκευής ανίχνευσης (sniffer) και μια παρεμβολής (jammer), μια κακόβουλη οντότητα έχοντας τις κατάλληλες γνώσεις μπορεί να πραγματοποιήσει τη συγκεκριμένη επίθεση σκουληκότρυπας. Με τη χρήση της συσκευής ανίχνευσης έχει τη δυνατότητα υποκλοπής των πακέτων και όταν το πετύχει στέλνει σήμα στην συσκευή παρεμβολής. Το πακέτο δεν φτάνει στον εξυπηρετητή παρά μόνο όταν το θελήσει η οντότητα, που μπορεί να είναι οποιαδήποτε στιγμή. Ως εκ τούτου, έχει τη δυνατότητα να παρακρατεί τα σημαντικά μηνύματα προειδοποίησης (alarm messages) και τα μηνύματα που έχει υποκλέψει η κακόβουλη οντότητα να πλαστογραφηθούν και να σταλθούν[42].

4.3.5.1 – Πιθανοί Τρόποι Αντιμετώπισης

Μέσω κάποιον εξελιγμένων μηχανισμών, οι πάροχοι υπηρεσιών έχουν τη δυνατότητα να προστατεύσουν το σύστημα τους από την επίθεση της σκουληκότρυπας, όπως για παράδειγμα:

- Στην έρευνα των [50] αναπτύχθηκε ο μηχανισμός των “packet leashes” όπου έχει αποδειχθεί ότι είναι αξιόπιστη λύση στην ανίχνευση των επιθέσεων σκουλικότρυπας. Ο μηχανισμός αυτός θέτει περιορισμούς στη μέγιστη απόσταση που επιτρέπει να διανύσει στο δίκτυο ένα πακέτο. Δύο τυποι “packetleashes” είναι οι “temporal” και ‘geographical”. Τα “temporal” απαιτούν αυστηρά συγχρονισμένα ρολόγια σε όλα τις τελικές συσκευές. Πρωτόκολλα που βασίζονται σε “temporal leashes” εξασφαλίζουν ότι τα πακέτα που μεταδίδονται στο δίκτυο έχουν ένα ανώτερο όριο για τη διάρκεια ζωής τους, το οποίο περιορίζει τη μέγιστη απόσταση των πακέτων

στο δίκτυο, και απορρίπτονται εάν το υπερβούν. Τα πρωτόκολλα που βασίζονται σε “geographical leash” διαφέρουν ελαφρώς από τα “temporal leash”. Η κάθε τελική συσκευή πρέπει να γνωρίζει τη θέση της και τα ρολόγια να μην είναι τόσο αυστηρά συγχρονισμένα όπως στα “temporal”. Χρησιμοποιώντας τη θέση και το χρόνο, οι συσκευές μπορούν να καθορίσουν εάν το πακέτο που έρχεται είναι απότη σωστή συσκευή ή από μία κακόβουλη συσκευή σκουλικότρυπας. Επίσης ενσωματώνει μερικές από τις ίδιες ιδέες που χρησιμοποιούνται στα συστήματα εντοπισμού κάνοντας χρήση της θέσης για την αποτροπή των επιθέσεων σκουλικότρυπας.

4.3.6 – Πλαστογράφηση μηνύματος επιβεβαίωσης - ACK

Η επίθεση της πλαστογράφησης μηνύματος επιβεβαίωσης χρησιμοποιείται στο δίκτυο μεταξύ του συγκεντρωτή και των εξυπηρετητών που το αποκαλούμε νέφος (LTE/3G/4G). Οι συγκεντρωτές στο LoRaWAN συνδέονται συνήθως στο νέφος με μία ή περισσότερες διεπαφές το οποίο σημαίνει και αύξηση του αριθμού πιθανών τρωτών σημείων. Για παράδειγμα, με τη χρησιμοποίηση επιθέσεων στο πρωτόκολλο Πακέτων του Χρήστη (User Datagram Protocol - UDP) είναι δυνατό να πλαστογραφηθεί και να δημιουργηθεί ένας συγκεντρωτής που θα εκτελεί τις εντολές μιας κακόβουλης οντότητας που μπορεί να προστεθεί στο δίκτυο. Η ευπάθεια του πρωτοκόλλου παρουσιάζεται στο γεγονός ότι το μήνυμα επιβεβαίωσης δεν διαθέτει πληροφορίες που αφορούν την ταυτότητα του πακέτου που στέλνεται, αλλά επιβεβαιώνει μόνο το τελευταίο πακέτο που έχει σταλθεί. Επομένως, είναι πιθανό αν μία κακόβουλη οντότητα έχει στη διάθεση ένα συγκεντρωτή συνδεδεμένο στο δίκτυο, μπορεί να αποθηκεύσει το μήνυμα επιβεβαίωσης με σκοπό να το χρησιμοποιεί για μελλοντικά πακέτα των τελικών συσκευών ξαναστέλνοντας το ίδιο μήνυμα επιβεβαίωσης. Συνοψίζοντας, για να μπορέσει μια κακόβουλη οντότητα να πετύχει την επίθεση αυτή θα πρέπει να έχει στη διάθεση της ένα συγκεντρωτή, τη δυνατότητα να καταλαβαίνει τα μηνύματα επιβεβαίωσης και να τα αφομοιώνει το σύστημα της και τέλος να μπορεί να τα στέλνει στις τελικές συσκευές

4.3.7 – Επίθεση ενδιάμεσου ανθρώπου

Στην επίθεση αυτή μία κακόβουλη οντότητα βρίσκεται μεταξύ της συνομιλίας των τελικών συσκευών και του συγκεντρωτή (μπορεί και ανάμεσα του συγκεντρωτή με τον εξυπηρετητή) αντιπροσωπεύοντας και τους δύο. Δηλαδή μία τελική συσκευή λαμβάνει μηνύματα σαν ένα συγκεντρωτή και για τη περίπτωση του συγκεντρωτή να στέλνει μηνύματα σαν τελική συσκευή στην περίπτωση της ανερχόμενης ζεύξης και στην περίπτωση της κατερχόμενης ζεύξης αντίστοιχα. Η επίθεση αυτή επιτρέπει στον επιτήδειο να υποκλέψει, να στείλει, να δεχθεί και να αλλάξει τα δεδομένα(συγκεκριμένα την Bit-Flipping Attack) που προορίζονται για κάποιον άλλο, χωρίς να το γνωρίζουν τα δύο μέρη που επικοινωνούν κανονικά [46].

4.3.7.1 – Επίθεση Μετατροπής Χαρακτήρα

Η επίθεση μετατροπής χαρακτήρα ή αλλιώς Bit-Flipping Attack όπως αναφέρθηκε στις επιθέσεις των LPWAN έχει ως στόχο την τροποποίηση των δεδομένων και αποτελεί παράγωγο μίας επίθεσης ενδιάμεσου ανθρώπου.

Το κρυπτογραφημένο μήνυμα δέχεται επίθεση από τη κακόβουλη οντότητα, η οποία μεταβάλλοντας το κείμενο του με τέτοιο τρόπο ώστε να γνωρίζει σε ποία θέση των bits γίνεται αυτή η αλλαγή. Στην επίθεση αυτή η κακόβουλη οντότητα όπως αναφέραμε, έχει τη δυνατότητα να μεταβάλει το κρυπτογραφημένο κείμενο, χωρίς να δημιουργεί όμως πρόβλημα στις μεθόδους κρυπτογράφησης. Η μέθοδος κρυπτογράφησης AES128 στη λειτουργία μετρητή που είναι η βασική μέθοδος της τεχνολογίας LoRaWAN είναι ευάλωτες στις επιθέσεις μετατροπής χαρακτήρα. Ο λόγος για το παραπάνω, είναι ότι ο κώδικας ακεραιότητας μηνύματος (MIC), έχει μια απλή σύνθεση και μπορεί να υποκύψει σε μία βίαιη επιβολή (brute forcing), η κίνηση αυτή δίνει τη δυνατότητα σε μία κακόβουλη οντότητα να πραγματοποιήσει την επίθεση μετατροπής χαρακτήρα χωρίς ο πάροχος να το καταλάβει [41].

4.3.7.2 – Πιθανοί Τρόποι Αντιμετώπισης

Ο διαχειριστής ή πάροχος του συστήματος, για να μπορέσει να προστατέψει το σύστημα του θα πρέπει να διασφαλίσει κυρίως την αυθεντικοποίηση των πακέτων που ανταλλάσσονται στο δίκτυο, οι βασικοί μηχανισμοί που θα πρέπει να θωρακίσει είναι:

- Η χρήση της αποτελεσματικής κρυπτογράφησης για τα δεδομένα που αποστέλλονται και η ασφαλής λειτουργία του κώδικα ακεραιότητας μηνύματος (Message Integrity Code) ώστε ο παραλήπτης να είναι σίγουρος για την ταυτότητα του αποστολέα.
- Ακόμα ένας σημαντικός τρόπος αντιμετώπισης είναι η χρησιμοποίηση της μεθόδου μέτρησης πακέτων (Counter Mode) με τη λειτουργία της τυχαίας τιμής «nonce number» η οποία βοηθά στη διασφάλιση ακεραιότητας των μηνυμάτων που αποστέλλονται μεταξύ τελικής συσκευής, συγκεντρωτή και εξυπηρετητή.

4.4 – Επιθέσεις Ασφαλείας Sigfox

Το επίπεδο δικτύου του Sigfox αποτελεί το βασικό λόγο που το Sigfox είναι μία από τις κυρίαρχες τεχνολογίες LPWAN. Σύμφωνα με την εταιρεία Sigfox είναι η "secret sauce" (μυστική σάλτσα) του πρωτοκόλλου, όπου συνεπάγεται η μη ύπαρξη δημοσιεύσεων παρά μόνο από την ίδια εταιρεία. Παρακάτω αναφέρουμε τις επιθέσεις στο επίπεδο δικτύου και εφαρμογής καθώς και τις λύσεις που προτείνονται σύμφωνα με την έκθεση [51].

4.4.1 – Έκθεση των συσκευών σε κινδύνους

Το κεφάλαιο αυτό αναλύει τους κινδύνους που δέχονται οι πιστοποιημένες συσκευές Sigfox λόγο της μειωμένης ασφάλειας που παρέχουν, τους κινδύνους αυτούς μπορούμε να τους δούμε και στον πίνακα 3. Αποτελεί και μια επιλογή για τα μέτρα που θα μπορούσαν να απαιτηθούν για το σχεδιασμό, την υλοποίηση και την κατασκευή των συσκευών Sigfox.

4.4.1.1 – Κίνδυνοι που επηρεάζουν την εφαρμογή

Όπως αναφέραμε στο κεφάλαιο των χαρακτηριστικών ασφαλείας, η μοναδική ταυτότητα της συσκευής και ο μετρητής αλληλουχίας βρίσκονται στα πακέτα που αποστέλλονται από τις συσκευές στους συγκεντρωτές, δίνοντας τη δυνατότητα να υποκλαπούν χωρίς καμία πρόσβαση στη συσκευή. Η μετατροπή όμως αυτών των τιμών στη συσκευή θα έχει ως αποτέλεσμα την αποτροπή της επικοινωνίας της συσκευής με το συγκεντρωτή και τους εξυπηρετητές και ταυτόχρονα με τις εφαρμογές των τελικών χρηστών.

Το Κλειδί ελέγχου ταυτότητας δικτύου (NAK) είναι ακόμα ένα σημαντικό στοιχείο αυθεντικότητας για τα πακέτα και πρέπει να προστατεύεται από την τροποποίηση διότι θα είχε τις ίδιες συνέπειες με τις τροποποιήσεις της ταυτότητας και του μετρητή αλληλουχίας. Πράγματι, εάν κάποιος υποκλέψει αυτό το κλειδί, θα είναι σε θέση να δημιουργήσει μηνύματα ίδιου τύπου και ιδιοτήτων που θα γίνουν δεκτά από το βασικό πυρήνα του Sigfox. Οι κίνδυνοι που παράγονται από το παραπάνω γεγονός είναι η υπερφόρτωση του δικτύου με άχρηστα μηνύματα, αλλά και με μηνύματα που διαθέτουν ψεύτικες πληροφορίες με σκοπό την υποβάθμιση των υπηρεσιών και των εφαρμογών που στηρίζονται σε αυτές τις πληροφορίες.

Επιπλέον στην κρυπτογράφηση των δεδομένων, το κλειδί που χρησιμοποιείται για την μέθοδο κρυπτογράφησης (Ke) και ο μετρητής κρυπτογράφησης (CTR) πρέπει να προστατεύονται στη συσκευή. Όπως και παραπάνω, αν μία από αυτές τις τιμές τροποποιηθεί, η αποκρυπτογράφηση των δεδομένων θα είναι εσφαλμένη και θα οδηγήσει σε έναν αποτυχημένο έλεγχο ταυτότητας του διακομιστή και τα δεδομένα θα απορριφθούν και δεν θα παραδοθούν στον τελικό χρήστη. Επιπλέον, η υποκλοπή αυτών των δύο στοιχείων έχει ως αποτέλεσμα τη δυνατότητα αποκρυπτογράφησης των μηνυμάτων που αποστέλλονται μέσω του δικτύου, παραβιάζοντας το απόρρητο δεδομένων του πελάτη.

Πίνακας 3 Οι κίνδυνοι έκθεσης των βασικών στοιχείων των πακέτων[51].

Parameter	Action	Risk
device ID	Alteration in the device	Denial of device connectivity
Sequence counter	Alteration in the device	Denial of device connectivity Loss of applicative data
Network Authentication Key (NAK)	Alteration in the device	Denial of device connectivity
Network Authentication Key (NAK)	Disclosure	Device cloning, identity theft Fake message injection
Encryption Key Ke	Alteration in the device	Loss of applicative data
Encryption Key Ke	Disclosure	Leak of sensitive applicative data
CTR	Alteration in the device	Loss of applicative data

4.4.1.1 – Κίνδυνοι στο δίκτυο του Sigfox

Τα ευαίσθητα στοιχεία που αναφέραμε παραπάνω είναι μοναδικά για κάθε συσκευή, που σημαίνει ότι στην περίπτωση που κάποια συσκευή εκτεθεί και της υποκλέψουν τα στοιχεία, δεν θα επηρεάστει αρνητικά το δίκτυο Sigfox.

Ωστόσο, υπάρχουν πιθανές επιθέσεις στο δίκτυο του Sigfox, όπως η περίπτωση να έχουν εκτεθεί αρκετά ευαίσθητα στοιχεία συσκευών, που συνεπάγεται με μια έκθεση μεγάλου αριθμού συσκευών. Ακόμα, αν χρησιμοποιηθούν οι εκτεθειμένες συσκευές μπορεί να πραγματοποιηθεί επίθεση άρνησης παροχής υπηρεσιών στο δίκτυο, όπου ένας μεγάλος αριθμός γνήσιων μηνυμάτων από τη στιγμή που οι επιτιθέμενοι γνωρίζουν τα στοιχεία, τροφοδοτείται στο δίκτυο Sigfox.

Στην πρώτη περίπτωση, μία κακόβουλη οντότητα θα μπορούσε να χρησιμοποιήσει τα ευαίσθητα στοιχεία της συσκευής που έχει υποκλέψει για να δημιουργήσει γνήσια μηνύματα που θα μεταδίδονταν στο δίκτυο προκαλώντας παραπλάνηση των τελικών χρηστών και θα επηρέαζε την αξιοπιστία της τεχνολογίας του Sigfox.

Στη δεύτερη περίπτωση μια κακόβουλη οντότητα δημιουργεί επίσης γνήσια μηνύματα που μεταδίδονται μέσω του δικτύου. Η διαφορά όμως είναι ότι ο στόχος είναι να υπερφορτωθούν οι πόροι του δικτύου, προκειμένου να επιτευχθεί η άρνηση υπηρεσιών στις συσκευές. Στην περίπτωση αυτή, η επίθεση δεν απαιτεί τα πλαστά μηνύματα να είναι αυθεντικά αφού οι πόροι του κεντρικού δικτύου είναι ουσιαστικά οι ίδιοι για να επεξεργαστούν αυθεντικά ή πλαστά μηνύματα. Παρόλα αυτά, δεν αποτελεί εύκολα υλοποιήσιμο σενάριο διότι ο μικρός ρυθμός μετάδοσης των μηνυμάτων Sigfox και η χωρητικότητα των σταθμών βάσης περιορίζουν τον αριθμό των μηνυμάτων που μπορούν να τροφοδοτηθούν στο δίκτυο.

Σαν συμπέρασμα μπορούμε να πούμε ότι η έκθεση των ευαίσθητων στοιχείων της συσκευής επηρεάζει ουσιαστικά την ίδια τη συσκευή και ταυτόχρονα το δίκτυο Sigfox θα παραμείνει ανεπηρέαστο.

4.4.2 – Σενάρια επιθέσεων

Στην ενότητα αυτή αναλύονται τα σενάρια επιθέσεων που μπορούν να επιτευχθούν σε ένα δίκτυο Sigfox με σκοπό την υποκλοπή προσωπικών στοιχείων των τελικών χρηστών.

4.4.2.1 – Απομακρυσμένη πρόσβαση συσκευών

Οι συσκευές δεν είναι προσβάσιμες από το διαδίκτυο μέσω του δικτύου Sigfox οπότε δεν υπάρχει δυνατότητα πρόσβασης εξ αποστάσεως των συσκευών και υποκλοπής των δεδομένων είτε για τροποποίηση είτε για απλή ανάγνωση. Υπάρχει όμως η περίπτωση η συσκευή να διαθέτει εναλλακτική συνδεσιμότητα όπως Wi-Fi και Bluetooth. Αυτή η δυνατότητα διπλής συνδεσιμότητας θα μπορούσε να χρησιμοποιηθεί ως τρόπος επίθεσης στις συσκευές και την δυνατότητα εγκατάστασης κακόβουλου λογισμικού.

4.4.2.2 – Φυσική πρόσβαση συσκευών

Απεναντίας, στις περιπτώσεις που η συσκευή δεν είναι προσβάσιμη μέσω διαδικτύου, όπως ενός συστήματος συναγερμού, οι πιθανότητες να μην πάθει τίποτα και να συνεχίσει την λειτουργία της ακόμα και αν ένας εισβολέας προσπαθήσει να την αποκτήσει πρόσβαση είναι με το μέρος του συστήματος.

Το παραπάνω δεν σημαίνει ότι δεν διατρέχουν κανένα κίνδυνο, σε πολλές περιπτώσεις χρήσης, οι συσκευές παραμένουν χωρίς επίβλεψη και ενδέχεται να είναι φυσικά προσβάσιμες σε κακόβουλες οντότητες. Στις περιπτώσεις αυτές, οι κίνδυνοι που διατρέχουν οι συσκευές είναι είτε να καταστραφούν και να σταματήσει η λειτουργία τους χωρίς όμως να εκτεθούν τα δεδομένα και τα στοιχεία που έχουν, είτε θα μπορούσαν να διακυβεύονται από το λεγόμενο hacking. Ο κίνδυνος να εκτεθούν οι συσκευές στον τελευταίο κίνδυνο είναι ανάλογος με το επίπεδο ασφάλειας που έχει σχεδιαστεί στη συσκευή.

Στις επιθέσεις αυτές, είναι σημαντικό ακόμα και αν είναι περίπλοκη η επίθεση να υπάρχει η δυνατότητα πρόβλεψης και διασφάλισης ώστε να μην επαναληφτούν οι επιθέσεις. Ωστόσο, αν πραγματοποιηθεί μία φυσική πρόσβαση σε μία συσκευή είναι αρκετή για να εκτεθεί. Η έκθεση ενός μεγάλου αριθμού συσκευών σε μία κακόβουλη οντότητα αποτελεί μία πολύ δαπανηρή και καταστροφική επίθεση.

4.4.2.3 – Κίνδυνοι κατά την παραγωγή και την συντήρηση

Στις συσκευές διατίθενται είτε από προεπιλογή, είτε από επιλογή μηχανισμοί ασφαλείας για την αντιμετώπιση των κίνδυνων δικτύου, υπάρχουν όμως και περιπτώσεις επίθεσης που πραγματοποιούνται κατά τη διάρκεια τεχνικής συντήρησης ή κατά τη διάρκεια της κατασκευής των συσκευών. Τέτοιες επιθέσεις πραγματοποιούνται για την κλοπή προσωπικών στοιχείων της συσκευής και τα συναφή κλειδιά κρυπτογράφησης. Επίσης δίνεται η δυνατότητα κλοπής διαπιστευτηρίων των τεχνικών που εμπλέκονται στη διαδικασία συντήρησης.

4.4.2.4 – Επίθεση κρυφής ακρόασης του σήματος

Με τον κατάλληλο εξοπλισμό μπορεί κάποιος να «ακούει» τις ραδιοσυχνότητες και τα σήματα που εκπέμπουν. Στην περίπτωση της υποκλοπής των μηνυμάτων μέσω κρυφής ακρόασης (eavesdropping) όπως είδαμε παραπάνω, δεν τροποποιούνται τα μηνύματα που υποκλέπτονται.

Η ιδιότητα του Sigfox να διαθέτει χαμηλό ρυθμό μετάδοσης μηνυμάτων από τις συσκευές, καθιστά πρακτικά αδύνατο να μπορέσει μια κακόβουλη οντότητα να υποκλέψει το Κλειδί ελέγχου ταυτότητας δικτύου μιας συσκευής ακούγοντας τις μεταδόσεις των σημάτων. Πράγματι, αυτό το κλειδί είναι ένα παράγωγο της μεθόδου AES-128 που επιστρέφει 2128 πιθανές τιμές. Σύμφωνα με αυτό συνεπάγεται, ότι δεν υπάρχει πρακτική επίθεση στην μέθοδο κρυπτογράφησης έχοντας ακόμα και διαθέσιμα και κρυπτογραφημένα ζευγάρια δεδομένων.

Η κρυφή ακρόαση της ραδιοσυχνότητας στην περίπτωση που δεν εφαρμόζεται κάποια μέθοδος κρυπτογράφησης, δίνει τη δυνατότητα σε μία κακόβουλη οντότητα πετυχαίνοντας την επίθεση αυτή να έχει στη διάθεση της τα δεδομένα των πακέτων.

4.4.3 – Πιθανοί τρόποι αντιμετώπισης

Υπάρχουν πιθανοί τρόποι για την αντιμετώπιση των λιγότερο σύνθετων επιθέσεων. Η δυνατότητα του επιπέδου ασφαλείας που χρησιμοποιείται σε μία τεχνολογία είναι ένας συνδυασμός μεταξύ του κόστους των μηχανισμών ασφαλείας, του επιπέδου απειλής που δέχεται καθημερινά και το κόστους των επιπτώσεων που δέχεται από τις επιθέσεις. Στην ενότητα αυτή περιγράφονται

κάποιοι μηχανισμοί ασφαλείας που θα μπορούσε ένας πάροχος να χρησιμοποιεί στο σύστημα του.

4.4.3.1 – Αξιολόγηση ασφαλείας

Η διασφάλιση και η προστασία των συσκευών δεν είναι εύκολη υπόθεση, ειδικά όταν η συσκευή πρέπει να είναι φτηνή και κατασκευασμένη με απλά εξαρτήματα για να τηρεί τις προδιαγραφές των τεχνολογιών LPWAN. Προκειμένου να διασφαλιστεί ότι οι βασικές επιθέσεις αποτρέπονται και ότι ακολουθούνται οι τυποποιημένες βέλτιστες πρακτικές, οι πάροχοι των συστημάτων που χρησιμοποιούν τεχνολογία Sigfox μπορούν να ζητήσουν μια αξιολόγηση ασφάλειας από τους ειδικούς τεχνικούς που διαθέτει.

Οι συγκεκριμένοι τεχνικοί θα εκτελέσουν πρώτα μια αξιολόγηση του επιπέδου ασφαλείας της συσκευής και ύστερα θα υποδείξουν τις κατάλληλες ενημερώσεις για να διορθωθούν και να διασφαλιστούν τυχόν τρωτά σημεία. Για τον καλύτερο έλεγχο χρησιμοποιούνται διάφορες τεχνικές αξιολόγησης της ασφάλειας εναντίων των διαφόρων σεναρίων επίθεσης που απαιτούν επαγγελματικό εξοπλισμό. Υπάρχει η δυνατότητα ακόμα να ζητηθεί παροχή συμβουλευτικών υπηρεσιών από την πρώτη μέρα για να δημιουργήσει ο πάροχος μια ασφαλής υπηρεσία.

4.4.3.2 – Ασφάλεια των πιστοποιητικών

Όπως αναφέρθηκε και στην ενότητα των χαρακτηριστικών ασφαλείας, το Sigfox παραδίδει τα διαπιστευτήρια που χρησιμοποιούνται και είναι αποθηκευμένα στις συσκευές στους παρόχους των τελικών συστημάτων που χρησιμοποιούν την τεχνολογία του Sigfox. Η μεταφορά των διαπιστευτηρίων όμως μπορεί να οδηγήσει σε διαρροή όλων των κλειδιών για την συγκεκριμένη παρτίδα παραγωγής. Σε περίπτωση που δεν ανιχνευτεί το λάθος διακυβεύονται πολλές παρτίδες και ολόκληρη η λειτουργία του συστήματος. Σύμφωνα με το παραπάνω, είναι σημαντικό να εξασφαλιστεί η επικοινωνία και ο ασφαλής διαμοιρασμός των διαπιστευτηρίων. Τα κρυπτογραφημένα πακέτα που περιέχουν τα διαπιστευτήρια παρέχονται στους κατασκευαστές των συσκευών μέσω της πύλης Sigfox. Οι κατασκευαστές συσκευών πρέπει να διασφαλίζουν την ασφάλεια του κλειδιού που χρησιμοποιείται για την αποκρυπτογράφηση του αρχείου. Προκειμένου να

διασφαλιστεί η επικοινωνία και να μεταδίδονται με ασφάλεια, το Sigfox διαθέτει προοδευτικά μέτρα φυσικής ασφάλειας για να εξασφαλίσει ότι τα διαπιστευτήρια μεταφέρονται με ασφάλεια στο εργοστάσιο.

Τέλος, εξίσου σημαντικό είναι η εξασφάλιση της εμπιστοσύνης των διαπιστευτηρίων στο εργοστάσιο παραγωγής, αυτό πετυχαίνεται με την εφαρμογή μιας αυστηρής διαδικασίας ασφάλειας. Μία τέτοια διαδικασία είναι η χρήση μιας υλικής μονάδας ασφαλείας HSM (Hardware Security Module) ή του φυσικού σήματος που παρέχεται από το Sigfox θα αποτρέψει την εξωτερική ή εσωτερική πειρατεία.

4.4.3.3 – HSM - υλική μονάδα ασφαλείας

Μια υλική μονάδα ασφαλείας (HSM) είναι ένας ασφαλής εξυπηρετητής ή μία κάρτα PCI, που διασφαλίζει την αποθήκευση ευαίσθητων κλειδιών. Με την χρησιμοποίηση αυτού του υλικού υπάρχει η δυνατότητα να ανιχνεύονται τυχόν προσπάθειες εισβολής και στην περίπτωση που ανιχνευτούν, τότε θα καταργήσει αυτόματα τα μυστικά κλειδιά.

Με την χρησιμοποίηση αυτού του εξοπλισμού στο εργοστάσιο, και το ειδικό κλειδί (MasterKey - MK) υπολογίζονται τα κλειδιά και τα υπόλοιπα στοιχεία. Το κλειδί αυτό παρέχεται από το Sigfox στην HSM μέσω της διαδικασίας ενσωμάτωσης του. Στους κατασκευαστές των συσκευών δίνονται μόνο τα απαραίτητα στοιχεία και όχι το MasterKey, εξασφαλίζοντας ότι ακόμη και σε περίπτωση επιτυχούς επίθεσης στη διαδικασία αποθήκευσης κλειδιών της συσκευής δεν θα υπάρχει πρόβλημα.

4.4.3.4 – Ασφάλεια των MicroControlerUnit

Μετά το πέρας της ασφαλούς αποθήκευσης των διαπιστευτηρίων στη συσκευή, διατρέχουν άλλους κινδύνους κυρίως φυσικών επιθέσεων. Οι μικροελεγκτές (MCU) ενσωματώνουν λειτουργίες ασφαλείας όπως η διάθεση ειδικής μνήμης για την αποθήκευση των κλειδιών. Η μνήμη αυτή είναι μόνο για εκτέλεση και διαθέτει μηχανισμούς ανίχνευσης παραβιάσεων (Tampering alerts). Παραδείγματα των συγκεκριμένων μικροελεγκτών υπάρχουν στην καθημερινότητα μας, όπως για παράδειγμα το POS.

4.4.3.5 – Στοιχείο Ασφαλείας

Η πιο αποτελεσματική ασφάλιση διαπιστευτηρίων των συσκευών στη τεχνολογία του Sigfox παρέχεται από το Στοιχείο Ασφαλείας (Secure Element - SE), ένα τσιπ ανθεκτικό στην παραβίαση, σχεδιασμένο να αντιστέκεται στις πιο πολύπλοκες επιθέσεις. Παραδείγματα που χρησιμοποιούν το αντίστοιχο στοιχείο ασφαλείας είναι η χρησιμοποίηση του σε πιστωτικές κάρτες, κάρτες SIM, βιομετρικά διαβατήρια.

4.4.3.6 – Κρυπτογράφηση δεδομένων

Το Sigfox προσφέρει την δυνατότητα στους χρήστες των συστημάτων του να εμπλουτίσουν το σύστημά τους με τη μέθοδο κρυπτογράφησης δεδομένων. Για να μπορέσει να το προσφέρει αυτό, το Sigfox συνεργάζεται με το εξειδικευμένο ερευνητικό ίδρυμα κρυπτογραφίας [52]. Μέσω της συνεργασίας δημιουργήθηκε ένας ισχυρός αλγόριθμος κρυπτογράφησης δεδομένων που δεν επηρεάζει το μέγεθος μετά το πέρας της κρυπτογράφησης. Η μέθοδος κρυπτογράφησης χρησιμοποιεί το AES-128 σε λειτουργία CTR.

Η αποκρυπτογράφηση στην περίπτωση χρησιμοποίησης της παραπάνω μεθόδου κρυπτογράφησης από τον χρήστη, πραγματοποιείται πριν την παράδοση των δεδομένων στον χρήστη, που σημαίνει ότι εκτελείται στον βασικό πυρήνα και τους εξυπηρετητές του Sigfox. Στην περίπτωση που ο χρήστης επιθυμεί να εμπλουτίσει έναν δικό του μηχανισμό κρυπτογράφησης, τον συμπεριλαμβάνει στη σύνδεση των διεπαφών του με τους εξυπηρετητές του Sigfox. Οπότε το Sigfox δεν θα μπορεί να «βλέπει» τα δεδομένα του χρήστη, καθώς θα τα αποκρυπτογραφεί ο ίδιος. Και στις δύο περιπτώσεις, με την χρήση των μεθόδων κρυπτογράφησης εμποδίζεται η υποκλοπή και η κρυφή ακρόαση των προσωπικών δεδομένων από επιτήδειους.

4.5 – Επιθέσεις ασφαλείας NB-IoT

Οι επιθέσεις ασφαλείας που παρατηρούνται στη τεχνολογία του NB-IoTμπορούν να στοχεύουν στα αρχιτεκτονικά επίπεδα του. ΤοNB-IoTαποτελεί ένα αποτέλεσμα έρευνας του 3GPP που συνεπάγεται ότι έχει κληρονομήσει τα χαρακτηριστικά των προτύπων τους, άρα και τα ευάλωτα χαρακτηριστικά τους.

4.5.1 – Επίπεδα Αρχιτεκτονικής NB-IoT

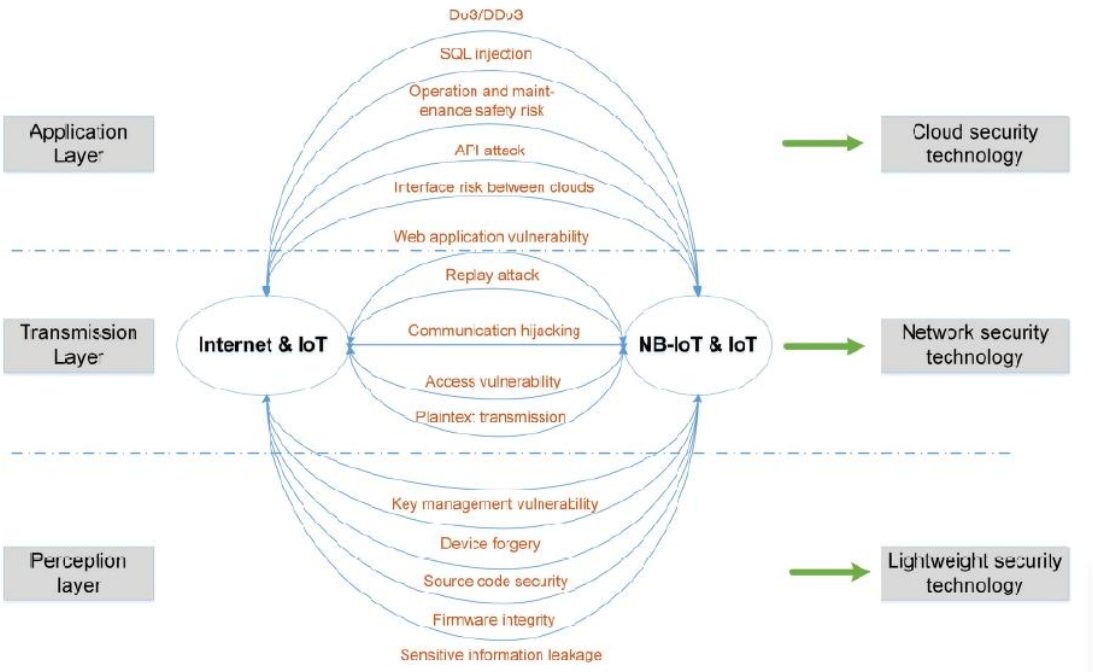
Τα βασικά χαρακτηριστικά της τεχνολογίας του NB-IoT μπορούν να διαχωριστούν και να αναλυθούν σε τρία επίπεδα βασισμένα στην αρχιτεκτονική του TCP/IP μοντέλου [53]. Στη εικόνα 24 αναγράφονται και απεικονίζονται τα βασικά χαρακτηριστικά των επιπέδων τα οποία είναι::

- Το επίπεδο των αισθητήρων και τελικών συσκευών, «επίπεδο Αντίληψης» (Perception Layer),
- Το επίπεδο επικοινωνίας των συσκευών δικτύου, «επίπεδο Δικτύου» (Network Layer),
- το επίπεδο των δεδομένων και των διεπαφών, «επίπεδο Εφαρμογών» (Application Layer).

Εικόνα 24 Επίπεδα αρχιτεκτονική συστημάτων βασισμένα στο μοντέλο TCP/IP[54].

Τα επίπεδα αρχιτεκτονικής για τον διαχωρισμό των επιθέσεων αντιστοιχούν και στα επίπεδα ασφαλείας του NB-IoT όπως απεικονίζεται στην εικόνα 25.

- Στο επίπεδο Εφαρμογών χρησιμοποιούνται οι τεχνολογίες ασφαλείας του TMSI που δέχεται επιθέσεις τύπου τεχνικών παρεμβολών.
- Στο επίπεδο Δικτύου χρησιμοποιούνται οι τεχνολογίες ασφαλείας που κληρονομούνται από τα δίκτυα LTE (EPSAKA). Στο επίπεδο αυτό πραγματοποιούνται οι περισσότερες επιθέσεις δικτύου όπως για παράδειγμα η επίθεση επανάληψης και γενικότερα τεχνικές παρεμπόδισης.
- Στο επίπεδο Αντίληψης χρησιμοποιούνται οι τεχνολογίες ασφαλείας της μονάδας ταυτότητας χρήστη (UICC) που δέχονται φυσικές επιθέσεις με κύριο στόχο τα διαπιστευτήρια των συσκευών.



Εικόνα 25 Αντιστοιχία επιθέσεων στο μοντέλο TCP/IPμε τα επίπεδα ασφαλείας του NB-IoT[54]

4.5.1.1 – Επίπεδο Αντίληψης

Το επίπεδο αντίληψης, γνωστό και ως επίπεδο τελικών συσκευών αποτελείται όπως είναι λογικό από τις τελικές συσκευές και το δίκτυο αισθητήρων που τις διακατέχουν. Η κύρια λειτουργία του οι λειτουργικές απαιτήσεις του συστήματος που αφορούν τη συλλογή δεδομένων όπως τηλεμέτρησης νερού. Ασχολείται δηλαδή με τη συλλογή μετρητικών δεδομένων από αισθητήρες που μετράνε νερό, αντιλαμβάνονται καπνό και κίνηση αλλά εκτελούν και διεργασίες όπως δημιουργία ήχου (ήχοι προειδοποίησης), άνοιγμα κλείσιμο ηλεκτροβάνας και ανάλογες λειτουργίες των περιπτώσεων χρήσης τους. Στη συνέχεια οι πληροφορίες αυτές αποστέλλονται στο επίπεδο δικτύου [55].

Παρόμοια με το επίπεδο αντίληψης των IoT δικτύων, το επίπεδο αντίληψης της τεχνολογίας του NB-IoT δέχεται παθητικές επιθέσεις (Passive attacks) και ενεργές επιθέσεις (active attacks), οι οποίες έχουν στόχο τους μηχανισμούς αυθεντικοποίησης των τελικών συσκευών προς το σύστημα.[54].

4.5.1.1.1 – Παθητικές επιθέσεις

Στις παθητικές επιθέσεις, όπως αναφέρθηκε και στις γενικές επιθέσεις των LPWAN μία κακόβουλη οντότητα έχει σαν στόχο να υποκλέπτει μόνο τις πληροφορίες χωρίς να παραποιήσει τα δεδομένα. Η κύρια μέθοδος παθητικής επίθεσης είναι αυτή του κρυφακούσματος, όπου αν η κακόβουλη οντότητα καταφέρει και υποκλέψει τα διαπιστευτήρια θα έχει στη διάθεση της τη δυνατότητα να αποκρυπτογραφήσει και τα δεδομένα που αποστέλλονται στο δίκτυο.

4.5.1.1.2 – Ενεργές επιθέσεις

Στις ενεργές επιθέσεις περιλαμβάνονται οι επιθέσεις που στοχεύουν την ακεραιότητα και παραποίηση δεδομένων. Συνεπώς οι επιθέσεις αυτές έχουν μεγαλύτερο αντίκτυπο στην ομαλή λειτουργία του δικτύου σε σχέση με τις παθητικές επιθέσεις, που μπορούν όμως να αποβούν μοιραίες για τη λειτουργία του παρόχου(πχ εκβιασμός). Οι τεχνικές επιθέσεων ενεργούς επίθεσης στο επίπεδο αντίληψης, περιλαμβάνουν την φυσική επίθεση στις τελικές συσκευές (την έκθεση των τελικών συσκευών και των κλειδιών τους) αλλά και τεχνικές όπως του

ενδιάμεσου ανθρώπου με τις επιθέσεις που παράγονται από αυτό, όπως η επίθεση μετατροπής χαρακτήρα.

4.5.1.1.3 – Πιθανοί Τρόποι αντιμετώπισης

Αποτελεσματικοί μέθοδοι κρυπτογράφησης των δεδομένων, η ταυτοποίηση των συσκευών και η ακεραιότητα τους, μπορούν να υιοθετηθούν για την αντιμετώπιση των παραπάνω επιθέσεων. Μία αποτελεσματική μέθοδος κρυπτογράφησης μπορεί να χρησιμοποιήσει σαν παράμετρο την τιμή που είναι αποτέλεσμα του τυχαίου μηχανισμού προ-κατανομής κλειδιού (random key pre-allocation mechanism), τον προκαθορισμένο μηχανισμό κατανομής κλειδιών (deterministic key pre-allocation mechanism) και το μηχανισμό κωδικού πρόσβασης που βασίζεται στην ταυτότητα (password mechanism based on identity)[54].

4.5.1.2 – Επίπεδο Δικτύου

Το επίπεδο δικτύου βρίσκεται ενδιάμεσα από τα επίπεδα αντίληψης και εφαρμογών που το καθιστά υπεύθυνο για την ασφαλή μεταφορά των πακέτων ανάμεσα τους. Έχει στη διάθεση του ένα μεγάλο εύρος πρωτοκόλλων, τα οποία καθορίζουν τον τρόπο με τον οποίο αποστέλλονται τα δεδομένα, τον τρόπο λήψης τους αλλά και την διάταξή τους.

Στα πρωτόκολλα LPWAN όπως αποτελούν οι τεχνολογίες του NB-IoT, LoRaWAN και Sigfox για την αποτελεσματική λειτουργία τους και την εφαρμογή των χαρακτηριστικών (μεγάλης εμβέλειας, μικρού κόστους και ελάχιστης κατανάλωσης ενέργειας), το δίκτυο των συστημάτων που διαχειρίζονται αποτελείτε όπως είδαμε και παραπάνω από μία πύλη αναμετάδοσης τον συγκεντρωτή (gateway) ο οποίος συλλέγει δεδομένα και πληροφορίες από τις τελικές συσκευές (end-device) και μετά τα τροφοδοτεί στον εξυπηρετητή του συστήματος. Συνεπώς, τα προβλήματα όπως η δικτύωση των συσκευών, η συνεχώς αναβάθμιση των μπαταριών υψηλού κόστους και μεγάλης διάρκεια ζωής, αλλά και η απόσταση που πρέπει να καλύψει με ασφάλεια ένα πακέτο, επιλύονται. Ωστόσο, όπου υπάρχει ασύρματο δίκτυο

υπάρχουν και επιθέσεις ασφαλείας που πρέπει να αντιμετωπιστούν και το επίπεδο δικτύου του NB-IoT δεν αποτελεί εξαίρεση[54].

Οι επιθέσεις ασφαλείας που πραγματοποιούνται στο επίπεδο δικτύου έχουν σαν στόχο την ταυτότητα των συσκευών ~~και~~ την πιθανή πλαστογράφηση τους αλλά και τη παρεμβολή του δικτύου και τη συνδεσιμότητα των συσκευών με αυτό. Με αποτέλεσμα, τα δεδομένα να μην μπορούν να συλλεχθούν αποτελεσματικά [55]. Αναφορικά κάποιες από τις επιθέσεις που στοχεύουν το επίπεδο δικτύου της τεχνολογίας NB-IoT είναι:

4.5.1.2.1 – Έκθεση τελικών συσκευών και των κλειδιών τους

Η τεχνολογία του NB-IoT σύμφωνα με τα χαρακτηριστικά της είναι σε θέση να υποστηρίξει την επικοινωνία σε ένα μεγάλο αριθμό τελικών συσκευών ανάλογα με τη περίπτωση χρήση της. Η κύρια πρόκληση στην επίθεση έκθεσης των τελικών συσκευών είναι για να εκτεθούν τα κλειδιά τους που είναι απαραίτητα για την αυθεντικοποίηση της ταυτότητας του αποστολέα και τον έλεγχο πρόσβασης του, που είναι απαραίτητος για τη διασφάλιση της ακεραιότητας των δεδομένων.

4.5.1.2.2 – Τεχνικές παρεμβολών

Μία κακόβουλη οντότητα είναι σε θέσει με το κατάλληλο υλικό και τις γνώσης της να καταφέρει να μεταδίδει σήματα παρεμβολής με σκοπό την άρνηση παροχής υπηρεσιών του δικτύου που είναι συνδεδεμένες οι συσκευές του συστήματος. Όπως αναφέρθηκε οι τεχνολογίες των πρωτοκόλλων LPWAN έχουν τη δυνατότητα να υποστηρίξουν ένα μεγάλο αριθμό τελικών συσκευών, γεγονός το οποίο μία κακόβουλη οντότητα θα μπορούσε να εκμεταλλευτεί για να πραγματοποιηθεί η επίθεση Άρνηση Παροχής Υπηρεσιών(Denial of Service DoS) με τη εκμετάλλευση τελικών συσκευών που ελέγχει ο ίδιος επηρεάζοντας την απόδοση του δικτύου.

4.5.1.2.3 – Πιθανοί Τρόποι αντιμετώπισης

Για να μπορέσει ένας πάροχος υπηρεσιών που χρησιμοποιεί τη τεχνολογία NB-IoTθα πρέπει να διαθέτει στο σύστημα του έναν αποτελεσματικό μηχανισμό ελέγχου ταυτότητα από άκρο σε άκρο και την κατάλληλη λειτουργία μεθόδου κρυπτογράφησης. Με την αξιοποίηση των μηχανισμών ανίχνευσης και προστασίας που το NB-IoTέχει κληρονομήσει από τα δίκτυα LTE προλαμβάνει τις επιθέσεις αυτές, και διασφαλίζει την εντόπιση κακόβουλων πληροφοριών που εισάγονται από κακόβουλες συσκευές. Ένας τέτοιος τρόπος αντιμετώπισης είναι ο μηχανισμός “Colonel blotto” που αναφέρθηκε στο κεφάλαιο των επιθέσεων ασφαλείας του πρωτοκόλλου LoRaWAN[45].

4.5.1.3 – Επίπεδο Εφαρμογών

Ο στόχος του επιπέδου εφαρμογή στην τεχνολογία του NB-IoT είναι η αποτελεσματική αποθήκευση, ανάλυση και διαχείριση των δεδομένων που προέρχονται από τις τελικές συσκευές και την διάθεση τους στους τελικούς χρήστες και παρόχους του συστήματος. Μετά από το επίπεδο αντίληψης και το επίπεδο δικτύου, τα δεδομένα που παράγονται από τις τελικές συσκευές και αποστέλλονται μέσω του επιπέδου δικτύου έχουν σαν τελικό αποδέκτη το πλήθος των εξυπηρετητών που διαχειρίζεται το επίπεδο εφαρμογής. Στη συνέχεια, αποθηκεύονται στους εξυπηρετητές και με την χρησιμοποίηση διαφόρων εφαρμογών και μηχανισμών οπτικοποίησης δρομολογούνται με την εκμετάλλευση διεπαφών στους χρήστες του συστήματος αναλόγως τη περίπτωση χρήσης του συστήματος. Σε σύγκριση με το επίπεδο εφαρμογής του ενός παραδοσιακού δικτύου IoT, το επίπεδο εφαρμογής της τεχνολογίας NB-IoT μεταφέρει μεγαλύτερο μέγεθος δεδομένων[54].

Δεδομένου των παραπάνω ότι τα ένα μεγάλο πλήθος δεδομένων ανταλλάσσονται μεταξύ πολλών οντοτήτων, όπως είναι οι βάσεις δεδομένων των εξυπηρετητών και οι διεπαφές, είναι αρκετά πιθανό η ασφάλεια τους να εκτίθεται σε επιθέσεις προτού η πληροφορία να φτάσει στους τελικούς χρήστες. Οι απειλές ασφάλειας μπορεί να προέρχονται από το εσωτερικό του επιπέδου μέσω κάποιας μη εξουσιοδοτημένης πρόσβασης που συνεπάγεται με κλοπή δεδομένων, εισαγωγή πλαστών δεδομένων, ιών. Υπάρχει και η πιθανότητα επίθεσης μέσω του επιπέδου

δικτύου με τη μεταβολή των πληροφοριών προορισμού για τα δεδομένα που αποθηκεύονται [55]. Επιθέσεις που στοχεύουν τη ταυτότητα των δεδομένων που προέρχονται από το δίκτυο του NB-IoT είναι:

4.5.1.3.1 – Επίθεση στην Ακεραιότητα και στον Έλεγχο ταυτότητας και πρόσβασης δεδομένων

Η γενική αυτή επίθεση αποτελεί το βασικό πρόβλημα του επιπέδου εφαρμογών του NB-IoT, όπου η αποτελεσματική αυθεντικοποίηση και η σωστή διαχείριση των δεδομένων με τους υπολογιστικούς πόρους που υπάρχουν να είναι η μοναδική λύση.

Τα δεδομένα που λαμβάνονται επίπεδο εφαρμογής όπως αναφέρθηκε, προέρχονται από το επίπεδο δικτύου και αντίληψης. Οι επιθέσεις που πραγματοποιούνται πριν το επίπεδο εφαρμογής, μπορεί να προκύψουν κατά τη συλλογή και μετάδοση των δεδομένων από τις τελικές συσκευές και του συγκεντρωτή, όπου υπάρχει η πιθανότητα η ακεραιότητα των δεδομένων να υπόκειται σε διάφορους βαθμούς βλάβης και εκτός αυτού μια παράνομη κίνηση παραποίησης δεδομένων από κάποια κακόβουλη οντότητα θα είχε ως αποτέλεσμα την απώλεια ακεραιότητας των δεδομένων αυτών. Επομένως, το επίπεδο εφαρμογής και η χρήση των δεδομένων σε αυτό μπορεί να επηρεαστεί αρνητικά. Επιπλέον, το επίπεδο εφαρμογής μπορεί να πραγματοποιηθούν επιθέσεις ακεραιότητας και πρόσβασης δεδομένων διότι στο σύστημα ενός δικτύου NB-IoT υπάρχουν αρκετές ομάδες χρηστών. Η πρόσβαση και η επεξεργασία των δεδομένων που έχει ο κάθε χρήστης είναι διαφορετική. Οπότε οι μηχανισμοί ελέγχου πρόσβασης για τα δεδομένα είναι υποχρεωτικοί.

4.5.1.3.2 – Πιθανοί Τρόποι αντιμετώπισης

Η επίλυση αυτών των προβλημάτων ασφάλειας, διασφαλίζεται με τη υλοποίηση αποτελεσματικών μηχανισμών επαλήθευσης της ταυτότητας των δεδομένων. Επιπλέον, η εξασφάλιση της ασφάλειας των δεδομένων από τους μη εξουσιοδοτημένους χρήστες απαιτεί την υλοποίηση μηχανισμών ταυτοποίησης χρηστών κατά τη διάρκεια διαδικασιών αποθήκευσης και αποστολής των δεδομένων στους τελικούς χρήστες.

4.6 – Επίλογος κεφαλαίου

Στο κεφάλαιο αυτό πραγματοποιήθηκε μία αναφορά των επιθέσεων που στοχεύουν τα δίκτυα LPWAN. Στη συνέχεια αναφέρθηκαν οι επιθέσεις που δέχονται τα δίκτυα ανάλογα με την αρχιτεκτονική τους, κάθε βασικό πρότυπο δικτύων LPWAN καθώς και οι τρόποι αντιμετώπισης τους. Οι επιθέσεις αυτές κατηγοριοποιήθηκαν ανάλογα με τον τρόπο λειτουργία τους, και αναφέρθηκαν σε κάθε ένα πρωτόκολλο που αναλύεται στην εργασία.

Τα πρωτόκολλα αποτελούν τα βασικά πρότυπα δικτύων LPWAN, έχουν χρησιμοποιηθεί σε πολλά καινοτόμα συστήματα IoT, όπου συνεπάγεται ότι τα συστήματα αυτά δέχονται κατά την διάρκεια ζωής τους συνεχώς τις επιθέσεις που αναφέρθηκαν παραπάνω. Κάθε σύστημα αποτελεί μία περίπτωση χρήσης των πρωτοκόλλων αυτών και κάθε επίθεση μία ακόμα δυσκολία στο σύστημα ασφαλείας τους.

ΚΕΦΑΛΑΙΟ 5 – ΠΕΡΙΠΤΩΣΕΙΣ ΧΡΗΣΗΣ LPWAN

5.1 – Εισαγωγή

Στο κεφάλαιο αυτό αναφέρονται οι περιπτώσεις χρήσης των βασικών προτύπων LPWAN. Τα βασικά πρότυπα αποτελούν τη κινητήρια «δύναμη» των συστημάτων IoT που κάνουν χρήση των πρωτοκόλλων αυτών. Οι περιπτώσεις χρήσης των πρωτοκόλλων που αναφέρονται στην εργασία είναι τρείς και αντιπροσωπεύουν ένα «έξυπνο» σύστημα υποδομής IoT, ένα για κάθε πρωτόκολλο.

Για την σύγκριση και την αποτελεσματικότητα των χαρακτηριστικών ασφαλείας των τεχνολογιών LPWAN που αναλύουμε στην εργασία αυτή, εξετάζουμε ένα σύνολο παραδειγμάτων περιπτώσεων χρήσης. Επιλέχθηκαν τρεις “έξυπνες” υποδομές συστημάτων, αυτή της έξυπνης τηλεμέτρησης κατανάλωσης νερού, του έξυπνου οδικού φωτισμού και της έξυπνης ανίχνευσης καπνού καθώς και τις περιπτώσεις χρήσεων που χρησιμοποιήθηκαν για κάθε μία από τις υποδομές, παράλληλα με τις τεχνολογίες LPWAN (NB-IoT, LoRaWAN, Sigfox αντίστοιχα) που χρησιμοποιούν.

Για να οργανώσουμε τους κινδύνους που διατρέχουν τα παραπάνω έξυπνα συστήματα υποδομών, αναφερόμαστε στις κατηγορίες STRIDE από τη Διαδικασία Μοντελοποίησης Απειλών της Microsoft[56].

Στη συνέχεια για κάθε μία περίπτωση χρήσης, αναφέρονται οι επιθέσεις που μπορεί να δεχθεί το σύστημά τους, αλλά και οι τρόποι αντιμετώπισης και διασφάλισης του συστήματος απέναντι στις επιθέσεις που αναλύονται.

5.2 – Διαδικασία Μοντελοποίησης - STRIDE

Το **STRIDE** είναι ένα μοντέλο κατηγοριοποίησης απειλών που αναπτύχθηκε από τη Microsoft για τον εντοπισμό απειλών για την ασφάλεια των συστημάτων. Όπως βλέπουμε και στο πίνακα 4 οι απειλές ασφάλειας χωρίζονται σε έξι κατηγορίες:

- **S**poofing - Πλαστογράφηση: Ένας εισβολέας προσπαθεί να είναι κάτι ή κάποιος που δεν είναι.
- **T**ampering - Αλλοίωση: Τροποποίηση δεδομένων ή κώδικα.

- **R**epudiation - Απάρνηση: Ισχυρισμός ότι δεν έχει εκτελεστεί κάποια ενέργεια.
- **I**nformation Disclosure - Αποκάλυψη πληροφοριών: Έκθεση πληροφορίας σε κάποιον που δεν είναι εξουσιοδοτημένος να το δει.
- **D**enial of Service - Άρνηση παροχής υπηρεσιών: Άρνηση ή υποβάθμιση της υπηρεσίας προς το χρήστη.
- **E**levation of privilege - Παραποίηση Προνομίων: Πρόσβαση στις υπηρεσίες χωρίς τη σωστή εξουσιοδότηση.

Οι κατηγορίες Απάρνησης και Παραποίησης Προνομίων έχουν σαν σημείο αναφοράς την εξουσιοδότηση ανθρωπίνου δυναμικού που περιλαμβάνει και την έναρξη κάποιας ενέργειας, για περιπτώσεις χρήσης IoT, οι οποίες συνήθως δεν περιλαμβάνουν ανθρώπινη αλληλεπίδραση, είναι λιγότερο σχετικές.

Πίνακας 4 Κατηγορίες απειλών του μοντέλου STRIDE [57]

Property	Threat	Definition	Example
Authentication	**S**poofing	Impersonating something or someone else.	Pretending to be any of billg, microsoft.com or ntdll.dll
Integrity	**T**ampering	Modifying data or code	Modifying a DLL on disk or DVD, or a packet as it traverses the LAN.
Non-repudiation	**R**epudiation	Claiming to have not performed an action.	"I didn't send that email," "I didn't modify that file," "I *certainly* didn't visit that web site, dear!"
Confidentiality	**I**nformation Disclosure	Exposing information to someone not authorized to see it	Allowing someone to read the Windows source code; publishing a list of customers to a web site.
Availability	**D**enial of Service	Deny or degrade service to users	Crashing Windows or a web site, sending a packet and absorbing seconds of CPU time, or routing packets into a black hole.
Authorization	**E**levation of Privilege	Gain capabilities without proper authorization	Allowing a remote internet user to run commands is the classic example, but going from a limited user to admin is also EoP.

Στις παρακάτω υποενότητες αναπτύσσονται οι περιπτώσεις χρήσης των LPWAN και τα θέματα ασφαλείας τους σύμφωνα με το STRIDE.

5.3 – Έξυπνη τηλεμέτρηση κατανάλωσης νερού

Η έξυπνη τηλεμέτρηση κατανάλωσης νερού ή Smart Water Metering είναι μια τεχνολογία IoT που αποτελεί βασικό παράγοντα για την ανάπτυξη των **ευφυών πόλεων** (smart cities) που είναι απαραίτητη για την εξέλιξη της τεχνολογίας και της βιωσιμότητας των ανθρώπων.

Αποτελεί μια «έξυπνη» υποδομή συστήματος για τις σημερινές παγκόσμιες βιομηχανίες νερού όπως βλέπουμε στην εικόνα 26, όπου μέσω της παρουσίας των τεχνολογικά ανεπτυγμένων μετρητών νερού (ηλεκτροβάνες-υδρόμετρα) μετρούν και διαχειρίζονται τη κατανάλωση κατά τη διάρκεια συγκεκριμένων χρονικών περιόδων και μέσω διεπαφών μπορούν να μοιράζονται τις μετρήσεις αυτές καθημερινά στους χρήστες. Ακόμα, μέσω ενός καναλιού επικοινωνίας, πετυχαίνεται η χρησιμότητα του συστήματος, όπου έχει τη δυνατότητα να διαβάζει τη ζήτηση και την καθημερινή κατανάλωση του νερού, για να διαπιστωθεί αν υπάρχει κάποια διαρροή στο μετρητή και στις εγκαταστάσεις του, και να εκδίδει εντολές προς το μετρητή για την εκτέλεση ειδικών καθηκόντων, όπως η αποσύνδεση-σύνδεση ή ο περιορισμός της ροής του νερού. Τα αποτελέσματα αυτά της κατανάλωσης και των διαφόρων λειτουργιών, απεικονίζονται και σε μια μικρή οθόνη που υπάρχει στους μετρητές για την διευκόλυνση των εξουσιοδοτημένων τεχνικών. Αυτά μπορούν να βοηθήσουν τους πελάτες να ελέγξουν για διαρροές, να μειώσουν την κατανάλωση και να ελέγξουν τη συμμόρφωση με τους τοπικούς περιορισμούς.

Ο μετρητής νερού που αναφέρθηκε παραπάνω είναι μια συσκευή (end-device) που χρησιμοποιείται για τη μέτρηση της ποσότητας νερού που καταναλώνεται σε ένα κτίριο. Ένας "έξυπνος" μετρητής νερού είναι μια συσκευή μέτρησης που έχει τη δυνατότητα να αποθηκεύει και να μεταδίδει συχνά δεδομένα κατανάλωσης. Ακόμα, εκτός από τη μέτρηση του όγκου που καταναλώνεται, καταγράφουν επίσης την ημερομηνία και την ώρα της κατανάλωσης, τις φυσικές επιθέσεις που δέχονται

αλλά και τις κατάλληλες εντολές για την σύνδεση-αποσύνδεση και μείωση της ροής νερού στις ηλεκτροβάνες[58].

Εικόνα 26 Αρχιτεκτονική «έξυπνης» υποδομής συστήματος τηλεμέτρησης κατανάλωσης νερού[58]

5.3.1 – Περίπτωση χρήσης

Η εταιρεία επικοινωνίας Vodafone και ο πάροχος νερού Aguas de Valencia διαχειρίζονται έξυπνους μετρητές νερού μέσω μιας υποδομής συστήματος τηλεμέτρησης κατανάλωσης νερού στην Ισπανία, χρησιμοποιώντας την τεχνολογία LPWAN και συγκεκριμένα NB-IoT. Οι LPWAN τεχνολογίες είναι πολύ χρήσιμες για τις επιχειρήσεις που ζητούν «έξυπνες» λύσεις, διότι πετυχαίνεται η συχνότερη ανάγνωση μετρητών και η απόκτηση τους χωρίς να χρειάζεται να επισκεφθούν τη θέση του μετρητή. Το NB-IoT είναι ελκυστικό για αυτή τη χρήση λόγω της χαμηλής κατανάλωσης ενέργειας και της καλής διάδοσης σε δύσκολες τοποθεσίες. Οι μετρητές εγκαθίστανται σε οικιακούς και εμπορικούς χώρους εκτελώντας τις παραπάνω έξυπνες λειτουργίες [26].

Υπάρχει μια σειρά σημαντικών απειλών στην περίπτωση χρήσης του Water Metering σύμφωνα με τα Security Threats του STRIDE:

- **Tampering- Αλλοίωση**
- **Spoofing - Πλαστογράφηση**

- **Information Disclosure- Αποκάλυψη πληροφοριών**
- **Denial of Service - Άρνηση παροχής υπηρεσιών**

5.3.1.1 – Αλλοίωση

Ένας επιτιθέμενος μπορεί να προσπαθήσει να τροποποιήσει τις μετρήσεις που έστειλε η συσκευή και για να το πετύχει αυτό χρησιμοποιεί επιθέσεις όπως τις παρακάτω.

5.3.1.1.1 – Έκθεση τελικών συσκευών και των κλειδιών τους

Η συγκεκριμένη επίθεση έχει ως στόχο την υποκλοπή των κλειδιών που είναι απαραίτητα για την ασφαλή επικοινωνία στο LPWAN δίκτυο. Αν κάποιος βρεθεί στον φυσικό χώρο που υπάρχουν οι τελικές συσκευές μπορεί αρχικά να υποκλέψει τα κλειδιά ή και να θέσει σε κίνδυνο τις ίδιες συσκευές και να υποκλέψει σημαντικές πληροφορίες για την ασφάλεια του συστήματος. Με τις πληροφορίες που μπορεί να υποκλέψει ο επιτήδειος, μπορεί να δημιουργήσει μία συσκευή με τα ίδια διαπιστευτήρια και να προχωρήσει σε επιθέσεις όπως του Ενδιάμεσου Ανθρώπου που είδαμε παραπάνω στις επιθέσεις των LPWAN και Μετατροπής Χαρακτήρα[42].

Με την χρησιμοποίηση μηχανισμών αντιμετώπισης δολιοφθοράς (tamper-proof) υπάρχει η δυνατότητα αποστολής μηνυμάτων ειδοποιήσεων για την άμεση ενημέρωση των ειδικών.

5.3.1.1.2 Επίθεση Μετατροπής Χαρακτήρα

Μία επίθεση Μετατροπής Χαρακτήρα στην περίπτωση χρήσης της τηλεμέτρησης κατανάλωσης νερού είναι μία επίθεση στον αλγόριθμο κρυπτογράφησης στον οποίο ο επιτήδειος μπορεί να αλλάξει το κρυπτογραφικό κείμενο που παράγεται. Σε μια τέτοια κατάσταση, ο επιτήδειος μπορεί να μετατρέψει το αρχικό μήνυμα σε ένα παρόμοιο μήνυμα στο οποίο μεταβάλλονται ορισμένες σημαντικές πληροφορίες. Όπως να αλλάξει την μέτρηση κατανάλωσης νερού του υδρομέτρου για να μειώσει την κατανάλωση του ή να κάνει κακό σε κάποιον τρίτο και να αυξήσει την κατανάλωσή του συγκεκριμένου [59].

5.3.1.2 – Πλαστογράφηση

Ένας επιτιθέμενος μπορεί να προσπαθήσει να αντικαταστήσει μια συσκευή και να έχει τη δυνατότητα να πραγματοποιήσει αλλαγές στο δίκτυο χωρίς την έγκριση από τους υπεύθυνους. Η ενέργεια αυτή πραγματοποιείται με την επίθεση Ενδιάμεσου Ανθρώπου.

5.3.1.2.1 – Επίθεση Ενδιάμεσου Ανθρώπου

Στην επίθεση αυτή μία κακόβουλη οντότητα βρίσκεται μεταξύ της συνομιλίας της τελικής συσκευής και του συγκεντρωτή (μπορεί και ανάμεσα του συγκεντρωτή με τον εξυπηρετητή) αντιπροσωπεύοντας και τους δύο. Δηλαδή για τη συσκευή λαμβάνει μηνύματα σαν έναν συγκεντρωτή και για το συγκεντρωτή στέλνει μηνύματα σαν συσκευή, στην περίπτωση της ανερχόμενης ζεύξης και στην περίπτωση της κατερχόμενης αντίστοιχα. Ένας επιτιθέμενος δηλαδή, μπορεί να προσπαθήσει να αντικαταστήσει μια νόμιμη συσκευή με μια πλαστογραφημένη συσκευή η οποία μεταδίδει εντολές σαν ένα συγκεντρωτή όπως το άνοιγμα και το κλείσιμο μιας ηλεκτροβάνας [46].

5.3.1.3 – Αποκάλυψη πληροφοριών

Η επίθεση αυτή, επιτυγχάνεται μέσω της πιο γνωστής επίθεσης του Κρυφακούσματος και της επίθεσης σκουληκότρυπας.

5.3.1.3.1 – Κρυφάκουσμα

Η επίθεση αυτή έχει ως στόχο την υποκλοπή πακέτων μεταξύ των τελικών συσκευών (ηλεκτροβανών-υδρομέτρων) και του συγκεντρωτή. Αυτό το πετυχαίνει “σπάζοντας” τον τρόπο κρυπτογράφησης του LPWAN που χρησιμοποιείται. Από την στιγμή που ο επιτήδειος θα μπορεί να «ακούσει» τα πακέτα-μηνύματα και συγχρόνως τα δεδομένα τους, αποτελεί πρόβλημα για την προστασία της ιδιωτικής ζωής. Δεδομένου ότι τα δεδομένα χρήσης νερού από μια ιδιωτική κατοικία και όχι μόνο θα μπορούσαν να χρησιμοποιηθούν για την εξαγωγή συμπερασμάτων σχετικά με τις δραστηριότητες των κατοίκων[46].

5.3.1.3.2 – Επίθεση σκουληκότρυπας

Σε αυτό τον τύπο επίθεσης, μια κακόβουλη συσκευή υποκλέπτει τα πακέτα από μία συσκευή και τα μεταδίδει σε μία άλλη. Ως εκ τούτου, τα σημαντικά μηνύματα συναγερμού (alarm messages) μπορούν να μπλοκαριστούν και τα μηνύματα που έχει υποκλέψει η κακόβουλη συσκευή να σταλθούν σαν να μην υπάρχει συναγερμός. Με αυτόν τον τρόπο οι επιθέσεις για την υποκλοπή των προσωπικών δεδομένων όπως το κρυφάκουσμα αλλά και επιθέσεις όπως ενδιάμεσου ανθρώπου δεν ανιχνεύονται εύκολα [42].

5.3.1.4 – Άρνηση παροχής υπηρεσιών

Ένας επιτιθέμενος μπορεί να προσπαθήσει να απενεργοποιήσει μεγάλο αριθμό συσκευών ή την υπηρεσία δικτύου. Για να επιτευχθεί η ενέργεια αυτή μπορούν να χρησιμοποιηθούν επιθέσεις όπως οι τεχνικές παρεμβολών και επιθέσεις επανάληψης.

5.3.1.4.1 – Τεχνικές Παρεμβολών

Η τεχνική αυτή επίθεσης είναι πολύ γενικό πρόβλημα στο IoT, κατά την οποία, κάποια κακόβουλη οντότητα μεταδίδει ένα ισχυρό ραδιοκύμα (radiosignal) κοντά στις συσκευές και διακόπτουν τις εκπομπές τους. Διακόπτοντας τις εκπομπές των εντολών στις ηλεκτροβάνες, προκαλεί σοβαρό πρόβλημα με το άνοιγμα/κλείσιμο της ροής του νερού. Ακόμα διακόπτοντας τις εκπομπές των υδρομέτρων προς το δίκτυο και τον εξυπηρετητή, δεν στέλνονται οι μετρήσεις κατανάλωσης. Με αυτά τα προβλήματα ουσιαστικά εκβιάζεται ο πάροχος υπηρεσιών[42].

5.3.1.4.2– Επίθεση επανάληψης

Η επίθεση αυτή πετυχαίνεται με το να ξαναστέλνονται ή να επαναλαμβάνονται δεδομένα από μία κακόβουλη οντότητα. Ο κύριος σκοπός αυτής της επίθεσης είναι να προκαλέσει σφάλμα στην συσκευή και να την απενεργοποιήσει πετυχαίνοντας ουσιαστικά μια επίθεση παρεμβολής. Σαν αποτέλεσμα της επίθεσης είναι τα παραπάνω προβλήματα επηρεάζοντας σημαντικά τον πάροχο υπηρεσιών[42]

5.4 – Έξυπνος οδικός φωτισμός

Ο έξυπνος οδικός φωτισμός είναι ακόμα μια πρωτοποριακή τεχνολογία IoT αποτελώντας μία από της αρχικές αλλά και βασικές τεχνολογίες των ευφυών πόλεων.

Το “έξυπνο” σύστημα αυτό, αναφέρεται στον δημόσιο φωτισμό που ενεργοποιείται ανάλογα της κίνησης των πεζών, των ποδηλάτων και των αυτοκινήτων. Ο έξυπνος φωτισμός του δρόμου, που μπορεί να αναφερθεί και ως «προσαρμοστικός» φωτισμός του δρόμου, σβήνει όταν οι αισθητήρες δεν ανιχνεύουν κάποια κινητικότητα, και φωτίζει όταν υπάρχει.

Αυτός ο τύπος φωτισμού του δρόμου όπως αναφέραμε είναι πολύ πιο πρακτικός και διαφορετικός από τον παραδοσιακό φωτισμό που είναι ενεργοποιημένος συνέχεια ή τον φωτισμό που απενεργοποιείται σε προκαθορισμένο χρόνο. Τα φώτα στο δρόμο μπορούν να γίνουν «έξυπνα» και να χρησιμοποιηθούν από τέτοιου είδους συστήματα, τοποθετώντας κάμερες και αισθητήρες πάνω τους, που τους επιτρέπει να ανιχνεύσουν κίνηση. Τεχνολογίες του τύπου LPWAN επιτρέπουν στα φώτα του δρόμου να επικοινωνούν μεταξύ τους. Διαφορετικές εταιρείες έχουν διαφορετικές παραλλαγές αυτής της τεχνολογίας. Όταν ένας πεζός ή κάποιο όχημα παντός τύπου ανιχνεύεται από μια κάμερα ή έναν αισθητήρα, θα επικοινωνήσει αυτό με τα γειτονικά φώτα του δρόμου, τα οποία θα αρχίσουν να φωτίζουν έτσι ώστε η παραπάνω οντότητα να είναι πάντα φωτισμένη [8] Ακόμα, προσθέτοντας στα έξυπνα φώτα λαμπτήρες τύπου LED, οι επιχειρήσεις κοινής ωφέλειας και άλλες επιχειρήσεις ηλεκτρισμού πετυχαίνουν και την μείωση του κόστους ενέργειας και λειτουργίας κατά 50% ή περισσότερο [9].

5.4.1 – Περίπτωση χρήσης

Η εταιρία Flashnet SRL με έδρα τη Ρουμανία που ειδικεύεται στις τεχνολογίες αιχμής, δημιούργησε και έχει στην διάθεση της το έξυπνο σύστημα του Streetlight InteliLIGHT® που φαίνεται και στην εικόνα 27 χρησιμοποιώντας LPWAN δίκτυο και συγκεκριμένα το πρωτόκολλο LoRaWAN. Το σύστημα αυτό έχει την δυνατότητα να χρησιμοποιηθεί είτε δημοσίως είτε από ιδιώτες, όπου είναι και ο κύριος στόχος.

Η χρησιμότητα ενός τέτοιου έξυπνου συστήματος είναι η εξοικονόμηση ενέργειας (τα φώτα λειτουργούν μέσω ενός ή περισσοτέρων αυτόνομων χρονοδιακοπτών, χωρίς να απαιτείται συνεχής και τακτική επικοινωνία από το διακομιστή) και παρακολούθηση της απόδοση ισχύος και η απομακρυσμένη ενημέρωση συντήρησης.

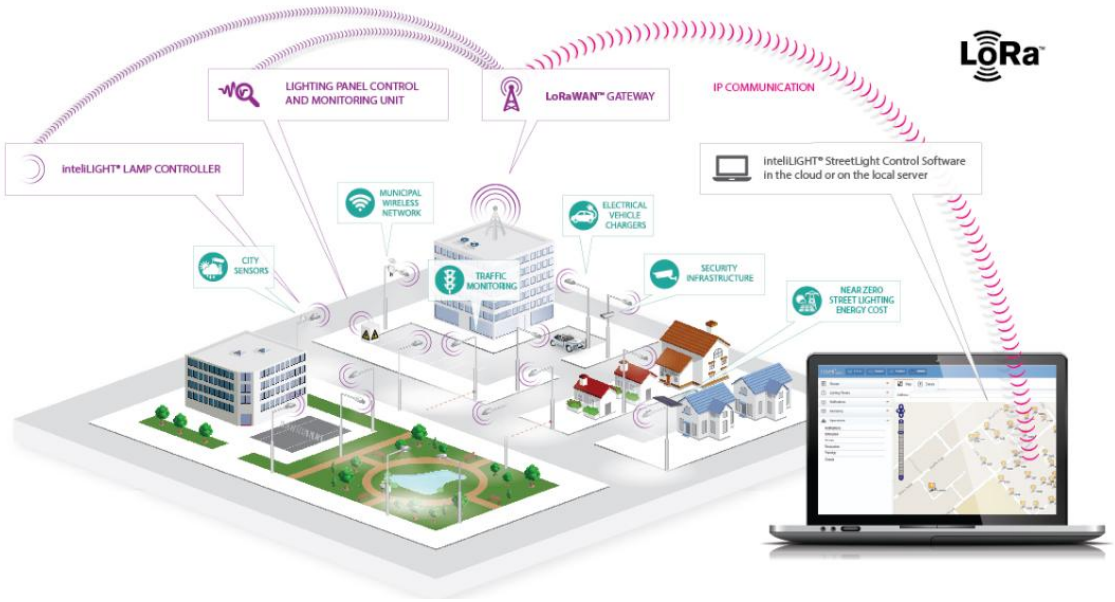
Για ένα τέτοιο αυτόνομο σύστημα ελέγχου φωτισμού υπάρχει μια σειρά πιθανών απειλών. Όπως για ένα ιδιωτικό σύστημα ενός διαμερίσματος/πολυκατοικίας οι κάτοικοι ενδέχεται να επιθυμούν να αλλάξουν το χρονοδιάγραμμα φωτισμού ώστε να παράγουν περισσότερη ώρα φωτισμού από ότι έχει ο προϋπολογισμός του συστήματος. Ακόμα μια πολύ σημαντική συνέπεια επίθεσης είναι η απενεργοποίηση του φωτισμού του δρόμου που μπορεί να σημαίνει ακόμα και πιθανή τρομοκρατική ενέργεια [26].

Παρόλα αυτά, με βάση την αυτόνομη λειτουργία του συστήματος για κάθε συσκευή, μετριάζεται ο κίνδυνος επιθέσεων άρνησης παροχής υπηρεσιών (Denial of Service) και δεν αποτελεί σοβαρό πρόβλημα. Επίσης δεν φαίνεται να υπάρχουν εμπιστευτικά δεδομένα ούτε επεξεργασία προσωπικών στοιχείων σε επιθέσεις υποκλοπής δεδομένων.

Οι παραπάνω σημαντικές απειλές στην περίπτωση χρήσης του έξυπνου οδικού φωτισμού σύμφωνα με το μοντέλο του STRIDE:

- **Spoofing -Πλαστογράφηση**
- **Tampering -Αλλοίωση**

Οι κυριότερες κινήσεις και έλεγχοι που μετριάζουν αυτούς τους παραπάνω κινδύνους είναι η επαλήθευση δικτύου (Network Authentication) και η ακεραιότητα των δεδομένων (Data Integrity). Η ανάκληση και η αντικατάσταση ελαττωματικών αισθητήρων και καμερών είναι εφικτή, καθώς έχουν την δυνατότητα μέσω τεχνικών συνεργείων την συντήρηση εξαρτημάτων των φώτων του δρόμου, καθιστώντας και δυνατή την ενημέρωση των συσκευών αυτών είτε απομακρυσμένα μέσω δικτύου είτε στην διάρκεια της συντήρησης.



Εικόνα 27 Αρχιτεκτονική δικτύου έξυπνου συστήματος Streetlight InteliLIGHT® [60]

5.4.1.1 – Πλαστογράφηση

Ένας επιτιθέμενος μπορεί να προσπαθήσει να αντικαταστήσει μια συσκευή εντός του δικτύου. Σαν αποτέλεσμα μπορεί να πραγματοποιήσει αλλαγές στο δίκτυο χωρίς την έγκριση από τους υπεύθυνους στέλνοντας τις επιθυμητές για αυτόν εντολές. Η ενέργεια αυτή είναι πολύ επικίνδυνη διότι του δίνεται η δυνατότητα να διαχειρίζεται τον φωτισμό ενός διαμερίσματος, μιας πολυκατοικίας ή ακόμα και μιας περιοχής, δίνοντας τη δυνατότητα ακόμα και μιας τρομοκρατικής επίθεσης. Η επίθεση αυτή μπορεί να πραγματοποιηθεί με την επίθεση Ενδιάμεσου Ανθρώπου.

5.4.1.1.1 – Επίθεση Ενδιάμεσου Ανθρώπου

Στην επίθεση αυτή μία κακόβουλη οντότητα βρίσκεται μεταξύ της συνομιλίας της τελικής συσκευής και της συσκευής που περιέχει τον μικροελεγκτή (Micro Controller Module) και τον πομποδέκτη (Transceiver Module) επηρεάζοντας την αποστολή των δεδομένων τους προς το συγκεντρωτή. Με αυτόν τον τρόπο χρησιμοποιεί την συσκευή χωρίς διαπιστευτήρια για να δίνει εντολές στις τελικές συσκευές και να επηρεάζει την λειτουργία τους μεταδίδοντας εντολές σαν ένα συγκεντρωτή, όπως το άνοιγμα και το κλείσιμο των φώτων σε μια περιοχή προκαλώντας σοβαρές επιπτώσεις [61].

5.4.1.2 – Αλλοίωση

Ένας επιτιθέμενος μπορεί να προσπαθήσει να τροποποιήσει είτε τις μετρήσεις που στέλνει η συσκευή προς τον εξυπηρετητή για την κατανάλωση είτε για να μπορέσει να τροποποιήσει το πρόγραμμα και την λειτουργία που έχουν προγραμματιστεί τα φώτα στη περιοχή που έχει σαν στόχο. Για να το πετύχει αυτό χρησιμοποιεί επιθέσεις όπως της Έκθεσης τελικών συσκευών και των κλειδιών τους και Μετατροπής Χαρακτήρα.

5.4.1.2.1 – Έκθεση τελικών συσκευών και των κλειδιών τους

Η συγκεκριμένη επίθεση έχει ως στόχο την υποκλοπή των κλειδιών που είναι απαραίτητα για την ασφαλή επικοινωνία στο LPWAN δίκτυο αλλά και να επηρεάσει πρακτικά τις τελικές συσκευές (αισθητήρες, LEDs). Αν κάποιος γνωρίζει και έχει τη δυνατότητα να βρεθεί στον φυσικό χώρο που υπάρχουν οι αισθητήρες και οι συσκευές που είναι υπεύθυνες για την ανταλλαγή πληροφοριών και εντολών, μπορεί αρχικά να υποκλέψει τα κλειδιά ή και να θέσει σε κίνδυνο τις ίδιες συσκευές και να υποκλέψει σημαντικές πληροφορίες για την ασφάλεια του συστήματος. Με τις πληροφορίες που μπορεί να υποκλέψει ο επιτήδειος, μπορεί να δημιουργήσει μία συσκευή με τα ίδια διαπιστευτήρια και να προχωρήσει σε επιθέσεις όπως του Ενδιάμεσου Ανθρώπου που είδαμε παραπάνω και Μετατροπής Χαρακτήρα[42].

Με την χρησιμοποίηση μηχανισμών αντιμετώπισης δολιοφθοράς (tamper-proof) υπάρχει η δυνατότητα αποστολής μηνυμάτων ειδοποιήσεων για την άμεση ενημέρωση των ειδικών.

5.4.1.2.2 – Επίθεση Μετατροπής Χαρακτήρα

Η επίθεση αυτή στην περίπτωση του έξυπνου οδικού φωτισμού είναι μία επίθεση στον αλγόριθμο κρυπτογράφησης στον οποίο ο επιτήδειος μπορεί να αλλάξει το κρυπτογραφικό κείμενο που παράγεται. Ο επιτήδειος έχει την δυνατότητα να αλλάξει δηλαδή το περιεχόμενο των δεδομένων είτε γνωρίζοντας τον τρόπο που

θα επηρεάσει την αλλαγή είτε όχι. Μια τέτοια περίπτωση επίθεσης αφορά τις ιδιωτικές κατοικίες, όπου ο επιτιθέμενος μπορεί να αλλάξει την μέτρηση κατανάλωσης ρεύματος των LED αισθητήρα για να μειώσει την κατανάλωση του ή ακόμα και για να αλλάξει τον τρόπο λειτουργίας τους αυξάνοντας και μειώνοντας τον χρόνο λειτουργίας τους [59].

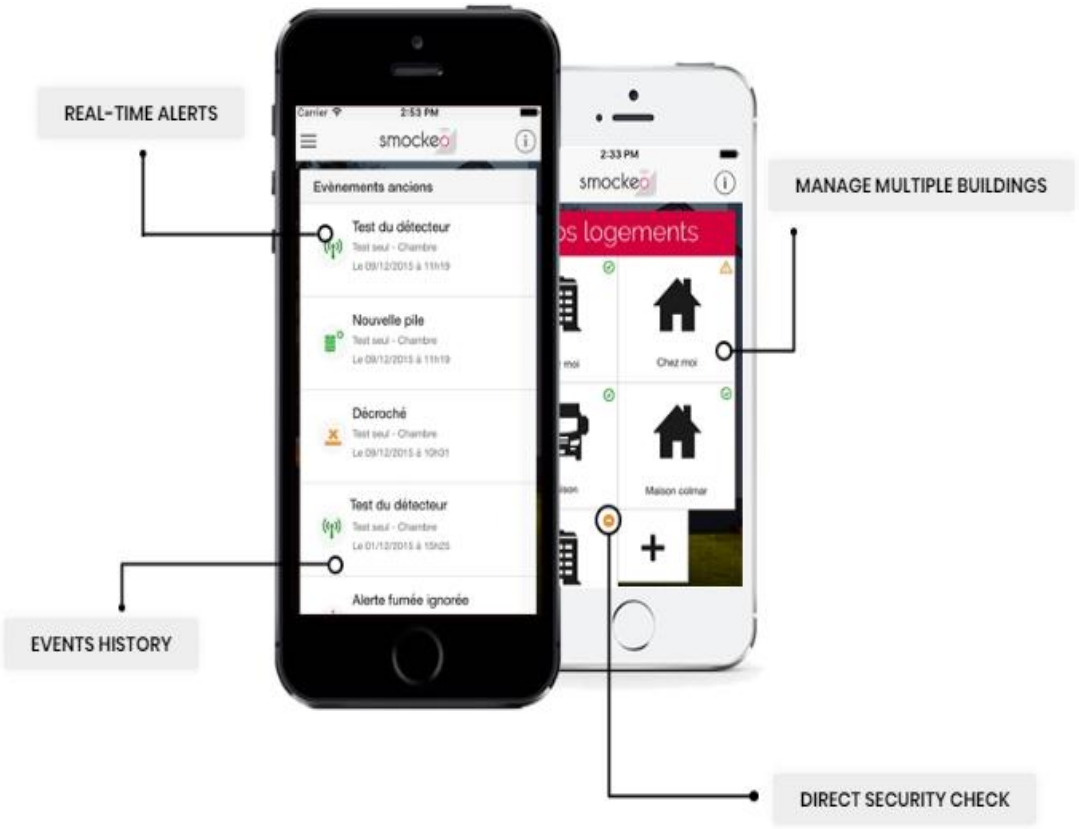
5.5 – Έξυπνη ανίχνευση καπνού

Έναν σύγχρονο, αξιόπιστο και με χαμηλό κόστος τρόπο ανίχνευσης πυρκαγιών προσφέρει η τεχνολογία «έξυπνης» ανίχνευσης καπνού. Ένας έξυπνος ανιχνευτής καπνού που χρησιμοποιεί η παραπάνω τεχνολογία, είναι μια συσκευή που αισθάνεται τον καπνό, συνήθως ως ένδειξη φωτιάς και την ίδια στιγμή παράγει έναν δυνατό προειδοποιητικό ήχο κίνδυνου, για να μπορέσει να ειδοποιήσει τους ενοίκους ή τους ανθρώπους που είναι κοντά.

Ο έξυπνος ανιχνευτής καπνού πέρα από συναγερμούς κινδύνου, στέλνει μηνύματα στην εφαρμογή του εξουσιοδοτημένου χρήστη όταν αισθάνεται καπνό, καθώς και ποιο δωμάτιο ή διαμέρισμα κινδυνεύει, παράδειγμα εφαρμογής μπορούμε να δούμε στην εικόνα 28. Επίσης περιλαμβάνει ειδοποιήσεις όταν η μπαταρία βρίσκεται σε χαμηλά επίπεδα και δίνει την δυνατότητα σίγασης των συναγερμών και ειδοποιήσεων από τον χρήστη μέσω της εφαρμογής. Ορισμένα άλλα χαρακτηριστικά που συμπεριλαμβάνονται στις έξυπνες συσκευές είναι οι φωνητικές προειδοποιήσεις, οι έλεγχοι που γίνονται ανά ορισμένα διαστήματα από την ίδια την συσκευή και οι αναφορές τους, καθώς και η δυνατότητα αυτόματης επικοινωνίας με ένα πρόσωπο ή κατά περιπτώσεις σε υπηρεσίες έκτακτης ανάγκης εάν δεν απαντηθούν οι συναγερμοί κινδύνου. Με αυτόν τον τρόπο, εάν ο κάτοικος βρίσκεστε μακριά για να επέμβει, δύνεται η δυνατότητα από την έξυπνη συσκευή ανίχνευσης καπνού να ειδοποιηθεί η πυροσβεστική υπηρεσία ή κάποιο κοντινό πρόσωπο, για να επέμβουν άμεσα [62].

Ένα ακόμα πολύ σημαντικό χαρακτηριστικό των συσκευών αυτών, είναι ότι υπάρχει η δυνατότητα να επικοινωνούν μεταξύ τους. Αυτό σημαίνει ότι όταν μία συσκευή αισθάνεται τον κίνδυνο του καπνού, θα ακούγονται όλοι οι συναγερμοί των συσκευών που είναι συνδεδεμένοι. Αυτό είναι ένα κρίσιμο χαρακτηριστικό

ασφαλείας που μπορεί να εξοικονομήσει πολύτιμα δευτερόλεπτα για να εκκενωθεί μία κατοικία ή πολυκατοικία.



Εικόνα 28 Εφαρμογή ενός εξουσιοδοτημένου χρήστη στην περίπτωση χρήσης του SMOCKEO [63].

5.5.1 – Περίπτωση χρήσης

Η Cobject SAS δημιούργησε μια έξυπνη συσκευή ανίχνευσης καπνού με όνομα SMOCKEO η οποία προσφέρει με την βοήθεια της τεχνολογίας του Sigfox την απομακρυσμένη επικοινωνία και τη διαχείριση της κατάστασης και των ειδοποιήσεων μέσω μίας ειδικά διαμορφωμένης εφαρμογής όπως βλέπουμε και στην παραπάνω εικόνα 28. Το κύριο πλεονέκτημα του παραπάνω έξυπνου ανιχνευτή καπνού, είναι ότι οι χρήστες λαμβάνουν απομακρυσμένες ειδοποιήσεις συναγερμών, κατευθείαν στην εφαρμογή μέσω μιας φωνητικής κλήσης, SMS, email ή ειδοποίηση στην εφαρμογής. Ένα δευτερεύον όφελος είναι η λήψη ειδοποίησης όταν απαιτείται αντικατάσταση μπαταρίας.

Οι απειλές που δέχονται οι έξυπνες συσκευές ανίχνευσης καπνού και η χρήση της τεχνολογίας LPWAN είναι χαμηλές. Η σημαντικότερη από τις απειλές που μπορεί να δεχθεί η τεχνολογία αυτή είναι, η πιθανότητα ένας εμπρηστής να προσπαθήσει να αποτρέψει την ενεργοποίηση του συναγερμού. Η χειρότερη περίπτωση αυτής της επίθεσης εφαρμόζεται όταν κάποιος φαίνεται να εμποδίζει την απομακρυσμένη ειδοποίηση όταν ο χρήστης είναι απομακρυσμένος, αλλά η προσωπική του ασφάλεια δεν κινδυνεύει. Ακόμα υπάρχει η απειλή εκβιασμού ή βλάβης της φήμης στον πάροχο υπηρεσιών μέσω της επίθεσης Άρνησης παροχής υπηρεσιών, αλλά επειδή δεν είναι εφικτή η απενεργοποίηση της αυτόνομης τοπικής λειτουργίας συναγερμού του ανιχνευτή, οι συνέπειες δεν θα ήταν καταστροφικές. Μια άλλη απειλή θα μπορούσε να είναι η παρεμπόδιση αποστολής μιας προειδοποίησης για χαμηλή μπαταρία, αλλά αυτό μετριάζεται από το σχεδιασμό του συστήματος που περιλαμβάνει έναν περιοδικό έλεγχο της κατάστασης, η απουσία του οποίου θα παρατηρηθεί από το χρήστη.

Σύμφωνα με τα παραπάνω, χρησιμοποιώντας το μοντέλο STRIDE η μοναδική επίθεση που προκύπτει είναι:

- **Denial of Service – Άρνηση παροχής υπηρεσιών**

Οι κυριότερες κινήσεις και έλεγχοι που μετριάζουν τον παραπάνω κίνδυνο είναι η προστασία από φυσικές επιθέσεις και η χρήση ενός μη-IP δικτύου. Εάν χρησιμοποιηθεί μια τεχνολογία LPWAN με χρήση δικτύου IP, τότε η

παρακολούθηση του δικτύου και το φιλτράρισμα του θα ήταν ιδανικό για την μείωση των άρνησης παροχής υπηρεσιών [26].

5.5.1.1 – Άρνηση παροχής υπηρεσιών

Ένας επιτιθέμενος μπορεί να προσπαθήσει να αχρηστεύσει ένα μεγάλο αριθμό συσκευών εντοπισμού καπνού ή το δίκτυο που συντηρούνται και στέλνουν δεδομένα τους. Σκοπός αυτής της επίθεσης είναι κυρίως η δυσλειτουργία των συσκευών ώστε να μην στέλνουν μηνύματα αλερτ σε περιπτώσεις ανάγκης, με απώτερο σκοπό ίσως τον εκβιασμό του παροχέα υπηρεσιών (service provider) αλλά ακόμα και για να κάνουν κακό στους ενοίκους των διαμερισμάτων που λειτουργούσαν οι συσκευές αυτές. Για να επιτευχθούν οι επιθέσεις αυτές μπορούν να χρησιμοποιηθούν επιθέσεις όπως Τεχνικές Παρεμβολών και Επίθεση επανάληψης.

5.5.1.1.1 – Τεχνικές Παρεμβολών

Οι τεχνικές επίθεσης παρεμβολής είναι πολύ γενικό πρόβλημα στο IoT, κατά την οποία, κάποια κακόβουλη οντότητα μεταδίδει ένα ισχυρό ραδιοκύμα (radiosignal) κοντά στις συσκευές και διακόπτουν τις εκπομπές τους. Διακόπτοντας τις εκπομπές των εντολών στις συσκευές για τον εντοπισμό καπνού, προκαλεί σοβαρό πρόβλημα με την αναγνώριση του καπνού αλλά και για την αποστολή προειδοποιητικών μηνυμάτων στους ενοίκους και στην πυροσβεστική. Με αυτά τα προβλήματα ουσιαστικά εκβιάζεται ο πάροχος υπηρεσιών και δημιουργείται μια πολύ επικίνδυνη κατάσταση χωρίς την ύπαρξη των προειδοποιητικών μηνυμάτων που μπορεί να επιφέρει θανάσιμες επιπτώσεις[42].

5.5.1.2 – Επίθεση Επανάληψης

Η επίθεση αυτή πετυχαίνεται με το να ξαναστέλνονται ή να επαναλαμβάνονται δεδομένα από μία κακόβουλη οντότητα. Ακόμα μπορεί να στέλνονται διαρκώς προειδοποιητικά μηνύματα χωρίς να υπάρχει πρόβλημα, δημιουργώντας σύγχυση στους ενοίκους και στις δημόσιες υπηρεσίες που λογικά θα ενημερώνονται. Ο κύριος σκοπός αυτής της επίθεσης είναι να προκαλέσει σφάλμα στην συσκευή και να την απενεργοποιήσει πετυχαίνοντας ουσιαστικά μια επίθεση παρεμβολής. Σαν

αποτέλεσμα της επίθεσης είναι τα παραπάνω προβλήματα επηρεάζοντας σημαντικά τον πάροχο υπηρεσιών και βάζει σε κίνδυνο τους ενοίκους του διαμερίσματος αλλά και της πολυκατοικίας[42].

5.6 – Επίλογος κεφαλαίου

Στο κεφάλαιο αυτό, πραγματοποιήθηκε μία αναφορά των επιθέσεων ασφαλείας που πραγματοποιούνται στα καινοτόμα έξυπνα συστήματα IoT. Οι επιθέσεις αυτές, ανάλογα με τη περίπτωση χρήσης και το πρωτόκολλο που χρησιμοποιείται σε κάθε σύστημα, κατηγοριοποιήθηκαν για την καλύτερη κατανόηση τους και για την ευκολότερη αντιμετώπιση τους σύμφωνα με τη Διαδικασία Μοντελοποίησης Απειλών της Microsoft.

Η περίπτωση χρήσης του πρωτοκόλλου NB-IoT πραγματοποιήθηκε από την υποδομή συστήματος της έξυπνης τηλεμέτρησης νερού, όπου διαπιστώθηκε ότι οι επιθέσεις που μπορούν να πραγματοποιηθούν στο σύστημα αυτό, μπορούν να επιφέρουν πολύ κακές συνέπειες. Συνεπώς, η κατάλληλη επιλογή πρωτοκόλλου δικτύων LPWAN αποτελεί βασικό παράγοντα για τη διασφάλιση της ομαλής λειτουργίας ενός συστήματος IoT.

ΚΕΦΑΛΑΙΟ 6 – Συμπεράσματα και μελλοντική έρευνα

6.1 – Ανασκόπηση

Στην πτυχιακή εργασία αυτή, πραγματοποιήθηκε μία έρευνα των ζητημάτων ασφαλείας των Low Power Wide Area Network. Για την έρευνα αυτή, ήταν απαραίτητο να παραχωρηθεί ένα κεφάλαιο που αναφέρεται στα βασικά χαρακτηριστικά των δικτύων LPWAN αλλά και για τα χαρακτηριστικά του κάθε πρωτόκολλου που αναφέρθηκαν στην εργασία, όπως είναι η τεχνολογία LoRaWAN, Sigfox, NB-IoT. Ακόμα χρησιμοποιήθηκε ξεχωριστό κεφάλαιο για την τεχνική αναφορά των μηχανισμών ασφαλείας που διαθέτει κάθε τεχνολογία, όπως είναι τα κλειδιά ασφαλείας και ο μηχανισμός κρυπτογράφησης που αποτελούν το βασικό μηχανισμό ασφαλείας τους. Περεταίρω, αναφέρθηκαν σε επόμενο κεφάλαιο τα ζητήματα ασφαλείας που δημιουργούνται σε κάθε τεχνολογία, καθώς και διάφοροι μηχανισμοί αντιμετώπισης τους. Και τέλος έγινε μία έρευνα με την χρησιμοποίηση της μοντελοποίησης κινδύνου STRIDE της Microsoft [57], για τους κινδύνους που διατρέχουν τα έξυπνα συστήματα IoT με τη χρησιμοποίηση των δικτύων LPWAN.

6.2 – Συμπεράσματα

Η πτυχιακή εργασία αναφέρθηκε στην θεωρητική ανάλυση των βασικών προτύπων των δικτύων LPWAN που χρησιμοποιούνται στα καινοτόμα συστήματα IoT, όπως είναι η τεχνολογία του LoRaWAN, Sigfox και NB-IoT. Ακόμα αναφέρθηκε στα τεχνικά χαρακτηριστικά και στους μηχανισμούς ασφαλείας που διαθέτει κάθε τεχνολογία. Στη συνέχεια ερευνήθηκαν τα ζητήματα ασφαλείας που διέπουν τα δίκτυα LPWAN και τις τεχνολογίες αντιστοίχως. Και τέλος εφαρμόστηκε η μοντελοποίηση κινδύνων του παραπάνω κεφαλαίου με τις επιθέσεις ασφαλείας των πρωτοκόλλων, για την παρουσίαση των περιπτώσεων χρήσης των τεχνολογιών.

Σύμφωνα με τη παραπάνω παράγραφο, η πτυχιακή εργασία κατάφερε να δώσει απάντηση στα ζητήματα που δημιουργούνται με την χρησιμοποίηση των δικτύων LPWAN στο επίπεδο ασφαλείας τους. Η τεχνολογία του NB-IoT προτιμήθηκε όπως είδαμε στη περίπτωση χρήσης της έξυπνης τηλεμέτρησης κατανάλωσης νερού που οι επιθέσεις ασφαλείας της μπορούν να βλάψουν πολύ σοβαρά τον τελικό χρήστη ακόμα και στην φυσική επίθεση που μπορεί να δεχθούν οι τελικές συσκευές, αλλά και να εκβιαστεί ο πάροχος του συστήματος. Ακόμα, η τεχνολογία του LoRaWAN που αποτελεί μέχρι σήμερα το δημοφιλέστερο πρωτόκολλο LPWAN που συνεπάγεται και μεγαλύτερο εύρος μηχανισμών ασφαλείας και υλικού άρα και μικρότερο κόστος, χρησιμοποιήθηκε στη περίπτωση χρήσης του έξυπνου οδικού φωτισμού που απαιτεί τη χρησιμοποίηση μεγάλου πλήθους τελικών συσκευών. Τέλος στην περίπτωση του Sigfox που είναι μία διαφορετική σχετικά τεχνολογία από τις υπόλοιπες δύο λόγο του μικρότερου μεγέθους μηνυμάτων και της μετάδοσης δεδομένων, που συνεπάγεται λιγότερες λειτουργικές απαιτήσεις των συστημάτων άρα και πιο «απλό» σύστημα, χρησιμοποιήθηκε στη περίπτωση χρήσης της έξυπνης ανίχνευσης καπνού που ακόμα και να υπάρξει η σημαντικότερη επίθεση της άρνησης παροχής υπηρεσιών, υπάρχει η δυνατότητα ηχητικής προειδοποίησης.

6.3 – Μελλοντική έρευνα

Η ιδανικότερη μελλοντική ερεύνα για τα δίκτυα LPWAN και τα ζητήματα ασφαλείας τους, αποτελεί η υλοποίηση μεθόδων και αλγορίθμων που μπορούν να εμπλουτίσουν τον μηχανισμό ασφαλείας των τεχνολογιών LPWAN. Ο αλγόριθμος κρυπτογράφησης αποτελεί το βασικότερο μηχανισμό ασφαλείας των δικτύων LPWAN, είναι υπεύθυνος για την ακεραιότητα του συστήματος και των μηνυμάτων καθώς και για την ταυτοποίηση των συσκευών στο σύστημα. Οι σημερινοί μέθοδοι κρυπτογράφησης όπως είναι ο AES 128 που χρησιμοποιείται σε κάθε τεχνολογία όπως αναφέρθηκε στο κεφάλαιο 3, ο οποίος όμως δεν είναι σε θέση να προστατεύσει πλήρως τις ιδιότητες που αναφέρθηκαν, οπότε είναι πολύ σημαντικό να υλοποιηθεί ένας τέτοιος μηχανισμός. Ακόμα, η αναβάθμιση του μηχανισμού ασφαλείας για τα δίκτυα LPWAN μπορεί να πραγματοποιηθεί από την υλοποίηση αυτόνομων μηχανισμών αντιμετώπισης επιθέσεων όπως για παράδειγμα είναι ο

μηχανισμός αντιμετώπισης της επίθεσης σκουληκότρυπας «colonel blotto game» που αναφέρθηκε στο κεφάλαιο των επιθέσεων ασφαλείας και συγκεκριμένα σε υποκεφάλαιο του πρωτοκόλλου LoRaWAN.

Βιβλιογραφία

[1] M. Rouse, S. Shea και M. Haughn, «Internet of Things Agenda,» 2017. [Ηλεκτρονικό]. Available: https://.techtarget.com/definition/LPWAN-low-power-wide-area-network.

[2] U. Raza, M. Sooriyaband και P. Kulkarni, «Low Power Wide Area Networks: An Overview,» 2017.

[3] U. Raza, P. Kulkarni και M. Sooriyabandara, *Low Power Wide Area Networks: An Overview,* arXiv.

[4] Techplayon, [Ηλεκτρονικό]. Available: http://www.techplayon.com/low-power-wide-area-networks-lpwan/.

[5] F. Adelantado, X. Vilajosana, P. T. Peiro, B. Martinez, J. M. Seguí και T. Watteyne, «Understanding the Limits of LoRaWAN,» *IEEE Communications Magazine,* 2017.

[6] R. K. Kodali, «Radio Data Infrastructure for Remote Monitoring System using LoRa Technology,» IEEE, WARANGAL, INDIA.

[7] LoRa Alliance, «A technical overview of LoRa and LoRaWAN,» 2015.

[8] Sigfox, «Sigfox IoT Radio Technology,» [Ηλεκτρονικό]. Available: https://www.sigfox.com/en/sigfox-iot-radio-technology.

[9] Sigfox, «Sigfox Technical Overview,» 2017.

[10] B. Ray, «Link Labs,» [Ηλεκτρονικό]. Available: https://www.link-labs.com/blog/what-is-sigfox.

[11] S. Chacko και D. Job, «Security mechanisms and Vulnerabilities in LPWAN».*IOP Conf. Ser..*

[12] «3GPP,» [Ηλεκτρονικό]. Available: http://www.3gpp.org/about-3gpp/about-3gpp.

[13] G. Schatz, «NB-IoT Architecture As It Compares To LTE-M,» 2018.

[14] S. Landström, J. Bergström, E. Westerberg και D. Hammarwall, «NB-IoT: a sustainable technology for connecting billions of devices,» 2016.

[15] GSMA, «Official Document CLP.28 - NB-IoT Deployment Guide to Basic Feature set Requirements,» GSMA, 2018.

[16] Digi International, «Introducing NB-IoT Technologies for Cellular IoT,» 2017.

[17] I. Chatzigiannakis, V. Liagkou και P. G. Spirakis, «Providing End-to-End Secure Communication in Low-Power Wide Area Networks (LPWANs)».

[18] LoRa Alliance, «LoRaWAN™ 1.1 Specification,» LoRa Alliance, 2017.

[19] E. van ES, «LORAWAN VULNERABILITY ANALYSIS,» Open Universiteit, Heerlen, Netherlands, 2018.

[20] IBM, «IBM,» [Ηλεκτρονικό]. Available: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.2.0/com.ibm.zos.v2r2.csfb400/csfb4429.htm.

[21] Sigfox, «Sigfox Technical Overview,» Sigfox, 2017.

[22] Wikipedia, [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Message_authentication_code.

[23] R. Ratasuk, N. Mangalvedhe, Y. Zhang, M. Robert και J. Koskinen, «Overview of narrowband IoT in LTE Rel-13,» σε*2016 IEEE Conference on Standards for Communications and Networking (CSCN)*, Berlin, 2016 .

[24] A. Hoglund, «Overview of 3GPP Release 14 Enhanced NB-IoT,» *IEEE Network,* pp. 16-22, 2017.

[25] A. Bovone, Nokia, 2017.

[26] F. H. Ltd, «LPWA Technology Security Comparison,» A White Paper from Franklin Heath Ltd, 2017.

[27] T-Mobile, «NarrowBand IoT Groundbreaking in the IoT,» T-Mobile, 2017.

[28] GSMA, Remote Provisioning Architecture for Embedded UICC Technical Specification, 2017.

[29] ETSI, Smart Cards Remote APDU structure for UICC based applications (Release 12).

[30] NIST, NIST: SP 800-57 Part 1: Recommendation for Key Management, 2016.

[31] BSI, BSI: TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen.

[32] Vodafone, «Narrowband-IoT: pushing the boundaries of IoT , Vodafone NB-IoT White Paper,» Vodafone, 2017.

[33] . A. A. Mohammed , A. D. Elbayoumy και E. A. EI-Wanis, «LTE Authentication Protocol (EPS-AKA) Weaknesses Solution,» IEEE, 2015.

[34] M. Balachandra και K. Prakash, «AUTHENTICATION AND KEY AGREEMENT IN 3GPP NETWORKS,» Department of Information and Communication Technology Manipal Institute of Technology, Manipal, India, 2015.

[35] M.-O. Park, D.-W. Park και S.-G. Kim, «TMSI Allocation Mechanism Using a Secure VLR Authorization in the GSM System,» IFIP International Federation for Information Processing, 2006..

[36] Rapid 7, [Ηλεκτρονικό]. Available: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/.

[37] J. Kohout, «Teskalabs,» [Ηλεκτρονικό]. Available: https://teskalabs.com/blog/protect-mobile-app-and-prevent-man-in-the-middle-attack.

[38] V. Gkioulos, S. D. Wolthusen και A. Iossifides, «A Survey on the Security Vulnerabilities of Cellular Communication Systems (GSM-UMTS-LTE),» *Presented at the Norwegian Information Security Conference 2016,* 2016.

[39] C. Kowalczyk, «crypto-it,» [Ηλεκτρονικό]. Available: http://www.crypto-it.net/eng/attacks/replay.html.

[40] R. K. Mojjada, «Wireless Networks – Analysis on Prevention of Jamming Attacks,» *International Journal Of Engineering And Computer Science ISSN:2319-7242,* pp. 12033-12039, 2015.

[41] V. Brtnik, «Master thesis Security Risk Assessment of LoRaWan,» Leiden, Leiden University, 2017.

[42] E. Aras, G. S. Ramachandran, . P. Lawrence και D. Hughes, «Exploring the Security Vulnerabilities of LoRa,» σε*2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*, Exeter, 2017.

[43] «Xignal Mousetrap,» 2016. [Ηλεκτρονικό]. Available: https://www.xignal.com/products/xignal-mousetrap.

[44] B. Reynders, W. Meert και S. Pollin, «Range and coexistance analysis of long range unlicensed communication,» *Internal Conference on Telecommunications,* 2016.

[45] M. Labib, S. Ha, W. Saad και J. H. Reed, «A colonel blotto game for anti-jamming in the internet of things,» σε*Global Communications Conference (GLOBECOM)*, San Diego, CA, 2015.

[46] Y. Xueying, «LoRaWAN: Vulnerability Analysis and Practical Exploitation,» Delf tUniversity of Technology, Delft, July21,2017.

[47] «Github,» [Ηλεκτρονικό]. Available: https://lzutao.github.io/cribdrag/.

[48] S. Iskhakov, A. Iskhakova, R. Meshcheryakov και S. Bondarchuk, «Analysis of vulnerabilities in low-power wide-area networks by example of the LoRaWAN,» *Advances in Computer Science Research (ACSR),* 2017.

[49] X. Yang, E. Karampatzakis, C. Doerr και F. Kuipers, «Security Vulnerabilities in LoRaWAN,» σε*2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, Orlando, 2018.

[50] Y. Hu, A. Perrig και D. B. Johnson, «Packet leashes: a defense against wormhole attacks in wireless networks,» σε*IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428)*, San Francisco, 2003.

[51] Sigfox, «Secure Sigfox Ready devices - Recommendation guide».

[52] LETI CEA, «Leti Cea,» [Ηλεκτρονικό]. Available: http://www.leti-cea.com/cea-tech/leti/english.

[53] Oracle, «Oracle docs,» [Ηλεκτρονικό]. Available: https://docs.oracle.com/cd/E19683-01/806-4075/ipov-10/index.html.

[54] M. CHEN, Y. MIAO, Y. HAO και K. HWANG, «Narrow Band Internet of Things,» IEEE Access, 2017.

[55] K. Rwanshane, «STRUCTURE OF TYPICAL IOT SETUP,» 2016.

[56] P. Garg και L. Kohnfelder, 11 12 2009. [Ηλεκτρονικό]. Available: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20).

[57] A. Shostack, «cloudblogs microsoft,» [Ηλεκτρονικό]. Available: https://cloudblogs.microsoft.com/microsoftsecure/2007/09/11/stride-chart/).. [Πρόσβαση 2007].

[58] Alliance for water efficiency, «Alliance for water efficiency,» [Ηλεκτρονικό]. Available: http://www.allianceforwaterefficiency.org/smart-meter-introduction.aspx.

[59] «Bit-Flipping attack,» 2013. [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Bit-flipping_attack.

[60] Intelilight, «Intelilight,» [Ηλεκτρονικό]. Available: https://intelilight.eu/technology/intelilight-lorawan-compatible-street-lighting-remote-management/.

[61] S. Malhotra και V. Kumar, «Smart Street Lighting System: An Energy Efficient Approach,» *International Journal of Science and Research (IJSR) ,* 2013.

[62] J. P. Tuohy, «engadget,» [Ηλεκτρονικό]. Available: https://www.engadget.com/2018/04/01/the-best-smart-smoke-alarm/.

[63] Cobject SAS, «SMOCKEO,» [Ηλεκτρονικό].