ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΗΣ ΣΧΕΔΙΑΣΗΣ ΚΑΙ ΠΑΡΑΓΩΓΗΣ

Διπλωματική Εργασία

Ενίσχυση της αξιοπιστίας του LoRaWAN: μια καινοτόμα πρακτική που προσφέρεται ως Υπηρεσία Ασφαλείας, βασισμένη στην τεχνική των κυλιόμενων κλειδιών

Συγγραφέας:

Γριτσόπουλος Αλέξανδρος

Αριθμός Μητρώου : 70147144

Επιβλέπων :

Ευάγγελος Πάλλης

Καθηγητής

Αθήνα, Μάρτιος, 2023

UNIVERSITY OF WEST ATTICA

SCHOOL OF ENGINEERING

DEPARTMENT OF INDUSTRIAL DESIGN AND PRODUCTION ENGINEERING

Diploma Thesis

Enhancing LoRaWAN's reliability: a prototype Security as a Service (SaaS) approach based on rolling-code (hopping code) technique

Author:

Gritsopoulos Alexandros

Registration Number: 70147144

Supervisor:

Pallis Evangelos

Professor

Athens, March, 2023

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Γριτσόπουλος Αλέξανδρος του Παναγιώτη, με αριθμό μητρώου 70147144 φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής του Τμήματος Μηχανικών Βιομηχανικής Σχεδίασης και Παραγωγής, δηλώνω υπεύθυνα ότι:

«Είμαι συγγραφέας αυτής της πτυχιακής/διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

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

Ο Δηλών

ΓΡΙΤΣΟΠΟΥΛΟΣ ΑΛΕΞΑΝΔΡΟΣ

Μέλη Εξεταστικής Επιτροπής συμπεριλαμβανομένου και του Εισηγητή

Η διπλωματική εργασία εξετάστηκε επιτυχώς από την κάτωθι Εξεταστική Επιτροπή:

α/α	ΟΝΟΜΑ ΕΠΩΝΥΜΟ	ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ
1	ΕΥΑΓΓΕΛΟΣ ΠΑΛΛΗΣ	Evangelos Pallis Digitally signed by Evangelos Pallis Date: 2023.03.13 12:34:20 +02'00'
2	ΕΛΕΝΗ ΑΙΚΑΤΕΡΙΝΗ ΛΕΛΙΓΚΟΥ	Eleni Aikaterini Leligkou Digitally signed by Eleni Aikaterini Leligkou Date: 2023.03.13 16:38:36 +02'00'
3	ΧΡΗΣΤΟΣ ΔΡΟΣΟΣ	Christos Drosos Digitally signed by Christos Drosos Date: 2023.03.13 21:28:13 +02'00'

Περίληψη

Η παραγωγή χαμηλού κόστους αλλά με βελτιωμένες δυνατότητες συσκευών του Διαδικτύου των Αντικειμένων (Internet of Things-IoT) έχει αυξηθεί εκθετικά τα τελευταία χρόνια, ανοίγοντας το δρόμο προς τη μεγάλης κλίμακας ανάπτυξη έξυπνων περιβαλλόντων, τα οποία μεταμορφώνουν τον τρόπο που οι άνθρωποι ζουν, εργάζονται, εμπορεύονται, επικοινωνούν και κοινωνικοποιούνται. Τα έξυπνα σπίτια, οι ευφυείς πόλεις, η εξ αποστάσεως υγειονομική περίθαλψη, η έξυπνη βιομηχανία, η γεωργία ακριβείας και οι ευφυείς μεταφορές είναι μόνο μερικά ενδεικτικά πεδία εφαρμογών όπου οι προσιτές (προς το κόστος) συσκευές IoT μπορούν να χρησιμοποιηθούν σήμερα, όχι μόνο για τη συλλογή, την επεξεργασία και την αποθήκευση πληροφοριών, αλλά και για την κοινή χρήση τους σε αποστάσεις που κυμαίνονται από τις εγκαταστάσεις του χρήστη έως τις αγροτικές και αστικές περιοχές. Για να γίνει αυτό, τα σύγχρονα IoT χρησιμοποιούν τεχνικές ραδιομετάδοσης που διευρύνουν το εύρος της επικοινωνίας από εκατοντάδες μέτρα έως μερικά χιλιόμετρα, και εκμεταλλεύονται πρωτόκολλα ασύρματης επικοινωνίας τα οποία μειώνουν δραματικά την κατανάλωση ενέργειας, επεκτείνοντας με αυτό τον τρόπο τον κύκλο ζωής, ειδικά όταν οι συσκευές IoT τροφοδοτούνται με μπαταρίες. Ένα τέτοιο πρωτόκολλο είναι το δίκτυο μεγάλης εμβέλειας ευρείας περιοχής (LoRaWAN), το οποίο μπορεί να φιλοξενήσει ασύρματη επικοινωνία συσκευών IoT με το δίκτυο οπίσθιας ζεύξης (backhaul) σε αποστάσεις πολλών χιλιομέτρων. Το δίκτυο LoRaWAN ανήκει στη σουίτα πρωτοκόλλων δικτύου ευρείας περιοχής χαμηλής κατανάλωσης (LPWAN) και προσφέρεται για φιλική-προς-το-περιβάλλον και ενεργειακά αποδοτική λειτουργία.

Ωστόσο, η εκθετική αύξηση των IoT συσκευών σε συνάρτηση με τον κύριο στόχο της LPWAN τεχνολογίας για μικρότερη κατανάλωση ενέργειας και μεγαλύτερης εμβέλειας επικοινωνία, έχει φέρει στο προσκήνιο το ζήτημα της ασφάλειας. Η αξιόπιστη μετάδοση δεδομένων και η διασφάλιση του απορρήτου των χρηστών απαιτούν μηχανισμούς και πρωτόκολλα επικοινωνίας που ενισχύουν την ακεραιότητα των συσκευών IoT και την ικανότητα των δικτυακών υποδομών να περιορίζουν πιθανές υποκλοπές και παραβίαση δεδομένων.

Στόχος της διπλωματικής μου εργασίας, είναι η παρουσίαση μιας τεχνικής που επιτρέπει στις συσκευές του Διαδίκτυού των πραγμάτων (IoT) να ανανεώνουν συνεχώς το κλειδί τους (AppKey) με σκοπό την εκ νέου επαλήθευση της ταυτότητας τους, δημιουργώντας ένα ασφαλέστερο περιβάλλον επικοινωνίας. Η προτεινόμενη μέθοδος, βασίζεται στην τεχνική των κυλιόμενων κλειδιών (Rolling Key) που χρησιμοποιείται στα συστήματα κλειδώματος των αυτοκινήτων και πιο συγκεκριμένα θα ασχοληθούμε με το μοντέλο ψευδοτυχαίων αριθμών, ενισχύοντας έτσι την αντίσταση του δικτύου και των συσκευών έναντι διαφόρων κυβερνητικών επιθέσεων (Cybersecurity attack).

Λέξεις Κλειδιά: Διαδίκτυο των Πραγμάτων, LoRa, LoRaWAN, Άνθρωπος-στη-μέση, Ασφάλεια LoRaWAN , Κυλιόμενα κλειδιά, AppKey, Ψευδοτυχαίων αριθμών, LPWAN

Abstract

The production of low-cost but improved internet of Things (IoT) devices has grown exponentially in recent years, paving the way for the large-scale development of smart environments that transform the way people live, work, trade, communicate and socialize. Smart homes, smart cities, remote healthcare, smart industry, precision agriculture and intelligent transportation are just a few indicative application fields where affordable (cost-effective) IoT devices can be used today, not only to collect, process and store information, but also to share it across distances ranging from user facilities to rural and urban areas. To do this, modern IoT uses radio transmission techniques that extend the range of communication from hundreds of meters to a few kilometers, and exploit wireless communication protocols that dramatically reduce energy consumption, thus extending the life cycle, especially when IoT devices are powered by batteries. One such protocol is the wide-area long-range network (LoRaWAN), which can host wireless communication of IoT devices with the rear-Link network (backhaul) over distances of many kilometers. The LoRaWAN network belongs to the suite of low-power wide area network protocols (LPWAN) and lends itself to eco-friendly and energy-efficient operation.

However, the exponential growth of IoT devices in connection with LPWAN's main goal of lower power consumption and longer communication range has brought the issue of security to the fore. Reliable data transmission and ensuring user privacy require communication mechanisms and protocols that enhance the integrity of IoT devices and the ability of network infrastructure to limit potential eavesdropping and data breach.

The aim of my thesis is to present a novel technique that allows internet of Things devices (IoT) to constantly update their AppKey key in order to re-verify their identity, creating a safer communication environment. The proposed method is based on the Rolling key technique used in car locking systems and more specifically we will deal with the pseudorandom number model. In a try to strengthening the resistance of the devices and the network against various cyber-attacks.

Keywords: Internet of Things, LoRa, LoRaWAN, Man-In-The-Middle, LoRaWAN Security, Rolling Code, AppKey, Pseudorandom Number, LPWAN

Ευχαριστίες

Με την ολοκλήρωση της διπλωματικής μου εργασίας, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες σε όλους όσους συνέβαλλαν στην εκπόνησή της.

Ευχαριστώ θερμά τον επιβλέπων καθηγητή μου κ. Ευάγγελο Πάλλη για τις συμβουλές και την εμπιστοσύνη που μου έδειξε εξ' αρχής, αναθέτοντάς μου το συγκεκριμένο θέμα, το αμείωτο ενδιαφέρον του και την καθοδήγησή του καθ' όλη την διάρκεια της παρούσας διπλωματικής μου εργασίας.

Τέλος, θα ήθελα εκφράσω την ευγνωμοσύνη μου στην οικογένειά μου και τα κοντινά μου πρόσωπα για όλη τη στήριξη, τη συμπαράσταση και την κατανόησή τους, καθ' όλη τη διάρκεια των σπουδών μου.

Περιεχόμενα

Περιεχόμενα Εικόνων

Εισαγωγή

Στη σημερινή κοινωνία, πολλές συσκευές λειτουργούν στο κόσμο του Διαδικτύου των πραγμάτων (IoT), παρέχοντας πρόσβαση σε μια πληθώρα μετρήσεων και δεδομένων σε ένα τεράστιο δίκτυο συνδεδεμένων συσκευών. Αυτό μπορεί και επιτυγχάνεται, στο γεγονός ότι χρησιμοποιείται το δίκτυο LoRaWAN, καθώς χρησιμοποιεί πρωτόκολλα χαμηλής ισχύος (LP) και μεγάλης εμβέλειας (LoRa) που μειώνουν την κατανάλωση ενέργειας των συσκευών ενώ μεγιστοποιούν το εύρος επικοινωνίας. Οι συσκευές για να φτάσουν στο σημείο της μετάδοσης των δεδομένων, ακολουθούν μια αρχική διαδικασία μη κρυπτογραφημένου αιτήματος συμμετοχής (Join Procedure) σύμφωνα με την οποία γίνεται η πιστοποίηση της ταυτότητας τους στον αέρα (cloud) από το δίκτυο (Network Server). Για να υπάρξει μια κρυπτογράφηση στο μη κρυπτογραφημένο αίτημα, εισάγεται μια τιμή Message Integrity Code (MIC) με την μορφή ενός AppKey. Το AppKey αποθηκεύεται στον αέρα (cloud) με σκοπό τον έλεγχο της ταυτότητας της συσκευής στην διαδικασία του αιτήματος συμμετοχής (Join Request). Το πρόβλημα που δημιουργείται με αυτή την διαδικασία ονομάζεται Man-In-The-Middle (MITM), σύμφωνα με το οποίο κακόβουλοι χρήστες (Attackers) παρεμβαίνουν στο κανάλι επικοινωνίας με σκοπό, να υποκλέψουν το AppKey κλειδί και να ξεκινήσουν ένα αίτημα συμμετοχής (Join Request) αντιγράφοντας την ταυτότητα της νόμιμης συσκευής και αποκτώντας πρόσβαση στο κανάλι επικοινωνίας. Με σκοπό την υπερφόρτωση του δικτύου και την καταστροφή του ή την υποκλοπή των δεδομένων ή ακόμα και την παραποίηση των δεδομένων με στόχο την παραπλάνηση του χρήστη. Αυτή η εργασία, παρουσιάζει μια τεχνική που επιτρέπει στις συσκευές του Διαδίκτυού των πραγμάτων (IoT) να ανανεώνουν συνεχώς το AppKey κλειδί τους με σκοπό την εκ νέου επαλήθευση της ταυτότητας τους, δημιουργώντας ένα ασφαλέστερο περιβάλλον επικοινωνίας για τον χρήστη.

Αντικείμενο της Διπλωματικής Εργασίας

Το πρόβλημα που πρέπει να αντιμετωπιστεί σε αυτή την διπλωματική εργασία, είναι η ενίσχυση της ασφάλειας ενός LoRaWAN δικτύου και η άμεση αντιμετώπιση στο ενδεχόμενο επίθεσης Man-In-The-Middle.

Σκοπός και Στόχοι

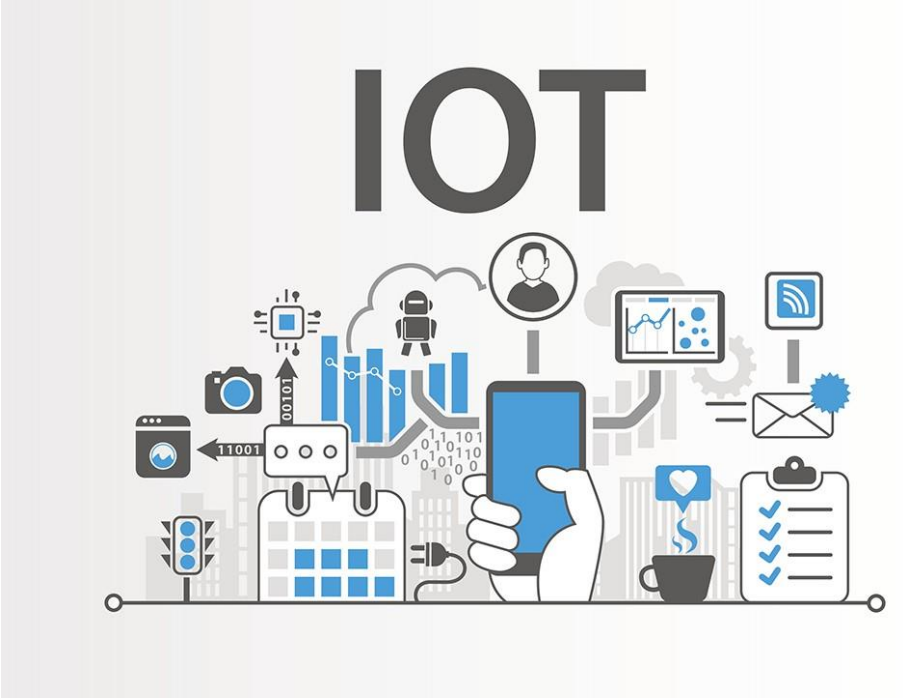
Σκοπός αυτής της διπλωματικής εργασίας είναι η ενίσχυση της αντίστασης ενός LoRaWAN δικτύου έναντι διαφόρων Man-In-The-Middle (MITM) επιθέσεων σύμφωνα με το πρότυπο του LoRaWAN 1.0.1. Για να μπορέσει να χαρακτηριστεί αυτό το σύστημα ασφαλές και αυτή η προσπάθεια ενίσχυσης επιτυχημένη, θα πρέπει να επιτευχθούν οι παρακάτω στόχοι.

1. Δημιουργία γεννήτριας για την συνεχή κατασκευή του νέου κλειδιού.
2. Κατάλληλη σύνδεση και άμεση επικοινωνία μεταξύ τελικής συσκευής-γεννήτριας-δικτύου.
3. Ενίσχυση της ακεραιότητας του δικτύου.
4. Σε περίπτωση που επιτευχθεί η εισαγωγή ενός κακόβουλου χρήστη, να υπάρχει άμεση αντιμετώπιση του προβλήματος.

1. ΚΕΦΑΛΑΙΟ 1

1.1 *Εισαγωγή στο IoT*

Ο όρος "Διαδίκτυο των Πραγμάτων (Internet of Things)" χρησιμοποιήθηκε για πρώτη φορά το 1999 από τον Άγγλο πρωτοπόρο στην τεχνολογία Kevin Ashton, για να περιγράψει ένα σύστημα στο οποίο ο "φυσικός κόσμος" θα μπορεί να συνδεθεί στο διαδίκτυο με τη χρήση αισθητήρων. Ο Kevin Ashton επινόησε αυτόν τον όρο για να απεικονίσει τη δύναμη που έχει η ταυτοποίηση των προϊόντων μέσω ετικετών με την σύνδεση ραδιοσυχνοτήτων (RFID) ώστε να μετρηθούν τα προϊόντα σε μια παραγωγή χωρίς την παρέμβαση του ανθρώπου. Παλιότερα, η πρόσβαση στο διαδίκτυο ήταν περιορισμένη για συσκευές όπως τα smartphone, τους σταθερούς υπολογιστές κ.α., όμως με το διαδίκτυο των πραγμάτων, σήμερα όλες οι συσκευές μπορούν να συνδεθούν στο διαδίκτυο και να ελεγχθούν ασύρματα. Επομένως, το διαδίκτυο των πραγμάτων έχει εξελιχθεί σε μια ασύρματη τεχνολογία που εφαρμόζεται σε πολλούς διαφορετικούς τομείς. Στην ουσία, πρόκειται για ένα δίκτυο επικοινωνίας μεταξύ διαφόρων συσκευών που είναι εφοδιασμένα με αισθητήρες, λογισμικά και άλλες τεχνολογίες που επιτρέπουν την μετάδοση και την λήψη δεδομένων. Πλέον, ο στόχος του IoT είναι να επιτρέπει την σύνδεση, την λήψη, και την μετάδοση δεδομένων ανά πάσα στιγμή από οποιοδήποτε μέρος.



Εικόνα 1 Διαδίκτυο των Πραγμάτων[1]

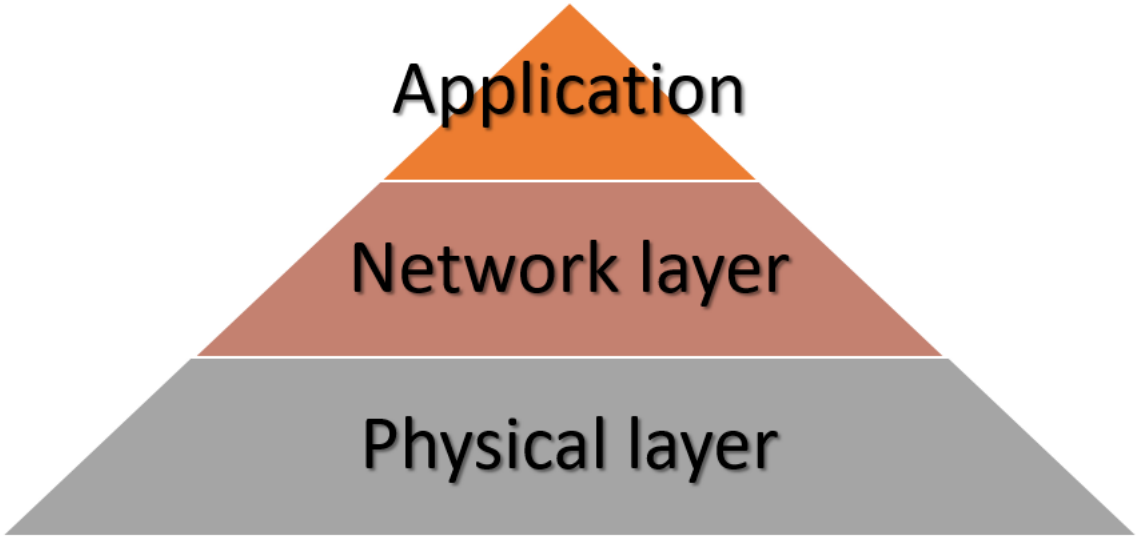
[1] https://seecontrol.com/what-is-iot-the-internet-of-things-explained

Το διαδίκτυο (Internet) αποτελεί μια καινοτόμα εφεύρεση, η οποία μεταμορφώνεται συνέχεια προσθέτοντας καινούργιες ιδέες σε hardware και software, αναγκάζοντας τους πάντες να ακολουθήσουν την νέα τάση. Οι τρόποι επικοινωνίας που ξέρουμε μέχρι σήμερα είναι είτε ανθρώπου προς ανθρώπου ή ανθρώπου προς συσκευή. Παρόλα αυτά το Διαδίκτυο των Πραγμάτων (IoT) υπόσχεται ένα μέλλον όπου ο τρόπος επικοινωνίας θα είναι μηχανή προς μηχανή (Machine-Machine (M2M)[(1)]. Στη σημερινή κοινωνία το Διαδίκτυο των Πραγμάτων (IoT) κατέχει μεγάλο ρόλο στην ζωή μας, καθώς καθημερινά μπαίνουν σε λειτουργία χιλιάδες IoT συσκευές. Σύμφωνα με τις προβλέψεις, δισεκατομμύρια συσκευές θα συνδεθούν χρησιμοποιώντας διάφορες τεχνολογίες αλληλεπίδρασης με το περιβάλλον. Μια έκθεση από την Ericsson προβλέπει ότι έως το τέλος του 2022, ο αριθμός των συνδεδεμένων συσκευών που βασίζονται στις τεχνολογίες όπως το Sigfox, το LoRaWAN θα φτάσουν τα 2,1 δισεκατομμύρια και ο αριθμός των συσκευών μικρής εμβέλειας όπως το Wi-Fi, Bluetooth και ZigBee θα φτάσουν τα 15,5 δισεκατομμύρια[2]. Όπως καταλαβαίνουμε λοιπόν τα τελευταία χρόνια πολλές μικρής εμβέλειας τεχνολογίες επικοινωνιών όπως το ZigBee, το Bluetooth έχουν αναδυθεί στο προσκήνιο λόγω της μικρής κατανάλωσης ενέργειας που απαιτούν. Παρόλα αυτά, λόγω της μικρής εμβέλειας τους η χρήση τους για σημαντικές εφαρμογές που απαιτούν μεγάλη εμβέλεια όπως οι έξυπνες πόλεις, είναι αδύνατη. Την λύση, σε αυτό το πρόβλημα το δίνουν οι τεχνολογίες LPWAN (Low Power Wide Area Network). Η τεχνολογία LPWAN επιτρέπει στις συσκευές να έχουν μεγαλύτερη εμβέλεια στην επικοινωνία τους, σπαταλώντας ταυτόχρονα λιγότερη ενέργεια. Οι δύο κυριότερες τεχνολογίες είναι το Narrow-Band (NB-IoT) και το Long Range (LoRa). Ουσιαστικά, αυτές οι τεχνολογίες επιτρέπουν στις συσκευές που απαρτίζονται από κάποιους αισθητήρες (sensors) ή από ενεργοποιητές (actuators) ή και τα δυο, να στέλνουν και να λαμβάνουν μηνύματα σε απόσταση μεγαλύτερη των 10 χιλιομέτρων και να επιβιώνουν για πολλά χρόνια ακόμα και χωρίς τροφοδοσία. Η εκθετική αύξηση των IoT συσκευών σε συνάρτηση με τον κύριο στόχο της LPWAN τεχνολογίας για μικρότερη κατανάλωση ενέργειας και μεγαλύτερης εμβέλειας επικοινωνία, έχει φέρει στο προσκήνιο το ζήτημα της ασφάλειας.

Οι IoT συσκευές αποτελούν μεγάλη απειλή για την ιδιωτικότητα του ατόμου, καθώς είναι συνδεδεμένες με την καθημερινότητα του χρήστη. Ένα από τα προβλήματα που έχουν εντοπιστεί από προηγούμενες έρευνες είναι η διαχείριση των κλειδιών [11]. Σύμφωνα, με τις έρευνες τα κρυπτογραφικά κλειδιά μπορούν να διαβαστούν από έναν κακόβουλο χρήστη, καθώς τα κλειδιά αυτά μεταδίδονται σε περιοχές όπου ο επιτιθέμενος (Attacker) έχει πρόσβαση. Αυτό συμβαίνει και στις LoRaWAN συσκευές. Σύμφωνα με τις LoRaWAN προδιαγραφές το κλειδί πρέπει να είναι μοναδικό, αυτό σημαίνει ότι κάθε κλειδί αντιστοιχεί σε μια και μόνο τελική συσκευή (end-device). Αυτό αποσκοπεί στο γεγονός, ότι και να υπάρξει μια επίθεση και να γίνει διαρροή κλειδιών, δεν θα επηρεαστούν άλλες τελικές συσκευές στο δίκτυο παρά μόνο η επιτιθέμενη. Ως απάντηση σε αυτό οι συσκευές LoRaWAN χρησιμοποιούν επιπλέον κρυπτογραφικά κλειδιά ως μηχανισμούς ασφαλείας για την πραγματοποίηση του ελέγχου ταυτότητας (Join Procedure) και του ελέγχου ακεραιότητας. Παρόλα αυτά, κάποιες συσκευές χρειάζεται να χρησιμοποιούν συγκεκριμένα κλειδιά χωρίς να τα αλλάζουν καθόλη την διάρκεια της ζωής τους. Επομένως, σε περίπτωση που υπάρξει διαρροή κλειδιών ο επιτιθέμενος (Attacker) θα αποκτήσει πρόσβαση σε όλα τα δεδομένα που έχουν μεταφερθεί από την συσκευή.

1.2 *Αρχιτεκτονική IoT*

Ένα ολοκληρωμένο σύστημα IoT αποτελείται από τα παρακάτω τρία στρώματα.

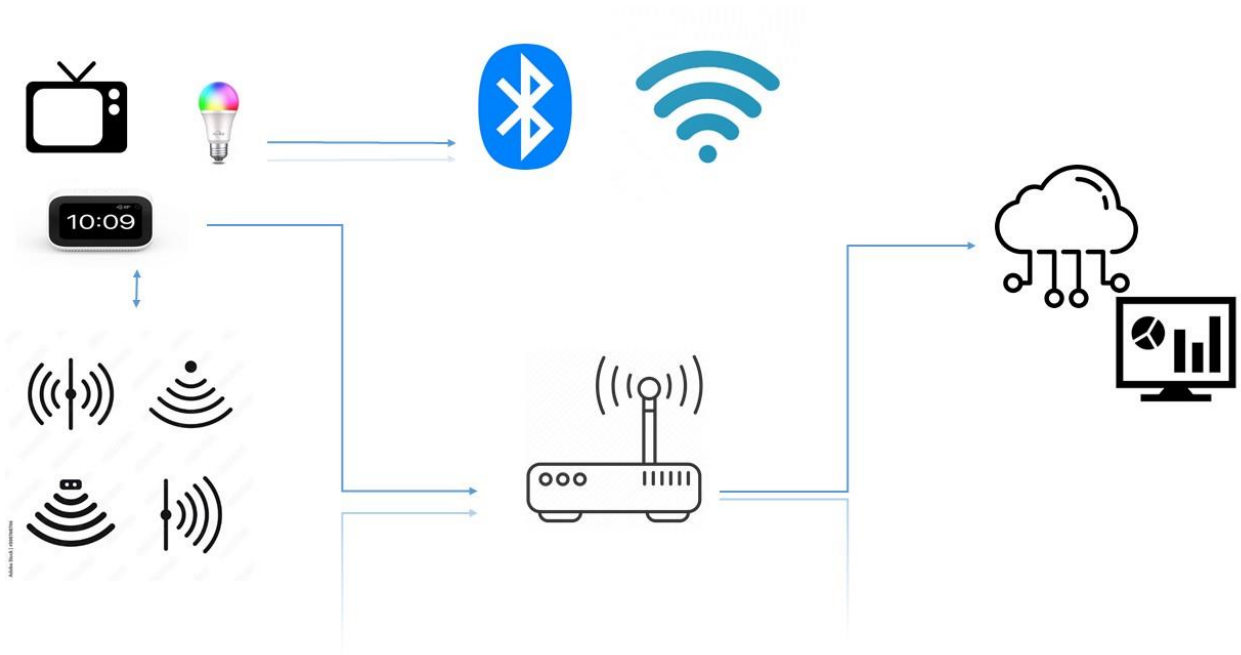


Εικόνα 2 Αρχιτεκτονική IoT

1. Στο πρώτο επίπεδο συναντάμε το φυσικό στρώμα (Physical layer), το οποίο συλλέγει δεδομένα και πληροφορίες. Σε αυτό το στρώμα όλοι οι ενεργοποιητές λειτουργούν σύμφωνα με τις πληροφορίες που έχουν συλλεχθεί από τους αισθητήρες με σκοπό την εκτέλεση συγκεκριμένων λειτουργιών. [3]
2. Στο δεύτερο επίπεδο βρίσκουμε το Network layer. Σε αυτό το επίπεδο δημιουργείται η σύνδεση μεταξύ της εφαρμογής (Application layer) και του φυσικού στρώματος (perceptual layer). Το Network layer είναι υπεύθυνο για την μετάδοση των δεδομένων και την σύνδεση των συσκευών. [3]
3. Στο τελευταίο επίπεδο της πυραμίδας συναντάμε το Application layer. Σε αυτό το επίπεδο ουσιαστικά βρίσκεται η εφαρμογή, η οποία αλληλοεπιδρά με τον χρήστη, απεικονίζοντας τα δεδομένα που αποστέλλονται από τους αισθητήρες. [3]

1.3 *Παράδειγμα Λειτουργίας IoT*

Ένα ολοκληρωμένο σύστημα IoT απαρτίζεται από τελικές συσκευές, οι οποίες συνδέονται ενσύρματα ή ασύρματα και αποτελούνται από διάφορα εξαρτήματα, όπως οι αισθητήρες ή ενεργοποιητές. Είναι υπεύθυνα για την συλλογή όλων των δεδομένων και την ανταλλαγή μηνυμάτων. Οι συσκευές συνδέονται στο δίκτυο με την βοήθεια πυλών (gateway), οι οποίες επεξεργάζονται τα δεδομένα που έχουν συλλεχθεί από τους αισθητήρες και τα μεταβιβάζουν στον cloud. Ο cloud αποθηκεύει τα δεδομένα και ο χρήστης πραγματοποιεί διάφορες ενέργειες για την περαιτέρω κατανόηση τους.



Εικόνα 3 Παράδειγμα Λειτουργίας IoT

Το έξυπνο σπίτι (Smart Home –βλέπε Εικόνα 4) είναι ένα παράδειγμα για το πως το Διαδίκτυο των Πραγμάτων έχει αλλάξει το τρόπο ζωής μας. Πλέον, ένας χρήστης μέσω μιας έξυπνης συσκευής (smartphone,tablet) μπορεί να ελέγχει, να αυτοματοποιεί και να συλλέγει δεδομένα από το κλιματιστικό, τον φούρνο μικροκυμάτων, το κουδούνι της πόρτας, τις κάμερες ασφάλειας κ.α., δημιουργώντας, μια σχέση συνεργατική μεταξύ των συσκευών, έχοντας ως σκοπό την απλοποίηση της ζωής του.

Εικόνα 4 Smart Home[2]

1.4 *LoRa: Ένα Πρότυπο για την Επικοινωνία σε Περιβάλλον IoT*

Το LoRa το οποίο σημαίνει "Long Range" είναι μια τεχνολογία ασύρματης διαμόρφωσης σήματος που ονομάζεται chirp spread spectrum (css). Αναπτύχθηκε από την Cycleo στη Γαλλία και το 2012 εξαγοράστηκε από την Semtech, που είναι ιδρυτικό μέλος της LoRa Alliance. Ο τρόπος που λειτουργεί, θυμίζει τον τρόπο επικοινωνίας των δελφινιών και των νυχτερίδων. Δηλαδή, η πληροφορία μεταδίδεται μέσω ραδιοκυμάτων και αποκρυπτογραφείτε με παλμούς. Το LoRa είναι ιδανικό για εφαρμογές που μεταδίδουν μικρά πακέτα δεδομένων με αργό ρυθμό (Low Bit Rate) και σε συνδυασμό με την μεγάλη εμβέλεια που έχει, η τεχνολογία αυτή είναι ιδανική για αισθητήρες και ενεργοποιητές που λειτουργούν με χαμηλή ισχύ. Επιπρόσθετα, λειτουργεί στις χωρίς άδεια ζώνες συχνοτήτων όπως το Wi-Fi και παρουσιάζεται ως αρκετά ασφαλές σύστημα. Συγκεκριμένα, εκπέμπει στα 868MHz, 915MHz και στα 433MHz για τις ηπείρους Ευρώπη, Αμερική και Ασία αντίστοιχα. Το LoRa επιτρέπει στις συσκευές να μεταδίδουν δεδομένα σε μεγάλες αποστάσεις (10-40km σε μη αστικές περιοχές, 1-5km σε αστικές περιοχές) καταναλώνοντας ελάχιστη ενέργεια και ταυτόχρονα παρέχετε μεγάλη ενεργειακή ζωή (πάνω από 10+ χρόνια η διάρκεια της μπαταρίας).

[2] https://smarthomemart.in/smart-home-ideas-to-transform-your-home/

Εικόνα 5 LoRa[3]

Η τεχνολογία LoRa επιτρέπει την λειτουργία πληθώρας έξυπνων εφαρμογών IoT που έχουν στόχο να επιλύσουν προκλήσεις όπως την διαχείριση ενέργειας, την μείωση φυσικών πόρων, τον έλεγχο της ρύπανσης και την πρόληψη καταστροφών. Το πλεονέκτημα των αισθητήρων LoRa είναι ότι λειτουργούν στο ISM δηλαδή στο βιομηχανικό, επιστημονικό και ιατρικό τομέα σε ελεύθερες συχνότητες, χωρίς κάποια επιπρόσθετη άδεια. Το επίπεδο της εφαρμογής που ορίζεται από τον χρήστη είναι πάνω στο MAC το οποίο έχει καθοριστεί από το LoRa Alliance και δεν είναι συνδεδεμένο πάνω σε κάποιο τηλεφωνικό δίκτυο δίνοντας έτσι την δυνατότητα στον χρήστη να χρησιμοποιήσει μια εφαρμογή ενός ανοιχτού δικτύου.

Στο πεδίο εφαρμογής του Διαδίκτυού των Πραγμάτων (IoT) το πρωτόκολλο επικοινωνίας LoRa λύνει πολλά προβλήματα καθώς διασφαλίζει την μετάδοση των δεδομένων σε μεγάλες αποστάσεις κάνοντας το ιδανικό για μεγάλης κλίμακας αισθητήριών όπως αυτοί χρησιμοποιούνται σε μια "έξυπνη" πόλη.

Εικόνα 6 LoRa Συχνότητες[4]

[3] https://pplware.sapo.pt/internet/lora-a-tecnologia-de-radio-frequencia-para-a-internet-das-coisas/

[4] http://pdacontrolen.com/introduction-lora-module-rfm95-hoperf/

1.5 *Ενδεικτικές Χρήσεις του LoRa*

Στον τομέα της Έξυπνης Πόλης (Smart City)

- Έξυπνος Φωτισμός
- Καλύτερη διαχείριση αποβλήτων
- Άμεσος εντοπισμός πυρκαγιάς
- Καλύτερη διαχείριση στάθμευσης οχημάτων

Στον τομέα της Βιομηχανίας (Industrial)

- Εντοπισμός και παρακολούθηση μεταφοράς προϊόντων
- Εντοπισμός και παρακολούθηση στην Ναυτιλία
- Έξυπνη τεχνολογία αισθητήρων
- Ανίχνευση ακτινοβολίας και άλλων διαρροών

Στον τομέα της Γεωργίας (Agriculture)

- Παρακολούθηση θερμοκρασίας και υγρασίας
- Έξυπνη μέτρηση και διαχείριση νερού
- Παρακολούθηση και άντληση σημαντικών πληροφοριών για τα ζώα

Στον τομέα της Υγείας (Healthcare)

- Σύνδεση και διαχείριση συσκευών παρακολούθησης της υγείας
- Φορητή/ ασύρματα τεχνολογία

1.6 *Πλεονεκτήματα και Μειονεκτήματα Τεχνολογίας LoRa*

Πλεονεκτήματα τεχνολογίας LoRa

- Χαμηλή κατανάλωση ενέργειας
- Μεγάλη εμβέλεια
- Χαμηλό κόστος
- Ευκολία στην δημιουργία επικοινωνίας μέσω LoRa
- Λειτουργεί χωρίς Internet

Μειονεκτήματα τεχνολογίας LoRa

- Μη συμβατότητα με όλες τις εφαρμογές
- Χαμηλός βαθμός μετάδοσης
- Χαμηλό εύρος ζώνης
- Αρκετή παρεμβολή φάσματος

2. ΚΕΦΑΛΑΙΟ 2

2.1 *LoRaWAN*

Το πρότυπο LoRa, όπως περιληπτικά παρουσιάστηκε στο προηγούμενο κεφάλαιο, αφήνει την επιλογή στον χρήστη να επιλέξει το πρωτόκολλο επικοινωνίας και το δίκτυο που θα χρησιμοποιήσει. Αυτό πρακτικά σημαίνει ότι κάποιος μπορεί να δημιουργήσει ένα δίκτυο LoRa χωρίς περιορισμούς, χρησιμοποιώντας όποιο προϊόν ικανοποιεί καλύτερα τις ανάγκες του.

Ένα τυπικό δίκτυο LoRa αποτελείται από τερματικές συσκευές (end-devices), οι οποίες επικοινωνούν με την πύλη (gateway) χρησιμοποιώντας το LoRaWAN. Στην συνέχεια οι πύλες (gateway) μεταφέρουν τις πληροφορίες σε έναν Server συνήθως με την βοήθεια του ασύρματου Wi-Fi ή του ενσύρματου (Ethernet). Ουσιαστικά, ο τρόπος επικοινωνίας ενός LoRa δικτύου είναι αρκετά απλός. Μια πύλη (gateway) επικοινωνεί, "μιλάει" με τους τελικούς κόμβους και αντίστροφα. Πιο συγκεκριμένα, κάθε κόμβος μπορεί να επικοινωνεί ή τουλάχιστον να προσπαθεί να επικοινωνήσει με το gateway, αλλά το gateway δεν μπορεί να ακούσει όλους του κόμβους ταυτόχρονα.

Το LoRaWAN είναι ένα πρωτόκολλο επιπέδου ελέγχου πρόσβασης πολυμέσων (Media Access Control, (MAC)) που είναι χτισμένο πάνω στην τεχνολογία LoRa. Είναι ένα επίπεδο λογισμικού που καθορίζει τον τρόπο με τον οποίο οι συσκευές χρησιμοποιούν το υλικό LoRa, για παράδειγμα όταν μεταδίδουν ένα μήνυμα αλλά και τη μορφή των μηνυμάτων. Το πρωτόκολλο LoRaWAN και οι συσκευές LoRa συνδυάζουν αυτά τα χαρακτηριστικά του Wi-Fi και του δικτύου κινητής για να προσφέρουν αποδοτική, ευέλικτη και οικονομική λύση συνδεσιμότητας ιδανική για εφαρμογές IoT. Αναλυτικότερα, απλοί αισθητήρες μπορούν να τροφοδοτούν με δεδομένα πλατφόρμες ανάλυσης, όπως αυτές της τεχνητής νοημοσύνης και της μηχανικής μάθησης [4].

Η ¨συμμαχία¨ LoRa Alliance είναι μια ανοιχτή, μη κερδοσκοπική ένωση που ιδρύθηκε το 2015. Υποστηρίζει την ανάπτυξη του πρωτοκόλλου LoRaWAN και διασφαλίζει τη λειτουργικότητα όλων των προϊόντων και τεχνολογιών LoRaWAN. Ακόμα, παρέχει πιστοποίηση LoRaWAN για τις τελικές συσκευές, μετρώντας σήμερα πάνω από 500 μέλη σε όλο τον κόσμο. Οι πιστοποιημένες τελικές συσκευές, παρέχουν στους χρήστες εμπιστοσύνη, ότι η τελική συσκευή είναι αξιόπιστη και συμβατή με τις προδιαγραφές LoRaWAN [5].

2.2 *Πλεονεκτήματα LoRaWAN*

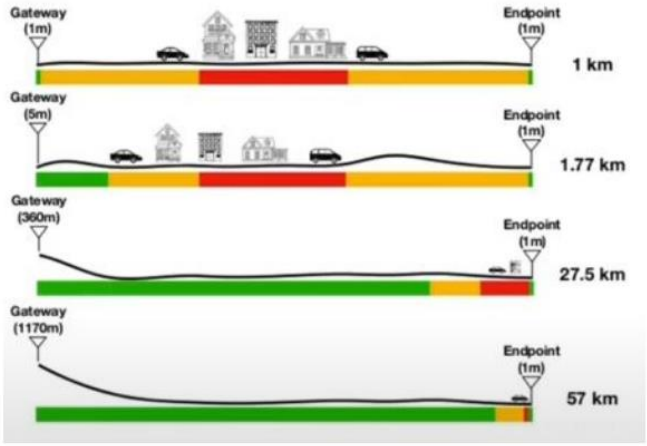
Πλεονεκτήματα του LoRaWAN

- Χαμηλή Κατανάλωση Ενέργειας

Η διάρκεια ζωής μιας συσκευής που λειτουργεί με το πρότυπο LoRaWAN μπορεί να φτάσει μέχρι τα 10 χρόνια καταναλώνοντας μόνο μια μπαταρία.

- Μεγάλη Εμβέλεια

Η θεωρητική μέγιστη εμβέλεια που μπορεί να έχει ένα LoRaWAN σύστημα είναι στα 850km. Το 2020 το The Things Conference πέτυχε ρεκόρ εμβέλειας στα 832km με την χρησιμοποίηση μπαλονιών. Αυτή η εμβέλεια, μπορεί να πραγματοποιηθεί μόνο όταν μια πύλη είναι στον αέρα, όταν βρίσκεται στο έδαφος τα πράγματα είναι διαφορετικά, καθώς υπάρχουν παρεμβολές. Πιο συγκεκριμένα, στο έδαφος η αναμενόμενη εμβέλεια είναι στα 500 μέτρα σε κλειστούς χώρους, 2 χιλιόμετρα όταν μια πύλη βρίσκεται στη στέγη ενός σπιτιού και στα 10 χιλιόμετρα όταν η πύλη βρίσκεται σε ουρανοξύστη.



Εικόνα 7 LoRaWAN εμβέλεια[5]

- Γεωτοποθεσία

Μέσω του LoRaWAN δικτύου είναι δυνατόν να καθοριστεί η θέση των τελικών συσκευών χωρίς την χρήση του Παγκόσμιου συστήματος Θεσιθεσίας (GPS)

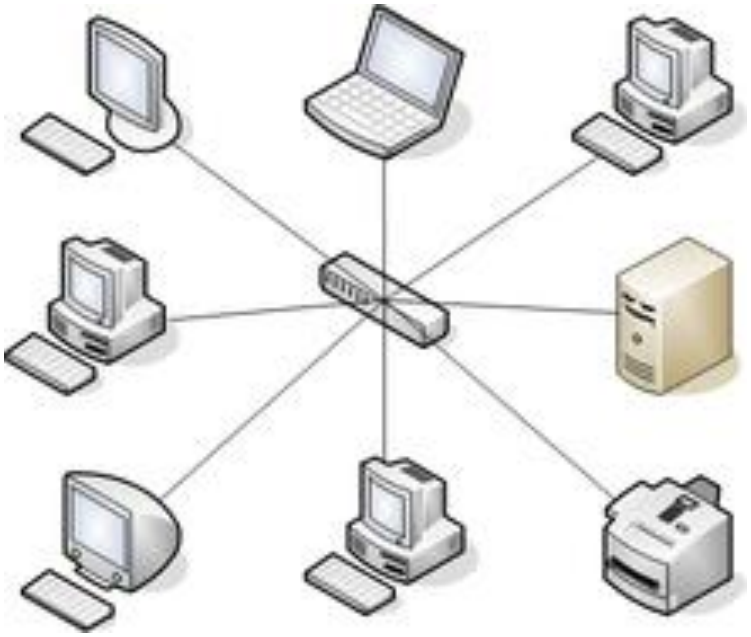
- Πρωτόκολλο Ασφαλείας

Η ασφαλή μεταφορά των δεδομένων από την τελική συσκευή προς το δίκτυο και αντίστροφα εξασφαλίζεται με την χρησιμοποίηση κρυπτογραφικού πρωτοκόλλου, που ονομάζεται AES-128.

[5] https://www.techinform-an.it/files/[EduGreen]_Presentazione_IOT_-_Lorawan.pdf

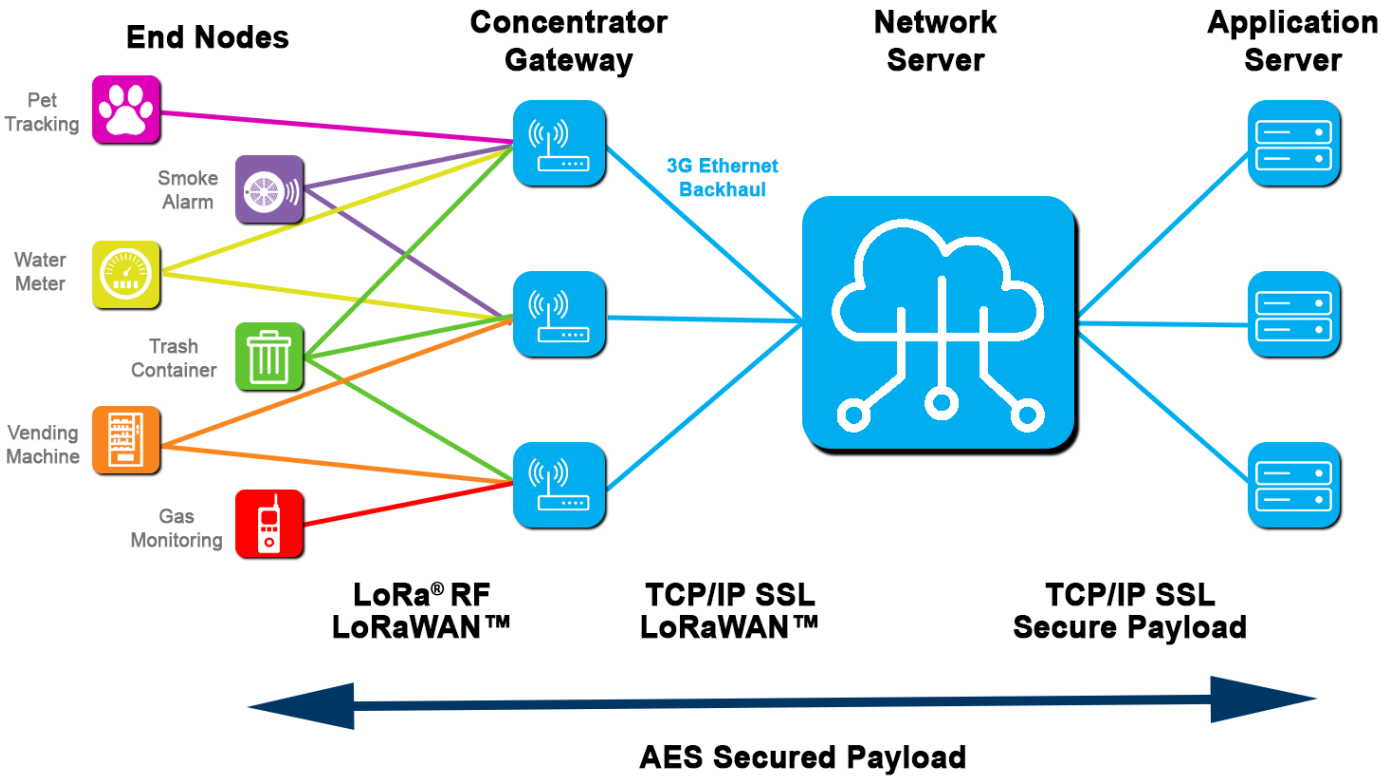
2.3 *Αρχιτεκτονική LoRaWAN*

Το LoRaWAN είναι ένα δίκτυο αστέρα, δηλαδή κάθε τελική συσκευή συνδέεται σε ένα κεντρικό κόμβο, ο οποίος είναι υπεύθυνος για τη διατήρηση και τον έλεγχο της επικοινωνίας μεταξύ των κόμβων και του κεντρικού δικτύου. Στο LoRaWAN δίκτυο, κάθε τελική συσκευή (end device) δεν είναι συνδεδεμένη σε μια συγκεκριμένη πύλη, αλλά τα δεδομένα που αποστέλλονται λαμβάνονται από όλες τις κοντινές πύλες (Gateways). Η πύλη (Gateway) είναι συνδεδεμένη με το Network Server μέσω μια σταθερής IP σύνδεσης και δεν εκτελεί καμία λειτουργία ασφαλείας απλώς δρα σαν διαφανείς γέφυρα (transparent bridge) μετατρέποντας τα RF πακέτα σε IP πακέτα και αντίστροφα. Στην συνέχεια, ο Network Server είναι υπεύθυνος για την ασφάλεια της τελικής συσκευής, επιτρέποντας της να αποστείλει τα δεδομένα. Τέλος, σε ένα δίκτυο αστέρα οι μεταδόσεις μιας τελικής συσκευής (end-device) μεταδίδονται μέσω του κόμβου μόνο στην συνδεδεμένη συσκευή και όχι σε κάθε συσκευή του δικτύου.



Εικόνα 8 Δίκτυο Αστέρα

Στην παρακάτω εικόνα (βλέπε εικόνα 9) παρουσιάζεται ένα τυπικό δίκτυο LoRa το οποίο αποτελείται από τέσσερα διαφορετικά στοιχεία: τις τελικές συσκευές (end-node), την πύλη (gateway), το δίκτυο (Network Server) και τον Application Server. Οι τελικές συσκευές (οι οποίες συχνά αναφέρονται και ως τελικοί κόμβοι – end nodes), χρησιμοποιούνται για να συλλέξουν και να αποστείλουν δεδομένα από τους αισθητήρες προς τις πύλες (Gateways) και κάποιες φορές για να ελέγξουν μακρινά εξωτερικά συστήματα. Συνήθως είναι χαμηλής ισχύος συσκευές και επικοινωνούν ασύρματα με μια ή παραπάνω πύλες [4] . Οι πύλες στην συνέχεια λαμβάνουν τα μηνύματα και τα μεταβιβάζουν χρησιμοποιώντας τυπικές συνδέσεις TCP/IP στον Network Server που είναι υπεύθυνος για τον έλεγχο της ασφάλειας των μηνυμάτων. Ως εκ τούτου, η αρχιτεκτονική ενός δικτύου LoRaWAN όπως αναφέραμε παραπάνω βασίζεται στην τοπολογία αστεριών. Τέλος, αν ο Network Server εγκρίνει αυτά τα μηνύματα, τα προωθεί στην εφαρμογή.



Εικόνα 9 Τυπικό Δίκτυο LoRa[6]

Τελικές Συσκευές (End-Devices)

Μια LoRaWAN συσκευή μπορεί να είναι ένας αισθητήρας ή ένας ενεργοποιητής[7] ή και τα δύο, και συνδέεται ασύρματα στο LoRaWAN δίκτυο μέσω της πύλης χρησιμοποιώντας RF modulation.

Πύλη (Gateways)

Μια LoRaWAN πύλη (gateway), στέλνει ή λαμβάνει μηνύματα από την τελική συσκευή (End-Device) και τα προωθεί στο LoRaWAN δίκτυο (Network Server). Οι πύλες συνδέονται στο δίκτυο

[6] https://ecsxtal.com/news-resources/electronic-components-technical-guides?id=382:quartz-crystal-design-parameters&catid=382:electronic-component-technical-guides

[7] Ένας ενεργοποιητής είναι ένα εξάρτημα μιας μηχανής που είναι υπεύθυνο για τη μετακίνηση και τον έλεγχο ενός μηχανισμού ή συστήματος.

μέσω του Wi-Fi, Ethernet, Cellular (3G/4G/5G). Οι πύλες LoRaWAN χωρίζονται σε δύο κατηγορίες, για εσωτερική χρήση (Picocell) ή για εξωτερική χρήση (Macrocell).

- Εσωτερικής Χρήσης (Picocell): Αυτός ο τύπος πυλών είναι πιο οικονομικός και κατάλληλος για χρήσεις σε κλειστούς χώρους όπως ένα υπόγειο, σε ένα εργοστάσιο, σε ένα νοσοκομείο κλπ. Η απόσταση που μπορεί να καλύψει είναι περίπου στα 200 μέτρα.
- Εξωτερικής Χρήσης (Microcell): Οι εξωτερικές πύλες παρέχουν μεγαλύτερη κάλυψη από τις εσωτερικές πύλες. Είναι κατάλληλες για την κάλυψη τόσο σε αγροτικές όσο και σε αστικές περιοχές. Αυτές οι πύλες μπορούν να τοποθετηθούν στις στέγες πολύ ψηλών κτιρίων, σε μεταλλικούς ιστούς κ.α. . Συνήθως μια εξωτερική πύλη έχει μια εξωτερική κεραία (δηλαδή κεραία από υαλοβάμβακα) συνδεδεμένη με ένα ομοαξονικό καλώδιο.

Network Server

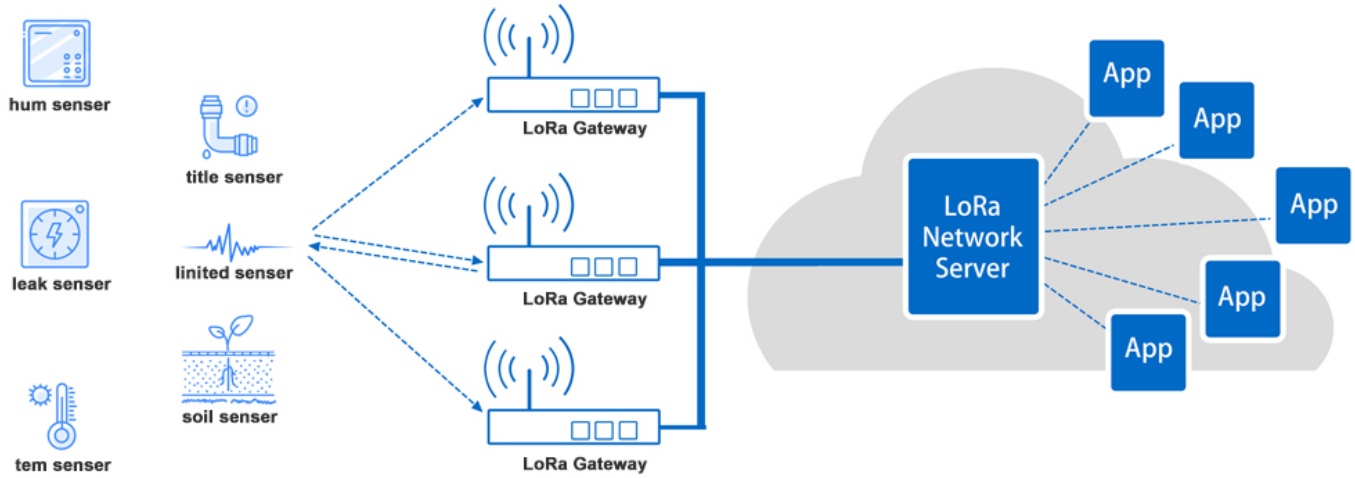
Ο διακομιστής δικτύου (Network Server) διαχειρίζεται τελικές συσκευές, πύλες, εφαρμογές και όλους τους χρήστες στο LoRaWAN δίκτυο.

Αναλυτικότερα είναι υπεύθυνος :

1. Για την δημιουργία ασφαλών συνδέσεων χρησιμοποιώντας το πρωτόκολλο AES-128 για την μεταφορά των μηνυμάτων μεταξύ των τελικών συσκευών
2. Για τον έλεγχο και την επικύρωση της αυθεντικότητας των τελικών συσκευών
3. Για την ακεραιότητα των μηνυμάτων
4. Για την επιλογή της γρηγορότερης πύλης για την αποστολή downlink μηνυμάτων
5. Για την απάντηση σε όλες τις MAC εντολές
6. Για την προώθηση των Join Request και των Join Accept μηνυμάτων μεταξύ των τελικών συσκευών και του Server

Application Server

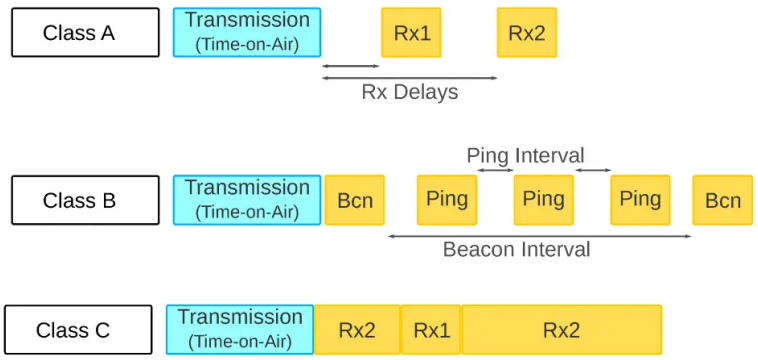
Είναι το λογισμικό που τρέχει στον Server που είναι υπεύθυνο για τα θέματα ασφαλείας και την διαχείριση των δεδομένων που αποστέλλονται. Επίσης, παράγει τα downlinks payload και τα στέλνει στις συνδεδεμένες τελικές συσκευές μέσω του δικτύου.



Εικόνα 10 Ολοκληρωμένο Σύστημα LoRaWAN[8]

2.4 *Κλάσεις του LoRaWAN*

Το LoRaWAN καθορίζει το πρωτόκολλο δικτύωσης για τις συσκευές LoRa. Οι προδιάγραφες λειτουργίας μια συσκευής που ορίζονται από το LoRaWAN αφορούν, το τρόπο λειτουργίας μιας τελικής συσκευής και τα κλειδιά που θα χρησιμοποιούνται με σκοπό την κατασκευή ενός ασφαλούς ασύρματου δικτύου. Σύμφωνα λοιπόν με τα παραπάνω και τις προδιαγραφές LoRaWAN, οι τελικές συσκευές LoRa χωρίζονται σε 3 διαφορετικές κατηγορίες [5], οι οποίες αναφέρονται ως Κλάσεις λειτουργίας (Κλάση A, Κλάση B, και Κλάση C). Πιο συγκεκριμένα:



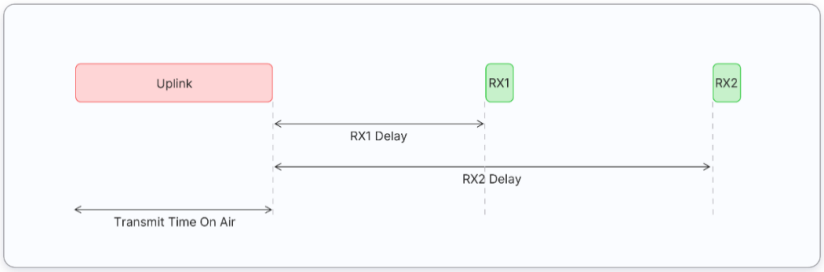
Εικόνα 11 Κλάσεις LoRaWAN[9]

[8] https://www.nicerf.com/articles/detail/lorawan-gateway.html

[9] https://www.mdpi.com/1424-8220/20/15/4273

Κλάση Α

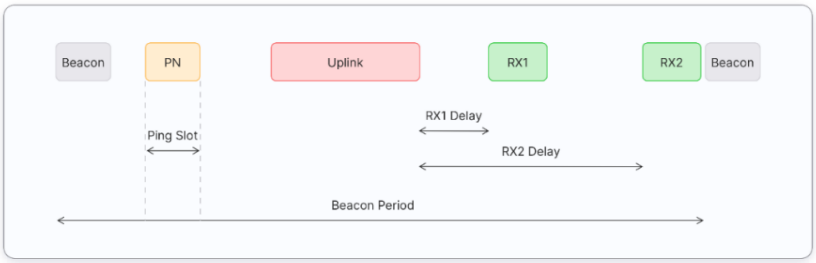
Είναι μια κλάση που ονομάζεται ALOHA σύστημα και είναι πλήρως ασύγχρονο. Αναλυτικότερα, η επικοινωνία μεταξύ των τελικών κόμβων και του gateway γίνεται μόνο όταν οι κόμβοι έχουν κάτι να αναφέρουν, και μέχρι εκείνη την στιγμή παραμένουν σε αδράνεια. Πιο συγκεκριμένα, ένας αισθητήρας στέλνει δεδομένα περιοδικά σε μια πύλη (gateway). Εφόσον, γίνει η αποστολή των δεδομένων ο κόμβος διατηρεί τον δέκτη ενεργό για μικρό χρονικό διάστημα στο οποίο μπορεί να λάβει σαν απάντηση ένα downlink μήνυμα από τον Network Server. Μόλις αυτή η διαδικασία φτάσει στο τέλος της, ο αισθητήρας εισέρχεται σε κατάσταση ύπνου (sleep mode) με σκοπό την εξοικονόμηση ενέργειας [6].



Εικόνα 12 Κλάση Α LoRaWAN[10]

Κλάση Β

Η συγκεκριμένη κλάση έχει μικρότερη καθυστέρηση μετάδοσης μηνύματος σε σχέση με την κλάση Α, διότι τα μηνύματα μεταδίδονται σε προκαθορισμένο χρόνο και δεν χρειάζεται να σταλθεί ένα uplink για να ληφθεί ένα downlink. Παρόλα αυτά, η κατανάλωση ενέργειας είναι μεγαλύτερη διότι η συσκευή παραμένει για περισσότερο χρόνο ενεργή κατά την διάρκεια των beacons και του Ping slot. Αναλυτικότερα, οι συσκευές που λειτουργούν με το πρότυπο της κλάσης Β ανοίγουν Downlink ping slots σε καθορισμένες στιγμές για να λάβουν ένα downlink μήνυμα από τον Network Server. Αυτό επιτρέπει στον Server να γνωρίζει την ακριβή στιγμή που μια τελική συσκευή "ακούει" [6].



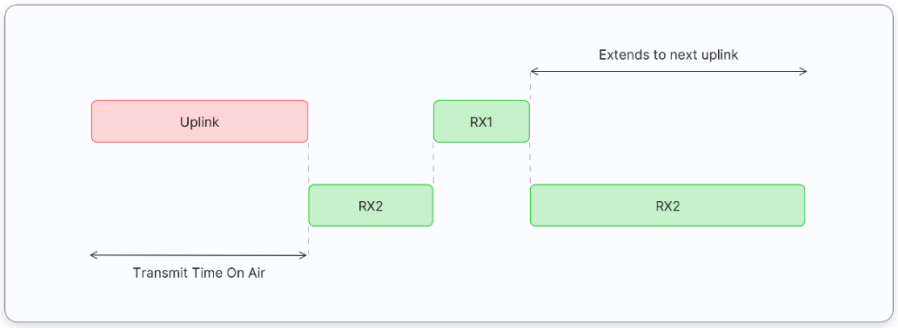
Εικόνα 13 Κλάση Β LoRaWAN[11]

[10] https://www.thethingsnetwork.org/docs/lorawan/classes/

[11] https://www.thethingsnetwork.org/docs/lorawan/classes/

Κλάση C

Αυτή η κλάση ουσιαστικά χρησιμοποιεί την μεγαλύτερη ενέργεια καθώς επιτρέπει στους κόμβους να είναι ενεργοί και να επικοινωνούν συνέχεια μέχρι τον τερματισμό της λειτουργίας τους. Συνιστάτε να την χρησιμοποιούν εφαρμογές που δεν λειτουργούν με την χρήση μπαταριών, λόγω της πολύς ενέργειας που απαιτούν για την λειτουργία τους [6].



Εικόνα 14 Κλάση C LoRaWAN[12]

2.5 *Τρόποι Σύνδεσης και Ενεργοποίησης των Τελικών Συσκευών*

Κάθε συσκευή που είναι συμβατή με το LoRa για να συνδεθεί σε ένα δίκτυο LoRaWAN πρέπει πρώτα να ενεργοποιηθεί. Οι δυνατοί τρόποι ενεργοποίησης των συσκευών που στηρίζονται στην έκδοση 1.0.1 του LoRaWAN είναι δύο και περιγράφονται παρακάτω :

- **1ος Τρόπος (ABP)**: Με αυτόν τον τρόπο, ο τελικός κόμβος προσπαθεί να συνδεθεί με το LORAWAN μέσω του ABP (Authentication By Personalization). Η τελική συσκευή συνδέεται με ένα συγκεκριμένο δίκτυο χρησιμοποιώντας τα ίδια κλειδιά καθόλη την διάρκεια λειτουργείας του. Δηλαδή, αυτή η διαδικασία συνδέει απευθείας τις τελικές συσκευές στο καθορισμένο δίκτυο, χωρίς να ξεκινάει κάποιο αίτημα συμμετοχής (Join Request) ώστε να απαιτεί την αποδοχή του (Accept Procedure) [8] . Πιο συγκεκριμένα, ο τελικός κόμβος συνδέεται με το Device Address (DevADDr) (παρόμοιο με το IP) με το Network Session Key (NwkSKey) που είναι υπεύθυνο για την ασφάλεια του Server και το App Session Key (AppS Key) που είναι υπεύθυνο για την ασφάλεια της εφαρμογής. Αυτά τα κλειδιά είναι μοναδικά και αποθηκεύονται από τον χρήστη στον τελικό κόμβο. Αφού ολοκληρωθεί η διαδικασία ανταλλαγής των απαραίτητων κλειδιών, ο τελικός κόμβος ξεκινάει την επικοινωνία με τον Server. Επομένως, δεν δημιουργούνται νέα κλειδιά με αποτέλεσμα η κρυπτογράφηση των μηνυμάτων να γίνεται με τα προ ανάθεσα κλειδιά.

[12] https://www.thethingsnetwork.org/docs/lorawan/classes/

- **2ος Τρόπος (OTAA)**: αυτός ο τρόπος ενεργοποίησης των συσκευών LoRa ονομάζεται OTAA (Over-The-Air-Authentication). Με αυτόν τον τρόπο η τελική συσκευή στέλνει μη κρυπτογραφημένο αίτημα σύνδεσης στον αντίστοιχο Server με σκοπό την αμφίδρομη επικοινωνία τους. Αναλυτικότερα, το αίτημα σύνδεσης (Join Request) που στέλνετε περιέχει το AppEUI, DevEUI μια τυχαία τιμή που ονομάζεται DevNonce, το Message Integrity Code (MIC) και το Media Access Control (MHDR) Header. Το MAC header ορίζει το τύπο του μηνύματος και την έκδοση που χρησιμοποιείται από το πρωτόκολλο LoRaWAN για την αποκρυπτογράφηση. Η τιμή MIC είναι το αποτέλεσμα της αποκρυπτογράφησης ενός από τα AppEUI, DevEUI, DevNonce, MHDR ή όλων μαζί χρησιμοποιώντας ένα κλειδί που ονομάζεται AppKey. Κάθε τελική συσκευή για να στείλει ένα αίτημα σύνδεσης στον Server αναπτύσσει ένα μοναδικό 128bit AppKey, το οποίο πρέπει να εισαχθεί χειροκίνητα στην τελική συσκευή και στον Network Server. Το αίτημα αυτό δεν είναι κρυπτογραφημένο αλλά επειδή συνδέεται με ένα AppKey περιέχονται σε αυτό τα μοναδικά AppEUI και DevEUI του τελικού κόμβου και μια τιμή 2 byte του DevEUI η οποία είναι τυχαία. Όταν στέλνεται το αίτημα συμμετοχής (Join Procedure) χρησιμοποιείται το AppKey για να γίνει η αποκρυπτογράφηση της τιμής MIC με σκοπό να ταυτοποιηθεί η συσκευή. Το AppEUI είναι μοναδικό για κάθε διαχειριστή της συσκευής. Τέλος, ο Server ελέγχει τα κλειδιά και σε περίπτωση που είναι έγκυρα προχωράει στην αποδοχή του αιτήματος σύνδεσης. Γενικά ο τρόπος σύνδεσης OTAA περιγράφεται ως ο πιο ασφαλής τρόπος ελέγχου ταυτότητας, καθώς αυτή η διαδικασία πρέπει να ακολουθείται κάθε φορά από την τελική-συσκευή αν θέλει να συμμετάσχει σε ένα νέο δίκτυο ή αν έληξε η σύνδεση με το προ υπάρχον [8].

  Αφού ολοκληρωθεί η διαδικασία σύνδεσης με οποιαδήποτε μέθοδο (ABP ή OTAA), η τελική συσκευή ξεκινάει να ανταλλάζει μηνύματα με το Network Server. Σύμφωνα με το πρωτόκολλο LoRaWAN υπάρχουν δύο τύποι μηνυμάτων, το Uplink και το Downlink. Ο τύπος μηνυμάτων Uplink αποστέλλεται μόνο από τις τελικές συσκευές (End-Devices) έχοντας ως αποδέκτη τον Network Server. Οι πύλες (Gateway) δρουν ως μεσολαβητής αυτών των μηνυμάτων προωθώντας τα στο τελικό στόχο όπου είναι ο Network Server. Από την άλλη πλευρά, ο τύπος μηνυμάτων Downlink αποστέλλεται μόνο από τον Network Server έχοντας ως αποδέκτη μόνο μια τελική συσκευή και ως μεσολαβητή μόνο μια πύλη (Gateway).

Επομένως, η διαφορά ανάμεσα σε ένα ABP και OTAA σύστημα, είναι ότι με το ABP χρησιμοποιείται ένα σταθερό σύστημα ασφαλείας, σε αντίθεση με την μέθοδο OTAA ο Server διαπραγματεύεται και ελέγχει τα κλειδιά, ώστε να προχωρήσει στην σύζευξη των συσκευών. Μια διαδικασία που επαναλαμβάνεται κάθε φορά, που μια τελική συσκευή θέλει να συνδεθεί με ένα δίκτυο.

2.6 *Διαδικασία Σύνδεσης και Ενεργοποίησης με τον τρόπο OTAA*

Βήμα 1ο

Η τελική συσκευή στέλνει ένα μη κρυπτογραφημένο αίτημα σύνδεσης (Join Request) στο δίκτυο (Network). Αυτό, το αίτημα σύνδεσης αποτελείται από:

- AppEUI: Είναι ένα παγκόσμιο μοναδικό αναγνωριστικό 64-Bit (8 bytes) που προσδιορίζει τον αντίστοιχο Network Server που είναι υπεύθυνος για την επεξεργασία του Join Request μηνυμάτων
- DevEUI: Είναι ένα 64bit (8 bytes) μοναδικό αναγνωριστικό της κάθε συσκευής και ορίζεται από τον κατασκευαστή ή από τον ιδιοκτήτη.
- DevNonce : Είναι ένα μοναδικό τυχαίο 2 byte αναγνωριστικό που παράγεται από την τελική συσκευή. Ο Network Server αποθηκεύει το DevNonce κάθε συνδεδεμένης συσκευής. Σε περίπτωση, που σταλθεί ένα αίτημα σύνδεσης με χρησιμοποιημένο DevNonce (Replay Attack) γίνεται απόρριψη του αιτήματος εκείνης της συσκευής.
- AppKey: Είναι ένα μοναδικό μυστικό αναγνωριστικό AES-128bit.

Πριν σταλθεί το αίτημα σύνδεσης (Join Request) για απόκτηση πρόσβασης στο δίκτυο, θα πρέπει το AppEUI, το DevEUI και το AppKey να αποθηκευτούν στην τελική συσκευή. Ακόμα, τα ίδια αναγνωριστικά θα πρέπει να αποθηκευτούν επίσης και στον Network Server. Το AppEUI και το DevEUI είναι ορατά σε όλους. Ο κωδικός ακεραιότητας μηνύματος (MIC) χρησιμοποιώντας το AppKey κρυπτογραφεί όλα τα πεδία και στην συνέχεια προστίθεται στο αίτημα σύνδεσης/συμμετοχής.

Βήμα 2ο

Εφόσον γίνει η αποδοχή της συσκευής ο Network Server με την βοήθεια του AppKey αποκρυπτογραφεί το DevNonce ή μια τιμή που ονομάζεται AppNonce και παράγει δύο κλειδιά τα (NwkSKey και AppSKey).

- AppNonce: Είναι ένας τυχαίος αριθμός ή ένα μοναδικό ID που παρέχεται από το Network Server, και χρησιμοποιείται από την τελική συσκευή για να αποκτήσει πρόσβαση στο NwkSKey και AppSKey.
- NEtID: Αποτελείται από τα πιο σημαντικά 7 bits και είναι ένα Network αναγνωριστικό (NwkID)
- DevAddr: Είναι ένα 32-bit αναγνωριστικό που χρησιμοποιείται από το Network Server για να αναγνωρίζει την τελική συσκευή μέσα στο δίκτυο.
- DLSettings: Αποτελείται από ένα πεδίο μεγέθους 1-byte που περιέχει τις ρυθμίσεις που μπορεί να κάνει η τελική συσκευή για ένα downlink message.
- RxDelay: Περιέχει τις καθυστερήσεις TX και RX.
- CFList: Αποτελεί μια λίστα με τις συχνότητες που μπορεί η τελική συσκευή να συνδεθεί. Αυτές η συχνότητες είναι χωρισμένες ανά περιοχή.

Βήμα 3ο

Ο Network Server στέλνει κρυπτογραφημένο αίτημα αποδοχής σύνδεσης στην τελική συσκευή με την μορφή ενός Downlink. Αυτό το μήνυμα περιλαμβάνει το AppNonce και ολοκληρώνει την διαδικασία του αιτήματος συμμετοχής.

Βήμα 4ο

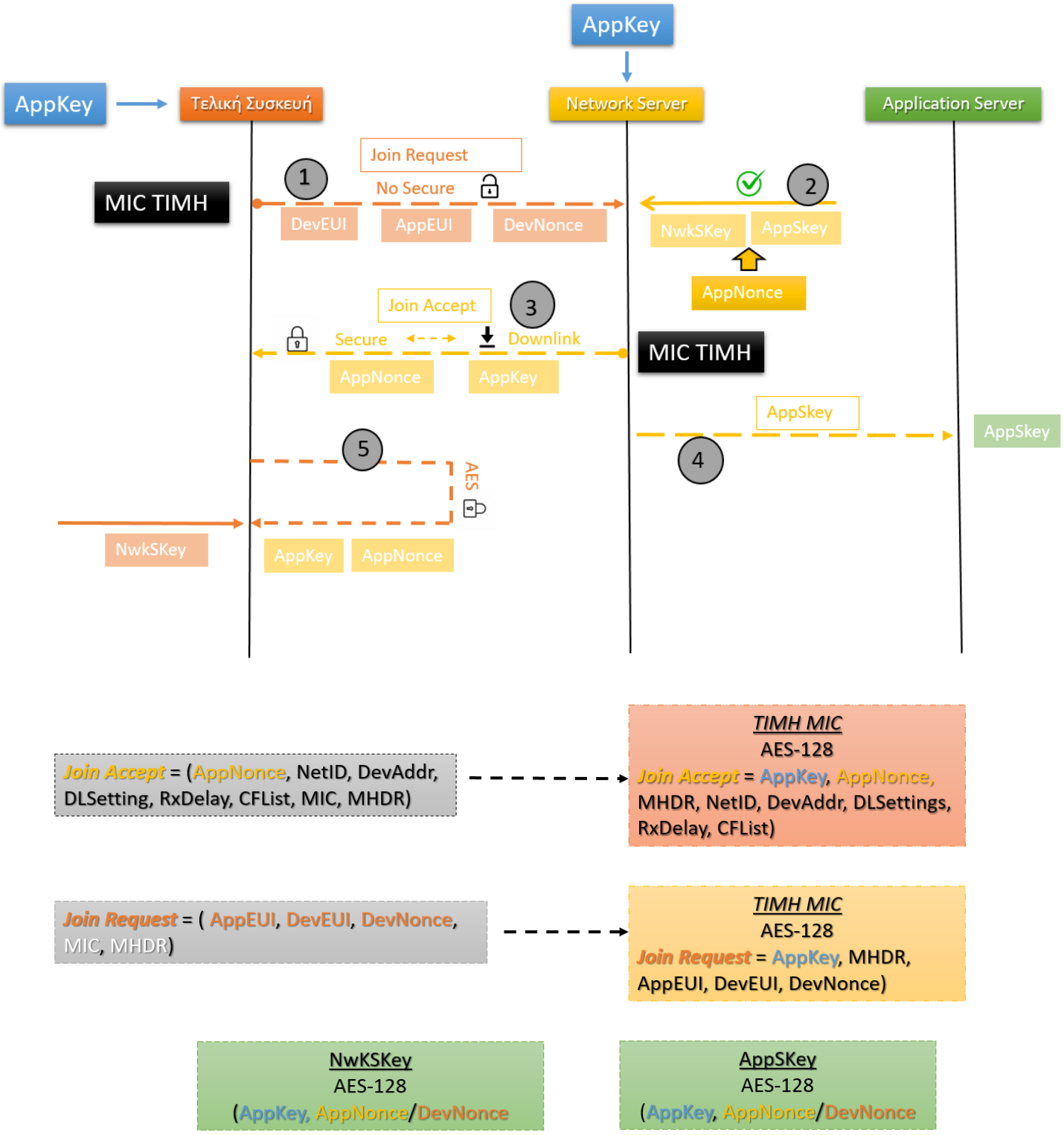
Ο Network Server κρατάει το NwkSKey κλειδί και προωθεί το AppSkey στον Application Server.

Βήμα 5ο

Η τελική συσκευή αποκρυπτογραφεί το Join-accept μήνυμα χρησιμοποιώντας την μέθοδο αποκρυπτογράφησης AES (Advanced Encryption Standard). Στη συνέχεια χρησιμοποιεί, τα κλειδιά AppKey και AppNonce για να αποκτήσει πρόσβαση στο Network Session Key (NwkSkey) και στο Application Session Key (AppSkey), αποκτώντας έτσι πρόσβαση στο δίκτυο.

Μετά, την ενεργοποίηση, η τελική συσκευή αποθηκεύει το :

- DevAddr : Είναι ένα 32-bit αναγνωριστικό που χρησιμοποιεί ο Network Server για να μπορεί να αναγνωρίζει την τελική συσκευή
- NwkSkey : Το κλειδί αυτό χρησιμοποιείται από την τελική συσκευή (End-Device) και το Network Server ώστε να γίνεται ο υπολογισμός και να ελέγχεται η αυθεντικότητα του MIC (Message Integrity Code). Τέλος, το κλειδί χρησιμοποιείται για να κρυπτογραφεί και να αποκρυπτογραφεί τα payload.
- AppSkey : Χρησιμοποιείται για να κρυπτογραφεί και να αποκρυπτογραφεί τα Application payload σε μηνύματα δεδομένων για την διασφάλιση του απορρήτου [6] .



Εικόνα 15 Αναλυτική περιγραφή βημάτων OTAA

2.7 *LoRaWAN Security*

Όταν μια συσκευή συνδέεται στο δίκτυο δημιουργείται ένα Application session key (AppSKey) και ένα Network Session key (NwKSKey). Το πρώτο (NwKSKey) είναι γνωστό στο δίκτυο, ενώ το δεύτερο (AppSKey) είναι κρυπτογραφημένο και παραμένει κρυφό μεταξύ του Application Server και της τελικής συσκευής. Και τα δύο αυτά, χρησιμοποιούνται για όσο διαρκέσει το Session. Επιπλέον, το LoRaWAN κάνει χρήση και ενός τρίτου κλειδιού, το οποίο παραμένει γνωστό μεταξύ της τελικής συσκευής και της εφαρμογής και ονομάζεται Application key (AppKey).

- **Application Session Key (AppSKey)**: Χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση του ωφέλιμου φορτίου (payload). Το ωφέλιμο φορτίο, είναι κρυπτογραφημένο μεταξύ της τελικής συσκευής (τελικού κόμβου) και του Application Server και επομένως με αυτό τον τρόπο διασφαλίζεται η ακεραιότητα του, καθώς ο χρήστης είναι ο μοναδικός που μπορεί να στείλει ή να λάβει μηνύματα. Το πρωτόκολλο LORAWAN για να διασφαλίσει την αξιοπιστία του βασίζεται στο AES (Advanced Encryption Standard) το οποίο είναι ένας μηχανισμός ασφάλειας, σύμφωνα με το οποίο παρέχετε σύνδεση και κρυπτογράφηση σε κάποια διαδικτυακά πακέτα. Αυτό επιτυγχάνεται με την χρησιμοποίηση κλειδιών (AppKey,AppNonce ή DevNonce) που είναι γνωστά μεταξύ των τελικών κόμβων, του Server και της διαδικτυακής εφαρμογής που βρίσκεται πίσω από τον Server.
- **Network Session Key (NwKSKey)**: Χρησιμοποιείται για την αλληλεπίδραση μεταξύ του κόμβου και του Server (Network Server). Αυτό το κλειδί χρησιμοποιείται για να διασφαλίσει την ακεραιότητα του μηνύματος μέσω του MIC Check (Message Integrity Code). Ο κωδικός ακεραιότητας μηνυμάτων (Message Integrity Code, MIC) εισάγεται για την διασφάλιση των δεδομένων κατά την μεταφορά. Πιο συγκεκριμένα, το MIC παράγεται από έναν αλγόριθμο που είναι γνωστό στον δέκτη και στον πομπό, ως αποτέλεσμα μια συσκευή που δεν είναι εξουσιοδοτημένη, δεν μπορεί να δημιουργήσει το MIC. Σε περίπτωση που ο δέκτης και ο πομπός συμφωνούν στον MIC κωδικό τότε θεωρούνται αυθεντικά από τον Server και προχωράνε στην ανταλλαγή των δεδομένων. Το NwkSKey περιλαμβάνει το AppKey, AppNonce ή το DevNonce.
- **Application key (AppKey)** είναι γνωστό μόνο από την συσκευή και την εφαρμογή. Όταν ενεργοποιείται μια συσκευή με την μέθοδο OTAA (Over-the-Air). [4]

Πρέπει να σημειωθεί ότι τα δύο κλειδιά AppSKey και NwKSKey είναι μοναδικά για κάθε συσκευή και για κάθε session. Με την χρήση της μεθόδου OTAA τα κλειδιά δημιουργούνται ξανά και ξανά για κάθε σύνδεση, ενώ αν επιλεγεί η σύνδεση με ABP τα κλειδιά παραμένουν σταθερά μέχρι να γίνει η αλλαγή από τον χρήστη.

2.8 *Προβλήματα Ασφαλείας στο LoRaWAN Δίκτυο*

Παρόλο που όλα τα δίκτυα και οι συσκευές LoRaWAN ακολουθούν τις προδιαγραφές που καθορίζονται από το LoRa Alliance και αναφέρονται ως ασφαλή, η ασφάλεια αυτών των δικτύων είναι αμφιλεγόμενη και έχουν εντοπιστεί αρκετά ανοιχτά ζητήματα. Για παράδειγμα, σύμφωνα με το πρωτόκολλο LoRaWAN όλα τα δίκτυα που λειτουργούν με την μέθοδο OTAA (Over-the-Air-Authentication) αντιμετωπίζουν σοβαρά ζητήματα ασφαλείας, στην διαδικασία σύνδεσης/συμμετοχής (Join Procedure/Join Request). Το πρόβλημα που αντιμετωπίζεται στο αίτημα συμμετοχής (Join Procedure/Join Request), είναι ότι το αίτημα μεταδίδεται σε μη κρυπτογραφημένη μορφή στο διαδίκτυο, κάνοντας τις συσκευές που χρησιμοποιούν τα LoRaWAN δίκτυα για μεγάλες αποστάσεις ευάλωτες σε επιθέσεις *man-in-the-middle (MITM)* και στην υποκλοπή των δεδομένων τους. Ένας κακόβουλος χρήστης (Attacker) μπορεί να παρέμβει στην επικοινωνία και να αντλήσει την τιμή MIC δηλαδή το AppKey με σκοπό να μιμηθεί την συσκευή και να υποκλέψει τα δεδομένα ή να καταρρεύσει το δίκτυο. Η τιμή MIC που μεταδίδεται μέσω δικτύων LoRaWAN δημιουργείται από τον αλγόριθμο AES-CMAC, ο οποίος χρησιμοποιεί το πρωτόκολλο κρυπτογράφησης AES-128 που αναφέραμε σε παραπάνω κεφάλαιο και χρειάζεται μεγάλη υπολογιστική δύναμη για να σπάσει. Ωστόσο, σύμφωνα με κάποιες ερευνητικές εργασίες υπάρχουν διάφορες τεχνικές και αλγόριθμοι που μπορούν να μειώσουν ραγδαία τον απαιτούμενο χρόνο για την αποκρυπτογράφηση του AES-128 [22]. Τέλος, το AppKey όπως αναφέρθηκε σε προηγούμενο κεφάλαιο, μετά το αίτημα σύνδεσης (Join Request) και την επιτυχή σύζευξη της συσκευής με το δίκτυο, παραμένει σταθερό για το υπόλοιπο της λειτουργίας της συσκευής καθώς παράγεται μόνο μια φορά. Συνοψίζοντας, όλα τα παραπάνω δημιουργούν μια συνθήκη όχι και τόσο ασφαλή για τα δίκτυα LoRaWAN, κάνοντας το ευάλωτο σε επιθέσεις *man-in-the-middle (MITM)*. Κάτι το οποίο μπορεί να αποφευχθεί μοιραίο για την ακεραιότητα του δικτύου και των δεδομένων του.

Συμπερασματικά, η ασφάλεια του LoRaWAN χαρακτηρίζεται ως υψηλού επιπέδου, αφού η παραβίασή του έγκειται συνήθως μόνο σε δύο περιπτώσεις:

- ο κακόβουλος χρήστης να έχει αποκρυπτογραφήσει το MIC (AES-128), μέσω του οποίου θα υποκλέψει το AppKey. Αναλυτικότερα, στην περίπτωση που θα αποκρυπτογραφήσει την τιμή MIC μέσω αντίστροφης μηχανικής (Reverse Engineering) στο Join Request μήνυμα της τελικής συσκευής προς το Network Server, θα μπορέσει να "ακούσει" τις τιμές AppKey, MHDR, AppEUI, DevEUI και DevNonce. Στην περίπτωση που αποκρυπτογραφήσει, την τιμή MIC στο Join Accept μήνυμα του Network Server προς την τελική συσκευή θα "ακούσει" τις τιμές AppKey, AppNonce, MHDR, NetID, DevAddr, DLSettings, RXDelay, CFList).
- ο κακόβουλος χρήστης να έχει πρόσβαση στο λογισμό (Software) και υλισμικό (Hardware) μιας πιστοποιημένης τελικής συσκευής του δικτύου, αποκτώντας πρόσβαση στον αλγόριθμο της τελικής συσκευής, μπορεί να μάθει την ακριβή λειτουργία του και το πως μπορεί να διεισδύσει στο δίκτυο.

Τυπικά σενάρια των παραπάνω δύο περιπτώσεων αναφέρονται συχνά ως επιθέσεις *man-in-the-middle-attack (MITM),* στα οποία ο κακόβουλος χρήστης – αφού υποκλέψει τα κλειδιά σύνδεσης

και πιστοποίησης – μεταδίδει εσφαλμένα δεδομένα σε ολόκληρο το δίκτυο LoRaWAN, είτε στοχεύοντας συγκεκριμένες συσκευές είτε τα λειτουργικά στοιχεία του δικτύου (π.χ. Servers) μέσω Replay Attacks. Σε τέτοια σενάρια, ο κακόβουλος χρήστης δρα ως ο αρχικός αποστολέας, και προσπαθεί με μη εξουσιοδοτημένη πρόσβαση να στείλει μηνύματα επικοινωνίας στον τελικό προορισμό (π.χ. σε έναν άλλο χρήστη ή Server). Ο τελικός προορισμός εσφαλμένα πιστεύει ότι τα αποσταλμένα μηνύματα προέρχονται από ένα πιστοποιημένο end-device, και αλληλοεπιδρά μαζί του. Ως αποτέλεσμα, ο κακόβουλος χρήστης αποκτά πρόσβαση σε ευαίσθητα/απόρρητα δεδομένα μέσω της απάντησης του δέκτη (τελικού προορισμού) ή εντοπίζει κάποιο άτρωτο μέρος του συστήματος, μέσω του οποίου κατευθύνει τις επιθέσεις του στο υπόλοιπο δίκτυο.

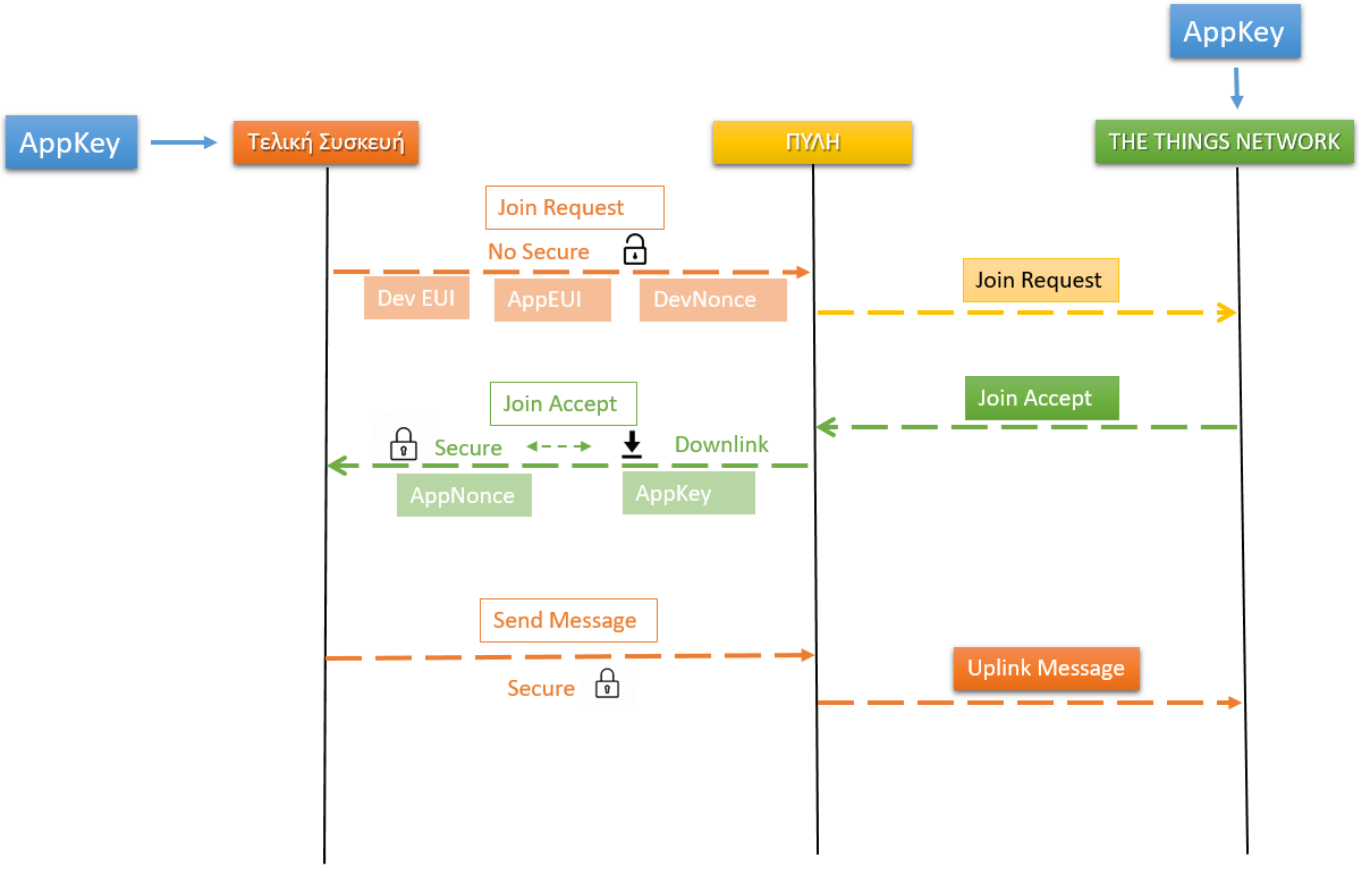
Για την διασφάλιση της ακεραιότητας της μεθόδου ασφαλείας του συστήματος, επιλέχθηκαν 6 σενάρια λειτουργίας με σκοπό την επισήμανση του προβλήματος ενάντια σε *man-in-the-middle επιθέσεις* και κατόπιν την επίλυσή του. Όπως αναφέρθηκε παραπάνω, ο αριθμός των σεναρίων ανέρχεται στα έξι. Κάθε σενάριο χωρίζεται σε ζεύγη. Σκοπός της ομαδοποίησης των σεναρίων είναι η λειτουργία ενός LoRaWAN συστήματος σύμφωνα με τους όρους που ορίζει το κάθε σενάριο και ακολούθως η συμπεριφορά του σε περίπτωση *man-in-the-middle (MITM)* επιθέσεις. Στο 1ο σενάριο, θα εξεταστεί αρχικά η λειτουργία ενός πρότυπου συστήματος LoRaWAN όπως αυτό ορίζεται από το LoRa Alliance και στην συνέχεια θα παρατηρηθεί η συμπεριφορά του σε man-in-the-middle επίθεση. Στην συνεχεία, στο 2ο σενάριο θα εισαχθεί ένα σύστημα που θα λειτουργεί με την μέθοδο του Rejoin όπου η τελική συσκευή θα επαναλαμβάνει την διαδικασία του αιτήματος σύνδεσης/συμμετοχής (Join Procedure), κάθε φορά που θα στέλνει δεδομένα. Ύστερα, θα εξεταστεί η λειτουργία αυτού του συστήματος απέναντι σε *man-in-the-middle (MITM)* επιθέσεις όπου α) ο Attacker θα λειτουργεί με βάση το πρότυπο του 1ο σεναρίου και β) ο Attacker θα λειτουργεί με την μέθοδο του Rejoin. Τέλος, στο 3ο σενάριο α) θα παρατηρηθεί η λειτουργία ενός LoRaWAN συστήματος με την χρήση των κυλιόμενων κλειδιών (ψευδοτυχαίων) και β) η συμπεριφορά του ενάντια σε man-in-the-middle επίθεση.

Εικόνα 16 Security Issue[13]

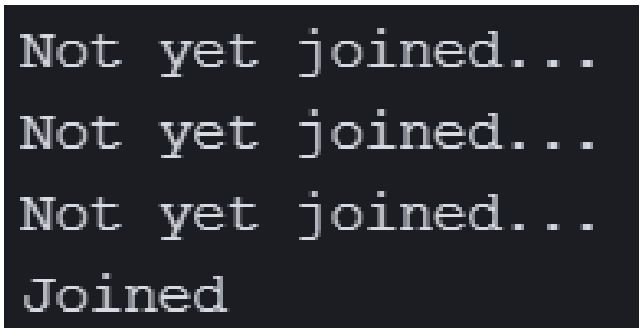
[13]https://www.malwarebytes.com/blog/news/2018/07/when-three-isnt-a-crowd-man-in-the-middle-mitm-attacks-explained

2.9 *Σενάριο 1ο*

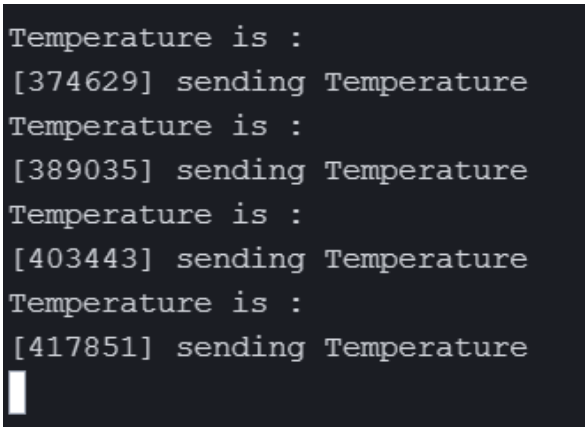
Στο Σενάριο αυτό θα προβληθεί ένα πρωτότυπο σύστημα LoRaWAN, το οποίο λειτουργεί με την μέθοδο OTAA σύμφωνα με το πρωτόκολλο επικοινωνίας 1.0.1. του LoRaWAN. Σε αυτό το σενάριο θα παρατηρήσουμε ένα σύστημα το οποίο μετά την ανταλλαγή των απαραίτητων κλειδιών (AppEUI, DevEUI, AppKey, DevNonce) αποκτά πρόσβαση στο δίκτυο με σκοπό την μέτρηση της υγρασίας και την θερμοκρασίας του περιβάλλοντα χώρου. Μόλις πραγματοποιηθεί η αποστολή των δεδομένων, η τελική συσκευή εισέρχεται σε κατάσταση αδράνειας και η διαδικασία αποστολής των δεδομένων επαναλαμβάνεται ξανά περίπου κάθε τέσσερις ώρες.



Εικόνα 17 Λειτουργία Συστήματος Σεναρίου 1ου



Εικόνα 18 Επιτυχής σύνδεση στο δίκτυο από την τελική συσκευή



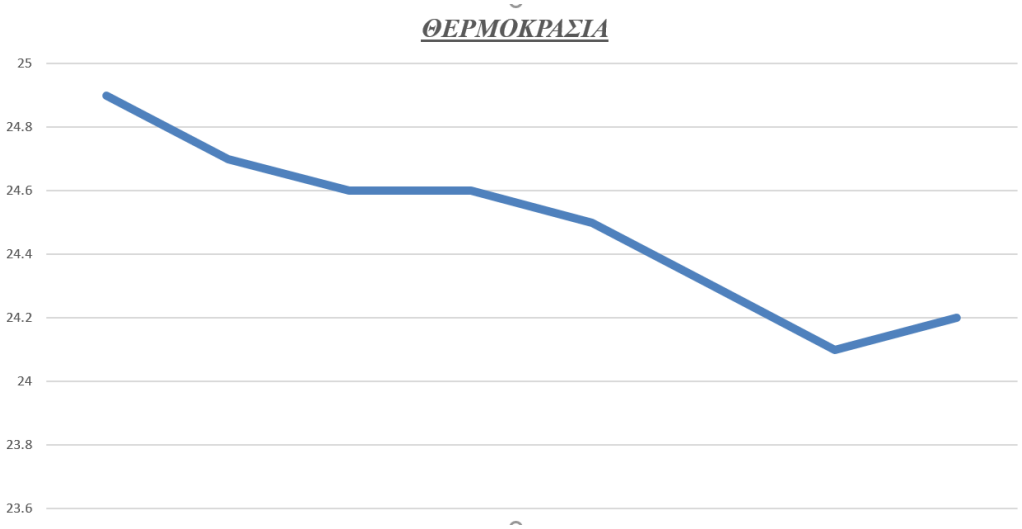
Εικόνα 19 Αποστολή δεδομένων από την τελική συσκευή

↑	10:52:25	same-eui	Forward uplink data message
↑	06:52:17	same-eui	Forward uplink data message
↑	02:52:10	same-eui	Forward uplink data message
↑	22:52:02	same-eui	Forward uplink data message
↑	18:51:54	same-eui	Forward uplink data message
↑	14:51:46	same-eui	Forward uplink data message
↑	10:51:37	same-eui	Forward uplink data message
↑	06:51:29	same-eui	Forward uplink data message
↑	02:51:21	same-eui	Forward uplink data message
↑	22:51:15	same-eui	Forward uplink data message
↑	18:51:06	same-eui	Forward uplink data message
↑	14:50:58	same-eui	Forward uplink data message
↑	10:50:50	same-eui	Forward uplink data message
↑	06:50:42	same-eui	Forward uplink data message

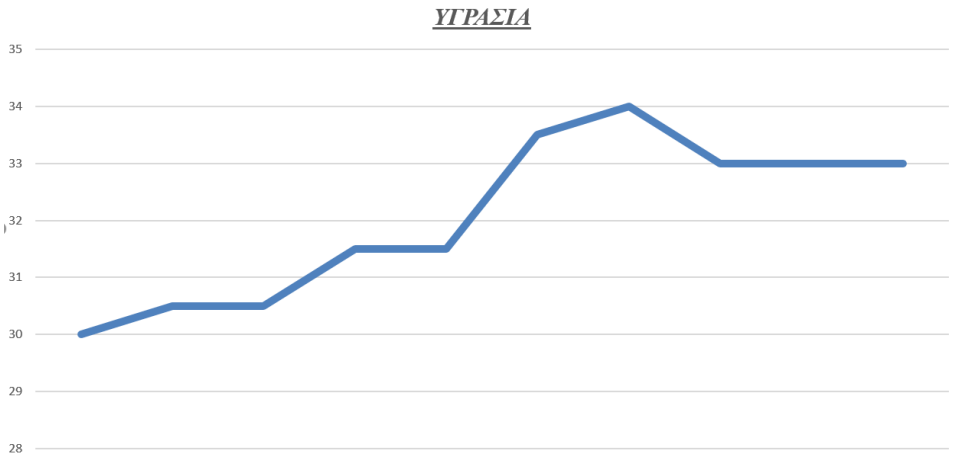
Εικόνα 20 Εμφάνιση δεδομένων στο TT

Παρατηρήσεις

Όπως παρατηρούμε στο 1ο σενάριο, η τελική μας συσκευή λειτουργεί σύμφωνα με το πρότυπο που ορίζει το LoRaWAN για την σύνδεση με την μέθοδο OTAA, ανταλλάζοντας τα απαραίτητα κλειδιά που έχουν αναφερθεί στο υποκεφάλαιο 2.6. Αφού γίνει η αποδοχή του αιτήματος ζεύξης (Join Accept) από τον Network Server, η τελική συσκευή ξεκινάει την επικοινωνία, αποστέλλοντας τα δεδομένα της θερμοκρασίας και της υγρασίας κάθε τέσσερις ώρες όπως φαίνεται και στις εικόνες 19 και 20. Η τιμή της θερμοκρασίας ανέρχεται περίπου στους 24ºC, ενώ η τιμή της υγρασίας βρίσκεται περίπου στο 30-34%.



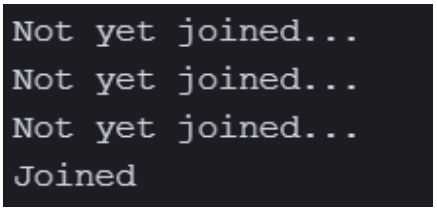
Εικόνα 21 Μέτρηση θερμοκρασίας χρήστη



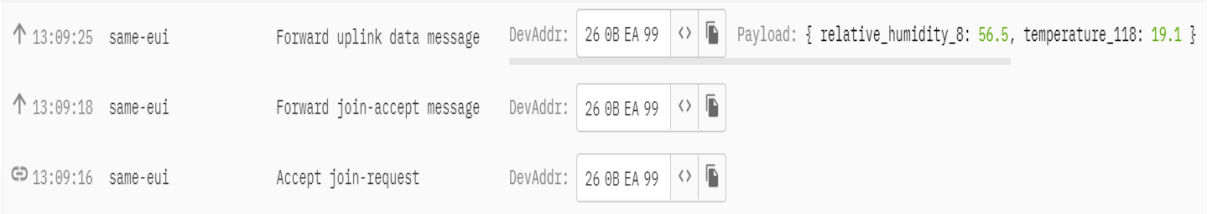
Εικόνα 22 Μέτρηση υγρασίας χρήστη

Εισαγωγή Attacker

Η δεύτερη φάση του σεναρίου πραγματοποιείται με την εισαγωγή του κακόβουλου χρήστη (Attacker), έχοντας την συμπεριφορά λειτουργείας του "υγιούς" χρήστη στο 1ο σενάριο. Ο κακόβουλος χρήστης, όπως φαίνεται και στην εικόνα 25 αποστέλλει δεδομένα περίπου κάθε 1 λεπτό. Σκοπός αυτής της εισαγωγής, είναι η παρατήρηση της ακεραιότητας του συστήματος, όταν πραγματοποιείται μια επίθεση *Man-In-The-Middle*.



Εικόνα 23 Σύνδεση Attacker



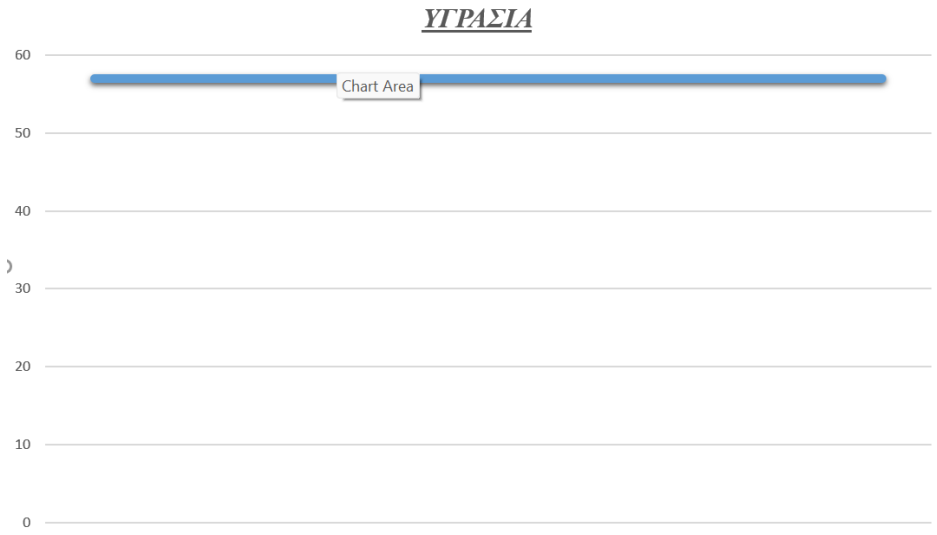
Εικόνα 24 Εμφάνιση σύνδεσης Attacker στο TTN

Εικόνα 25 Εμφάνιση δεδομένων που στάλθηκαν από Attacker

Παρατηρήσεις Σεναρίου 1 - Attacker

Όπως γίνεται αντιληπτό, ο Attacker πραγματοποιεί επιτυχώς την MITM επίθεση, καθώς καταφέρνει να υποκλέψει το Appkey και να αποκτήσει πρόσβαση στο δίκτυο μας, παριστάνοντας την "υγιή" συσκευή έχοντας τα ίδια ακριβώς στοιχεία (Όνομα, DevEUI,AppEUI,AppKey). Η συμπεριφορά του όμως είναι διαφορετική σε σχέση με του "καλού" χρήστη, καθώς αποστέλλει δεδομένα κάθε 1 λεπτό με την θερμοκρασία και την υγρασία σύμφωνα με τις εικόνες 25,26,27 να κυμαίνονται περίπου στους 19ºC και στο 57%.

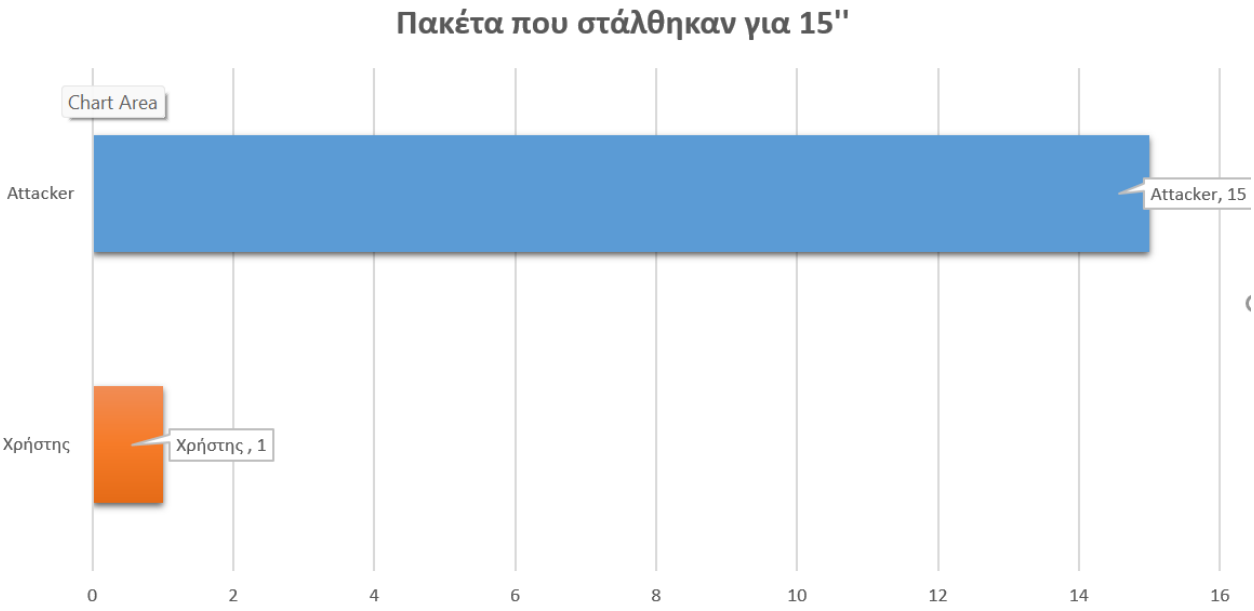
Εικόνα 26 Θερμοκρασία Attacker



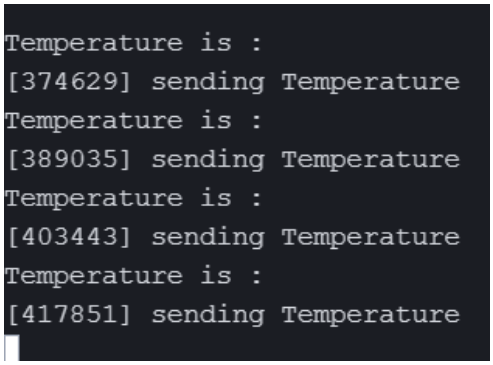
Εικόνα 27 Υγρασία Attacker

2.10 *Αποτελέσματα – Παρατηρήσεις Σεναρίου 1ου*

Όπως παρατηρούμε (βλέπε εικόνα 24), μόλις γίνει η επιτυχής αποδοχή του αιτήματος σύνδεσης/συμμετοχής (Join Procedure) από την πλατφόρμα The Things Network (Network Server), η επίθεση *Man-In-The-Middle* έχει πραγματοποιηθεί επιτυχώς. Ως αποτέλεσμα, ο κακόβουλος χρήστης έχει αποκτήσει πλήρως πρόσβαση στο δίκτυο μας και η συχνότητα των μηνυμάτων που αποστέλλονται είναι αρκετά ταχύτερη (1 λεπτό) (βλέπε εικόνα 25) σε σχέση με αυτή που έχουμε αρχικά ορίσει για τον "υγιή" χρήστη (4 ωρές), θέτοντας σε κίνδυνο την ομαλή λειτουργία του δικτύου μας και την πιθανή κατάρρευση του. Ακόμα, ο κακόβουλός χρήστης στέλνει διαφορετικές τιμές δεδομένων σε σχέση με αυτές του "υγιούς" χρήστη δημιουργώντας ψευδαίσθηση για την αληθινή συνθήκη που επικρατεί στο σύστημα μας, κάτι που μπορεί να ωθήσει τον "υγιή" χρήστη να προβεί σε λάθος αποφάσεις. Τέλος, η "υγιής" τελική συσκευή σύμφωνα με την εικόνα 29 συνεχίζει να αποστέλλει δεδομένα τα οποία όμως απορρίπτονται από τον Network Server, καθιστώντας αδύνατη την ενημέρωση του χρήστη για τις αληθινές συνθήκες που επικρατούν στο σύστημα του, για αυτό και ο αριθμός των πακέτων που έχει λάβει το δίκτυο μας (οριζόντιος άξονας) μετά την εισαγωγή του κακόβουλου χρήστη ανέρχεται στα 15 πακέτα για τον Attacker και στο μόλις 1 πακέτο για τον "υγιή" χρήστη. Συνοψίζοντας, η επίθεση MITM έχει στεφθεί επιτυχώς, εμφανίζοντας τα προβλήματα ακεραιότητας του πρωτοκόλλου LoRaWAN όπως αυτά αναφέρθηκαν σε προηγούμενα υποκεφάλαια.



Εικόνα 28 Αποστολή Δεδομένων από χρήστη (PyCom)

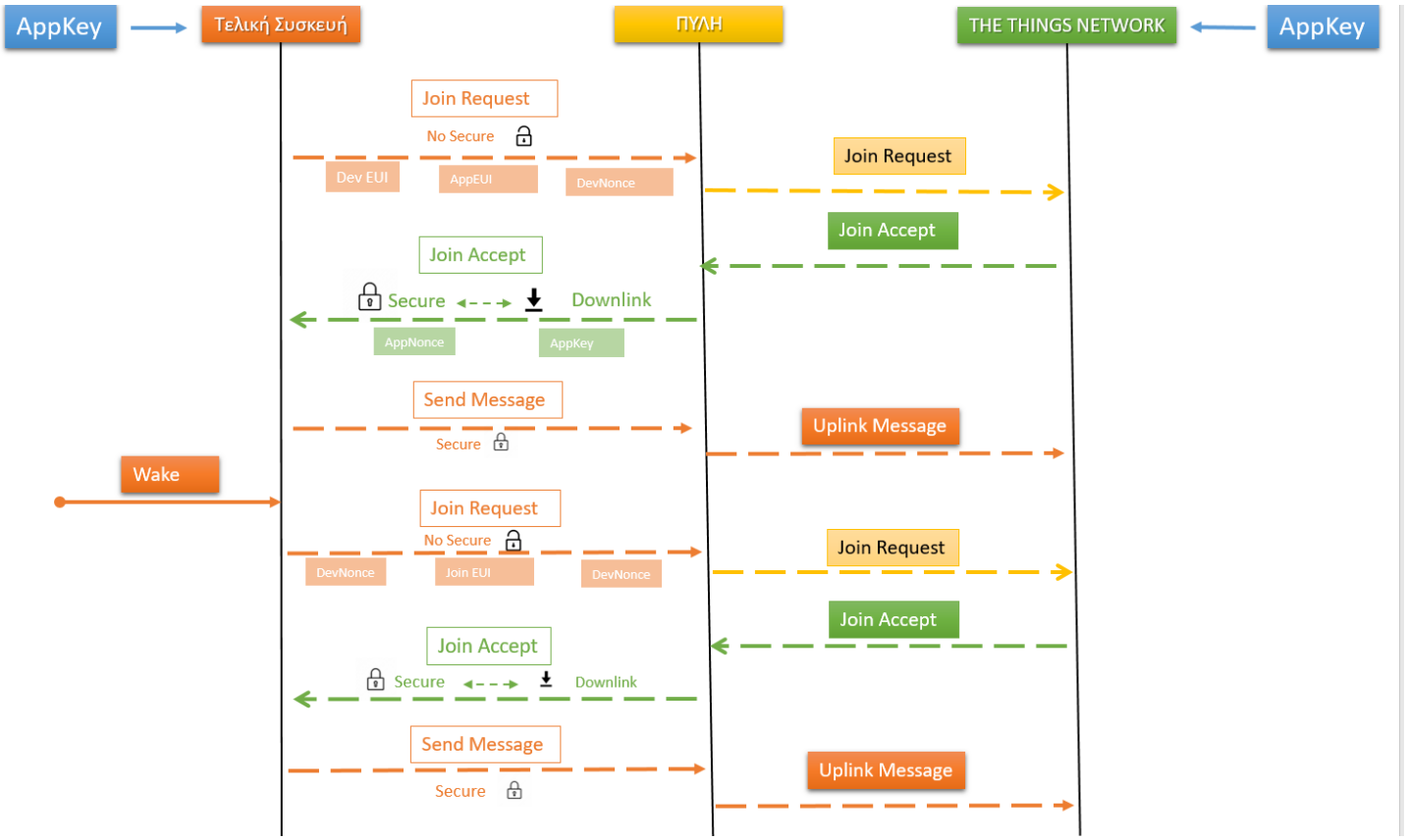


Εικόνα 29 Αποστολή Δεδομένων από χρήστη (PyCom)

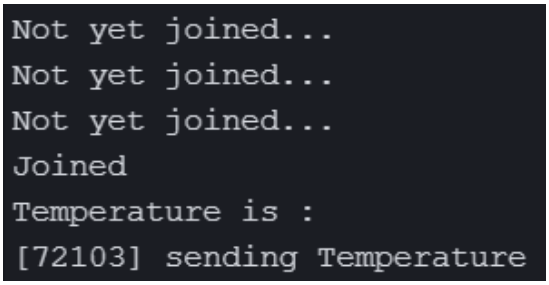
2.11 *Σενάριο 2ο*

Στο Σενάριο αυτό προβάλλεται ένα πιο ασφαλές σύστημα LoRaWAN, καθώς εισάγεται στην λειτουργία της τελικής συσκευής η εντολή Rejoin. Δηλαδή, για να μπορεί η τελική συσκευή να αποστείλει τα δεδομένα, θα πρέπει να πραγματοποιηθεί εκ νέου ο έλεγχος ταυτοτήτων (Join Procedure). Όταν ταυτοποιηθεί η συσκευή ως αυθεντική (Join Accept), πραγματοποιείται η αποστολή των δεδομένων. Έπειτα, η τελική συσκευή εισέρχεται σε κατάσταση αδράνειας, και ολόκληρη η διαδικασία θα επαναληφθεί ξανά μετά από 4 ώρες. Αυτή η τεχνική, χαρακτηρίζεται ως πιο ασφαλής διότι το δίκτυο LoRaWAN και πιο συγκεκριμένα ο Network Server, δέχεται δεδομένα μόνο από τον τελευταίο χρήστη που έχει πραγματοποιήσει επιτυχώς την διαδικασία ταυτοποίησης (Join Procedure).

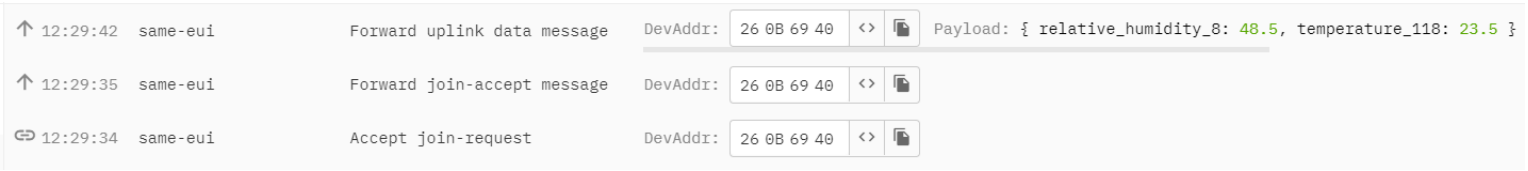
Επομένως με την διαδικασία του Rejoin, θα προσπαθήσουμε να εξαλείψουμε το πρόβλημα που αντιμετωπίσαμε στο 1ο σενάριο, όπου μετά την επιτυχή εισαγωγή του Attacker στο δίκτυο, ο "υγιής" χρήστης έστελνε δεδομένα χωρίς να τελικό αποδέκτη.



Εικόνα 30 Λειτουργία Συστήματος Σεναρίου 2ου



Εικόνα 31 Σύνδεση Τελικής Συσκευής

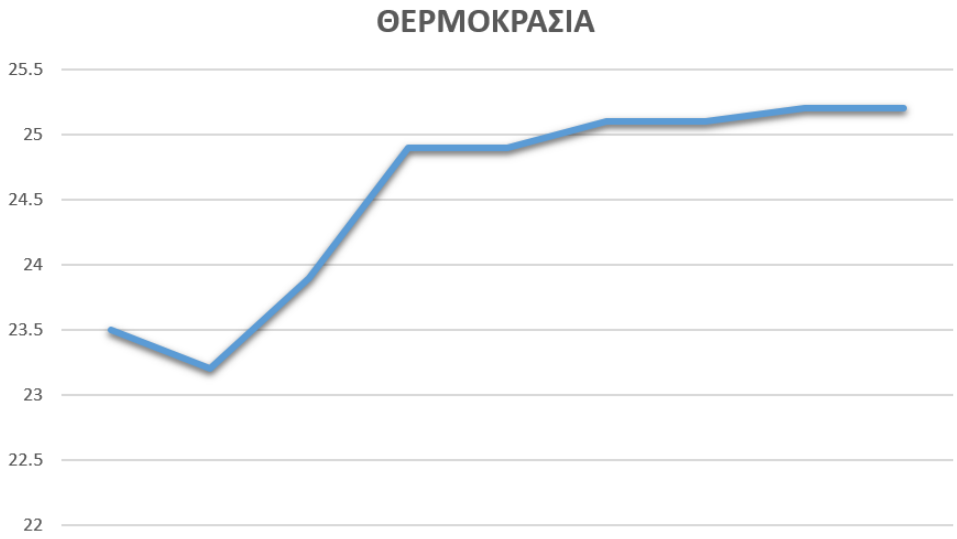


Εικόνα 32 Σύνδεση μέσα από την πλατφόρμα TTN

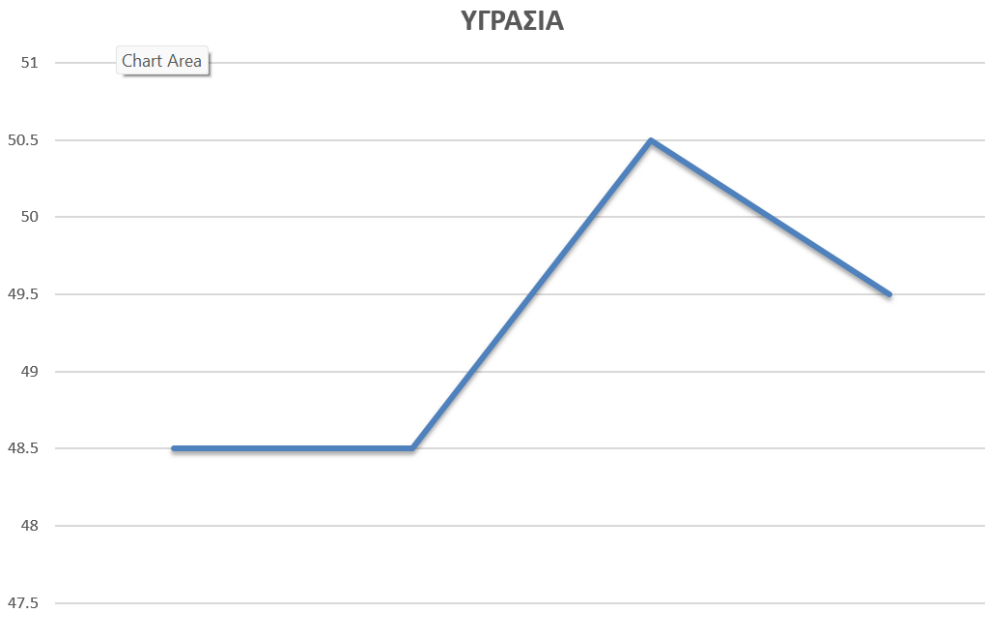
Εικόνα 33 TTN Rejoin και Αποστολή Δεδομένων

Παρατηρήσεις Σεναρίου 2

Όπως παρατηρούμε στο 2ο σενάριο, η τελική μας συσκευή συνδέεται με την μέθοδο OTAA ανταλλάζοντας τα απαραίτητα κλειδιά που έχουν αναφερθεί στο υποκεφάλαιο 2.6. Αφού γίνει η αποδοχή του αιτήματος ζεύξης (Join Accept), η τελική συσκευή ξεκινάει την επικοινωνία αποστέλλοντας τα δεδομένα της θερμοκρασίας και της υγρασίας. Στην συνέχεια μπαίνει σε κατάσταση αδράνειας και όπως φαίνεται και στην εικόνα 33, μετά από 4 ώρες ξεκινάει εκ νέου την διαδικασία για την ανταλλαγή των απαραίτητων κλειδιών, ώστε να γίνει η αποδοχή της από το δίκτυο. Η τιμή της θερμοκρασίας ανέρχεται περίπου στους 23.5 ºC με 25 ºC, ενώ η τιμή της υγρασίας βρίσκεται περίπου 48% με 50%.



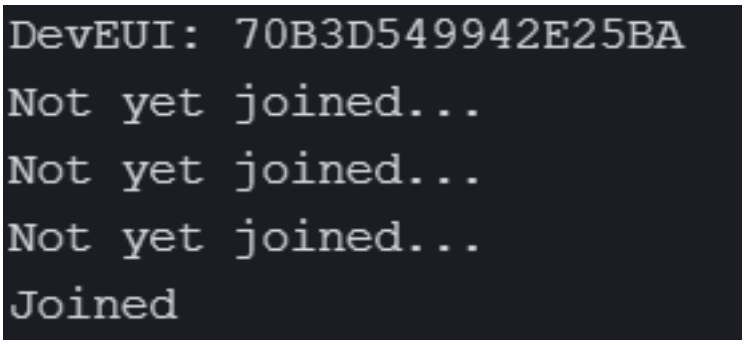
Εικόνα 34 Θερμοκρασία Χρήστη



Εικόνα 35 Υγρασία Χρήστη

Εισαγωγή Attacker

Η δεύτερη φάση του σεναρίου, πραγματοποιείται με την εισαγωγή του κακόβουλου χρήστη έχοντας την συμπεριφορά του αρχικού συστήματος, με σκοπό την παρατήρησή του έναντι κακόβουλής επίθεσης. Ο κακόβουλος χρήστης παραβιάζει το δίκτυο μας, έχοντας την ίδια συμπεριφορά με το σενάριο 1ο και αποστέλλει δεδομένα κάθε 1 λεπτό.



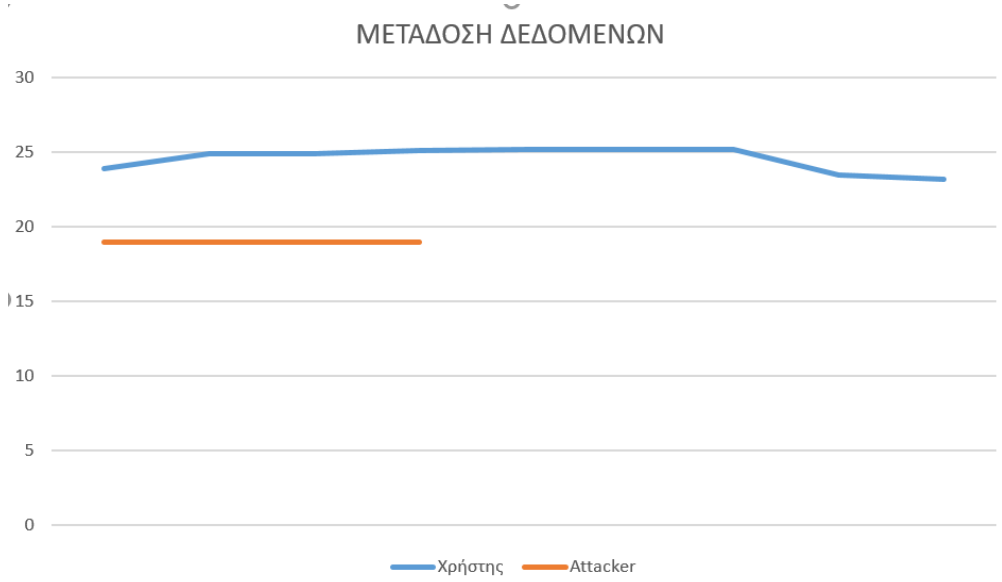
Εικόνα 36 Σύνδεση Attacker

Εικόνα 37 Αποστολή Δεδομένων Attacker

2.12 *Αποτελέσματα – Παρατηρήσεις Σεναρίου 2ου*

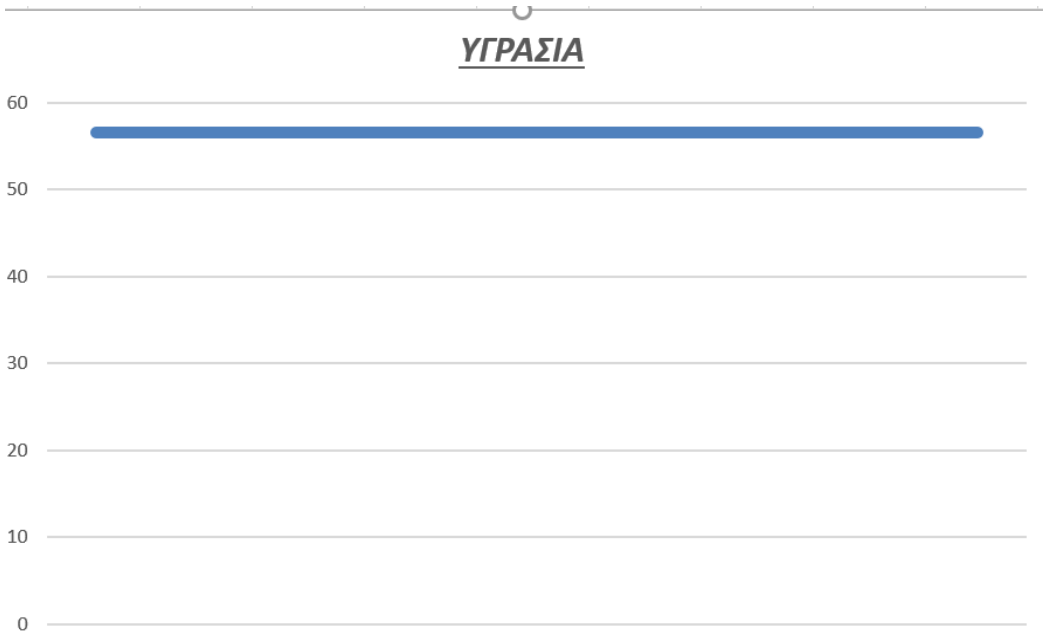
Σύμφωνα με την εικόνα 37, παρατηρούμε ότι ο Attacker ο οποίος έχει συνδεθεί στο δίκτυο μας, λειτουργώντας σύμφωνα με το πρότυπο του σεναρίου 1ο, στέλνει πακέτα δεδομένων με διαφορά 1 λεπτού, που αντικατοπτρίζονται σε θερμοκρασία 19 βαθμών κελσίου και υγρασία στο 57%. Ξαφνικά, διακόπτεται από τον "υγιή" χρήστη ο οποίος λειτουργεί με την μέθοδο του Rejoin που αναλύθηκε παραπάνω. Μελετώντας την εικόνα 37 και 38, αντιλαμβανόμαστε ότι ο "υγιής" χρήστης διακόπτει την αποστολή πακέτων από τον Attacker, πραγματοποιώντας την σύνδεση Rejoin. Αυτό συμβαίνει, διότι το δίκτυο μας, δέχεται δεδομένα από την συσκευή που έχει πραγματοποιήσει τελευταία την μέθοδο του Join Procedure.

Ως αποτέλεσμα, αποδεικνύεται ότι η μέθοδος Rejoin καταπολέμα τις επιθέσεις *Man-In-The Middle*, όταν ο επιτιθέμενος (Attacker) έχει την συμπεριφορά του 1ου σεναρίου.



Εικόνα 38 Λειτουργία Rejoin Χρήστη

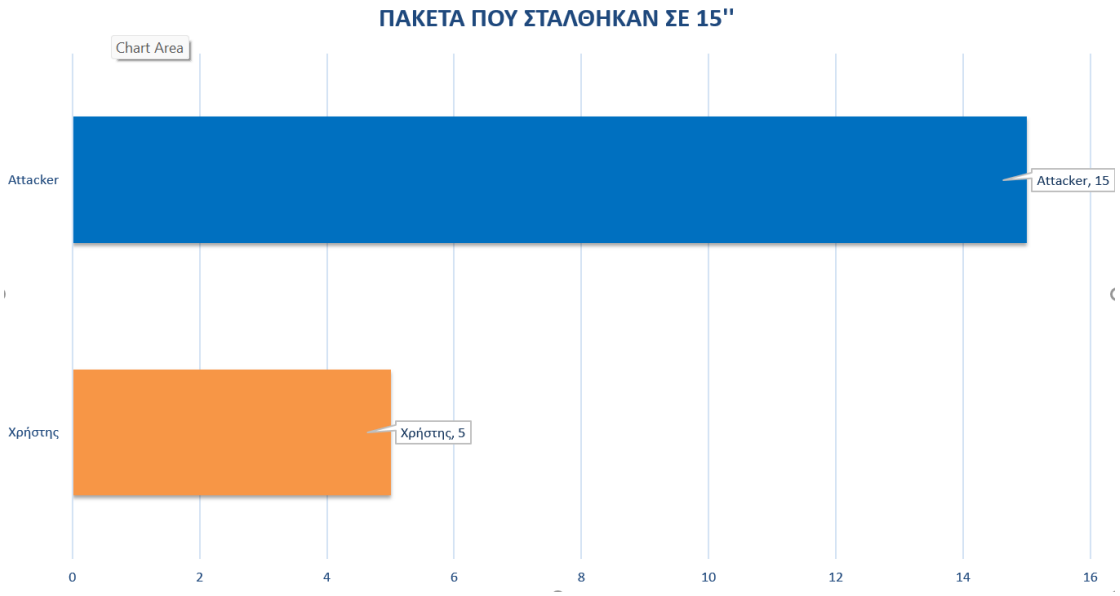
Εικόνα 39 Θερμοκρασία Attacker



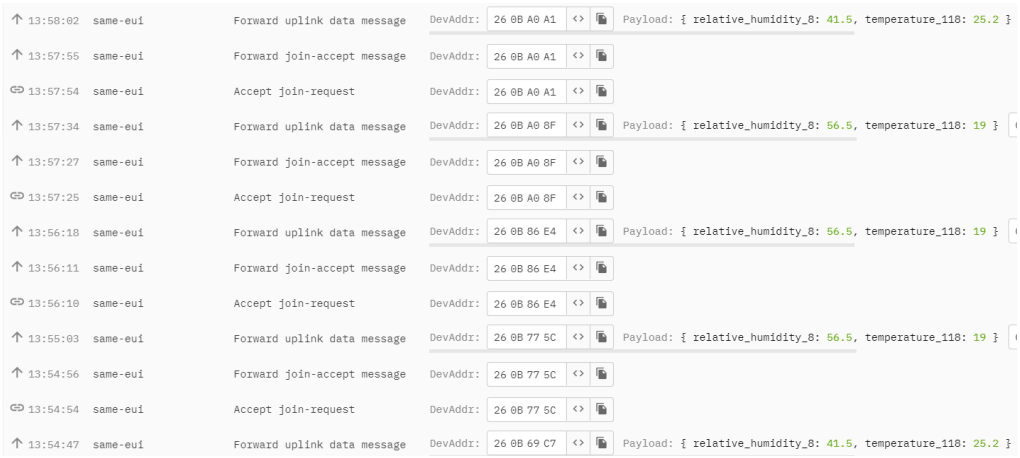
Εικόνα 40 Υγρασία Attacker

MITM επίθεση με την λειτουργία του Rejoin

Σύμφωνα με την εικόνα 42, μελετάμε το σενάριο όπου και οι δύο χρήστες (καλός, Attacker) λειτουργούν με το πρότυπο του Rejoin. Δηλαδή, και οι δύο χρήστες κάθε φορά που ενεργοποιούνται με σκοπό την αποστολή των δεδομένων τους, επαναλαμβάνουν την διαδικασία της αίτησης συμμέτοχης (Join Procedure). Οι χρόνοι αποστολής των πακέτων ορίζονται στα 3 λεπτά για τον "καλό" χρήστη και στο 1 λεπτό για τον Attacker. Τα αποτελέσματα που μας δίνονται μετά την διεξαγωγή του πειράματος και σε συνδυασμό με την εικόνα 41, όπου στον οριζόντιο άξονα παρουσιάζεται ο αριθμός των πακέτων/δεδομένων που έφτασαν στο δίκτυο, και σε αντίθεση με ότι υποδείξαμε στο σχολιασμό της εικόνας 38, παρατηρείται ότι η λειτουργία Rejoin δεν είναι το ίδιο αποτελεσματική, όταν ο Attacker λειτουργεί και αυτός με το πρότυπο του Rejoin. Καθώς και οι δύο χρήστες (Υγιής,Attacker) συνεχίζουν και αποστέλλουν τα δεδομένα τους κανονικά αφού έχουν πραγματοποιήσει επιτυχώς την διαδικασία ταυτοποίησης τους, έχοντας πρόσβαση στο δίκτυο σε διαφορετικά χρονικά διαστήματα. Το πρόβλημα που δημιουργείται είναι ότι ο Attacker αποστέλλει περισσότερα πακέτα/δεδομένα σε σχέση με τον "υγιή" χρήστη, κάτι που οφείλεται στο γεγονός ότι ο χρόνος επανεκκίνησης του μικροελεκτή του είναι ταχύτερος (1 λεπτό) από αυτόν του "υγιή" (3 λεπτά). Καταλήγοντας στο συμπέρασμα ότι, η επίθεση *Man-In-The-Middle* έχει στεφθεί επιτυχώς, θέτοντας σε κίνδυνο την ορθή λειτουργία του δικτύου μας.



Εικόνα 41 Σύγκριση πακέτων με λειτουργία Rejoin και από τις δυο τελικές συσκευές



Εικόνα 42 Αποστολή Δεδομένων Attacker Rejoin

3. ΚΕΦΑΛΑΙΟ 3

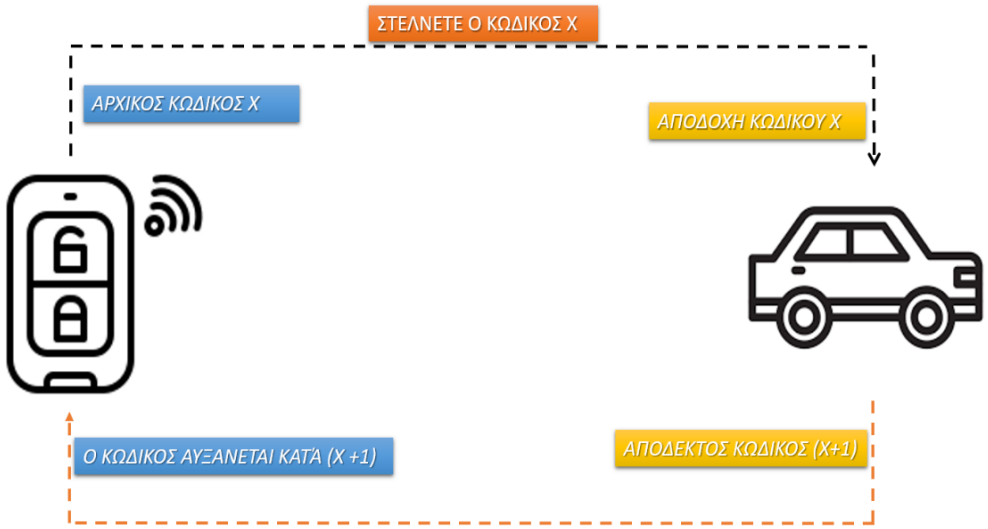
Η παρούσα διπλωματική εργασία, παρουσιάζει μια καινοτόμα τεχνική ασφαλείας, η οποία αυξάνει την αξιοπιστία και ακεραιότητα των IoT δεδομένων όταν αυτά μεταδίδονται μέσα από ασύρματα δίκτυα LoRaWAN, σύμφωνα με την διαδικασία ελέγχου συμμετοχής/ταυτότητας (Join Procedure) που περιγράφεται στο πρωτόκολλο επικοινωνίας 1.0.1 του LoRaWAN. Η εφαρμογή μας, λειτουργεί σύμφωνα με το πρότυπο σύνδεσης OTAA (Over The Air Authentication) που περιγράφεται στο υποκεφάλαιο 2.5. Η τεχνική που ακολουθείται για την ενίσχυση της ασφάλειας του συστήματος βασίζεται στην τεχνική των κυλιόμενων κλειδιών (Rolling Key) που χρησιμοποιείται στα συστήματα κλειδώματος των αυτοκινήτων και παρουσιάζεται στο υποκεφάλαιο 3.2. Μέσω της χρήσης των κυλιόμενων κλειδιών, το στατικό AppKey μετατρέπεται σε κυλιόμενο και σε συνδυασμό με την κρυπτογράφηση AES-128 της τιμής MIC καθίσταται εξαιρετικά δύσκολο για τους "κακόβουλους" χρήστες (Attacker) να παραβιάσουν και να υποκλέψουν δεδομένα του συστήματος. Αυτό οφείλεται στο γεγονός πως η κρυπτογράφηση του AES-128 απαιτεί μεγάλη υπολογιστική δύναμη και αρκετό χρόνο για να αποκρυπτογραφηθεί**,** πριν προλάβει να αλλάξει το AppKey κλειδί. Η προτεινόμενη τεχνική δοκιμάστηκε σε πραγματικό περιβάλλον, με σενάριο πραγματικών μικροελεγκτών (Pycom Fipy). Ο αριθμός των μικροελεκτών ανέρχεται στους δύο. Ο ένας δρα ως μικροελεκτής του "υγειούς" χρήστη και ο άλλος ως μικροελεκτής του "κακόβουλού" χρήστη, ώστε να μπορέσει να πραγματοποιηθεί μια συνθήκη επίθεσης βάση ρεαλιστικών γεγονότων. Τον ρόλο της πύλης (Gateway) του συστήματός μας κατέχει το Lorix One και το επιλεγμένο application που λειτουργεί και ως Network Server του δικτύου LoRaWAN είναι το The Things Network (TTN).

Τα αποτελέσματα των δοκιμών έδειξαν ότι αυτή η πρωτότυπη τεχνική βελτιώνει την ασφάλεια των δικτύων LoRaWAN και εμποδίζει τους κακόβουλους χρήστες, να εισέρχονται στο δίκτυο και να θέτουν σε κίνδυνο κρίσιμες υποδομές.

3.1 *Πιθανή Προσέγγιση για Επαυξημένη Ασφάλεια στο LoRaWAN*

Προκειμένου να μετριάσουμε ή ακόμα και να εξαλείψουμε τις πιθανότητες παραβίασης του δικτύου σε μια από τις παραπάνω περιπτώσεις MITM, προτείνεται η χρήση κλειδιών και κωδικών σύνδεσης/πρόσβασης που θα ανανεώνονται σε τακτά χρονικά διαστήματα, και τα οποία θα δημιουργούνται από κάποιον αλγοριθμικό μηχανισμό, ο οποίος δεν θα είναι προσβάσιμος από τις τελικές συσκευές αλλά και από τις μονάδες του δικτύου LoRaWAN (π.χ. Network Servers).

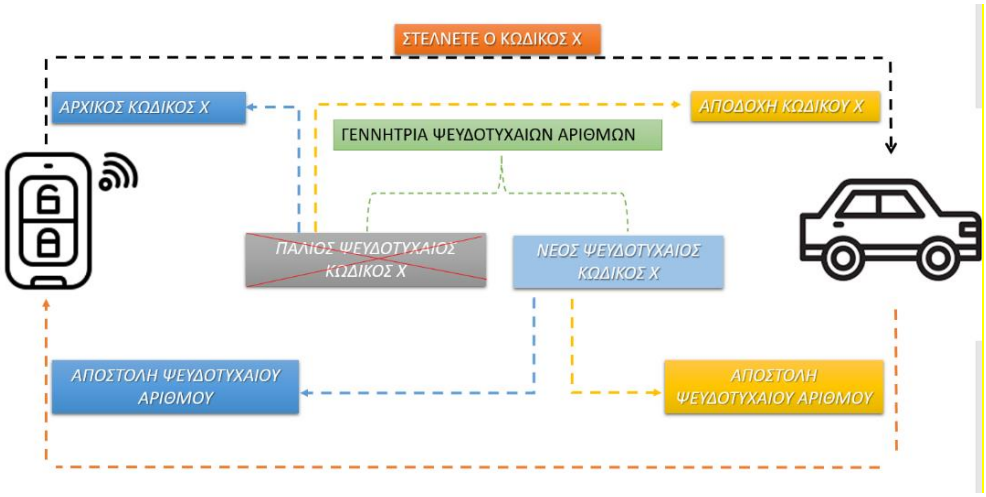
Παρόμοιες τεχνικές και μηχανισμοί ανανέωσης των κλειδιών σύνδεσης/πρόσβασης έχουν σχεδιαστεί και υλοποιηθεί και περιγράφει από την τεχνολογία των Κυλιόμενων Κλειδιών (Rolling Keys – Code/Hopping Codes), η οποία με επιτυχία έχει εφαρμοστεί εδώ και δεκαετίες σε εφαρμογές της αυτοκινητοβιομηχανίας και της προστασίας κατοικιών. Πιο συγκεκριμένα, η τεχνολογία των κυλιόμενων κλειδιών (Rolling key/ Hopping code) είναι ένα σύστημα ασφαλείας που χρησιμοποιείται ώστε η σύζευξη μεταξύ δύο η περισσοτέρων αντικειμένων να επιτυγχάνεται κάθε φορά με ένα κλειδί (password) μιας χρήσης. Η χρήση αυτής της τεχνολογίας μειώνει αισθητά την πιθανότητα για κακόβουλη ενέργεια και την υποκλοπή στοιχείων. Αναλυτικότερα, αντί να χρησιμοποιείται για την ζεύξη και την μετάδοση της εντολής κάθε φορά ο ίδιος κωδικός, δημιουργείται ένας καινούργιος κωδικός, με σκοπό να μην υπάρξει ποτέ επανάληψη ή επαναχρησιμοποίηση του ίδιου κωδικού. Για παράδειγμα, ο μεταδότης και ο δέκτης ξεκινάνε από τον αριθμό 0. Κάθε φορά που ο μεταδότης στέλνει ένα σήμα αυτός ο αριθμός θα αυξάνεται κατά ένα (π.χ. 1, 2, 3). Ο δέκτης θα ακούσει αυτούς τους αριθμούς και θα αυξήσει την δική του μέτρηση (π.χ.1,2,3) όποτε ακούει έναν έγκυρο αριθμό, έτσι ώστε κανένας αριθμός να μην επαναλαμβάνεται ποτέ. Για να μπορέσει να λειτουργήσει όμως αυτό, θα πρέπει ο μεταδότης και ο δέκτης να συμφωνούν στον αρχικό αριθμό που ονομάζεται seed και να χρησιμοποιούν την ίδια συνάρτηση για την παραγωγή των κλειδιών. Για αυτό τον λόγο, πάντοτε ο μεταδότης συγχρονίζεται με τον δέκτη πριν χρησιμοποιηθούν (βλέπε εικόνα 43).



Εικόνα 43 Λειτουργία Τεχνολογίας Κυλιόμενων Κλειδιών

3.2 *Προτεινόμενη Λύση*

Αυτή η παράγραφος αναλύει την προτεινόμενη λύση ασφάλειας για το σύστημα μας, καθώς και τον τρόπο λειτουργίας της. Η προτεινόμενη λύση που εξετάζεται σε αυτή την διπλωματική εργασία, εισάγει την τεχνική των κυλιόμενων κλειδιών με την μορφή ψευδοτυχαίων αριθμών, επεμβαίνοντας έτσι στο πρότυπο που έχει θέσει το πρωτόκολλο LoRaWAN, μετατρέποντας το στατικό AppKey κλειδί σε δυναμικό κλειδί. Σύμφωνα με την τεχνική των ψευδοτυχαίων αριθμών, αντί να χρησιμοποιείται ένας απλός αυξανόμενος μετρητής, χρησιμοποιείται μια σειρά από ψευδοτυχαίων αριθμών (Pseudo Random Number Generators, PRNGs). Η φιλοσοφία των ψευδοτυχαίων αριθμών είναι ίδια με την τεχνική των κυλιόμενων κλειδιών. Δηλαδή, ο μεταδότης και ο δέκτης θα πρέπει να συμφωνήσουν στην πρώτη τυχαία αλληλουχία αριθμών και στην συνέχεια να παράγεται κάθε φορά πριν την επικοινωνία τους μια τελείως διαφορετική αλληλουχία αριθμών (βλέπε εικόνα 44).

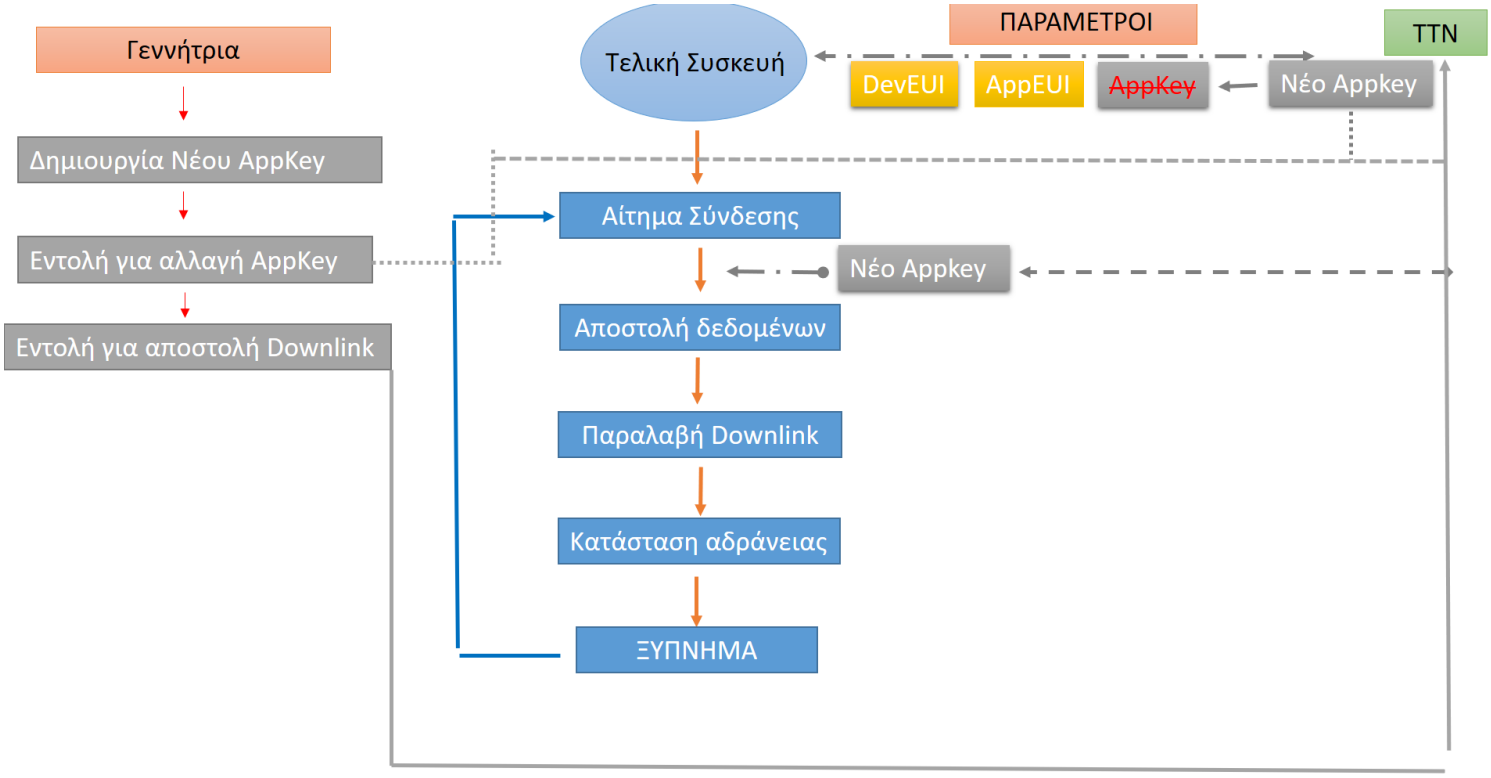


Εικόνα 44 Λειτουργία Ψευδοτυχαίων Αριθμών

Σύμφωνα με τα παραπάνω, κατασκευάζεται μια γεννήτρια που εφαρμόζει την τεχνική των κυλιόμενων κλειδιών σε ένα σύστημα LoRaWAN. Αυτόματα, η γεννήτρια που θα κατασκευαστεί θα πρέπει να λειτουργεί με βάση το πρωτόκολλο επικοινωνίας LoRaWAN 1.0.1 και να υπακούει στις ιδιαιτερότητες του. Η λειτουργίας της γεννήτριας χωρίζεται σε 3 βήματα.

1. Με την χρήση αλγόριθμου, δημιουργείται ένας 16byte κωδικός και στην συνέχεια μετατρέπεται στην σωστή μορφή ώστε να μπορεί να διαβαστεί από την τελική συσκευή αλλά και από το Network Server (TTN) (βλέπε εικόνα 48).
2. Μέσω του Command Line Interface (CLI) δίνεται η εντολή για αλλαγή του παλιού κωδικού με τον νέο (βλέπε εικόνα 52).
3. Μέσω του CLI δίνεται η εντολή για αποστολή με την μορφή Downlink του νέου κωδικού από τον Network Server (TTN) προς την τελική συσκευή (βλέπε εικόνα 53).

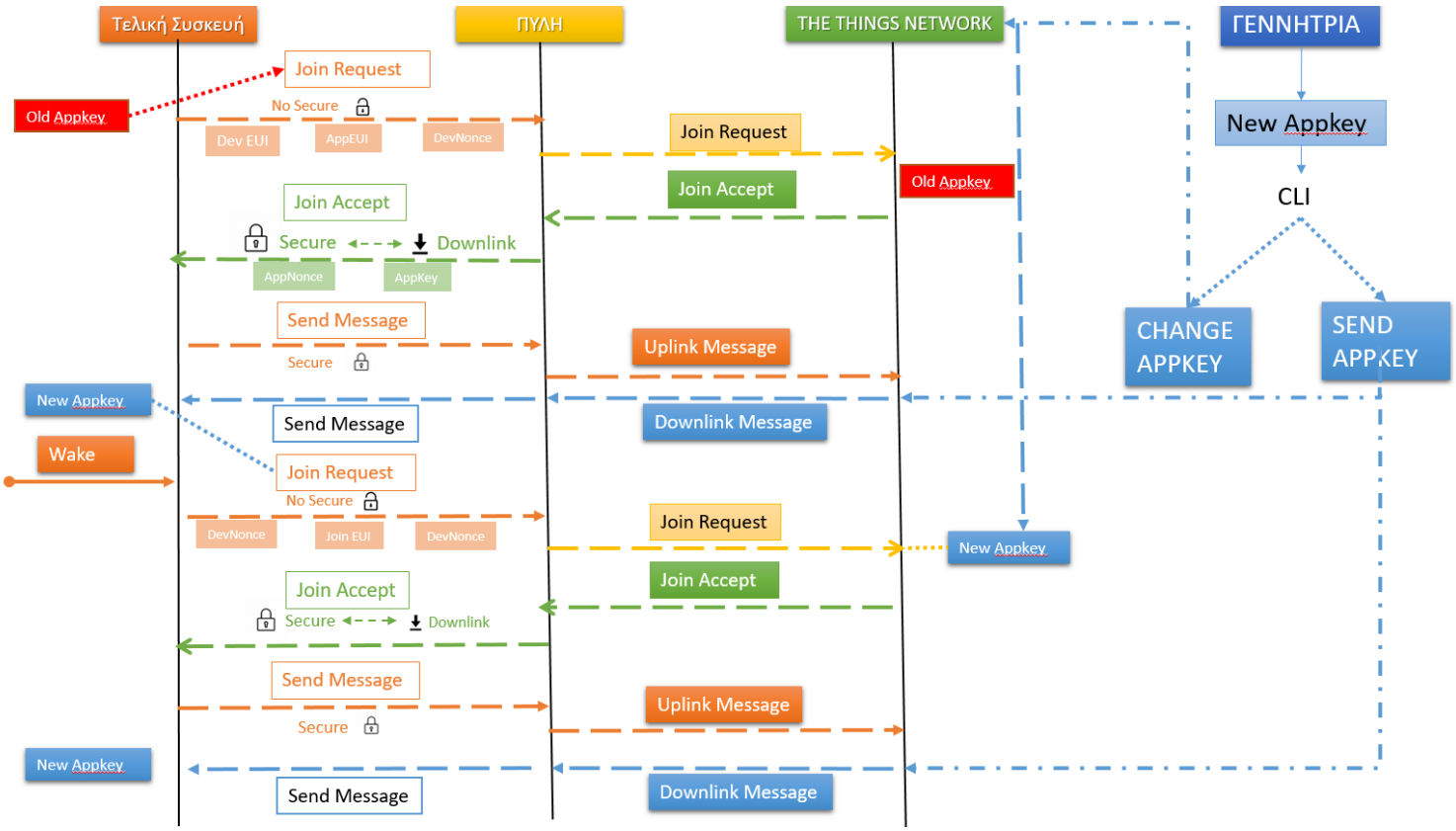
Αρχικά, για να διαβαστεί από την τελική συσκευή το Downlink μήνυμα που περιέχει το νέο κλειδί (AppKey), θα πρέπει η τελική συσκευή να έχει αποκτήσει πρόσβαση στο δίκτυο μας μέσω της επιτυχημένης διαδικασίας σύνδεσης/συμμετοχής (Join Procedure). Στην συνέχεια θα πρέπει η γεννήτρια να εκτελέσει τις εντολές για αλλαγή κωδικού (βλέπε εικόνα 52) και αποστολή του νέου κωδικού (βλέπε εικόνα 53). Για να μπορέσει το σωστό Downlink μήνυμα να έχει ως αποδέκτη την τελική συσκευή στο σωστό session, η διαδικασία αυτή θα πρέπει να εκτελεστεί τουλάχιστον 2sec πριν από την αποστολή δεδομένων του "υγιή" χρήστη. Διαφορετικά, η τελική συσκευή δεν θα λάβει κάποιο κλειδί. Στην περίπτωση που η τελική συσκευή χάσει ένα μήνυμα, τότε το ίδιο μήνυμα θα "ακουστεί" στο επόμενο session. Αυτό συμβαίνει, διότι η εφαρμογή λειτουργεί με το πρότυπο της κλάσης A (βλέπε υποκεφάλαιο 2.4) και τα Downlink μηνύματα διαβάζονται μόνο σαν απάντηση του μηνύματος (uplink) που έστειλε η τελική συσκευή. Ως αποτέλεσμα, η τελική συσκευή θα προσπαθήσει να συνδεθεί στο δίκτυο με λανθασμένο κλειδί (AppKey).



Εικόνα 45 Τρόπος Λειτουργίας Γεννήτριας

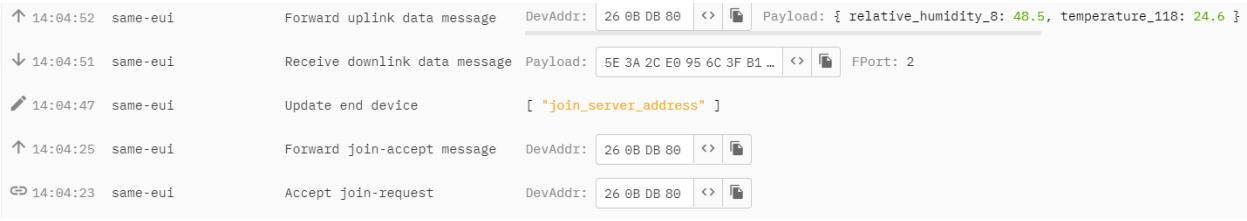
3.3 *Σενάριο 3ο*

Στο Σενάριο αυτό προβάλλεται ένα καινοτόμο σύστημα λειτουργίας LoRaWAN, καθώς εισάγεται η τεχνική των κυλιόμενων κλειδιών με την μορφή των ψευδοτυχαίων αριθμών. Μόλις πραγματοποιηθεί η αποστολή των δεδομένων, η τελική συσκευή εισέρχεται σε κατάσταση αδράνειας, και η διαδικασία επαναλαμβάνεται περίπου κάθε πέντε λεπτά. Αναλυτικότερα, αφού έχουμε ορίσει χειροκίνητα όπως και στα προηγούμενα σενάρια το AppKey στην τελική συσκευή και στον Network Server (TTN) ξεκινάει η διαδικασία του αιτήματος συμμετοχής (Join Request) από την τελική συσκευή. Εφόσον ο Network Server αποδεχτεί το μήνυμα (Join Accept) δημιουργείται η ζεύξη της συσκευής και του δικτύου και αρχίζει οι ανταλλαγή των μηνυμάτων. Παράλληλα, μπαίνει σε λειτουργία η γεννήτρια, η οποία παράγει ψευδοτυχαίους αριθμούς όπως αναλύσαμε στο παραπάνω υποκεφάλαιο (3.2). Το νέο κλειδί που δημιουργείται από την γεννήτρια αποστέλλεται στον κατάλληλο χρόνο στον Network Server (TTN), δίνοντας την εντολή για αλλαγή του κλειδιού και μεταφοράς του προς την τελική συσκευή από τον Network Server (TTN) με την μορφή του Downlink μηνύματος. Με αυτό τον τρόπο η τελική συσκευή και ο Network Server την επόμενη φόρα που θα διαπραγματευτούν τα μηνύματα ζεύξης (Join Request, Join Accept) θα το κάνουν με διαφορετικό AppKey από το αρχικό. Αυτή η διαδικασία επαναλαμβάνεται κάθε φορά που η τελική συσκευή θέλει να στείλει δεδομένα στο Network Server.

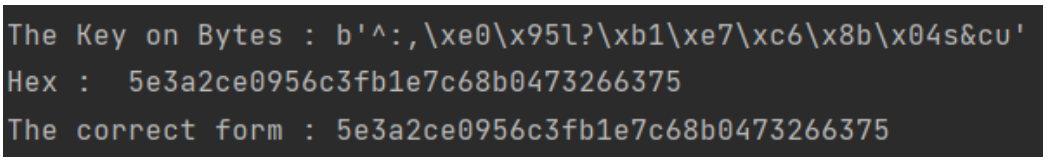


Εικόνα 46 Λειτουργία Συστήματος Σεναρίου 3ου

- Update end device : Το κλειδί AppKey άλλαξε στην πλατφόρμα του TTN
- Receive downlink data message : Το νέο κλειδί (AppKey) στάλθηκε στην τελική συσκευή με την μορφή Downlink από τον Network Server (TTN)
- Forward uplink data message : Τα δεδομένα που στάλθηκαν από την τελική συσκευή

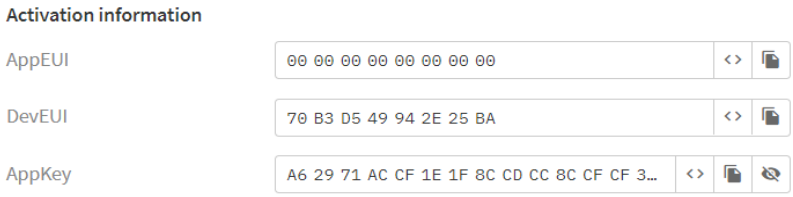


Εικόνα 47 Εμφάνιση σύνδεσης της τελικής συσκευής στο TTN

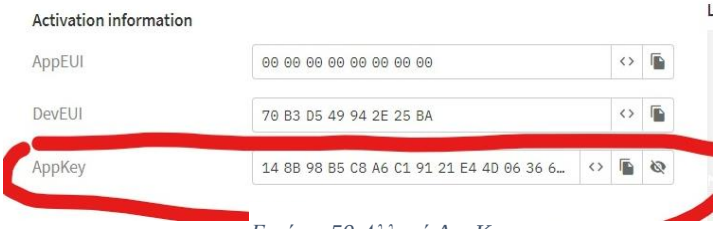


Εικόνα 48 Δημιουργία νέου κωδικού από την γεννήτρια

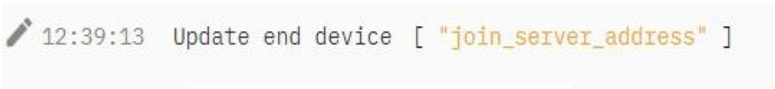
Οι εικόνες 49,50,51 μας δείχνουν την αλλαγή των αρχικών μας παραμέτρων και πιο συγκεκριμένα του AppKey όταν αποστέλλεται η εντολή αλλαγής για τον νέο κωδικό.



Εικόνα 49 Αρχικές Παράμετροι

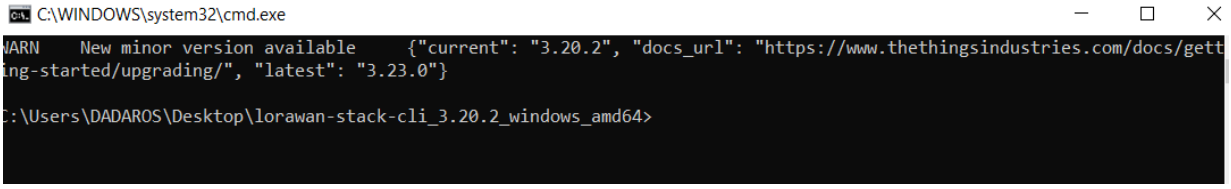


Εικόνα 50 Αλλαγή AppKey



Εικόνα 51 Εντολή Αλλαγής

Εικόνα 52 Εντολή για αλλαγή του κωδικού μέσω του CLI

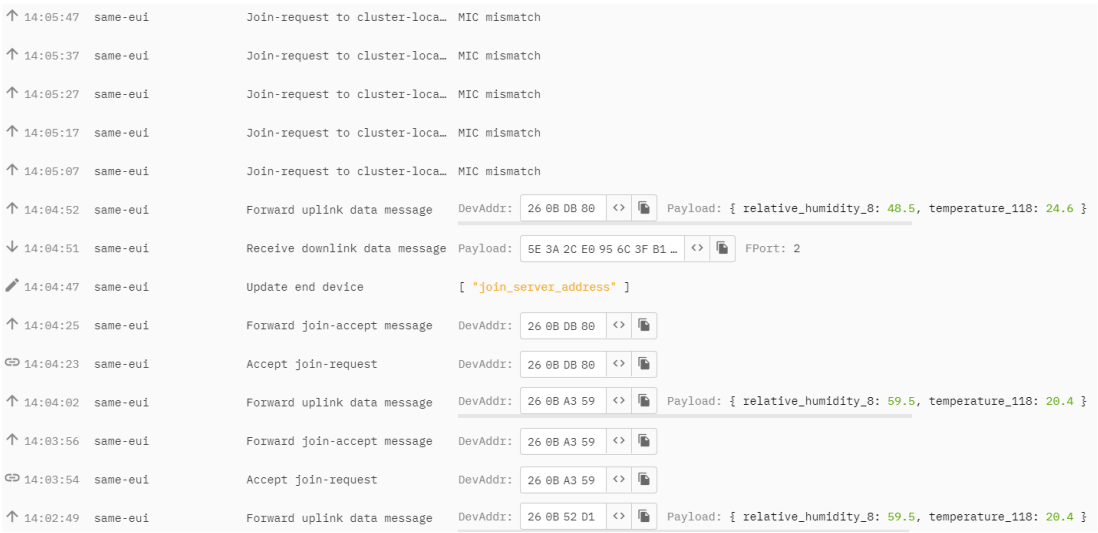


Εικόνα 53 Εντολή για αποστολή του νέου κωδικού μέσω του CLI

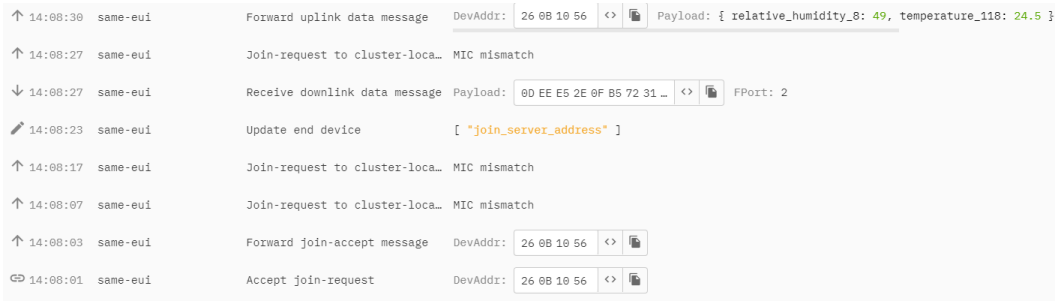
3.4 *Αποτελέσματα – Παρατηρήσεις Σεναρίου 3ου*

Όπως παρατηρούμε στις παρακάτω εικόνες (βλέπε εικόνα 54 και 55), η διάρκεια αποστολής των μηνυμάτων ανέρχεται για τον "υγιή" χρήστη στα 4 λεπτά και για τον Attacker στα 2 λεπτά. Αρχικά, ο κακόβουλος χρήστης συνδέεται στο δίκτυό μας και στέλνει δεδομένα. Τα δεδομένα αυτά, για την θερμοκρασία είναι 20,4 ºC και για το ποσοστό της υγρασίας στο 59.5%. Στην συνέχεια εισέρχεται ο καλός χρήστης με την λειτουργία των κυλιόμενων κλειδιών στο δίκτυο και στέλνει δεδομένα ορίζοντας την θερμοκρασία στους 24,6 ºC και το ποσοστό της υγρασίας στο 48,5%. Κατόπιν αυτό που γίνεται αντιληπτό είναι οι προσπάθειες του κακόβουλου χρήστη να συνδεθεί στο δίκτυο μας, χωρίς ανταπόκριση καθώς το κλειδί έχει αλλάξει. Το μήνυμα που εμφανίζεται είναι (Join-request to cluster location MIC mismatch).

Συνοψίζοντας, με την χρήση των κυλιόμενων κλειδιών και του Join Request καταφέραμε να παρεμποδίσουμε τον κακόβουλο χρήστη να θέσει σε κίνδυνο την λειτουργία του δικτύου μας.

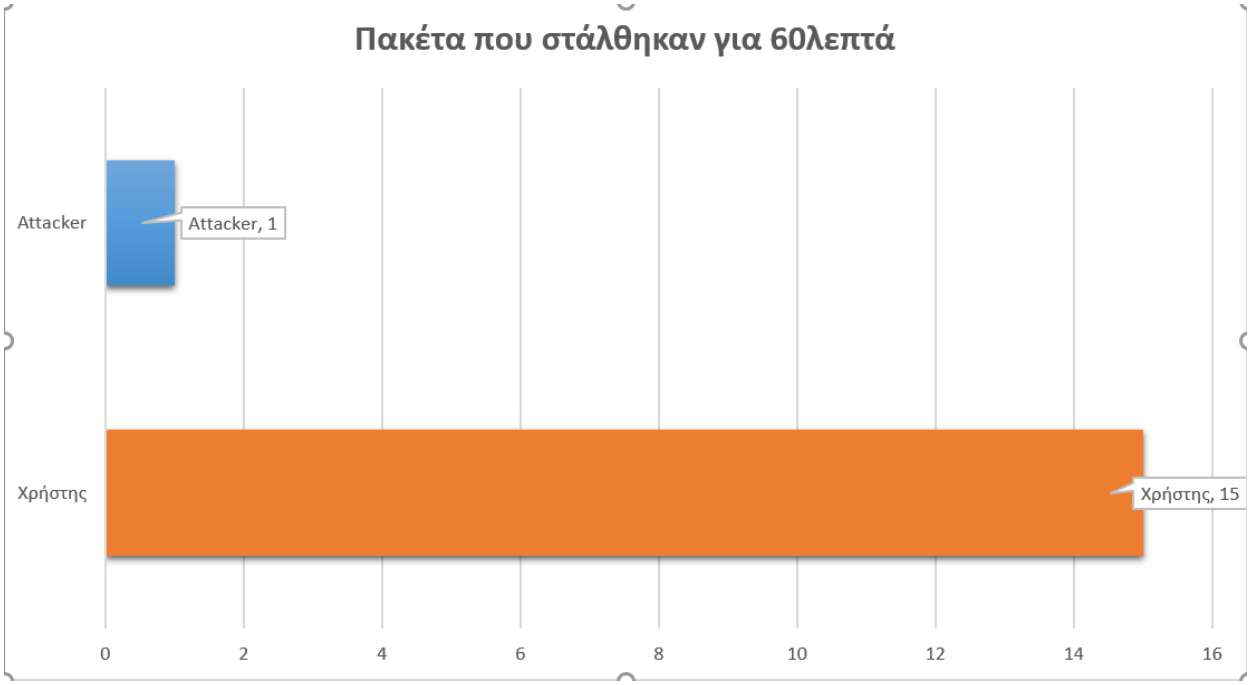


Εικόνα 54 Σύνδεση καλού χρήστη με την λειτουργία change AppKey



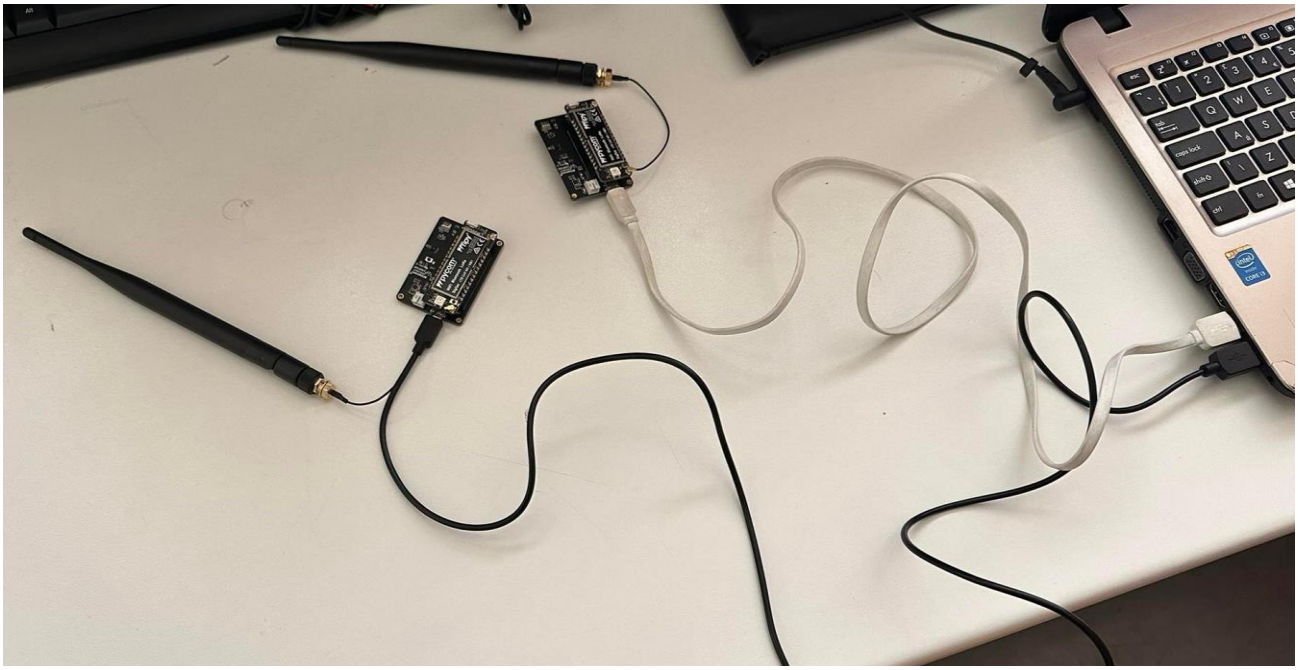
Εικόνα 55 Αποστολή δεδομένων με change AppKey

Σύμφωνα με την εικόνα 56 η οποία μας δείχνει στον οριζόντιο άξονα τον αριθμό των πακέτων/δεδομένων που έφτασαν στο δίκτυο, επιβεβαιώνετε πειραματικά ότι η χρήση κυλιόμενων κλειδιών προστατεύει την ακεραιότητα του δικτύου μας. Οι Εικόνες 57 και 58 παρουσιάζουν τις συσκευές LoRa που χρησιμοποιήθηκαν στο συγκεκριμένο πείραμα. Πιο συγκεκριμένα, γίνεται αντιληπτό ότι με την εισαγωγή του "καλού" χρήστη στο δίκτυο με την τεχνική των κυλιόμενων κλειδιών γίνεται απομάκρυνση του κακόβουλου χρήστη, ο οποίος δεν ξανά αποκτά πρόσβαση στο δίκτυο μας παρά τις προσπάθειες του. Αυτό συμβαίνει, διότι ο χρόνος που χρειάζεται για την αλλαγή του AppKey είναι αρκετά ταχύτερος από τον χρόνο που απαιτείται για την αποκρυπτογράφηση και την παραβίαση του δικτύου μας. Εν κατακλείδι, τα συνολικά πακέτα που στάλθηκαν από τον χρήστη με την χρήση της τεχνικής των κυλιόμενων κλειδιών ανέρχεται στα 15, ενώ τα πακέτα που στάλθηκαν από τον Attacker ανέρχεται στο μόλις 1 (βλεπε εικόνα 56).



Εικόνα 56 Πακέτα που στάλθηκαν με την χρήση των κυλιόμενων κλειδιών

Εικόνα 57 Lorix One



Εικόνα 58 PyCom

3.5 *Προβλήματα που Αντιμετωπίστηκαν*

Κατά την διάρκεια του πειραματικού μέρους, εντοπίστηκαν ορισμένα προβλήματα βελτιστοποίησης και λεπτοσυντονισμού (fine-tunning) της πειραματικής διάταξης και των επί μέρους λειτουργικών μονάδων του δικτύου LoRa. Ένα από αυτά, ήταν η αστάθεια που εμφάνιζε το δίκτυο (π.χ. jitter, transmission delay, κτλ.), και η οποία επηρέαζε την ομαλή/σταθερή επικοινωνία με την πλατφόρμα “The Things Network”, και πιο συγκεκριμένα τον συγχρονισμό του Network Server του LoRaWAN με τη γεννήτρια των ψευδοτυχαίων κλειδιών. Εξ’ αιτίας αυτής τη αστάθειας του δικτύου, παρατηρήθηκε ότι δεν ήταν δυνατή η συγχρονισμένη αλλαγή του κλειδιού/κωδικού (AppKey) τόσο στον Network Server όσο και στην τελική συσκευή, με αποτέλεσμα είτε ο Network Server είτε η τελική συσκευή να μην μοιράζονται το ίδιο AppKey. Η λύση που υιοθετήθηκε περιλάμβανε τον προγραμματισμό της τελικής συσκευής με την μορφή μιας επιπλέον ρουτίνας στον αρχικό κώδικα, η οποία επιτρέπει την σύνδεση και ταυτοποίηση της τελικής συσκευής με τη χρήση του προηγούμενου κλειδιού.

```
b'5e3a2ce0956c3fb1e7c68b0473266375'
To kleidi allaxe
Not yet joined...
Not yet joined...
Not yet joined...
Joined
```

Εικόνα 59 Το κλειδί άλλαξε

```
b'1abb9fa39c3cfb2e58ec58bc1ffa8f16'
To kleidi  den allaxe 2o
Not yet joined...
Not yet joined...
Not yet joined...
Joined
```

Εικόνα 60 Το κλειδί δεν άλλαξε

3.6 Συμπεράσματα

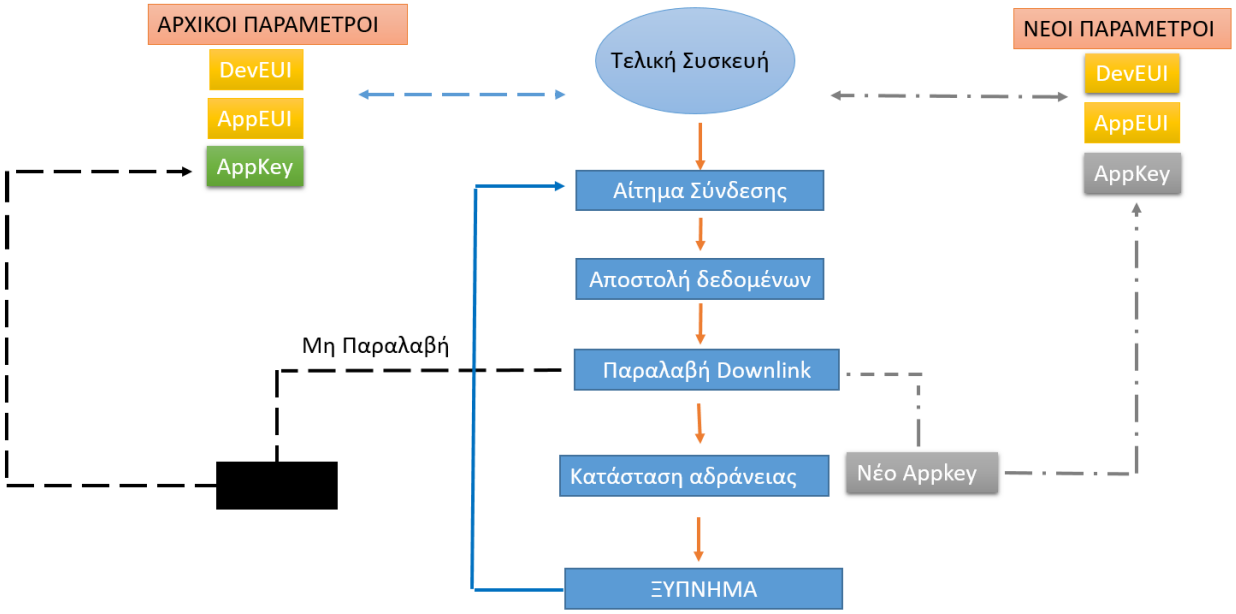
Αυτή η διπλωματική εργασία, προτείνει ένα καινοτόμο σύστημα με σκοπό την βελτιστοποίηση και την ενίσχυση ενός LoRaWAN δικτύου. Η προτεινόμενη μέθοδος όπως αποδείχθηκε βελτιώνει την ασφάλεια των δικτύων LoRaWAN χρησιμοποιώντας μια τεχνική κυλιόμενων κλειδιών παρόμοια με αυτή που χρησιμοποιείται για την ασφάλεια του κλειδώματος των αυτοκινήτων. Το δίκτυο LoRaWAN που δημιουργήθηκε με σκοπό την αντιμετώπιση του προβλήματος στην διαδικασία της ταυτοποίησης (Join Procedure) σύμφωνα με το πρότυπο OTAA , αποτελείται από τον μικροελεκτή PyCom (βλέπε εικόνα 58) έχοντας τον ρόλο της τελικής συσκευής, το Lorix One (βλέπε εικόνα 57) στον ρόλο της Πύλης (gateway) και το The Things Network (TTN) στον ρόλο του Network Server. Παρόλο που, η μετάδοση του μηνύματος για την αίτηση συμμετοχής (Join Request) μεταδίδεται στον αέρα σε μη κρυπτογραφημένη μορφή, η αντικατάσταση του στατικού AppKey με ένα δυναμικό κλειδί που αλλάζει συνέχεια, όπως αποδείχθηκε προσφέρει μια ασφάλεια στο δίκτυο αποτρέποντας τους κακόβουλους χρήστες να το παραβιάσουν. Η χρονική διάρκεια για την δημιουργία του νέου κλειδιού και την χρησιμοποίηση του είναι πολύ πιο σύντομη, για να μπορέσει ο κακόβουλος χρήστης να το αποκρυπτογραφήσει και να το υποκλέψει, καθώς η ασφάλεια του AES-128 απαιτεί μεγάλη διάρκεια και μεγάλη υπολογιστική δύναμη για να διαβαστεί και να αποκρυπτογραφηθεί. Επομένως, μετά την διεξαγωγή των διαδοχικών πειραμάτων σε πραγματικές συνθήκες, το δίκτυο LoRaWAN με την χρήση της τεχνικής των κυλιόμενων κλειδιών μπορεί να χαρακτηριστεί περισσότερο ασφαλές, εμποδίζοντας τον κακόβουλο χρήστη να πραγματοποιήσει μια *Man in the middle* επίθεση και να εισχωρήσει παράνομα στο δίκτυο μας, θέτοντας σε κίνδυνο την ακεραιότητα των δεδομένων μας.

4. ΚΕΦΑΛΑΙΟ 4

4.1 *Παράρτημα*

Περιγραφή Κώδικα

Σε αυτό το κεφάλαιο, γίνεται η ανάλυση κάποιων βασικών λειτουργιών της τελικής συσκευής. Αρχικά εισάγονται στην τελική συσκευή οι αρχικές παράμετροι (DevEUI, AppEUI, AppKey), ώστε η τελική συσκευή να μπορεί να προχωρήσει επιτυχώς στο αίτημα σύνδεσης/συμμετοχής (Join Procedure). Μετά την ταυτοποίηση της συσκευής από τον Network Server (TTN) και την επιτυχή σύνδεσή της στο δίκτυο (Join Accept), ξεκινάει η αποστολή των δεδομένων της θερμοκρασίας και την υγρασίας. Έπειτα η τελική συσκευή "ανοίγει ένα παράθυρο" για να μπορέσει να "ακούσει" το Downlink μήνυμα που θα σταλθεί από το TTN, το οποίο θα περιέχει το νέο κλειδί (AppKey) που θα πρέπει να χρησιμοποιηθεί στο επόμενο session. Μετά από αυτή την διαδικασία, η τελική συσκευή μπαίνει σε κατάσταση αδράνειας για το χρονικό περιθώριο που του έχουμε ορίσει. Μετά το πέρας της χρονικής διάρκειας της αδράνειάς του, η διαδικασία ξεκινάει από την αρχή. Πριν όμως προχωρήσει στο αίτημα σύνδεσης/συμμετοχής (Join Procedure), η τελική συσκευή ελέγχει αν έλαβε το νέο κλειδί (AppKey). Στην περίπτωση που, το νέο κλειδί στάλθηκε από το Network Server (TTN), η τελική συσκευή στέλνει το αίτημα σύνδεσης αντικαθιστώντας το παλιό κλειδί με το νέο κλειδί (AppKey). Διαφορετικά, το αίτημα σύνδεσης (Join Procedure) πραγματοποιείται με την χρήση του προηγούμενου κλειδιού.



Εικόνα 61 Λειτουργία τελικής συσκευής

Στην εικόνα 62 γίνεται η οριοθέτηση των αρχικών παραμέτρων/κλειδιών στην τελική συσκευή, με σκοπό την αρχική σύνδεση στο Network Server.

```
# create an OTAA authentication parameters, change them to the provided credentials

dev_eui = ubinascii.unhexlify('70B3D549942E25BA')
app_eui = ubinascii.unhexlify('0000000000000000')
app_key = ubinascii.unhexlify('1ABB9FA39C3CFB2E58EC58BC1FFA8F16')
```

Εικόνα 62 Αρχικά κλειδιά

Η τελική συσκευή στέλνει αίτημα σύνδεσης και περιμένει να αποκτήσει πρόσβαση στο δίκτυο

```
while not lora.has_joined():
 time.sleep(2.5)
 print('Not yet joined...')


print('Joined')
```

Εικόνα 63 Προσπάθεια σύνδεσης τελικής συσκευής

Η παρακάτω εντολή *(lpp.send)* είναι υπεύθυνη για την αποστολή των δεδομένων

```
# send some data
 lpp.add_relative_humidity(si.humidity())
 lpp.add_temperature(si.temperature(), channel = 118)
 lpp.send(reset_payload = True)
 print("[" + str(time.time()) + "] sending Temperature ")
```

Εικόνα 64 Αποστολή δεδομένων

Στις παρακάτω εικόνες (Εικόνα 65 και Εικόνα 66), παρατηρούμε την λειτουργία του κώδικα στο πρόβλημα που εντοπίσθηκε σύμφωνα με το υποκεφάλαιο 3.5. Ουσιαστικά, η τελική μας συσκευή αναζητά για το αν έχει λάβει το καινούργιο κλειδί (AppKey) με την μορφή του Downlink.

1. Στην περίπτωση που το πλαίσιο της αναμονής του μηνύματος είναι κενό, τότε η τελική συσκευή αντιλαμβάνεται ότι δεν έχει σταλθεί κάποιος νέος κωδικός με την μορφή του Downlink. Οπότε ξεκινάει την διαδικασία αιτήματος συμμετοχής χρησιμοποιώντας το αρχικό AppKey κλειδί.
2. Αντίθετα αν λάβει το καινούργιο κλειδί (AppKey), εμφανίζει το μήνυμα "Το κλειδί άλλαξε" και ξεκινάει την διαδικασία σύζευξης αντικαθιστώντας το παλιό κλειδί με το νέο κλειδί (Εικόνα 60).

```
if data == (b'') and i == 1 :

    same_key = ubinascii.hexlify(app_key)
    print("To kleidi den allaxe")

    dev_eui = ubinascii.unhexlify('70B3D549942E25BA')
    app_eui = ubinascii.unhexlify('0000000000000000')
    app_key = ubinascii.unhexlify(same_key)
```

Εικόνα 65 Το κλειδί δεν άλλαξε

```
    elif data != (b'') :

        new_key = ubinascii.hexlify(data)
        print(new_key)

        print("To kleidi allaxe")

        i = i + 1

        dev_eui = ubinascii.unhexlify('70B3D549942E25BA')
        app_eui = ubinascii.unhexlify('0000000000000000')
        app_key = ubinascii.unhexlify(new_key)
```

Εικόνα 66 Το Κλειδί άλλαξε

Με την εισαγωγή της παρακάτω εντολής *(s.recv)* πραγματοποιείται η προσπάθεια της τελικής συσκευής να λάβει, να διαβάσει και να εκτυπώσει το νέο Downlink μήνυμα του Network Server.

```
# get any data received (if any...)
data = s.recv(64)
print(data)
```

Εικόνα 67 Έλεγχος για Downlink

4.2 *Εργαλεία και Βιβλιοθήκες της Εφαρμογής*

Για την ανάπτυξη της εφαρμογής έγινε χρήση των παρακάτω εργαλείων και βιβλιοθηκών.

- Socket

  Η χρήση του Socket ενεργοποιεί την επικοινωνία και πιο συγκεκριμένα την αποστολή μηνυμάτων στο διαδίκτυο.

- Ubinascii

Βοηθά στην μετατροπή δυαδικών δεδομένων σε μορφή ASCII και αντίστροφα(American Standard Code for Information Interchange).

- Ubinascii.hexlify

  Μετατρέπει τα δεκαεξαδικά δεδομένα σε δυαδική μορφή επιστρέφοντας bytes.

- Ubinascii.unhexlify

  Αποκρυπτογραφεί Base64 δεδομένα και επιστρέφει bytes.

- CayenneLpp

  Με την χρήση αυτής της βιβλιοθήκης επιτυγχάνεται η επικοινωνία ανάμεσα στα LoRaWAN και το Cayenne, το οποίο είναι μια εφαρμογή αναπαράστασης και συλλογής δεδομένων.

- SI7006A20

  Με την χρήση αυτής της βιβλιοθήκης ενεργοποιείται ο αισθητήρας της θερμοκρασίας και της υγρασίας πάνω στο Pysense.

4.3 *Κώδικας*

Ο κώδικας του συστήματος παρατίθενται στον παρακάτω σύνδεσμο :

https://github.com/dados98/Thesis-LoRaWAN-.git

4.4 *Αναφορές – Πηγές*

[1] M.U. Farooq, Muhammad Wassem, Anjum Khairi, Talha Kamal, Sadia Mazhar (2015): "A Review on Internet of Things (IoT)", International Journal of Computer Applications, **113**, pp 7.

[2] Ericsson Mobility Report June 2017

[3] Krishan Kumar Goyal, Amit Garg, Ankur Rastogi, Saurabh Singhal (2018): "A Literature Survey on Internet of Things (IoT)", Int. J. Advanced Networking and Applications, **09,** pp 1-6.

[4] https://lora-alliance.org/about-lorawan/

[5] https://lora-alliance.org/

[6] https://www.thethingsnetwork.org/docs/lorawan/end-device-activation/

[7] Thadeu Brito, Ana I. Pereira, Jose Lima, Antonio Valente (2020): Wireless Sensor Network for Ignitions Detection: An IoT approach, pp 1-16

[8] E. Aras, G. S. Ramachandran, P. Lawrence and D. Hughes (2017), "Exploring the Security Vulnerabilities of LoRa", 3RD IEEE International Conference on Cybernetics (CYBCONF), pp 1-6

[9] https://www.thethingsnetwork.org/docs/lorawan/end-device-activation/

[10] Jaehyu Kim, JooSeok Song (2017): "A Dual Key-Based Activation Scheme for Secure LoRaWAN", Wiley Hindawi, 2017, pp 1-12

[11] S. Tomasin, S. Zulian and L. Vangelista (2017): "Security Analysis of LoRaWAN Join Procedure for Internet of Things Networks," IEE Wireless Communications and Networking Conference Workshops (WCNCW), pp 1-6

[12] Jun Lin, Zhiqi Shen, Chunyan Miao, Siyuan Liu (2017): "Using blockchain to build trusted LoRaWAN sharing server", International Journal of Crowd Science, Vol.1, No.3, pp 270-280

[13] Yonghua Song, Jin Lin, Ming Tang, Shufeng Dong (2017): "An Internet of Energy Things Based on Wireless LPWAN", Center of Internet of Energy Things, Tsinghua-Sichuan Energy Internet Institution, pp1-7

[14] Kais Mekki, Eddy Bajic, Frederic Chaxel, Fernand Meyer (2018): "A comparative study of LPWAN technologies for large-scale IoT deployment, The Korean Institute of Communication and Information Sciences, pp 1-7

[15] Bharat S. Chaudhari, Marco Zennaro, Suresh Borkar (2020), "LPWAN Technologies: Emerging Application Characteristics, Requirement and Design Consideration", future Internet, pp 1-25

[16] Alexandru Lavric (2018: "LoRa (Long-Range) High-Density Sensors for Internet of Things", Hinday Journal of Sensors, Vol 2019, pp 1-9

[17] Da-Wen Huang, Wanping Liu, and Jichao Bi. (2021), "Data tampering attacks diagnosis in dynamic wireless sensor networks", Computer Communications 172, pp 84-92

[18] Woo-Jin Sung et al. (2020), "Protecting end-device from replay attack on LoRaWAN", IEEE, Vol 2018, pp 167-171

[19] John Thomas et al. (2020), "Man in the Middle Attack Mitigation in LoRaWAN", IEEE, pp 353-358.

[20] Zhuoqun Xia et al. (2021), "Secure Session Key Management Scheme for Meter-Reading System Based on LoRa Technology", IEEE, pp 75015-75024.

[21] Stephen Ugwuanyi, Greig Paul, and James Irvine, (2021), "Survey of iot for developing countries: Performance analysis of lorawan and cellular nb-iot networks", Electronics (Switzerland).

[22] Herman Isa et al. (2011), "AES: Current security and efficient analysis of its alternatives", IEEE, pp 267-274

[23] Syed Muhammad Danish et al. (2019): "A lightweight blockchain based two factor authentication mechanism for LoRaWAN join procedure" IEEE International Conference on Communication Workshops

[24] SeungJae Na et al. (2017), "Scenario and countermeasure for replay attack using join request messages in LoRaWAN", IEEE.

[25] Jaehyu Kim and JooSeok Song (2017), "A Simple and efficient Replay Attack Prevention Scheme for LoRaWAN", ACM Press, pp 32-36

[26] Aloys Augustin, Jiazi Yi, Thomas Clausen, and William Mark Townsley (2016),” A Study of LoRa: Long Range & Low Power Networks for the Internet of Things”, Cisco Paris Innovation and Research Laboratory, pp 1-18