

Κοζάνη: Έξυπνη Πόλη- Παράθυρο στο Μέλλον

«Μετάδοση δεδομένων μέσω LoRaWan»

«Καταγραφή βιομετρικών στοιχείων με σκοπό τον εντοπισμό
διασποράς του Covid-19»

Ομάδα « BikeSignals»

Αμανατίδου Άννα

Θωμαΐδου Σοφία

Καράμωβ Γρηγόρης

Υπεύθυνος καθηγητής: Κασνάκης Γιώργος – 4^ο ΓΕΛ Κοζάνης

Περιεχόμενα

Εισαγωγή	4
Το Διαδίκτυο των Πραγμάτων(Internet of Things - IoT)	4
Ορισμός	4
Τα χαρακτηριστικά του IoT	5
Τα θεμελιώδη χαρακτηριστικά του IoT είναι τα εξής:	5
Τα επίπεδα της Έξυπνης Πόλης.....	6
Πλεονεκτήματα IoT	7
Μειονεκτήματα IoT	7
Ασύρματες λύσεις συνδεσιμότητας.....	8
Μικρής Εμβέλειας Ασύρματες Λύσεις	8
Bluetooth.....	8
Wi-Fi HaLow (IEEE802.11ah)	8
Z -Wave.....	8
Zigbee	9
NFC	9
Μεγάλης Εμβέλειας Ασύρματες Λύσεις (Low Power Wide Area Network, LPWAN)	9
LPWAN - μη αδειοδοτημένο φάσμα	9
LoRa-LoRaWAN.....	9
LoRaWAN.....	10
Α) Αρχιτεκτονική.....	10
LoRaWAN Επικοινωνία.....	11
Smart Cities.....	13
Ορισμός	13
Χαρακτηριστικά.....	13
Πλεονεκτήματα Έξυπνης Πόλης	15
Προβλήματα Έξυπνων Πόλεων	15
Αντιμετώπιση κινδύνων Έξυπνων Πόλεων	16
Πρόβλημα.....	17
Πρόταση	18
Υλοποίηση συστήματος.....	19
Hardware	19
1ο Υποσύστημα	19
2ο Υποσύστημα.....	19

Software	21
1 ^ο Υποσύστημα – Arduino uno master.....	21
2ο Υποσύστημα – Arduino -Dragino slave	22
Δήλωση συσκευής στο TTN.....	26
Καταγραφή δεδομένων.....	27
Ενδεικτικά αποτελέσματα.....	28
Όνομα Ομάδας	30
Αναφορές	31

Εισαγωγή

Με τον όρο Διαδίκτυο των Πραγμάτων (IoT) ορίζεται η σύνδεση των αντικειμένων που χρησιμοποιούν οι άνθρωποι καθημερινά με το Διαδίκτυο και τον υπολογιστή. Αυτές οι συνδέσεις έχουν σα σκοπό την αλληλεπίδραση και τον έλεγχο από τους ανθρώπους, των συσκευών που βρίσκονται σε απομακρυσμένες περιοχές καθώς και την παροχή από τις επιχειρήσεις υπηρεσιών στους πελάτες τους.

Ένα οικοσύστημα IoT αποτελείται από τις έξυπνες συσκευές που χρησιμοποιούν αισθητήρες καθώς και υλικό επικοινωνίας για να συλλέγουν και να επεξεργάζονται τα δεδομένα που έχουν. Οι έξυπνες συσκευές αυτές μοιράζονται τα δεδομένα τα οποία συλλέγουν και αποστέλλονται είτε στο cloud που πρόκειται να αναλυθούν εκεί είτε αναλύονται τοπικά. Ορισμένες φορές, αυτές οι συσκευές επικοινωνούν με άλλες σχετικές συσκευές και ενεργούν με βάση τις πληροφορίες που λαμβάνουν μεταξύ τους. Οι συσκευές παρόλο που δεν χρειάζονται ανθρώπινη παρέμβαση, είναι αυτές που πραγματοποιούν το μεγαλύτερο μέρος της εργασίας. Το IoT αποτελεί μια τεχνολογία που στο μέλλον θα ασκήσει μεγάλη επιρροή στις αγορές, τις υπηρεσίες υγείας και στο τομέα της βιομηχανίας. Τα δεδομένα που θα συγκεντρώνονται θα μπορούν να χρησιμοποιηθούν για τη βελτίωση της απόδοσης, τον εντοπισμό καθώς και την πρόβλεψη των αναγκών των ανθρώπων και των οργανισμών πριν αυτές εμφανιστούν.

Οι τεχνολογίες LPWAN επιτυγχάνουν λειτουργία ευρείας εμβέλειας και χαμηλής ισχύος σε βάρος του χαμηλού ρυθμού μετάδοσης δεδομένων και της υψηλότερης καθυστέρησης, συνήθως της τάξης κάποιων δευτερολέπτων ή λεπτών. Επομένως, οι τεχνολογίες LPWAN δεν προορίζονται για την αντιμετώπιση κάθε περίπτωση χρήσης του IoT. Οι τεχνολογίες LPWAN χωρίζονται σε αυτές που έχουν αδειοδοτούμενο φάσμα όπως LTE-M και NB-IoT και σε αυτές που δεν χρειάζεται κάποια άδεια, όπως LoRa και SigFox.

Πολλές από τις τεχνολογίες αυτές έχουν αξιοποιηθεί στις έξυπνες πόλεις με σκοπό τη διευκόλυνση και των ανθρώπων αλλά και της πολιτείας. Οι πολίτες μπορούν άνετα να αξιοποιήσουν τα Μέσα Μαζικής Μεταφοράς λόγω του IoT (εγκατάσταση ένδειξης αναμονής για την άφιξη του λεωφορείου στην στάση), ένας δήμος μπορεί εύκολα να αντιμετωπίσει την υπερβολική κατανάλωση ενέργειας με το να ρυθμίζει κατάλληλα το φωτισμό στους δρόμους ανάλογα τις καιρικές συνθήκες που υπάρχουν. Τέλος, πολλές εταιρείες τηλεπικοινωνιακών παροχών αξιοποιούν τις τεχνολογίες LPWAN, και συγκεκριμένα την τεχνολογία NB - IoT για πολλές χρήσεις στις ανθρώπινες εργασίες.

Το Διαδίκτυο των Πραγμάτων(Internet of Things - IoT)

Ορισμός

Το Διαδίκτυο των Πραγμάτων (IoT) πρόκειται για ένα σημαντικό θέμα που αφορά τους κλάδους της τεχνολογίας και των μηχανικών ηλεκτρονικών υπολογιστών και έχει γίνει τίτλος ειδήσεων, τόσο στον επιστημονικό τόπο, όσο και στα δημοφιλή μέσα ενημέρωσης. Αυτή η τεχνολογία ενσωματώνεται σε ένα ευρύ φάσμα δικτυωμένων προϊόντων, συστημάτων και αισθητήρων, τα οποία εκμεταλλεύονται τις προόδους στην υπολογιστική ισχύ, τη μείωση του μεγέθους των ηλεκτρονικών εξαρτημάτων και τις διασυνδέσεις δικτύων για να προσφέρουν νέες υπηρεσίες που στο παρελθόν δεν ήταν εφικτές. Μια πληθώρα συνεδρίων, εκθέσεων και ειδησεογραφικών άρθρων εστιάζουν στο μελλοντικό αντίκτυπο της «επανάστασης IoT», από τις νέες ευκαιρίες της αγοράς και τα επιχειρηματικά μοντέλα που καταλήγουν στις ανησυχίες, σχετικά με την ασφάλεια, την ιδιωτικότητα και τη διαλειτουργικότητά της [1].

Ο όρος «Διαδίκτυο των πραγμάτων» (IoT) χρησιμοποιήθηκε για πρώτη φορά το 1999 από το βρετανό πρωτοπόρο της τεχνολογίας Kevin Ashton για να περιγράψει ένα σύστημα στο οποίο αντικείμενα του φυσικού κόσμου θα μπορούσαν μέσω αισθητήρων να συνδεθούν με το Διαδίκτυο. Ο Ashton επινόησε τον όρο ώστε να περιγράφει την ισχύ των συστημάτων ταυτοποίησης με τη βοήθεια ραδιοσυχνοτήτων (RFID) που χρησιμοποιούνται σε εταιρικές εφοδιαστικές αλυσίδες, με σκοπό τη μέτρηση και τον εντοπισμό προϊόντων χωρίς την ανάγκη ανθρώπινης παρέμβασης [1].



Η εφαρμογή του IoT σε αστικό περιβάλλον έχει ιδιαίτερο ενδιαφέρον, καθώς ανταποκρίνεται στην πρόθεση πολλών εθνικών κυβερνήσεων να υιοθετήσουν λύσεις τεχνολογιών πληροφορικής και επικοινωνιών (ΤΠΕ) στη διαχείριση των δημοσίων υποθέσεων. Υλοποιούν έτσι την έξυπνη πόλη (Smart City), που έχει ως τελικό στόχο την καλύτερη δυνατή χρήση των δημοσίων πόρων, αποσκοπώντας στη βελτίωση της ποιότητας των προσφερόμενων υπηρεσιών, με παράλληλη μείωση των λειτουργικών δαπανών των δημοσίων φορέων. Η εισαγωγή των ΤΠΕ στην αστική διακυβέρνηση αποφέρει οφέλη στη διαχείριση και στη βελτίωση των παραδοσιακών δημοσίων υπηρεσιών, όπως οι μεταφορές και η στάθμευση, ο δημόσιος φωτισμός, η επιτήρηση και η συντήρηση των δημοσίων χώρων, η διατήρηση της πολιτιστικής κληρονομιάς, η συλλογή απορριμμάτων, η υγιεινή των νοσοκομείων και των σχολείων. Τα πρότυπα Διασύνδεσης IoT θα διαδραματίσουν θεμελιώδη ρόλο στην ανάπτυξη κατάλληλων υποδομών σε έργα μεγάλης κλίμακας [2].

Τα χαρακτηριστικά του IoT

Τα θεμελιώδη χαρακτηριστικά του IoT είναι τα εξής:

Υπηρεσίες που σχετίζονται με τα πράγματα: Το IoT παρέχει υπηρεσίες, που σχετίζονται με τα πράγματα, εστιάζοντας στη σημασιολογική συνοχή που υπάρχει μεταξύ των φυσικών και των εικονικών πραγμάτων. Αυτό θα οδηγήσει στην αλλαγή τόσο των τεχνολογιών του φυσικού κόσμου όσο, και του κόσμου της πληροφορίας.

Ετερογένεια: Οι συσκευές στο Διαδίκτυο είναι ετερογενείς επειδή βασίζονται σε διαφορετικές πλατφόρμες και δίκτυα. Μπορούν να αλληλοεπιδρούν με άλλες συσκευές ή πλατφόρμες υπηρεσιών μέσω διαφορετικών δικτύων.

Δυναμικές αλλαγές: Η κατάσταση των συσκευών αλλάζει δυναμικά, για παράδειγμα είναι ενεργές ή απενεργοποιημένες, συνδέονται ή αποσυνδέονται, αλλάζει η θέση και η ταχύτητά τους. Ακόμα, ο αριθμός των διασυνδεδεμένων συσκευών μπορεί να αλλάξει δυναμικά.

Μεγάλη κλίμακα χρηστών: Ο αριθμός συσκευών, που οι χρήστες διαχειρίζονται και επικοινωνούν μεταξύ τους μέσω IoT θα είναι μεγαλύτερος από το πλήθος των συσκευών που είναι συνδεδεμένες στο τρέχον Διαδίκτυο.

Ασφάλεια: Επιβάλλεται ασφαλής σχεδιασμός και για τους δημιουργούς αλλά και για τους παραλήπτες του IoT και ασφάλεια προσωπικών δεδομένων και ιδιωτικής ζωής. Η ασφάλεια πρέπει να κλιμακωθεί ανάμεσα στις συσκευές, τα δίκτυα και τα δεδομένα που διακινούνται.

Συνδεσιμότητα: Η συνδεσιμότητα αφορά την προσβασιμότητα και τη συμβατότητα του δικτύου. Η προσβασιμότητα επιτρέπει τη σύνδεση σε ένα δίκτυο, ενώ η συμβατότητα παρέχει την κοινή δυνατότητα δημιουργίας και χρήσης δεδομένων του δικτύου [3]

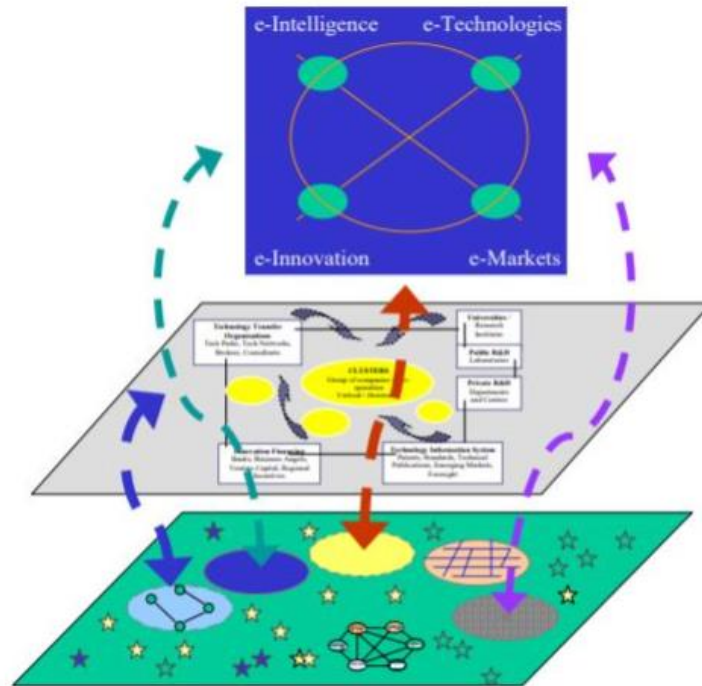
Τα επίπεδα της Έξυπνης Πόλης

Η ευφυής πόλη συνθέτει ανθρώπινες ικανότητες και δραστηριότητες γνώσεων, θεσμούς τεχνολογικής μάθησης, και ψηφιακούς χώρους επικοινωνίας, ώστε να μεγιστοποιείται η ικανότητα καινοτομίας της περιοχής αναφοράς της. Αποτελεί την πιο εξελιγμένη μορφή περιοχικών συστημάτων καινοτομίας, ένα σύστημα τρίτης γενιάς, μετά τα καινοτόμα clusters και τις μαθησιακές περιφέρειες. Αποτελείται από 3 επίπεδα, το φυσικό, το θεσμικό και το ψηφιακό [26].

Επίπεδο 1°: Είναι το επίπεδο βάσης και περιλαμβάνει τις δραστηριότητες έντασης-γνώσεων της πόλης. Πρόκειται για δραστηριότητες μεταποίησης και υπηρεσιών που (συνήθως) αυτοοργανώνονται σε συστάδες και συνοικίες (clusters). Η εγγύτητα στο φυσικό χώρο είναι το άμεσο συνδετικό στοιχείο που ενοποιεί τις επιμέρους μονάδες και οργανισμούς σε ένα ενιαίο σύστημα παραγωγής και καινοτομίας. Το επίπεδο αυτό συσχετίζεται με την ευφυΐα, εφευρετικότητα και τη δημιουργικότητα τους.

Επίπεδο 2°: Περιλαμβάνει τους θεσμικούς μηχανισμούς κοινωνικής συνεργασίας για μάθηση και καινοτομία. Το επίπεδο αυτό σχετίζεται με τη συλλογική ευφυΐα του πληθυσμού της πόλης που απορρέει από τους θεσμούς κοινωνικής συνεργασίας. Είναι η ευφυΐα ενός πληθυσμού, όπως αυτή κωδικοποιείται μέσα σε καθιερωμένες πρακτικές και καθημερινές ρουτίνες εργασίας.

Επίπεδο 3°: Αποτελείται από τα ψηφιακά εργαλεία και εφαρμογές υποστήριξης της καινοτομίας τα οποία είναι βασικά για τη δημιουργία ενός εικονικού περιβάλλοντος χειρισμού της πληροφορίας και των γνώσεων. Το επίπεδο αυτό υποστηρίζει τόσο τις ατομικές επιλογές του, όσο και τη συλλογική επικοινωνία και συνεργασία. Πρόκειται για το δημόσιο σύστημα ψηφιακής επικοινωνίας, με ψηφιακά δίκτυα και υπηρεσίες, εφαρμογές τεχνητής ευφυΐας, ψηφιακούς χώρους και εργαλεία επίλυσης προβλημάτων, την επικοινωνία σε εικονικό περιβάλλον, το δημόσιο ψηφιακό περιεχόμενο που είναι στη διάθεση του πληθυσμού της πόλης.



Πλεονεκτήματα IoT

Ορισμένα από τα πλεονεκτήματα του IoT αναλύονται παρακάτω:

Δεδομένα (Data): Όσο μεγαλύτερος είναι ο αριθμός των πληροφοριών τόσο πιο εύκολη είναι και η λήψη της ορθής απόφασης.

Παρακολούθηση (Tracking): Οι υπολογιστές παρακολουθούν την ποιότητα και τη βιωσιμότητα των αντικειμένων στο σπίτι.

Ώρα-Χρόνος (Time): Η ποσότητα του χρόνου που εξοικονομείται από την παρακολούθηση των αντικειμένων στο σπίτι είναι αρκετά μεγάλη.

Χρήμα (Money): Η οικονομική πλευρά είναι το μεγαλύτερο πλεονέκτημα καθώς μέσω του IoT μπορεί και γίνεται άμεσος έλεγχος σε όλους τους οικονομικούς τομείς της ζωής και της καθημερινότητας [4].

Μειονεκτήματα IoT

Ορισμένα από τα μειονεκτήματα του IoT παρατίθενται παρακάτω:

Συμβατότητα (Compatibility): Μέχρι σήμερα, δεν υπάρχει κάποιο πρότυπο για την τοποθέτηση και την παρακολούθηση ετικετών μέσω της χρήσης αισθητήρων.

Πολύπλοκότητα (Complexity): Υπάρχουν πολλές πιθανότητες αποτυχίας λόγω των πολύπλοκων συστημάτων υπάρχουν.

Προστασία προσωπικών δεδομένων / Ασφάλεια (Privacy/Security): Η προστασία των προσωπικών δεδομένων αποτελεί ένα μεγάλο ζήτημα για το IoT. Όλα τα δεδομένα πρέπει να είναι κρυπτογραφημένα για να μην γίνονται γνωστά σε τρίτους.

Ασφάλεια (Safety): Υπάρχει πιθανότητα να παραβιαστεί κάποιο λογισμικό με αποτέλεσμα να παραβιαστούν προσωπικά δεδομένα [4].

Ασύρματες λύσεις συνδεσιμότητας

Οι ασύρματες λύσεις συνδεσιμότητας χωρίζονται σε μικρές και σε μεγάλες εμβέλειες λύσεις. Παρακάτω παρουσιάζονται αυτές οι δύο κατηγορίες και εξαρτάται από την απόσταση που μεταφέρουν δεδομένα.

Μικρής Εμβέλειας Ασύρματες Λύσεις

Οι λύσεις συνδεσιμότητας μικρής εμβέλειας μεταφέρουν δεδομένα σε μικρές φυσικές αποστάσεις με την απόσταση μεταξύ των συσκευών που συλλέγουν τα δεδομένα και της πύλης που τις επεξεργάζεται να είναι μικρότερη των 150 μέτρων.

Bluetooth

Το Bluetooth Low Energy χρησιμοποιεί τη συχνότητα των 2.4 GHz για να επιτύχει μέγιστη ταχύτητα μετάδοσης (throughput) περίπου 2 Mbps. Το Bluetooth πρόκειται για μια τεχνολογία επικοινωνίας που παρουσιάζει μέτριο ρυθμό μεταφοράς δεδομένων για εφαρμογές μικρής εμβέλειας, με χαμηλή κατανάλωση ενέργειας. Η μέγιστη εμβέλεια που έχει είναι μέχρι 100m [42].



Wi-Fi HaLow (IEEE802.11ah)

Το Wi-Fi είναι μια τεχνολογία ασύρματης δικτύωσης τοπικής εμβέλειας, που επιτρέπει στις ηλεκτρονικές συσκευές να δικτυωθούν και βασίζεται στο πρότυπο 802.11 του Ινστιτούτου Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (Institute of Electrical and Electronics Engineers - IEEE). Το Wi-Fi παρέχει μεγαλύτερη απόσταση κάλυψης και μεγαλύτερο ρυθμό μετάδοσης δεδομένων. Η τεχνολογία Wi-Fi HaLow είναι κατάλληλη για μικρής εμβέλειας και χαμηλής ισχύος συσκευές IoT και βασίζεται στο IEEE 802.11ah και ενεργεί σε ζώνη συχνοτήτων μικρότερη από 1 GHz. Η μέγιστη εμβέλεια που έχει είναι μέχρι 1 km και μέγιστη απόδοση 40 Mbps [42].



Z-Wave

Η τεχνολογία Z-Wave έχει σχεδιαστεί για αισθητήρες, έξυπνο φωτισμό και ελαχιστοποιεί την κατανάλωση ενέργειας. Η συχνότητα είναι 800-900 MHz και έχει μέγιστη εμβέλεια μέχρι και 100m με ταχύτητες μετάδοσης έως και 100 Kbps [42],



Zigbee

Το ZigBee πρόκειται για μια τεχνολογία που τρέχει κυρίως στα 2.4 GHz, έχει ρυθμό μετάδοσης 250 Kbps στα 2.4 GHz και είναι κατάλληλο για διακοπτόμενες μεταδόσεις δεδομένων από αισθητήρα ή συσκευή εισόδου. Οι αποστάσεις μετάδοσης είναι έως 100 μέτρα και χρησιμοποιείται σε εφαρμογές χαμηλού ρυθμού μετάδοσης δεδομένων, χρησιμοποιούν κλειδιά κρυπτογράφησης μήκους 128 bit. Η τεχνολογία αυτή έχει σημαντικά πλεονεκτήματα όπως υψηλή ασφάλεια, ευστάθεια [42].



NFC

Η τεχνολογία NFC λειτουργεί στη ζώνη συχνοτήτων 13.56 MHz και έχει ως βάση την τεχνολογία RFID. Υποστηρίζει ρυθμό μετάδοσης δεδομένων έως και 424 Kbps και η εμβέλεια είναι 10 εκατοστά. Επιτρέπει τη πραγματοποίηση συναλλαγών ανέπαφα και την πρόσβαση σε ψηφιακό περιεχόμενο καθώς και τη σύνδεση συσκευών [42],



Μεγάλης Εμβέλειας Ασύρματες Λύσεις (Low Power Wide Area Network, LPWAN)

Οι τεχνολογίες LPWAN χωρίζονται σε δύο κατηγορίες, σε αυτές που χρησιμοποιούν αδειοδοτημένο φάσμα και σε αυτές που δεν χρειάζονται άδεια. Παρακάτω, πέρα από τις τεχνολογίες που ανήκουν σε αυτές τις κατηγορίες, θα αναλυθούν πιο συγκεκριμένα οι NB - IoT τεχνολογία που εκπέμπει σε αδειοδοτούμενο φάσμα αλλά και η τεχνολογία LoRa που δεν χρειάζεται κάποια άδεια.

LPWAN - μη αδειοδοτημένο φάσμα

LoRa-LoRaWAN

Η τεχνολογία LoRa έχει αναπτυχθεί από την εταιρία Semtech και αποτελεί ένα νέο ασύρματο πρωτόκολλο σχεδιασμένο για επικοινωνία μεγάλης εμβέλειας και χαμηλής ισχύος. Η συμμαχία LoRa (LoRa Alliance) πρόκειται για έναν οργανισμό μη κερδοσκοπικού χαρακτήρα που αποτελεί τον βασικό φορέα ανάπτυξης της συγκεκριμένης τεχνολογίας [6],



Η LoRa είναι μια τεχνολογία chirp-based διασποράς φάσματος (spread-spectrum), με μεγαλύτερο εύρος ζώνης αϊτό αυτό των ανταγωνιστών της. Λόγω της τεχνικής διαμόρφωσης και της ενσωματωμένης δυνατότητας διόρθωσης σφαλμάτων (forward error correcting, FEC), το σήμα LoRa μπορεί να μεταδώσει δεδομένα με ισχύ σήματος αρκετά κάτω από το επίπεδο θορύβου περιβάλλοντος (noise floor), επιτρέποντας με αυτόν τον τρόπο πολύ μεγάλες αποστάσεις επικοινωνίας. Ακόμα, προσφέρει αποτελεσματική αμφίδρομη λειτουργικότητα. Έτσι ως λύση είναι αποτελεσματική για τη λήψη μηνυμάτων από τελικά σημεία (endpoints), αλλά και για την αποστολή μηνυμάτων από σταθμούς βάσης σε τελικά σημεία (όπως για εφαρμογές εντολών και ελέγχου) [7].

Πρόκειται για μια τεχνολογία φυσικού επιπέδου, που ρυθμίζει τα σήματα στη ζώνη ISM sub - 1 GHz, χρησιμοποιώντας μια ιδιόκτητη τεχνική διασποράς φάσματος (spread spectrum). Χρησιμοποιεί μη αδειοδοτημένες ζώνες ISM, 863-870 MHz στην Ευρώπη, 902-928 MHz στη Βόρεια Αμερική, 779-787 MHz & 470-510 MHz στην Κίνα και 915-928 MHz στην Αυστραλία. Η αμφίδρομη επικοινωνία παρέχεται από την τεχνική διαμόρφωσης, που είναι παράγωγο της chirp διασποράς φάσματος (Chirp Spread Spectrum, CSS), που απλώνει ένα σήμα στενής ζώνης σε ένα μεγαλύτερο εύρος ζώνης καναλιού [8].

Το δίκτυο LoRa εφαρμόζει μια τεχνική προσαρμοστικής διαμόρφωσης με πολυκαναλικό, πολλαπλών διαύλων (multi-modem) πομποδέκτη στο σταθμό βάσης, με σκοπό τη λήψη πολλαπλού αριθμού μηνυμάτων από τα κανάλια. Η διαμόρφωση διασποράς φάσματος παρέχει ορθογώνιο διαχωρισμό, μεταξύ των σημάτων χρησιμοποιώντας ένα μοναδικό συντελεστή διασποράς (spreading factor) στο μεμονωμένο σήμα. Αυτή η μέθοδος παρέχει πλεονεκτήματα στη διαχείριση του ρυθμού μετάδοσης δεδομένων. Η σχέση μεταξύ του απαιτούμενου ρυθμού μετάδοσης δεδομένων (data bit rate), του ρυθμού chirp (chirp rate) και του ρυθμού συμβόλων (symbol rate) στην τεχνική διαμόρφωσης LoRa ορίζεται [9]:

$$R_b = SF * \frac{1}{2^{SF}} \frac{bits}{s} \cdot BW$$

R_b = ο ρυθμός μετάδοσης δεδομένων LoRa - modulation bit rate,

SF = συντελεστή διασποράς - spreading factor και

BW = εύρος ζώνης διαμόρφωσης (Hz) - modulation bandwidth.

LoRaWAN

Το LoRaWAN αποτελεί το επίπεδο δικτύου. Με τον όρο LoRa ορίζεται το φυσικό στρώμα (το chip) ενώ με τον όρο LoRaWAN ορίζεται το MAC στρώμα. Το LoRaWAN έχει σχεδιαστεί με σκοπό τη βελτιστοποίηση της λειτουργίας των LPWAN στη διάρκεια ζωής της μπαταρίας, τη χωρητικότητα, το εύρος αλλά και το κόστος.

A) Αρχιτεκτονική

Το LoRaWAN χρησιμοποιεί μια τοπολογία αστέρα (αρχιτεκτονική αστέρα μεγάλης εμβέλειας, Long Range Star Architecture). Οι πύλες χρησιμοποιούνται για την αναμετάδοση των μηνυμάτων μεταξύ των τελικών συσκευών και ενός διακομιστή

δικτύου. Σε ένα δίκτυο LoRaWAN, οι EDs δε συνδέονται με μια συγκεκριμένη πύλη. Αντ' αυτού, τα δεδομένα, που μεταδίδονται από μια ED, τυπικά λαμβάνονται από πολλαπλές GWs. Οι τερματικές συσκευές επικοινωνούν με μία ή περισσότερες πύλες, μέσω επικοινωνίας LoRa μονού άλματος (single-hop), ενώ οι πύλες συνδέονται με τον κεντρικό διακομιστή δικτύου, μέσω τυπικών συνδέσεων IP. Η επικοινωνία μεταξύ των συσκευών και των πυλών διανέμεται σε διαφορετικά κανάλια συχνότητας και οι ταχύτητες μετάδοσης δεδομένων καθορίζονται, ανάλογα με την εμβέλεια του δικτύου και τη διάρκεια του μηνύματος. Την επιλογή αυτή διαχειρίζεται μια υποδομή δικτύου LoRaWAN, η οποία επιλέγει το ρυθμό μετάδοσης δεδομένων και το κανάλι για κάθε συσκευή, χρησιμοποιώντας ένα προσαρμοστικό σχήμα μετάδοσης δεδομένων (Adaptive Data Rate, ADR) [10].

Ένα δίκτυο LoRaWAN αποτελείται από τα ακόλουθα στοιχεία:

Τελική συσκευή (End-Device, ED): Μπορεί να είναι οτιδήποτε στέλνει ή λαμβάνει πληροφορίες. Δεν υπάρχει πραγματικός ορισμός μιας ED, αλλά συνήθως αναφέρεται σε αισθητήρες (sensors), ανιχνευτές (detectors), ενεργοποιητές (actuators) και οτιδήποτε πραγματοποιεί ανίχνευση και έλεγχο.

Πύλη (GateWay, GW): Ονομάζεται επίσης μόντεμ (modem) ή σημείο πρόσβασης (access point). Χρησιμοποιείται για την προώθηση μηνυμάτων από και προς μια ED και το Διακομιστή Δικτύου (Network Server, NS). Στο LoRaWAN, οι EDs δε συνδέονται με την GW. Αντ' αυτού, οποιοδήποτε μήνυμα από μια ED, που λαμβάνεται από την GW θα παραδοθεί στο Διακομιστή Δικτύου.

Διακομιστής Δικτύου (Network Server, NS): Είναι υπεύθυνος για:

- Παρακολούθηση των GWs και EDs.
- Συγκέντρωση των εισερχομένων δεδομένων.
- Δρομολόγηση και προώθηση των εισερχομένων μηνυμάτων στον αντίστοιχο διακομιστή εφαρμογών (Application Server, AS).
- Αφαίρεση διπλοτύπων. Αφαιρεί τα διπλά μηνύματα που ελήφθησαν από μια ED, μέσω πολλαπλών GWs.
- Επιλογή μιας GW στην κατερχόμενη ζεύξη, με βάση την υψηλότερη αντοχή λήψης σήματος (Received Signal Strength, RSS).
- Αποθήκευση μηνυμάτων κατερχόμενης ζεύξης μέχρι να ξυπνήσουν οι προβλεπόμενες EDs.

Διακομιστής εφαρμογών (Application Server, AS): Αντιπροσωπεύει την εφαρμογή, για την ανάλυση των μηνυμάτων που ελήφθησαν από μια ED. Για παράδειγμα, σε μια εφαρμογή συστήματος ψύξης, αν η θερμοκρασία ανεβαίνει πάνω από 25o C, μπορεί να αποφασίσει να ενεργοποιήσει τον κλιματισμό για να την μειώσει [10].

LoRaWAN Επικοινωνία

Κάθε συσκευή (ED) ενός δικτύου εξυπηρετεί διαφορετικές εφαρμογές και έχει διαφορετικές προδιαγραφές. Το LoRaWAN εφαρμόζει διαφορετικές κλάσεις στους κόμβους. Οι κλάσεις είναι τρεις A, B και C, και προκύπτουν από το tradeoff μεταξύ της καθυστέρησης για downlink επικοινωνία και της διάρκειας ζωής της μπαταρίας (battery life time).

Κλάση A: Οι συσκευές Class A επιτρέπουν την αμφίδρομη επικοινωνία κατά την οποία κάθε μετάδοση ακολουθούν 2 μικρές λήψεις. Οι κόμβοι αυτής της κλάσης καταναλώνουν την χαμηλότερη ισχύ σε σχέση με τις συσκευές των άλλων κλάσεων, ωστόσο έχουν περιορισμό ως προς την downlink επικοινωνία. Η λειτουργικότητα της κλάσης A σύμφωνα με την οποία το πρώτο παράθυρο λήψης (Receive Window) Rx1 ενεργοποιείται ακριβώς μετά την καθυστέρηση λήψης (Receive Delay), 1 sec μετά το τέλος της διαμόρφωσης ανερχόμενης ζεύξης (uplink modulation). Η δεύτερη υποδοχή Rx2 έρχεται ακριβώς μετά την καθυστέρηση λήψης, 2 sec μετά το τέλος της διαμόρφωσης ανερχόμενης ζεύξης. Ο δέκτης (receiver) παραμένει ενεργός μέχρι να αποδιαμορφωθεί το πλαίσιο κατερχόμενης ζεύξης (downlink frame).

Κλάση B: Οι συσκευές Class B εκτός από τις λειτουργίες των συσκευών Class A, επιτρέπουν τη λήψη σε προγραμματισμένες στιγμές. Αυτό επιτυγχάνεται, λαμβάνοντας ένα σήμα συγχρονισμού από το gateway. Έτσι ο server γνωρίζει ποιες χρονικές στιγμές η συσκευή είναι διαθέσιμη να δεχτεί κάποιο μήνυμα.

Κλάση C: Οι συσκευές Class C έχουν τη δυνατότητα να δέχονται μηνύματα οποιαδήποτε στιγμή πλην των στιγμών μετάδοσης [10].

Για να επιτευχθεί η ασφάλεια και η ακεραιότητα των μηνυμάτων ανερχόμενης και κατερχόμενης ζεύξης μεταξύ ED και GW και για να αποτραπεί από ένα NS η ανάγνωση περιεχομένων μηνυμάτων, που σχετίζονται με άλλο δίκτυο ή υποδομή, το LoRaWAN ορίζει δύο διαφορετικά κλειδιά ασφαλείας. Αυτά τα δύο κλειδιά είναι:

- Το κλειδί συνόδου δικτύου (Network Session Key, NwkSKey): Χρησιμοποιείται για την κρυπτογράφηση ολόκληρου του πλαισίου (κεφαλίδες + ωφέλιμο φορτίο) σε περίπτωση, που αποστέλλεται μια εντολή MAC. Όταν αποστέλλονται δεδομένα, αυτό το κλειδί χρησιμοποιείται για την υπογραφή του μηνύματος, που επιτρέπει στο NS να επαληθεύσει την ταυτότητα του αποστολέα.
- Το κλειδί συνόδου εφαρμογής (Application Session Key, AppSKey):

Χρησιμοποιείται για την κρυπτογράφηση του ωφέλιμου φορτίου στο πλαίσιο. Αυτό το κλειδί δε χρειάζεται να είναι γνωστό από το NS. Ο AS αποκρυπτογραφεί τις πληροφορίες χρησιμοποιώντας το ίδιο κλειδί [10].

Μια ED δεν μπορεί να συμμετέχει στο δίκτυο LoRa WAN, εκτός αν έχει ενεργοποιηθεί, όπου και απαιτούνται τρεις τύποι πληροφοριών:

- Device Address (DevAddr): Αποτελείται από ένα αναγνωριστικό μήκους 32 bit που είναι μοναδικό στο δίκτυο. Αυτή η διεύθυνση αντιστοιχεί σε μια διεύθυνση IP ενός δικτύου TCP/IP. Είναι παρούσα σε κάθε πλαίσιο δεδομένων. Μοιράζεται μεταξύ ED, NS και AS.
- Network Session Key (NwkSKey): Αποτελείται από ένα κλειδί κρυπτογράφησης AES μήκους 128 bits, που είναι μοναδικό ανά NS. Αυτό το κλειδί μοιράζεται μεταξύ ED και NS. Χρησιμοποιείται για την παροχή ακεραιότητας μηνυμάτων και ασφάλειας για την επικοινωνία.
- Application Session Key (AppSKey): Είναι ένα κλειδί κρυπτογράφησης AES μήκους 128 bits, που είναι μοναδικό ανά AS. Αυτό το κλειδί μοιράζεται μεταξύ ED και AS. Χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων εφαρμογών και για την παροχή ασφάλειας για το φορτίο εφαρμογής (application payload) [10].

Μετά την ενεργοποίηση, μια ED εντάσσεται στο δίκτυο LoRaWAN και αρχίζει να στέλνει ή να λαμβάνει μηνύματα δεδομένων. Αυτά τα μηνύματα χρησιμοποιούνται για τη μεταφορά, τόσο των εντολών MAC, όσο και των δεδομένων εφαρμογής, τα οποία μπορούν ταυτόχρονα να συνδυαστούν σε ένα μόνο μήνυμα. Το LoRa επιτρέπει σε ένα ED να χρησιμοποιεί κάθε πιθανό ρυθμό (data rate) για τη μετάδοση του μηνύματος, χρησιμοποιώντας την τεχνική Adaptive Data Rate (ADR), όπως προαναφέρθηκε. Αυτή η τεχνική χρησιμοποιείται από το δίκτυο ή το επίπεδο εφαρμογής της ED για τη διαχείριση, προσαρμογή και βελτίωση του ρυθμού μετάδοσης δεδομένων μιας ED [10].

EDs και ASs μπορούν να ζητήσουν επιβεβαίωση μηνυμάτων. Στην περίπτωση (a) στην εικόνα 14, η ED μεταδίδει μια επιβεβαίωση εύκολα, δεδομένου ότι το ACK είναι μια λειτουργία αποστολής (uplink), όσον αφορά την ED. Στην περίπτωση (b) στην εικόνα 14, το δίκτυο θα στείλει την επιβεβαίωση, χρησιμοποιώντας ένα από τα παράθυρα λήψης, που ανοίγει από μια ED μετά την αποστολή. Οι επιβεβαιώσεις υποβάλλονται μόνο σε απάντηση στο τελευταίο ληφθέν μήνυμα και δεν επαναμεταδίδονται [10],

Smart Cities

Ορισμός

Η έξυπνη πόλη πρόκειται για μια πόλη που χρησιμοποιεί τις νέες τεχνολογίες με σκοπό την παροχή των απαραίτητων υπηρεσιών και υποδομών για να αυξήσει τα κοινωνικά, οικονομικά και περιβαλλοντικά οφέλη τα οποία συνδράμουν στη βελτίωση της ποιότητας ζωής και στη βιώσιμη αστική ανάπτυξη.



Χαρακτηριστικά

- Έξυπνη Οικονομία (Smart Economy): Η συμβολή της τεχνολογίας στην οικονομία είναι θεμελιώδης για την ανάπτυξη της παραγωγικότητας και της ανταγωνιστικότητας των προϊόντων και των υπηρεσιών. Με την αξιοποίηση της τεχνολογίας αναπτύσσονται οι αγορές καθώς και το διεθνές επενδυτικό ενδιαφέρον δημιουργώντας ταχύτερη ανάπτυξη και παραγωγικότητα. Ακόμα, η συμβολή της καινοτομίας βελτιώνει την παραγωγική λειτουργία, υλοποιούνται έργα και προσφέρονται προϊόντα και υπηρεσίες με μικρές και μεγάλες επιχειρήσεις. Η οικονομία μιας έξυπνης πόλης βασίζεται στην καινοτομία, την

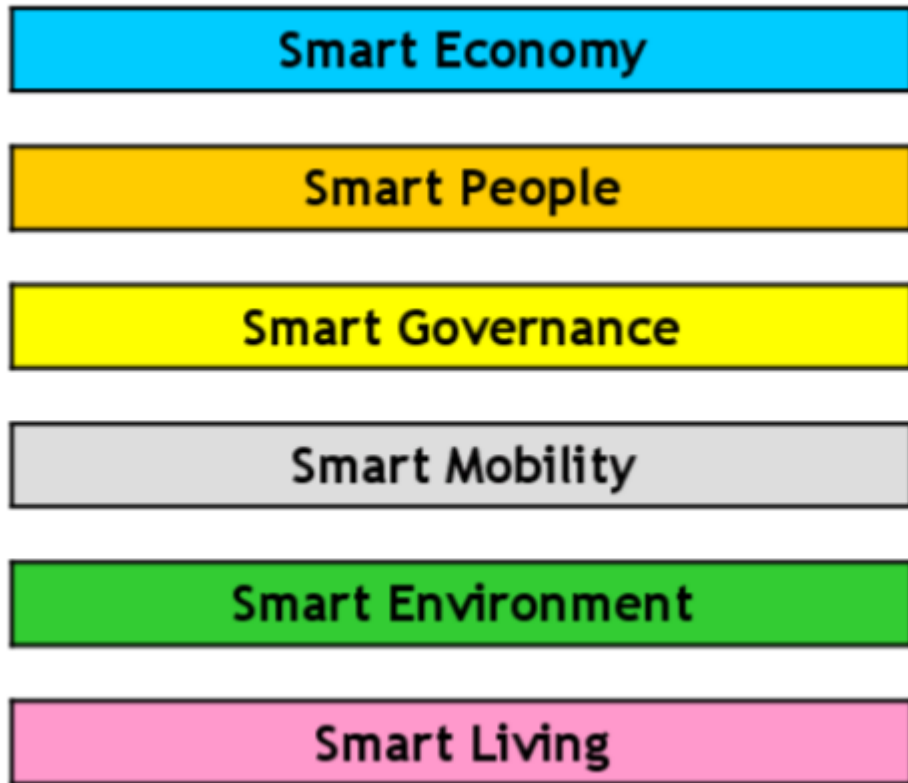
παραγωγικότητα και την επιχειρηματικότητα και για αυτό το λόγο κάθε Έξυπνη Οικονομία) πρέπει να προσαρμόζεται στις αλλαγές [21]. Έξυπνη Διακυβέρνηση (Smart Governance): Πρόκειται για το μέλλον των δημόσιων υπηρεσιών με σκοπό τη μεγαλύτερη αποτελεσματικότητα και συμμετοχή των πολιτών στη λειτουργία της διοίκησης. Στόχος είναι η λειτουργία της πόλης με μικρότερο κόστος διοίκησης και να είναι και αποτελεσματική [21].

Έξυπνοι Ανθρωποι (Smart People): Οι Έξυπνοι Ανθρωποι χαρακτηρίζονται και από την ποιότητα της κοινωνικής αλληλεπίδρασης σχετικά με την ολοκλήρωση και τη δημόσια ζωή. Είναι σημαντικό να υπάρχει πρόσβαση στην εκπαίδευση και την κατάρτιση με στόχο όλοι οι πολίτες να συμμετέχουν σε νέες δράσεις, στα δημόσια δρώμενα, να είναι ανοιχτοί σε νέες, καινοτόμες ιδέες και να χαρακτηρίζονται από δημιουργικότητα. "Έξυπνος" είναι ο ενεργός και ενημερωμένος άνθρωπος και δίχως αυτούς δεν υφίστανται "έξυπνες" πόλεις [21].

Έξυπνη Κινητικότητα (Smart Mobility): Η έξυπνη κινητικότητα περιλαμβάνει την εγκατάσταση των τεχνολογιών πληροφορίας και επικοινωνίας (ΤΠΕ), σε Μέσα Μαζικής Μεταφοράς, αυτοκίνητα, με σκοπό την εξοικονόμηση χρόνου, τη βελτίωση της μετακίνησης και αποδοτικότητας, την εξοικονόμηση δαπανών, τη μείωση εκπομπών διοξειδίου του άνθρακα με στόχο τη βελτίωση των υπηρεσιών και παροχή πληροφοριών [22],

Έξυπνη Διαβίωση (Smart Living): Πρόκειται για τις υπηρεσίες του κράτους οι οποίες βελτιώνουν την ποιότητα ζωής στην πόλη. Αξιοποιούνται οι υποδομές και δημιουργείται ανάπτυξη στους τομείς πολιτισμού, ασφάλειας, υγείας και τουρισμού. Ακόμα, δημιουργείται κοινωνική συνοχή με νέες προοπτικές σε εκπαιδευτικό, πολιτιστικό και τουριστικό επίπεδο [23].

Έξυπνο Περιβάλλον (Smart Environment): Γνωρίζοντας τα οφέλη του περιβάλλοντος χρησιμοποιείται η τεχνολογία με σκοπό την επίτευξη της βιωσιμότητας αλλά και της καλύτερης διαχείρισης και προστασίας των φυσικών πόρων του περιβάλλοντος. Το έξυπνο περιβάλλον χαρακτηρίζεται από τη χρήση της έξυπνης ενέργειας, συγκαταλέγοντας τις ανανεώσιμες πηγές ενέργειας, τα ενεργειακά δίκτυα μέσω ΤΠΕ, τον έλεγχο της ρύπανσης, την ανακαίνιση κτιρίων και υποδομών, τα πράσινα κτήρια, την πράσινη αστική ανάπτυξη και σχεδιάσμά, την αποδοτικότητα χρήσης πόρων, την ανακύκλωση και επαναχρησιμοποίηση υλικών [24],



Πλεονεκτήματα Έξυπνης Πόλης

Αξιοποιώντας τις "έξυπνες" λύσεις σε μια πόλη προκύπτουν τα παρακάτω οφέλη

Βελτίωση της καθημερινότητας των ανθρώπων

Εξοικονόμηση πόρων, ενέργειας, χρήματα

Δημιουργία εσόδων

Ανάπτυξη οικολογικών πρακτικών

Προβλήματα Έξυπνων Πόλεων

Τα προβλήματα που συνδέονται με τις λύσεις των έξυπνων πόλεων προκύπτουν συνήθως από τις παρακάτω πηγές [28]:

Η έξυπνη πόλη δεν αντιμετωπίζεται όπως πραγματικά είναι, δηλαδή ένα περίπλοκο σύστημα που αποτελείται από πολλές παραμέτρους, διαφορετικά αλλά και ανταγωνιστικά συμφέροντα.

Η έξυπνη πόλη εστιάζει στη δημιουργία τεχνικών και τεχνοκρατικών μορφών διακυβέρνησης που αποσκοπούν σε συμφέροντα μεγάλων εταιρειών ή κυβερνήσεων παραβλέποντας κάποιες φορές λύσεις που είναι προσανατολισμένες στον πολίτη.

Με τη δημιουργία των τεχνολογικών λύσεων οι πόλεις αντιμετωπίζονται ως αγορές, δίνοντας μια συγκεκριμένη λύση, χωρίς αυτή να έχει προσαρμοστεί στις ανάγκες κάθε πόλης.

Οι τεχνολογίες που χρησιμοποιούνται έχουν κοινωνικές, πολιτικές καθώς και ηθικές επιπτώσεις, παρόλο που εισάγονται νέες μορφές κοινωνικού ελέγχου και διακυβέρνησης, και έτσι διευκολύνεται η παραβίαση της ιδιωτικότητας.

Οι τεχνολογίες που χρησιμοποιούνται δεν προστατεύουν τα δεδομένα χρήστη. Ακόμα, οι δυσλειτουργικές συσκευές μπορούν να προκαλέσουν τη δημιουργία ευπαθών συστημάτων ασφάλειας.

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) πραγματοποίησαν μελέτη σχετικά με την ψηφιακή ασφάλεια των δημόσιων συγκοινωνιών σε μια έξυπνη πόλη. Σύμφωνα με την μελέτη ένα έξυπνο σύστημα δημόσιων συγκοινωνιών είναι ευάλωτο σε ψηφιακές κακόβουλες επιθέσεις. Υπάρχουν δύο κατηγορίες επιθέσεων, οι κακόβουλες και οι τυχαίες. Σχετικά με τις κακόβουλες επιθέσεις, οι ωτακουστές (eavesdropping) πρόκειται για προγράμματα τα οποία έχουν σα σκοπό την παρακολούθηση της κίνησης του δικτύου σε επίπεδο IP πακέτων και την ανακατασκευή των μηνυμάτων και έτσι υποκλέπτουν τους κωδικούς πρόσβασης. Η υποκλοπή αναφέρεται σε επιθέσεις κατά της εμπιστευτικότητας του συστήματος. Ο χαλκός είναι ευάλωτος σε επιθέσεις και οι εταιρείες επενδύουν σε ασύρματες υποδομές για τη μείωση του κινδύνου κακόβουλης επίθεσης. Επιπρόσθετα, στην κατηγορία των κακόβουλων επιθέσεων εντάσσεται και η μη εξουσιοδοτημένη πρόσβαση που γίνεται με τη διαδικασία αντιγραφής, τροποποίησης ή καταστροφής δεδομένων και πραγματοποιείται με βίαιες επιθέσεις αλλά και με χειραγώγηση και με την υποκλοπή συνθηματικών. Τέλος, είναι η συντονισμένη άρνηση εξυπηρέτησης λόγω του ότι καταρρέει ένα δίκτυο λόγω υπερφόρτωσης.

Η άλλη κατηγορία είναι οι τυχαίες επιθέσεις που δεν είναι σκόπιμες. Πρόκειται για αποτυχία του υλικού/λογισμικού που μπορεί να σχετίζεται με την έλλειψη συντήρησης. Επιπλέον, λάθη από πλευράς του operator που γίνονται στη συντήρηση ή αναβάθμιση μπορεί να προκαλέσουν ζημιά στα δεδομένα και να γίνουν ευάλωτα. Η διακοπή ρεύματος μπορεί να επηρεάσει τη διαθεσιμότητα ενός συστήματος και να το κάνει ευάλωτο. Τέλος, τα φυσικά φαινόμενα, όπως οι βροχές αποτελούν λόγο που ενδέχεται να βλάψουν τη λειτουργία των τηλεπικοινωνιακών δικτύων [29].

Αντιμετώπιση κινδύνων Έξυπνων Πόλεων

Για την αντιμετώπιση των κινδύνων προς την ασφάλεια και την ιδιωτικότητα είναι σημαντικό να εφαρμοστούν μέτρα πρόληψης που να ανήκουν στις παρακάτω κατηγορίες:

- 1) Αυθεντικοποίηση:** Όπου με βάση αυτή θα γίνεται επιβεβαίωση ότι είναι όντως η ταυτότητα του χρήστη αυτή και δεν γίνεται κάποια παραβίαση.
- 2) Εξουσιοδότηση:** Στο σύστημα εάν βρίσκονται αρκετοί χρήστες σε κάθε έναν από αυτούς εκχωρούνται από τον διαχειριστή τα ανάλογα δικαιώματα με βάση το ρόλο τους και τις υποχρεώσεις τους.
- 3) Αναγνώριση:** Πραγματοποιείται έλεγχος για το εάν τα δεδομένα που ζητούνται απαιτούν αυθεντικοποίηση αλλά και εξουσιοδότηση.
- 4) Κρυπτογραφία & Ανωνυμία:** Τα δεδομένα πρέπει να αποθηκεύονται κρυπτογραφημένα και να χρησιμοποιούνται μηχανισμοί ταυτοποίησης και εξουσιοδότησης χρηστών. Η κρυπτογράφηση πρόκειται για μια διεργασία

μετασχηματισμού ενός μηνύματος σε μια μη κατανοητή μορφή με τη χρήση κάποιου κρυπτογραφικού αλγόριθμου με σκοπό αυτό το μήνυμα να μην είναι αναγνώσιμο από τρίτα άτομα. Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος πραγματοποιείται μέσω ενός αλγορίθμου κρυπτογράφησης και ενός κλειδιού κρυπτογράφησης. Ακόμα, όσον αφορά την ανωνυμία πρόκειται για μια κατάσταση, όπου οι πληροφορίες που παρέχονται από τους χρήστες ενός συστήματος δεν πρέπει να παρέχουν αναφορές σχετικά με την ταυτότητά τους. Όμως, ρίσκο αποτελεί ότι με τη ψευδωνυμία και την ανωνυμία υπάρχει κίνδυνος να μη σκιαγραφούνται τα προφίλ των πολιτών σε περιπτώσεις στατιστικών.

Πρόβλημα

Διανύουμε μια περίοδο κατά την οποία το κύριο πρόβλημα που απασχολεί ολόκληρη την ανθρωπότητα είναι αυτό του ελέγχου της διασποράς του Covid – 19.

Σήμερα η πρόσβαση σε κλασσικά ασύρματα δίκτυα μεταφοράς δεδομένων 4G και τώρα 5G

- έχει υψηλό κόστος.
- απαιτεί κατανάλωση ενέργειας που σε ορισμένες περιπτώσεις είναι υψηλή.

Στην περίπτωση ασύρματων δικτύων Wi-fi έχουμε

- τον περιορισμό της απόστασης
- την υψηλή κατανάλωση ενέργειας.

Αν δεν μας ενδιαφέρει

- η μεγάλη ταχύτητα μεταφοράς δεδομένων και
- η μεταφορά μεγάλου όγκου δεδομένων ,

με αντάλλαγμα

- τη χαμηλή κατανάλωση ενέργειας
- την μεγάλη απόσταση μεταφοράς δεδομένων
- τον μικρό αριθμό αναγκαίων πυλών πρόσβασης στο cloud
- τη ανωνυμία στη μετάδοση δεδομένων

τότε μια πολύ καλή πρόταση είναι αυτή ενός LoRaWan όπως περιεγράφηκε σε προηγούμενη ενότητα.

Η αρχική ιδέα ήταν, η υλοποίησης ενός δικτύου μεταφοράς δεδομένων από αισθητήρες που κάνουν μετρήσεις χωρίς να απαιτείται η πρόσβαση σε κάποιο από τα διαθέσιμα εμπορικά δίκτυα δεδομένων. Το δεύτερο κριτήριο για την επιλογή του πρωτοκόλλου επικοινωνίας ήταν η κάλυψη μιας περιοχής με όσο το δυνατόν λιγότερες πύλες (Gateway). Η περίπτωση του LoRaWan και μάλιστα με διαθέσιμη εγκατεστημένη πύλη από το Πανεπιστήμιο Δυτικής Μακεδονίας ήταν μια πρόκληση.

Στις δοκιμές μας με τους διάφορους αισθητήρες προέκυψε η σκέψη ότι αισθητήρες βιομετρικών μετρήσεων θα μπορούσαν να μας δώσουν χρήσιμα δεδομένα για εξαγωγή συμπερασμάτων που αφορούν την εξάπλωση του covid-19.

Χωρίς να εγκαταλείπουμε την αρχική ιδέα που ήταν η καταγραφή δεδομένων που αφορούν έναν ποδηλάτη, θεωρήσαμε ότι θα ήταν πιο χρήσιμη πρόταση για ένα Δήμο να μελετήσουμε τη διασπορά του Covid-19 με αισθητήρες που έχουμε στη διάθεσή μας.

Πρόταση

Το σύστημά μας αποτελείται από δύο υποσυστήματα.

1. Σύστημα συλλογής δεδομένων από αισθητήρες.
2. Σύστημα μεταφοράς δεδομένων μέσω LoRaWan

Από πληροφορίες που έχουμε ο Covid – 19 επηρεάζει κυρίως το αναπνευστικό και συνεπώς το ποσοστό του κορεσμού του οξυγόνου στο αίμα. Ταυτόχρονα ένας άνθρωπος που νοσεί ξέρουμε ότι σε μεγάλο ποσοστό μπορεί να παρουσιάζει πυρετό.

Το 1^ο υποσύστημά μας λοιπόν διαθέτει :

1. Έναν αισθητήρα GPS οποίος μας δίνει πληροφορίες θέσης
2. Έναν αισθητήρα κορεσμού οξυγόνου και μέτρησης καρδιακών παλμών
3. Έναν αισθητήρα μέτρησης θερμοκρασίας.

Το 2^ο υποσύστημα διαθέτει ένα LoRa Shield που μπορεί να συνδεθεί σε εγκατεστημένη πύλη LoRaWan από το Πανεπιστήμιο Δυτικής Μακεδονίας με ABP μέθοδο. Μέσω LoRaWan τα δεδομένα μορφοποιούνται , μεταδίδονται και τέλος καταγράφονται σε επίπεδο εφαρμογής σε δωρεάν υπηρεσία που προσφέρεται σε Community Edition από το TTN(The Things NetWork) . Στη συνέχεια με διαθέσιμα Integrations όπως αυτό του TTNMapper ή με κώδικα σε οποιαδήποτε σύγχρονη γλώσσα μπορούν να αντληθούν τα δεδομένα μέσω API και στη συνέχεια να τα επεξεργαστούμε.

Τα δεδομένα που συλλέγουμε τοποθετούνται γεωγραφικά πάνω σε χάρτη Google και καταγράφονται κρίσιμες περιπτώσεις μετρήσεων. Κρίσιμη κατάσταση μέτρησης θα μπορούσε να είναι η συγκέντρωση σε μια περιοχή πολλών συμβάντων με:

- Χαμηλό κορεσμό οξυγόνου στο αίμα
- Υψηλό πυρετό
- Συνδυασμός μελλοντικά και από μετρήσεις άλλων αισθητήρων. Θα μπορούσε να συνεργαστεί με τον βιο-αισθητήρα του Γεωπονικού Πανεπιστημίου της Αθήνας.

Η καταγραφή δεδομένων είναι ανώνυμη και δεν υπάρχει θέμα παραβίασης προσωπικών δεδομένων.

Τα συμπεράσματα που θα προκύψουν μετά από στατιστική ανάλυση θα είναι ενδεικτικά, με την έννοια ότι σε κάποια περιοχή εντοπίζουμε αυξημένο κίνδυνο και συνεπώς προτείνεται η παραπέρα έρευνα με άλλα μέσα.

Το σύστημα θα μπορεί να μαθαίνει συγκρίνοντας τα αποτελέσματα που παράγει με αυτά που υπάρχουν στην πραγματικότητα και έτσι σιγά σιγά αυτό θα βελτιώνεται.

Πως θα μπορούσε να υλοποιηθεί στην πράξη ένα τέτοιο πείραμα πιλοτικά.

1^ο Σενάριο

- Θα μπορούσαν να μοιραστούν συσκευές σε κάθε σχολική μονάδα του Δήμου.
- Δεν είναι απαραίτητη η πρόσβαση στο Internet. Άρα υπάρχει η έννοια της φορητότητας.
- Τα παιδιά κατά την είσοδό τους στο σχολείο απλά βάζουν το δάκτυλό τους πάνω σε ειδικό υποδοχέα. Δεν υπάρχει πολυπλοκότητα στη μέτρηση.
- Καταγράφεται η μέτρηση και γίνεται αποστολή στο TTN.

2° Σενάριο

- Θα μπορούσαν να μοιραστούν συσκευές σε τυχαία σημεία του Δήμου Κοζάνης και υπηρεσίες .
- Οι εξυπηρετούμενοι μπορούν να κάνουν δειγματοληπτικά τη μέτρηση με αντάλλαγμα τη δωρεάν πληροφόρηση για τις μετρήσεις τους.
- Καταγράφεται η μέτρηση και γίνεται αποστολή στο TTN.

3° Μελλοντικό σενάριο

- Θα μπορούσε να μοιραστεί μια συσκευή δειγματοληπτικά σε τυχαίους πολίτες της πόλης.
- Σ' αυτή την περίπτωση θα μπορούσε να γίνεται συνεχής καταγραφή δεδομένων , με στόχο την αποτύπωση δεικτών που αφορούν την ποιοτική λειτουργία του συστήματος.

Υλοποίηση συστήματος

Hardware

Έγινε χρήση των Arduino Uno που είναι διαθέσιμα στο εργαστήριο. Ένα πρόβλημα που έπρεπε να αντιμετωπίσουμε ήταν αυτό της περιορισμένης μνήμης του Arduino Uno. Ο δεύτερος περιορισμός των Arduino Uno είναι οι διαθέσιμες αναλογικές και ψηφιακές θύρες. Για να αποφύγουμε υπερχειλίσσεις κώδικα και συγκρούσεις στη μεταφορά δεδομένων από τους αισθητήρες, αποφασίσαμε σε πρώτη φάση να χρησιμοποιήσουμε τουλάχιστον δύο Arduino Uno, ένα για κάθε υποσύστημα. Επίσης αντί να χρησιμοποιήσουμε σειριακή επικοινωνία μεταξύ των Arduino, κάναμε χρήση του I2C.

1ο Υποσύστημα

Αποτελείται από ένα Arduino Uno , έναν αισθητήρα DFRobots με το ολοκληρωμένο MAX30102 για τη μέτρηση καρδιακών παλμών κορεσμού οξυγόνου και θερμοκρασίας. Η σύνδεση του MAX30102 έγινε με I2C. Η βιβλιοθήκη που συνοδεύει τον αισθητήρα είναι αρκετά μεγάλη για να χωρέσει προγραμματιστικά και άλλος αισθητήρας.

Το 1° υποσύστημα λειτουργεί σαν master στο κανάλι I2C και στέλνει τα δεδομένα στο 2° υποσύστημα.

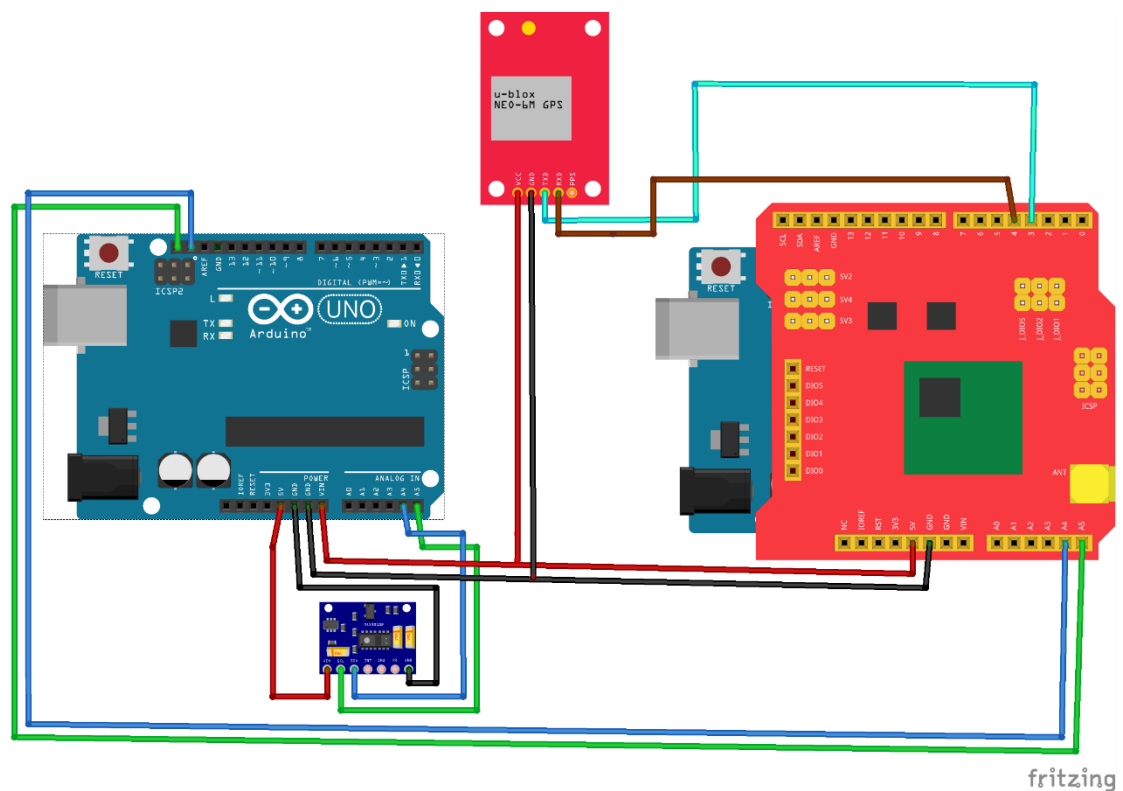
2° Υποσύστημα

Το δεύτερο υποσύστημα αποτελείται από ένα Arduino uno και ένα Dragino Lora Shield with GPS. Για το GPS χρησιμοποιήσαμε τη βιβλιοθήκη TinyGps ενώ για το LoRaWan τη βιβλιοθήκη LMIC της IBM. Η σύνδεση του GPS γίνεται μέσω σειριακής (3,4 pin) ενώ το Lora Shield δεσμεύει τις ψηφιακές 2,6,7,9,10. Επίσης η 0 και 1(Serial console) χρησιμοποιήθηκαν για debugging. Συμμετέχει σαν slave στο κανάλι I2C μεταξύ των δύο Arduino. Για το I2C χρησιμοποιήθηκε η βιβλιοθήκη Wire.

Για τη μορφοποίηση των δεδομένων χρησιμοποιήθηκε η βιβλιοθήκη Cayenne Lpp .

Η λήψη δεδομένων από τους αισθητήρες και η ενεργοποίηση της αποστολής μέσω LoraWan ενεργοποιείται με triggers.

Έγινε όσο ήταν δυνατόν μεγαλύτερη οικονομία στη χρήση μνήμης για να μπορέσει το σύστημά μας τελικά να είναι λειτουργικό.



Εικόνα 1- Κύκλωμα

Assembly List

Label	Part Type	Properties
M1	MAX30102	
Εξάρτημα1	Arduino Uno (Rev3)	τύπος Arduino UNO (Rev3)
Εξάρτημα2	Dragino LoRa Shield V1.4	form factor Arduino
Εξάρτημα3	u-blox NEO-6M GPS Breakout	
Εξάρτημα4	Arduino Uno (Rev3)	τύπος Arduino UNO (Rev3)

Software

Το προγραμματιστικό περιβάλλον που χρησιμοποιήθηκε ήταν αυτό του Arduino (micro c) κυρίως για τον προγραμματισμό των δύο υποσυστημάτων. Χρησιμοποιήθηκαν κατάλληλα βιβλιοθήκες και παραδείγματα που συνοδεύουν τα αντίστοιχα εξαρτήματα. Έγιναν επεκτάσεις και βελτιώσεις για τη δικιά μας υλοποίηση.

1^ο Υποσύστημα – Arduino uno master

```
/*!  
 * @file SPO2.ino  
 * @brief Display heart-rate and SPO2 on serial in real-time, normal SPO2 is within 95~100  
 * @n Try to fix the sensor on your finger in using to avoid the effect of pressure change on data output.  
 * @n This library supports mainboards: ESP8266, FireBeetle-M0, UNO, ESP32, Leonardo, Mega2560  
 * @copyright Copyright (c) 2010 DFRobot Co.Ltd (http://www.dfrobot.com)  
 * @licence The MIT License (MIT)  
 * @author [YeHangYu](hangyu.ye@dfrobot.com)  
 * @version V0.1  
 * @date 2020-05-29  
 * @url https://github.com/DFRobot/DFRobot_MAX30102  
 */  
#include <Wire.h>  
#include <DFRobot_MAX30102.h>  
DFRobot_MAX30102 particleSensor;  
/*  
Macro definition options in sensor configuration  
sampleAverage: SAMPLEAVG_1 SAMPLEAVG_2 SAMPLEAVG_4  
                SAMPLEAVG_8 SAMPLEAVG_16 SAMPLEAVG_32  
ledMode:      MODE_REDONLY MODE_RED_IR MODE_MULTILED  
sampleRate:   PULSEWIDTH_69 PULSEWIDTH_118 PULSEWIDTH_215 PULSEWIDTH_411  
pulseWidth:   SAMPLERATE_50 SAMPLERATE_100 SAMPLERATE_200 SAMPLERATE_400  
                SAMPLERATE_800 SAMPLERATE_1000 SAMPLERATE_1600 SAMPLERATE_3200  
adcRange:     ADCRANGE_2048 ADCRANGE_4096 ADCRANGE_8192 ADCRANGE_16384  
*/  
void setup()  
{  
  //Init serial  
  Serial.begin(9600);  
  Wire.begin(); // join i2c bus (address optional for master)  
  /*!  
  * @brief Init sensor  
  * @param pWire IIC bus pointer object and construction device, can both pass or not pass parameters (Wire in default)  
  * @param i2cAddr Chip IIC address (0x57 in default)  
  * @return true or false  
  */  
  while (!particleSensor.begin()) {  
    Serial.println("MAX30102 was not found");  
    delay(1000);  
  }  
  /*!  
  * @brief Use macro definition to configure sensor  
  * @param ledBrightness LED brightness, default value: 0x1F (6.4mA), Range: 0~255 (0=Off, 255=50mA)  
  * @param sampleAverage Average multiple samples then draw once, reduce data throughput, default 4 samples average  
  * @param ledMode LED mode, default to use red light and IR at the same time  
  * @param sampleRate Sampling rate, default 400 samples every second  
  * @param pulseWidth Pulse width: the longer the pulse width, the wider the detection range. Default to be Max range  
  * @param adcRange ADC Measurement Range, default 4096 (nA), 15.63(pA) per LSB  
  */  
  particleSensor.sensorConfiguration(/*ledBrightness=*/50, /*sampleAverage=*/SAMPLEAVG_4, \  
    /*ledMode=*/MODE_MULTILED, /*sampleRate=*/SAMPLERATE_100, \  
    /*pulseWidth=*/PULSEWIDTH_411, /*adcRange=*/ADCRANGE_16384);  
}
```

```

int32_t SPO2; //SPO2
int8_t SPO2Valid; //Flag to display if SPO2 calculation is valid
int32_t heartRate; //Heart-rate
int8_t heartRateValid; //Flag to display if heart-rate calculation is valid

void loop()
{
  Serial.println(F("Wait about four seconds"));
  particleSensor.heartRateAndOxygenSaturation(**SPO2=*&SPO2, **SPO2Valid=*&SPO2Valid, **heartRate=*&heartRate,
  /**heartRateValid=*&heartRateValid);
  // Print result
  Serial.print(F("heartRate="));
  Serial.print(heartRate, DEC);
  Serial.print(F(" , heartRateValid="));
  Serial.print(heartRateValid, DEC);
  Serial.print(F("; SPO2="));
  Serial.print(SPO2,DEC);
  Serial.print(F(" , SPO2Valid="));
  Serial.println(SPO2Valid, DEC);
  Wire.beginTransmission(8); // transmit to device #8
  Wire.write("x is "); // sends five bytes
  Wire.write(SPO2); // sends one byte
  Wire.endTransmission(); // stop transmitting
  delay(500);
}

```

2ο Υποσύστημα – Arduino -Dragino slave

```

/*****
 * Copyright (c) 2015 Thomas Telkamp and Matthijs Kooijman
 *
 * Permission is hereby granted, free of charge, to anyone
 * obtaining a copy of this document and accompanying files,
 * to do whatever they want with them without any restriction,
 * including, but not limited to, copying, modification and redistribution.
 * NO WARRANTY OF ANY KIND IS PROVIDED.
 *
 * This example sends a valid LoRaWAN packet with payload "Hello,
 * world!", using frequency and encryption settings matching those of
 * the The Things Network.
 *
 * This uses ABP (Activation-by-personalisation), where a DevAddr and
 * Session keys are preconfigured (unlike OTAA, where a DevEUI and
 * application key is configured, while the DevAddr and session keys are
 * assigned/generated in the over-the-air-activation procedure).
 *
 * Note: LoRaWAN per sub-band duty-cycle limitation is enforced (1% in
 * g1, 0.1% in g2), but not the TTN fair usage policy (which is probably
 * violated by this sketch when left running for longer)!
 *
 * To use this sketch, first register your application and device with
 * the things network, to set or generate a DevAddr, NwkSKey and
 * AppSKey. Each device should have their own unique values for these
 * fields.
 *
 * Do not forget to define the radio type correctly in config.h.
 *****/

```

```

#include <lmic.h>
#include <hal/hal.h>
#include <SoftwareSerial.h>
#include <TinyGPS.h>
#include <SPI.h>
TinyGPS gps;
#include <Wire.h>
SoftwareSerial ss(3,4 ); //3,4
#include <CayenneLPP.h>
CayenneLPP lpp(51);

```

```

static const PROGMEM u1_t NWKSKY[16] = { 0x0A, 0xC0, 0x16, 0xA4, 0xDD, 0x71, 0xE2, 0xF6, 0x85, 0x31, 0xAC, 0xEE, 0xF5,
0x63, 0x1E, 0x93 };
static const u1_t PROGMEM APPSKY[16] = { 0x3D, 0x2E, 0x31, 0x25, 0x9F, 0x4F, 0xC6, 0xDF, 0xCC, 0xCB, 0xAF, 0x75, 0xF9, 0x36,
0x3E, 0xF2 };
static const u4_t DEVADDR = 0x26013BCF ; // <-- Change this address for every node!
//static const PROGMEM u1_t NWKSKY[16] = {0xF4, 0x75, 0x8C, 0x4D, 0x7E, 0xB2, 0xC0, 0xC4, 0xB3, 0x1F, 0xD1, 0x2A, 0x09,
0xBB, 0x75, 0xBB};
//static const u1_t PROGMEM APPSKY[16] = {0x7A, 0xA2, 0x73, 0x8E, 0x89, 0xCD, 0xB8, 0x8A, 0x8F, 0x80, 0x22, 0xF6, 0x70,
0xC2, 0xAE, 0x69};
//static const u4_t DEVADDR = 0x260B0E58 ; // <-- Change this address for every node!

void os_getArtEui (u1_t* buf) { }
void os_getDevEui (u1_t* buf) { }
void os_getDevKey (u1_t* buf) { }
int x;
static osjob_t sendjob;

// Schedule TX every this many seconds (might become longer due to duty
// cycle limitations).
const unsigned TX_INTERVAL = 30;

// Pin mapping
const lmic_pinmap lmic_pins = {
    .nss = 10, //10
    .rxtx = LMIC_UNUSED_PIN,
    .rst = 9, //9
    .dio = {2,6,7}, //2,6,7
};

void onEvent (ev_t ev) {
    Serial.print(os_getTime());
    Serial.print(": ");
    Serial.println(ev);
    switch(ev) {
        case EV_SCAN_TIMEOUT:
            Serial.println(F("EV_SCAN_TIMEOUT"));
            break;
        case EV_BEACON_FOUND:
            Serial.println(F("EV_BEACON_FOUND"));
            break;
        case EV_BEACON_MISSED:
            Serial.println(F("EV_BEACON_MISSED"));
            break;
        case EV_BEACON_TRACKED:
            Serial.println(F("EV_BEACON_TRACKED"));
            break;
        case EV_JOINING:
            Serial.println(F("EV_JOINING"));
            break;
        case EV_JOINED:
            Serial.println(F("EV_JOINED"));
            break;
        case EV_RFU1:
            Serial.println(F("EV_RFU1"));
            break;
        case EV_JOIN_FAILED:
            Serial.println(F("EV_JOIN_FAILED"));
            break;
        case EV_REJOIN_FAILED:
            Serial.println(F("EV_REJOIN_FAILED"));
            break;
        case EV_TXCOMPLETE:
            Serial.println(F("EV_TXCOMPLETE (includes waiting for RX windows)"));
            if (LMIC.dataLen) {
                Serial.println(F("Received "));
                Serial.println(LMIC.dataLen);
                Serial.println(F(" bytes of payload"));
            }
            // Schedule next transmission
            os_setTimedCallback(&sendjob, os_getTime()+sec2osticks(TX_INTERVAL), do_send);
            break;
    }
}

```

```

    case EV_LOST_TSYNC:
        Serial.println(F("EV_LOST_TSYNC"));
        break;
    case EV_RESET:
        Serial.println(F("EV_RESET"));
        break;
    case EV_RXCOMPLETE:
        // data received in ping slot
        Serial.println(F("EV_RXCOMPLETE"));
        break;
    case EV_LINK_DEAD:
        Serial.println(F("EV_LINK_DEAD"));
        break;
    case EV_LINK_ALIVE:
        Serial.println(F("EV_LINK_ALIVE"));
        break;
    default:
        Serial.println(F("Unknown event"));
        break;
}
}

void do_send(osjob_t* j){
    // Check if there is not a current TX/RX job running
    float flat, flon, falt;
    unsigned long age;
    smartdelay(1000);
    gps.f_get_position(&flat, &flon, &age);
    falt=gps.f_altitude(); //get altitude
    flon == TinyGPS::GPS_INVALID_F_ANGLE ? 0.0 : flon, 6;//save six decimal places
    flat == TinyGPS::GPS_INVALID_F_ANGLE ? 0.0 : flat, 6;
    falt == TinyGPS::GPS_INVALID_F_ANGLE ? 0.0 : falt, 2;//save two decimal places
    Serial.print(flon);
    lpp.reset();
    lpp.addGPS(3, flat, flon, falt);
    lpp.addAnalogOutput(3,x);
    // send data
    if (LMIC.opmode & OP_TXRXPEND ) {
        Serial.println(F("OP_TXRXPEND, not sending"));
    } else {
        // Prepare upstream data transmission at the next possible time.
        LMIC_setTxData2(1, lpp.getBuffer(), lpp.getSize(), 0);
        Serial.println(F("Packet queued"));
    }
    // Next TX is scheduled after TX_COMPLETE event.
}

void setup() {
    Serial.begin(9600);
    ss.begin(9600);
    Serial.println(F("Starting"));
    Wire.begin(8); // join i2c bus with address #8
    Wire.onReceive(receiveEvent); // register event
    #ifdef VCC_ENABLE
    // For Pinoccio Scout boards
    pinMode(VCC_ENABLE, OUTPUT);
    digitalWrite(VCC_ENABLE, HIGH);
    delay(1000);
    #endif

    // LMIC init
    os_init();
    // Reset the MAC state. Session and pending data transfers will be discarded.
    LMIC_reset();

    // Set static session parameters. Instead of dynamically establishing a session
    // by joining the network, precomputed session parameters are be provided.
    #ifdef PROGMEM
    // On AVR, these values are stored in flash and only copied to RAM
    // once. Copy them to a temporary buffer here, LMIC_setSession will
    // copy them into a buffer of its own again.

```



```

uint8_t appskey[sizeof(APPSKEY)];
uint8_t nwkskey[sizeof(NWKSKEY)];
memcpy_P(appskey, APPSKEY, sizeof(APPSKEY));
memcpy_P(nwkskey, NWKSKEY, sizeof(NWKSKEY));
LMIC_setSession (0x1, DEVADDR, nwkskey, appskey);
#else
// If not running an AVR with PROGMEM, just use the arrays directly
LMIC_setSession (0x1, DEVADDR, NWKSKEY, APPSKEY);
#endif
#if defined(CFG_eu868)
// Set up the channels used by the Things Network, which corresponds
// to the defaults of most gateways. Without this, only three base
// channels from the LoRaWAN specification are used, which certainly
// works, so it is good for debugging, but can overload those
// frequencies, so be sure to configure the full frequency range of
// your network here (unless your network autoconfigures them).
// Setting up channels should happen after LMIC_setSession, as that
// configures the minimal channel set.
// NA-US channels 0-71 are configured automatically
LMIC_setupChannel(0, 868100000, DR_RANGE_MAP(DR_SF12, DR_SF7), BAND_CENTI); // g-band
LMIC_setupChannel(1, 868300000, DR_RANGE_MAP(DR_SF12, DR_SF7B), BAND_CENTI); // g-band
LMIC_setupChannel(2, 868500000, DR_RANGE_MAP(DR_SF12, DR_SF7), BAND_CENTI); // g-band
LMIC_setupChannel(3, 867100000, DR_RANGE_MAP(DR_SF12, DR_SF7), BAND_CENTI); // g-band
LMIC_setupChannel(4, 867300000, DR_RANGE_MAP(DR_SF12, DR_SF7), BAND_CENTI); // g-band
LMIC_setupChannel(5, 867500000, DR_RANGE_MAP(DR_SF12, DR_SF7), BAND_CENTI); // g-band
LMIC_setupChannel(6, 867700000, DR_RANGE_MAP(DR_SF12, DR_SF7), BAND_CENTI); // g-band
LMIC_setupChannel(7, 867900000, DR_RANGE_MAP(DR_SF12, DR_SF7), BAND_CENTI); // g-band
LMIC_setupChannel(8, 868800000, DR_RANGE_MAP(DR_FSK, DR_FSK), BAND_MILLI); // g2-band
// TTN defines an additional channel at 869.525Mhz using SF9 for class B
// devices' ping slots. LMIC does not have an easy way to define set this
// frequency and support for class B is spotty and untested, so this
// frequency is not configured here.
#elif defined(CFG_us915)
// NA-US channels 0-71 are configured automatically
// but only one group of 8 should (a subband) should be active
// TTN recommends the second sub band, 1 in a zero based count.
// https://github.com/TheThingsNetwork/gateway-conf/blob/master/US-global_conf.json
LMIC_selectSubBand(1);
#endif

// Disable link check validation
LMIC_setLinkCheckMode(0);

// TTN uses SF9 for its RX2 window.
LMIC.dn2Dr = DR_SF9;

// Set data rate and transmit power for uplink (note: txpow seems to be ignored by the library)
LMIC_setDrTxpow(DR_SF7,14);

// Start job
do_send(&sendjob);
}
static void smartdelay(unsigned long ms)
{
    unsigned long start = millis();
    do
    {
        while (ss.available())
        {
            //ss.print(Serial.read());
            gps.encode(ss.read());
        }
    } while (millis() - start < ms);
}
void receiveEvent(int howMany) {
    while (1 < Wire.available()) { // loop through all but the last
        char c = Wire.read(); // receive byte as a character
        Serial.print(c);        // print the character
    }
    x = Wire.read(); // receive byte as an integer
    Serial.println(x);        // print the integer
}

```

```

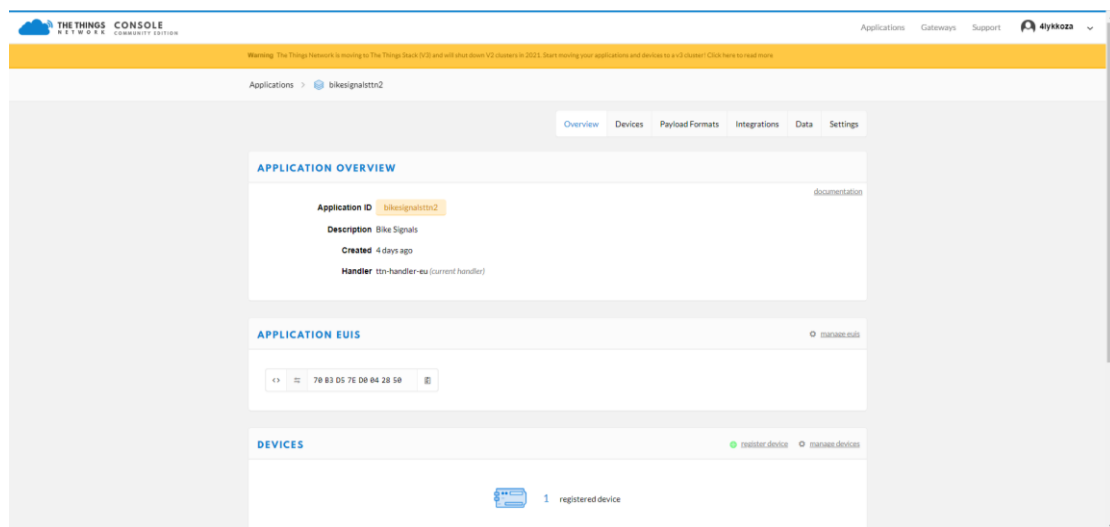
}
void loop() {
  os_runloop_once();
}

```

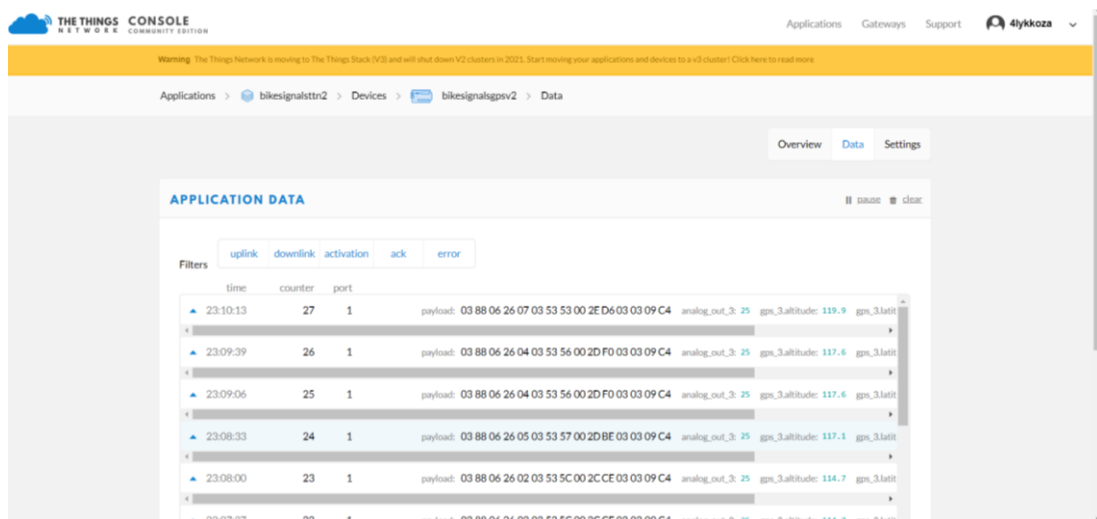
Δήλωση συσκευής στο TTN

Η συσκευή δηλώθηκε στο TTN κάτω από ένα application το οποίο ολοκληρώνεται με τα Integrations TTNMapper, ThingSpeak και Cayenne.

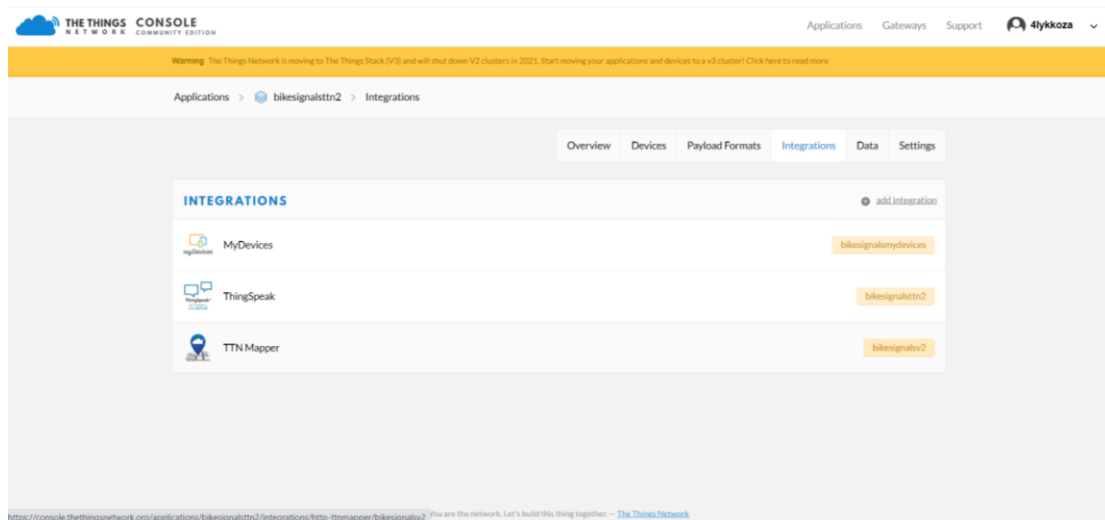
Η κωδικοποίηση των δεδομένων γίνεται με χρήση του Cayenne Lpp



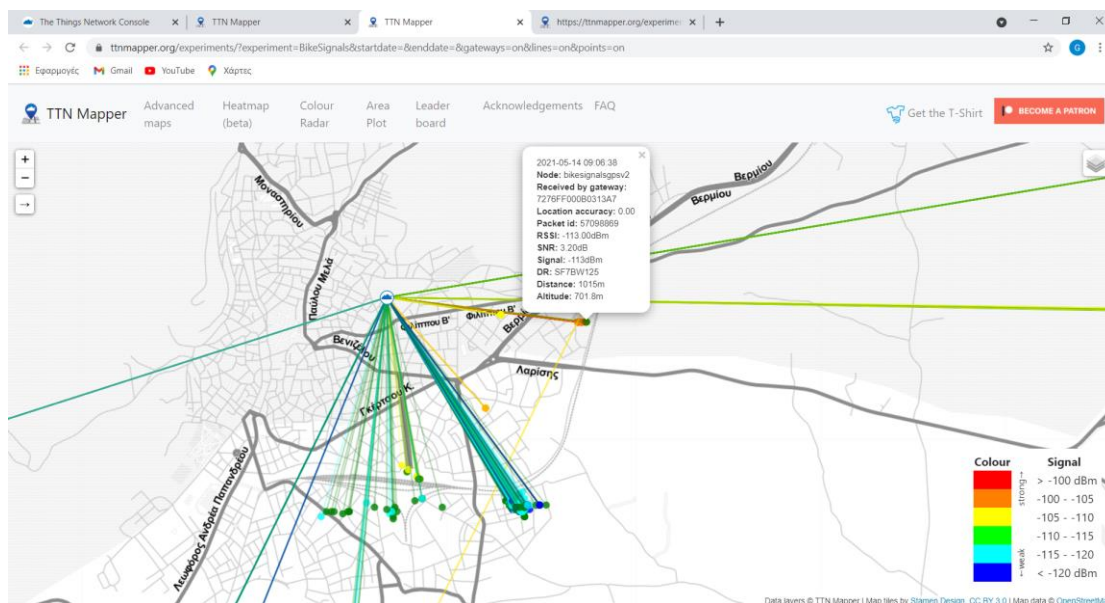
Εικόνα 2 – Application



Εικόνα 3 - Πακέτα στο TTN



Εικόνα 4 - Integrations



Εικόνα 5 - καταγραφή στο TTNMapper

Καταγραφή δεδομένων

Για την καταγραφή δεδομένων τοπικά χρησιμοποιήσαμε το TTNMapper και επίσης μια MQTT client εφαρμογή που υποστηρίζεται από το TTN . Η υλοποίηση έγινε σε Python 3.

```
import paho.mqtt.client as mqtt
import json
import base64
from geopy.distance import geodesic
APPEUI = *****
APPID = *****
PSW = *****
count=0
```

```

airtime=0
def bytes_to_decimal(i,d):
    xx = i - 127
    dec = (-d if xx < 0 else d)/100
    return xx + dec

def on_connect(client, userdata, flags, rc):
    client.subscribe('+/devices/+/up'.format(APPEUI))

def on_message(client, userdata, msg):
    j_msg = json.loads(msg.payload.decode('utf-8'))
    mcounter = j_msg['counter']
    dev_eui = j_msg['hardware_serial']
    mtime=j_msg['metadata']['time']
    mfreq=j_msg['metadata']['frequency']
    mdate=j_msg['metadata']['data_rate']
    mairtime=j_msg['metadata']['airtime']
    lat=j_msg['payload_fields']['gps_3']['latitude']
    lon=j_msg['payload_fields']['gps_3']['longitude']
    spo2= j_msg['payload_fields']['analog_3']
    snr=j_msg['metadata']['gateways'][0]['snr']
    rssi=j_msg['metadata']['gateways'][0]['rssi']
    gateway = (40.3050998,21.7964435)
    pycom = (lat,lon)
    apostasi=geodesic(gateway, pycom).meters
    print(apostasi)
    print('---')
    f = open("myfile.txt", "a+")
    f.write("%d,%7.5f,%7.5f,%7.2f,%5.2f,%5.2f,%9.2f,%d \n" %
(mcounter,lat,lon,apostasi,snr,rssi,mairtime,spo2))
    f.close()
    print('latitude:', lat, ' longitude:', lon, 'snr:',snr,'rssi:',rssi,'airtime:',mairtime,spo2)
    print('dev eui: ', dev_eui)
print('ok')
ttn_client = mqtt.Client()
print('test2')
ttn_client.on_connect = on_connect
print('test3')
ttn_client.on_message = on_message
print('test4')
ttn_client.username_pw_set(APPID, PSW)
ttn_client.connect("eu.thethings.network", 1883, 60) #MQTT port over TLS

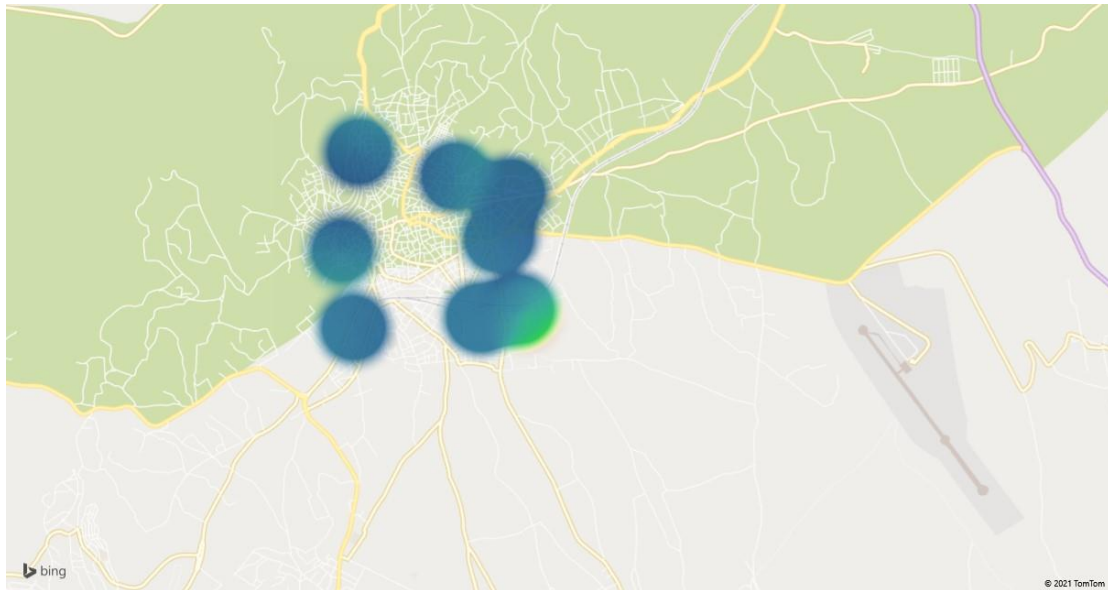
try:
    ttn_client.loop_forever()
except KeyboardInterrupt:
    print('disconnect')
    ttn_client.disconnect()

```

Ενδεικτικά αποτελέσματα

a/a	lat	lon	Dist	rss	snr	air	sf	br	airtime	spo2
					-					
0	40,2929	21,7966	1354,74	9,2	103	82176000	7	5	82,176	100
					-					
1	40,2929	21,7965	1354,68	6,2	109	82176000	7	5	82,176	100
					-					
2	40,2929	21,7964	1354,68	6,5	109	82176000	7	5	82,176	100
					-					
3	40,293	21,7963	1343,62	6,2	114	82176000	7	5	82,176	99
					-					
4	40,293	21,7963	1343,62	9	104	82176000	7	5	82,176	25
					-					
5	40,2931	21,7961	1332,78	6,2	105	82176000	7	5	82,176	25
6	40,2931	21,796	1333	8,5	-99	82176000	7	5	82,176	100
7	40,2931	21,7959	1333,26	9,8	-98	82176000	7	5	82,176	99
					-					
8	40,2932	21,7958	1322,49	7,2	110	82176000	7	5	82,176	99
					-					
0	40,2937	21,7997	1295,76	5,5	113	82176000	7	5	82,176	25
					-					
1	40,2937	21,7997	1295,76	6,5	110	82176000	7	5	82,176	25
					-					
2	40,2937	21,7998	1297,61	-4	111	82176000	7	5	82,176	25
					-					
3	40,2937	21,8	1301,45	6,5	108	82176000	7	5	82,176	99
					-					
4	40,2937	21,8	1301,45	7	113	82176000	7	5	82,176	98
					-					
5	40,2937	21,8001	1303,45	-5,2	116	82176000	7	5	82,176	25
					-					
6	40,2938	21,8002	1294,74	1,2	113	82176000	7	5	82,176	25
					-					
7	40,2938	21,8003	1296,87	6,2	107	82176000	7	5	82,176	25
					-					
8	40,2938	21,8004	1299,04	2,8	115	82176000	7	5	82,176	99
					-					
0	40,2931	21,8008	1382,98	3,2	113	82176000	7	5	82,176	99
					-					
1	40,2931	21,8008	1382,98	2,8	114	82176000	7	5	82,176	25
					-					
2	40,2931	21,8008	1382,98	2	116	82176000	7	5	82,176	25
					-					
3	40,2931	21,8008	1382,98	4,8	113	82176000	7	5	82,176	25
					-					
4	40,2931	21,8008	1382,98	4	113	82176000	7	5	82,176	100
					-					
5	40,2931	21,8008	1382,98	-1,5	113	82176000	7	5	82,176	99

Μετά από φιλτράρισμα μη έγκυρων τιμών μπορεί να γίνει χρωματική αναπαράσταση των δεδομένων πάνω στο χάρτη.



Εικόνα 6- Αποτύπωση αποτελεσμάτων με χρωματικό κώδικα

Σε επόμενη φάση σίγουρα πρέπει να καταγραφούν περισσότερα δεδομένα. Μεγάλο αντικείμενο μελέτης είναι αυτό της συλλογής, αποθήκευσης και επεξεργασίας των δεδομένων που προκύπτουν από μια τέτοια εφαρμογή. Επίσης το σύστημα θα πρέπει να είναι έξυπνο και σ' αυτό το επίπεδο. Δηλαδή θα πρέπει να μπορεί να πάρει αποφάσεις μόνο του εφαρμόζοντας κανόνες μηχανικής μάθησης.

Όνομα Ομάδας

Η τελική κατασκευή αυτού του πειραματικού έργου θα καταλήξει σ' ένα ποδήλατο, του οποίου θα καταγράφεται η θέση και βιομετρικά στοιχεία του ποδηλάτη. Το σύστημα θα είναι ενσωματωμένο στο ποδήλατο.

Έτσι δικαιολογείται το όνομα της ομάδας **BikeSignals**.

Αναφορές

(χ.χ.). Ανάκτηση από <https://e27.co/advantages-disadvantages-internet-things-20160615/>

(χ.χ.). Ανάκτηση από http://web.luxresearchinc.com/hubfs/Insight_Breakdown_of_LPWAN_Technologies.pdf

(χ.χ.). Ανάκτηση από <https://www.sciencedirect.com/science/article/pii/S2405959517300061?via=ihub>

Arduino. (2021). *Arduino IDE*. Ανάκτηση από Arduino IDE: <https://www.arduino.cc/>

DFRobot. (χ.χ.). *MAX30102* . Ανάκτηση από DFRobots: https://wiki.dfrobot.com/Heart_Rate_and_Oximeter_Sensor_SKU_SEN0344

Dragino. (2021). *Dragino Lora Shield*. Ανάκτηση από Dragino Lora Shield: https://wiki.dragino.com/index.php?title=Lora_Shield

<https://avbentem.github.io/airtime-calculator/ttn/eu868/27>. (2020, 12).
<https://avbentem.github.io/airtime-calculator/ttn/eu868/27>. Ανάκτηση από <https://avbentem.github.io/airtime-calculator/ttn/eu868/27>

Mehmood, Y. A. (2017). *Internet-of-thingsbased smart cities: Recent advances and challenges*.

Network, T. t. (2021). <https://www.thethingsnetwork.org/docs/lorawan/what-is-lorawan/>.
Ανάκτηση από The things Network.

Patel, K. K. (2016). *Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges*.

Rose, K. E. (2015). *The internet of things: An overview*. *The Internet Society*.

Ζαχαροπούλου Μαρία, Ε. Γ. (2020). *Έξυπνες Πόλεις και Τεχνολογίες Διασυνδεδεμένων Συσκευών*.