ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΣΥΡΜΑΤΟ ΔΙΚΤΥΟ ΑΙΣΘΗΤΗΡΩΝ ΜΕΤΡΗΣΗΣ ΑΤΜΟΣΦΑΙΡΙΚΗΣ ΡΥΠΑΝΣΗΣ

ΚΛΑΔΑΣ ΗΛΙΑΣ

Επιβλέπων καθηγητής: Τζήμας Γιάννης

Πάτρα – Φεβρουάριος 2020

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

Πάτρα, Ημερομηνία

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Ονοματεπώνυμο, Υπογραφή
2. Ονοματεπώνυμο, Υπογραφή
3. Ονοματεπώνυμο, Υπογραφή

Ευχαριστίες

Ολοκληρώνοντας αυτή την πτυχιακή εργασία θα ήθελα να αφιερώσω ένα κομμάτι της για να ευχαριστήσω τους ανθρώπους που μου έδωσαν κίνητρο να μην εγκαταλείψω τις προσπάθειες

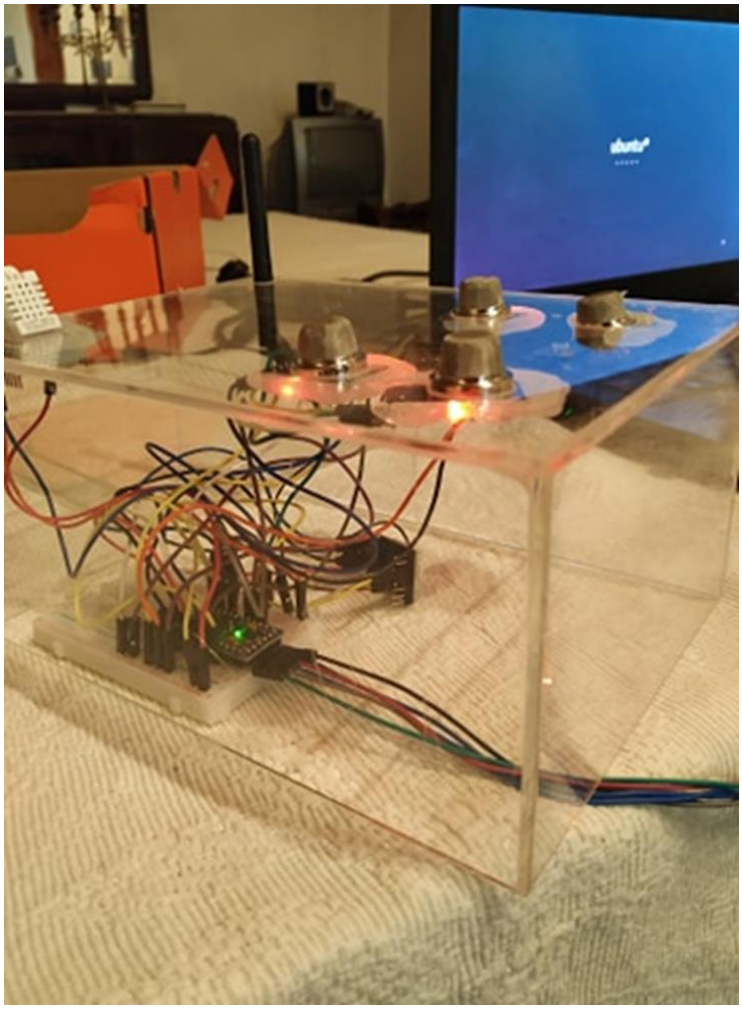
και να συνεχίσω την σχολή παρά την χρόνια απουσία μου. Πρώτα θα ήθελα να ευχαριστήσω των επιβλέποντα καθηγητή Ιωάννη Τζήμα που δέχθηκε να αναλάβει αυτήν την πτυχιακή εργασία μαζί μου και στήριξε την ιδέα μου για να μπορέσω να την υλοποιήσω .Τους συμφοιτητές μου Νίκο Κουνάβη, Γιάννη Ανδρέου και Θεοδώρα Κατινάρη που με βοηθήσανε και τους βοήθησα όλα αυτά τα φοιτητικά χρόνια, φτάνοντας και οι τέσσερις στο πτυχίο την ίδια στιγμή σαν ομάδα . Και τέλος θα ήθελα να πω το μεγαλύτερο ευχαριστήσω στον παππού μου Ηλία που με στήριξε οικονομικά και ψυχολογικά έτσι ώστε να καταφέρω να ολοκληρώσω την πτυχιακή μου εργασία.

1 Περιεχόμενα

Περίληψη

Η ατμοσφαιρική ρύπανση ειναι ενα θέμα που θα πρέπει να προβληματιζει τον καθε άνθρωπο ξεχωριστα καθώς τα τελευταία χρόνια λόγω της βιομηχανικής και τεχνολογικής ανάπτυξης ,της αύξηση πληθυσμού και την αύξηση της χρήσης οχημάτων έχει πάρει πολύ επικίνδυνη διάσταση.Η ρύπανση της ατμόσφαιρας αποτελεί σοβαρό υγειονομικό, περιβαλλοντικό, κοινωνικό και οικονομικό πρόβλημα, γιατί τα αέρια που τη ρυπαίνουν, όπως το διοξείδιο του άνθρακα έχουν σοβαρές συνέπειες, όπως την υπερθέρμασης της γης, αναπνευστικά προβλήματα και άλλα προβλήματα υγείας.Ένας απο τους τρόπους για τον έλεγχο και την παρακολούθηση της ρύπανσης ειναι η εγκατάσταση ασύρματων δικτύων αισθητήρων. Ασύρματο δίκτυο αισθητήρων (Wireless Sensor Network – WSN) ειναι ενας ή περισσότεροι αισθητήρες για την παρακολούθηση φυσικών ή περιβαλλοντολογικών συνθηκών (όπως θερμοκρασία , υγρασία , ποιότητα αέρα κα.), και μέσω συνεργασίας μεταφέρει πληροφορία μέσω του δικτύου σε μια συγκεκριμένη τοποθεσία.Στην συγκεκριμένη πτυχιακή εργασία θα δούμε ενα ασύρματο δίκτυο αισθητήρων του οποιου οι παράμετροι που θα παρακολουθήσουμε είναι η θερμοκρασία, η υγρασία , η ποσότητα καυσαερίου , η ποιότητα αέρα, το υδρογόνο και το μονοξείδιο του άνθρακα με την βοήθεια των αισθητήρων dht-22, mq-4, mq-135, mq-8 και mq-9 αντίστοιχα.Οι τιμές αυτών των παραμέτρων μεταδίδονται

χρησιμοποιώντας δυο lora ra -02 τα οποια ειναι πομπός και δέκτης αντίστοιχα και στην συνέχεια θα εμφανίζεται στο serial monitor αν ειναι επικύνδινες ή όχι.



ΑΤΜΟΣΦΑΙΡΙΚΟΙ ΡΥΠΟΙ

ΑΤΜΟΣΦΑΙΡΑ

Η ατμόσφαιρα είναι το αέριο σώμα που περιβάλλει τη Γη συγκρατείται λόγω της βαρύτητας ενω έχει ύψος 3.500 χιλιόμετρα. Τα σύνορα ατμόσφαιρας και διαστήματος δεν είναι αυστηρά καθορισμένα. Οσο αυξάνεται η απόσταση της από τη Γη η ατμόσφαιρα σταδιακά εξασθενεί και εξαφανίζεται στο διάστημα. Η ατμόσφαιρα προστατεύει τη ζωή στη Γη με το να απορροφά την υπεριώδη ηλιακή ακτινοβολία να θερμαίνει την επιφάνεια της με την παρακράτηση της

θερμότητας και να μειώνει τις αυξομειώσεις της θερμοκρασίας ,ανάμεσα στη μέρα και τη νύχτα. Η ατμόσφαιρα είναι αόρατη, άοσμη και παρουσιάζει ένα πλήθος ιδιοτήτων που αποτελούν τις συνθήκες επιβίωσης των ζωικών και φυτικών οργανισμών. Πρακτικά στην ατμόσφαιρα οφείλεται η ύπαρξη ζωής.

ΑΤΜΟΣΦΑΙΡΙΚΗ ΡΥΠΑΝΣΗ

Η ατμοσφαιρική ρύπανση και οι επιπτώσεις στην ποιότητα του αέρα και στο περιβάλλον αποτελούν ένα από τα σημαντικότερα προβλήματα στην Ελλάδα και παγκοσμίως. Είναι η ρύπανση που οφείλεται κυρίως στον άνθρωπο καθώς η ουσίες που ρυπαίνουν την ατμόσφαιρα υπό φυσιολογικές συνθήκες δε θα υπήρχαν ποτέ. Όμως και η ηφαιστειακές δράσεις επιβαρύνουν σε μεγάλη κλίμακα την ατμόσφαιρα με προσθήκη τοξικών στοιχείων και ραδιενέργειας. Ως Ατμοσφαιρική Ρύπανση χαρακτηρίζεται κάθε ανεπιθύμητη αλλαγή των φυσικών, χημικών, ραδιολογικών ή βιολογικών χαρακτήρων του αέρα, που προκαλείτε από τις ανθρώπινες δραστηριότητες και μπορεί να έχει ανεπιθύμητη επίδραση στη υγεία και ευεξία του ανθρώπου αλλά και να επηρεάσει τη φυσική ισορροπία(Οργανισμοί , φυσικά νερά , έδαφος). Οι βασικότερη ατμοσφαιρική ρύποι είναι:

1) Το διοξείδιο του θείου (SO2), που δημιουργείτε από την καύση στερεών και υγρών καυσίμων.

2)Τα οξείδια του αζώτου, τα οποία παράγονται κατά τη λειτουργία των βενζινοκινητήρων.

3) Το μονοξείδιο του άνθρακα (CO), το οποίο προέρχεται κυρίως από τις καύσεις στους κινητήρες των αυτοκίνητων.

4)Το διοξείδιο του άνθρακα (CO2), το οποίο παράγεται κατά την καύση στερεών και υγρών καυσίμων.

5)Διάφοροι υδρογονάνθρακες, οι οποίοι είναι συστατικά των καυσίμων που διαφεύγουν στην ατμόσφαιρα.

6)Αιωρούμενα σωματίδια, όπως για παράδειγμα η αιθάλη (σκόνη άνθρακα, κάπνα) και η σκόνη, η οποία προέρχονται κυρίως από τα τεχνικά έργα και τα ηφαίστεια.

Ανθρωπογενείς πηγές εκπομπής ατμοσφαιρικών ρύπων

Υπάρχουν δύο βασικές ανθρωπογενείς πηγές :

1) Σταθερές πηγές, η οποίες περιλαμβάνουν την παραγωγή ενέργειας της βιομηχανίας, την παραγωγή ηλεκτρικής ενέργειας και την θέρμανση κτιρίων.

2)Κινητές πηγές, όπως τροχοφόρα αεροπλάνα πλοία κτλ.

Ακόμα υπάρχει οι τοπικές πηγές από γεωργικές καύσεις και διατήρηση σκουπιδιών σε χωματερές όπου παράγεται μεθάνιο.

Φυσικές πήγες εκπομπής ατμοσφαιρικών ρύπων

Υπάρχουν φυσικές πήγες εκπομπής ατμοσφαιρικών ρύπων οι οποίες δεν μπορούν να ελεγχθούν από τον άνθρωπο και επηρεάζουν αρκετά την ποιότητα του αέρα. Οι σημαντικότερες από αυτές είναι :

1) Εκπομπές σκόνης από την αιολική διάβρωση των εδαφών:

Τέτοια φαινόμενα συναντάμε σε μεγάλες περιοχές με λίγη έως καθόλου βλάστηση. Η ατμόσφαιρα ρυπαίνεται αρκετά με αρκετά παραδείγματα και στην χώρα μας όπως Αφρικανική σκόνη κτλ.

2) Οι ηφαιστειακές εκρήξεις :

Οι εκρήξεις των ηφαιστείων απελευθερώνουν στην ατμόσφαιρα μεγάλες ποσότητες απο θειικά αερολύματα και τέφρες. Τέτοιες ουσίες κατά την έκρηξη φτάνουν σε πολύ μεγαλύτερα ύψη απο την επιφάνεια τις γης και λόγο αυτού έχουν μεγαλύτερο χρόνο παραμονής στην ατμόσφαιρα και μεταδίδονται σε μεγαλύτερη απόσταση. Επηρεάζουν την θερμοκρασία προκαλώντας ψύξη του αέρα διότι σκεδάζουν και απορροφούν το ηλιακό φως επηρεάζοντας τον τρόπο γένεσης των νεφών.

3)Δασικές πυρκαγιές :

Στις δασικές πυρκαγιές υπάρχουν εκπομπές αιωρούμενων σωματιδίων και αερίων όπως μονοξείδιο του άνθρακα που επιβαρύνουν την ποιότητα του αέρα.

Ιστορική αναδρομή

Από τα αρχαία χρόνια και πιο συγκεκριμένα από την ανακάλυψη της φωτιάς η ατμοσφαιρική ρύπανση υπήρχε είτε ατελή καύση του ξύλου είτε από καύσης των αποβλήτων των ζώων .Η "αιθάλη" που βρέθηκε στα πάνω μέρος των προϊστορικών σπηλαίων παρέχει άφθονες ενδείξεις για τα υψηλά επίπεδα ρύπανσης που συσχετίστηκαν με τον ανεπαρκή αερισμό των ανοιχτών πυρκαγιών. Ο Ρωμαίος φιλόσοφος Σενέκας το 61 μ.Χ έκανε μια πολύ χαρακτηριστική αναφορά σε αυτό το φαινόμενο της κακής ποιότητας αέρα λέγοντας «Μόλις έφυγα μακριά από τον πνιγερό αέρα της Ρώμης και από τη βρωμιά των καπνοδόχων που κάπνιζαν, διαχέοντας ολόγυρα θανατηφόρα αέρια και αιθάλη, ένοιωσα να αλλάζει η διάθεσή μου». Αρκετά αργότερα το 1157 η σύζυγος του βασιλιά Ερρίκου του 2ουτης Αγγλίας, Ελεονόρα, μετακόμισε από το Tutbury Castle του Nottingham, γιατί θεώρησε ανυπόφορη τη ρύπανση του αέρα λόγο της καύσης των ξύλων , ενώ υπάρχουν αρκετές αναφορές απο τα μεσαιωνικά χρόνια για το ατμοσφαιρικό ζήτημα . Η Βιομηχανική Επανάσταση ήταν το σημείο αναφοράς της ρύπανση του περιβάλλοντος τον 18ο με 19ο αιώνα λόγο τις συνεχούς καύσης κάρβουνου για την παραγωγή ενέργειας δημιουργώντας ατμοσφαιρική ρύπανση απο την στάχτη και τον καπνό. Κατά των 19ο αιώνα ο καπνός και η αιωρούμενη τέφρα δημιούργησαν μεγάλη ρύπανση με αποτέλεσμα το 1875 να έχουμε αρκετούς

θανάτους ανθρώπων και ζώων. Στον εικοστό αιώνα πολλά ήταν τα περιστατικά που κατέληξαν σε θάνατο όπως το 1909 η αιθαλομίχλη στη Γλασκόβη και το Εδιμβούργο που στοίχισε την ζωή σε περίπου 1000 ανθρώπους . Ακόμα ένα επεισόδιο αιθαλομίχλης 1930 στις βιομηχανικές περιοχές στο Βέλγιο όπου εκατοντάδες άνθρωποι αρρώστησαν με 60 νεκρούς εξ αυτών. Στην Donora των ΗΠΑ το 1948 λόγο τις ατμοσφαιρικής ρύπανσης σημειώθηκαν 20 θάνατοι και 6,000 ασθένειες ενώ το 1952 στο Λονδίνο να έχουμε 4.000 νεκρούς σε μια βδομάδα όντας το μεγαλύτερο ιστορικά επεισόδιο που συνέβη λόγο τις ρύπανσης του αέρα.

Λέξεις κλειδιά: ……

Abstract

Air pollution is an issue that should concern every individual as in recent years due to industrial and technological development, population growth and increasing vehicle use has taken on a very dangerous dimension. Air pollution is a serious health, environmental , social and economic problem, because the gases that pollute it, such as carbon dioxide have serious consequences, such as global warming, respiratory problems and other health problems.One way to control and monitor pollution is to install wireless sensor networks. Wireless Sensor Network (WSN) is one or more sensors for monitoring natural or environmental conditions (such as temperature, humidity, air quality, etc.), and through cooperation transmits information over the network to a specific location.

In this dissertation we will see a wireless network of sensors whose parameters we will monitor are temperature, humidity, amount of exhaust gas, air quality, hydrogen and carbon monoxide with the help of sensors dht-22, mq- 4, mq-135, mq-8 and mq-9 respectively. The values of these parameters are transmitted using two lora ra -02 which are transmitter and receiver respectively and will then be displayed on the serial monitor whether they are dangerous or no dangerous.

2 ΚΕΦΑΛΑΙΟ 1

ΑΙΣΘΗΤΗΡΕΣ

1.1 Τι είναι ο αισθητήρας

Αισθητήρας ονομάζεται μία συσκευή η οποία ανιχνεύει ένα φυσικό μέγεθος και παράγει από αυτό μία μετρήσιμη έξοδο. Οι πρώτοι αισθητήρες ήταν μηχανικοί.

Με την πρόοδο της τεχνολογίας των ηλεκτρονικών συστημάτων δημιουργήθηκαν νέοι τύποι αισθητήρων που σχετίζονται με στην μετατροπή του φυσικού μεγέθους (θερμοκρασία, υγρασία κτλ) σε ηλεκτρικό σήμα. Λόγω της ευκολίας ότι το ηλεκτρικό σήμα μεταφέρεται, ενισχύεται, φιλτράρεται, αποθηκεύεται και απεικονίζεται το κάνει να είναι ο ιδανικός τρόπος για την μέτρηση φυσικών μεγεθών. Με την τεχνολογική ανάπτυξη γύρω απο τον ηλεκτρισμό δημιουργήθηκαν νέοι τύποι αισθητήρων που σχετίζονται με ηλεκτρικά κυκλώματα και έχουν σαν έξοδο ψηφιακό ή αναλογικό σήμα.

Η ανάπτυξη των αισθητήρων αυξάνεται συνεχώς λόγω των αναγκών που δημιούργησαν οι θετικές επιστήμες αλλά και η πρόοδος της τεχνολογίας. Πλέον καλύπτεται μεγάλο φάσμα μετρήσεων φυσικών μεγεθών. Οι αισθητήρες και το μικροϋπολογιστικό σύστημα αποτελούν μια ενιαία μονάδα εξαιρετικά μικρών διαστάσεων που είναι κόμβος ενός ασύρματου δικτύου, με τη βοήθεια του οποίου, οι μετρήσεις στέλνονται σε μια κεντρική μονάδα που τις

επεξεργάζεται για να δοθούν οι σωστές τιμές στον χρήστη. Η χρήση των αισθητήρων είναι καθημερινή αφού υπάρχουν σχεδόν σε κάθε συσκευή.

1.2 Ιστορική Αναδρομή

Οι αισθητήρες υπήρχαν πάντα στην φύση από τα πρώτα χρόνια τις ζωής καθώς τα μάτια και τα αφτιά μπορούν να θεωρηθούν φυσική αισθητήρες. Με τα χρόνια ο άνθρωπος άρχισε να καταλαβαίνει ότι χρειάζεται όργανα για να μετρήσει φυσικά μεγέθη ή φυσικά φαινόμενα. Το 1585 χρησιμοποιήθηκε το πρώτο θερμόμετρο και το 1643 το πρώτο βαρόμετρο. Οι πρώτοι αισθητήρες ήταν μηχανικοί και με την πρόοδο της τεχνολογία όπως αναφέραμε και παραπάνω δημιουργήθηκαν νέοι τύποι αισθητήρων που σχετίζονται με στην μετατροπή του φυσικού μεγέθους σε ηλεκτρικό σήμα.

1.3 Αποκλήσεις αισθητήρων

1. Σφάλμα ευαισθησίας είναι όταν η ευαισθησία είναι διαφορετική απο την θεωρητική και αναμενόμενη.

2. Σφάλμα που προκαλείται λόγο τις ξεπέρασεις του μέγιστου ή ελάχιστου ορίου της εξόδου σε έναν μη ιδανικό αισθητήρα.

3. Απόκλιση μηδενός αισθητήρα (offset) δηλαδή να για μηδενική είσοδο δεν δίνει μηδενική έξοδο.

4. Μη γραμμικός αισθητήρας είναι όταν η ευαισθησία δεν είναι σταθερή στο διάστημα τις μέτρησης του αισθητήρα.

5. Δυναμικό σφάλμα όταν η απόκλιση προκαλείται απο γρήγορη αλλαγή εισόδου.

6. Ολίσθηση είναι όταν η έξοδος αλλάζει αργά και ανεξάρτητα απο την είσοδο.

7. Θόρυβος είναι όταν έχουμε τυχαία απόκλιση της εξόδου.

8. Υστέρηση είναι το σφάλμα που προκαλείται όταν η είσοδος αλλάζει κατεύθυνση και η έξοδος χρειάζεται κάποιο χρόνο αντίδρασης.

9. Σφάλμα ψηφιακοποίησης είναι όταν γίνεται η μετατροπή αναλογικού σε ψηφιακό σήμα.

10. Αρκετοί αισθητήρες έχουν ευαισθησία και σε άλλες φυσικές αλλαγές έκτος απο την προγραμματισμένης τους λειτουργίας.

1.4 Χαρακτηριστικά αισθητήρων

Τα χαρακτηριστικά των ασθητήρων ειναι τα εξής:

2 Εύρος	Τα όρια στα οποία η συσκευή λειτουργεί αξιόπιστα.
3 Ακρίβεια	Η εγγύτητα της τιμής εξόδου προς τη τιμή εισόδου.
4 Σφάλμα	Η διαφορά ανάμεσα στη μετρούμενη τιμή και τη πραγματική τιμή.
5 Ανοχή	Το μέγιστο σφάλμα που μπορεί να δημιουργήσει ο αισθητήρας.
6 Διακριτική ικανότητα	Η μικρότερη αλλαγή τιμής εισόδου που μπορεί να ανιχνεύσει.
7 Ευαισθησία	Η σχέση της αλλαγής εξόδου προς τη αλλαγή εισόδου, είναι ίση με τη διαφορά των τιμών της εξόδου προς τη διαφορά των αντίστοιχων τιμών εισόδου.
8 Βαθμονόμηση	Η βαθμολόγηση της κλίμακας σε μονάδες.
9 Νεκρή ζώνη	Το μέγιστο ποσό αλλαγής της εισόδου που δεν επιφέρει αλλαγή στην έξοδο.
10 Γραμμικότητα	Ο βαθμός στον οποίο η γραφική παράσταση της εξόδου προσεγγίζει ευθεία ως προς την είσοδο του αισθητήρα.
11 Απόκριση	Ο χρόνος που απαιτείται για να λάβει τη τελική τιμή η έξοδος.
12 Καθυστέρηση	Η καθυστέρηση της αλλαγής της εξόδου ως προς την είσοδο.
13 Ευστάθεια	Η μεταβολή της εξόδου σε μεγάλη χρονική περίοδο, χωρίς μεταβολή της εισόδου και των συνθηκών.
14 Υστέρηση	Η διαφορά στην έξοδο όταν η κατεύθυνση της μεταβολής της εισόδου αντιστραφεί.
15 Επαναληψιμότητα	Η παραγωγή του ιδίου αποτελέσματος, σε διαφορετικές χρονικές στιγμές, με την ίδια είσοδο.
16 Ολίσθηση	Η μεταβολή των χαρακτηριστικών του αισθητήρα με το χρόνο και το περιβάλλον.
17 Στατικό σφάλμα	Σταθερό σφάλμα σε όλο το εύρος λειτουργίας, το οποίο μπορεί να αντισταθμιστεί.
18 Χρόνος λειτουργίας	Ο εκτιμώμενος χρόνος λειτουργίας στα πλαίσια των προδιαγραφών του.

3 1.5 Εφαρμογές αισθητήρων

Οι αισθητήρες ταξινομούνται βάση της μορφής του σήματος διέγερσης και σύμφωνα με την ταξινόμηση αυτή πραγματοποιούνται και οι αντίστοιχες εφαρμογές. Αυτές είναι:

- **Μηχανική ενέργεια**: χρησιμοποιείται για μέτρηση επιτάχυνσης, ροής, δύναμης, ταχύτητας, θέσης, μάζας και ροπής.

- **Ηλεκτρική ενέργεια**: χρησιμοποιείται για μέτρηση έντασης, τάσης, πόλωσης αντίστασης, αγωγιμότητας και συχνότητας.

- **Ακουστική ενέργεια**: χρησιμοποιείται για μέτρηση φάσης, μήκους κύματος, πόλωσης, φάσματος και ταχύτητας κύματος.

- **Βιολογική ενέργεια**: χρησιμοποιείται για μέτρηση τύπου, κατάστασης και συγκέντρωσης βιόμαζας, σακχάρων και πρωτεϊνών.

- **Χημική ενέργεια**: η οποία χρησιμοποιείται για μέτρηση υγρασίας, pH, συγκέντρωσης και ιδιοτήτων συστατικών και συγκέντρωση αερίων και ατμών.

Μαγνητική ενέργεια: η οποία χρησιμοποιείται για μέτρηση έντασης μαγνητικού πεδίου, ροής και μαγνητικής διαπερατότητας.

Οπτική ενέργεια: χρησιμοποιείται για μέτρηση μήκους κύματος, φάσης, πόλωσης, φάσματος και απορρόφησης.

Ακτινοβολία: χρησιμοποιείται για μέτρηση ενέργειας, μικροκυμάτων και φωτεινότητας.

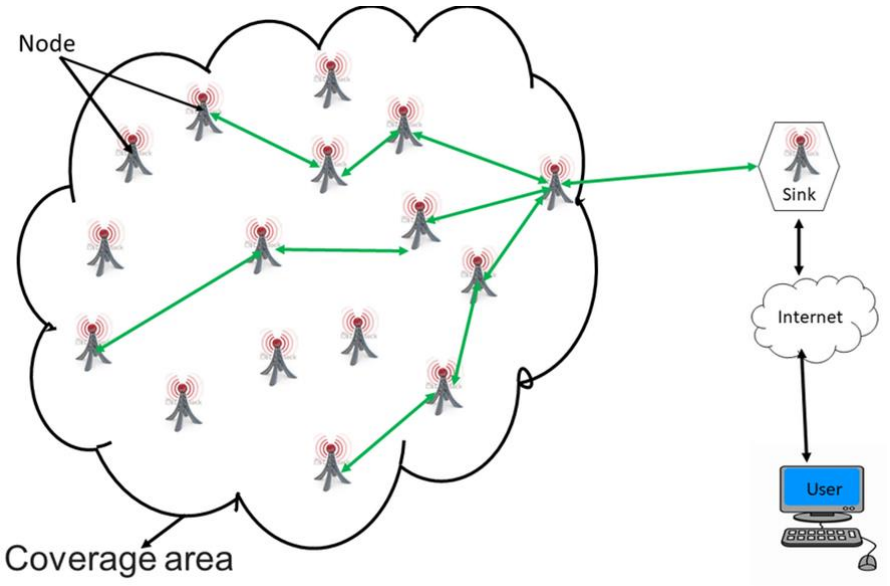
Θερμική ενέργεια: για μέτρηση θερμοκρασίας, θερμότητας, ροής θερμότητας και θερμικής αγωγιμότητας.

4 ΚΕΦΑΛΑΙΟ 2

Ασύρματο δικτυο αισθητηρων.

19 2.1 Τι ειναι;

Ένα ασύρματο δίκτυο αισθητήρων (wireless sensor network – WSN) είναι ενα δίκτυο το οποίο αποτελείται απο ενεργειακά αυτόνομους κόβους οι οποίοι μετρούν , παρατηρούν φυσικά μεγέθη (θερμοκρασία , υγρασία , πίεση , κίνηση, εικόνα , ήχο κτλ) και μεταδίδουν τη επεξεργασμένη (ή και όχι) μέτρηση τους , με τελική κατεύθυνση ένα σταθμό βάσης. Οι επικοινωνία των κόμβων ειναι αμφίδρομη, δηλαδή όπως μεταδίδουν πληροφορίες στο base station κάλλιστα μπορούν να δεχθούν πληροφορίες απο αυτόν. Τα ασύρματα δίκτυα αισθητήρων απαρτίζονται από μερικούς μέχρι χιλιάδες κόμβους και κάθε κόμβος συνδέεται με έναν ή και παραπάνω αισθητήρες. Το μέγεθος κάθε αισθητήρα διαφέρει αφού μπορεί να είναι από μικροσκοπικός(κόκκος άμμου) μέχρι και αρκετά μεγάλος μέχρι (κουτί από παπούτσια).Η τιμή τους μεταβάλλεται ανάλογα με την πολυπλοκότητα τους. Τα ασύρματα δίκτυα αισθητήρων παίζουν πολύ σημαντικό ρόλο στην επιστήμη των υπολογιστών και τηλεπικοινωνιών καθώς και σε άλλες επιστήμες και ερευνητικούς τομείς.



Τα ασύρματα δίκτυα αισθητήρων όπως και πόλλες άλλες εφαρμογές είναι μια στρατιωτικές εφαρμογές. Το SOSUS(Sound Surveillance System) ήταν η πρώτη εφαρμογή δικτύου αισθητήρων και ήταν ενα σύστημα για την παρακολούθηση ήχου προκειμένου να ανιχνεύσουν τα Σοβιετικά υποβρύχια που διανέμονται στους ωκεανούς του Ατλαντικού και του Ειρηνικού με την χρήση ειδικών ακουστικών αισθητήρων (υδρόφωνα) την περίοδο του ψυχρού πολέμου το 1950.Πλέον το SOSUS που λειτουργεί ακόμα έχει πιο ειρηνικό προφίλ και χρησιμοποιείται για την παρακολούθηση θαλάσσιων ζώων ,σεισμούς και της ηφαιστειακής δραστηριότητας.

Τα Ad-Hoc πρωτοεμφανίστηκαν το 1968 στην Χαβάη όπου το ξεκίνησε ένα έργο βασισμένο στο δίκτυο ALOHA για την διασύνδεση εκπαιδευτικών κτηρίων. Ταυτόχρονα, αναπτύχθηκαν δίκτυα με ραντάρ άμυνας με τη χρήση αερόστατων ως αισθητήρων. Ο προκάτοχος του διαδικτύου, το Advanced Research Project Agency (ARPANET) που ιδρύθηκε από την US DARPA το 1969, χρησίμευσε ως δοκιμαστική βάση για νέες τεχνολογίες δικτύωσης που συνδέουν διάφορα πανεπιστήμια και ερευνητικά κέντρα. Το πραγματικό WSN μπορεί να εντοπιστεί στο πρόγραμμα Κατανεμημένων Αισθητηρίων Δικτύων (DSN) που ξεκίνησε το 1980 στο Defense Advanced Research Projects Agency (DARPA).

5 2.3 Χαρακτηριστικά ασύρματων δικτύων αισθητήρων

1. Χαμηλή κατανάλωση: Τις περισσότερες των περιπτώσεων η τροφοδοσία των κόμβων του δικτύου γίνεται με μπαταρίες η οποίες μετά απο συγκεκριμένη χρήση και καποιο χρονικό

διάστημα τελειώνουν άρα και το δίκτυο αρχίζει να είναι άχρηστο.Ένα απο τα σημαντικότερα πράγματα που κοιτάμε σε ενα ασύματο δίκτυο αισθητήρων είναι η εξοικονόμηση ενέργειας.Σε πολλές περιπτώσεις χρησιμοποιούν ανανεώσιμες πηγές ενέργειας (πχ. Ηλιακή ενέργεια) αλλα κατι τέτοιο εξαρτάται απο την τοποθεσια και τις ανάγκες του κάθε δικτύου ξεχωριστά για παράδειγμα ένα δίκτυο που μέτραει τιμές στην θάλασσα σε μεγάλο βάθος δεν μπορεί να βασιστεί στον ήλιο σαν πηγή ενέργειας.

2. Αυτόνομη και προγαμματιζομενη λειτουργία: Κάθε κόμβος του δικτύου πρέπει να λειτουργει αυτόνομα , δηλαδή να ξέρει το τι μετρήσεις πρέπει να κάνει , ποια στιγμή θα τις κάνει (συχνότητα δειγματοληψίας) και που θα στείλει τις μετρήσεις (Broadcasting).Την ίδια στιγμή θα πρέπει να προγραμματίζεται δυναμικά δηλαδή αν το base station δώσει στο δίκτυο καινούργια δεδομένα λειτουργίας θα έχουμε σαν αποτέλεσμα δυναμικό επαναπρογραμματισμό του δικτύου.

3. Χαμηλό κόστος:Η τίμες των κόμβων στην αγόρα είναι άρκετα υψηλές με αποτέλεσμα να είναι απαγορευτικό η δημιουργία δίκτυων καθώς αν θέλουμε για παράδειγμα να κάνουμε μετρήσουμε σε μια μέγαλη έκταση όπως ένα βουνό ή στην θάλασσα οι περισσότεροι ασύρματοι ασθητήρες έχουν εμβελια κοντά στα 100 μέτρα αυτο σημαίνει οτι θα χρειαστούμε πολλούς χιλίαδες κόμβους αρα και πολλά χιλιάδες/εκατομμύρια ευρώ .

4. Γρήγορη δημουργία δικτύου : Τα δίκτυα θα πρέπει να σε αρκέτα μικρό διάστημα να έχουν χαρτογραφήσει το δίκτυο τους και να ξεκινήσουν τις λειτουργίες τους.

5. Προσαρμοστικότητα : Ένα απο τα βασικότερα χαρακτηριστίκα των ασύρματων δικτύων αισθητήρων είναι η ικανότητα τους να προσαρμόζονται στις αλλαγές του δίκτυου.Για παράδειγμα αν ένας οι περισσότεροι κόμβοι καταστραφούν το δίκτυο δεν “πέφτει” βρίσκει αλλα paths και διατήρει την επικοινωνία με τους εναπομείναντες κόμβους.

6. Απλότητα : Οι μίκρες υπολογιστικές και ενεργειακές ικανότητες του κάθε κομβου απαιτούν σχεδιασμό απλών και αποδοτικών αλγορίθμων για την διεκπεραίωση των διεργασιών κάθε δίκτυου.

7. Απόδοση : Οι κόμβοι μειώνουν τις επανεκπομπές πακέτων λόγω σφαλματος με αύτον τον τρόπο αυξάνουν την αξιοπιστία αλλα θυσιάζουν την ταχύτητα.

Όλα τα χαρακτηριστικά που αναφέραμε παραπανω ειναι γενίκα των ασύρματων δικτύων αισθητήρων αλλα δεν αντιπροσωπέυουν κάθε δίκτυο καθώς ορισμένα δίκτυα ενδεχομένος να μην νοιάζονται για την εξοικονόμηση ενέργειας ή το κόστος δημιουργείας του δικτύου.

6 2.4 ΕΦΑΡΜΟΓΕΣ

Στις σύνχρονες κοινωνίες τα ασύρματα δίκτυα αισθητήρων είναι αναγκαία σε αρκετούς τομείς στους οποίους εφαρμόζονται με τους αντίστοιχους τρόπους.

1) Στρατός

Η εξέλιξη και ανάπτυξη τέτοιον δικτύων ξεκίνησε για λογαριασμό στρατιωτικών επιχειρήσεων και στην συνέχεια ιοθετήθηκε απο άλλους εργασιακούς και επιστημονικούς τομείς.Χρησιμοποιούνται για : εντοπισμό εχθρικων δυνάμεων ,έλεγχο και κατεύθυνση πολεμικών μηχανών κτλ.

2) Βιομηχανία

Η τεράστιες δυνατότητες των δικτύων αισθητήρων κρίθηκαν απαραίτητες για την ανάπτυξη τις βιομηχανίας .Χρησιμοποιούνται για : παρακολούθηση κατάστασης μηχανών, ρομποτικές λειτουργίες, συνθήκες εργασίας , εντοπισμός προιόντων κτλ.

3) Πολιτικοί μηχανικοί:

Ολο και περισσότερο τον τελευταίο καιρό ακούμε για τα έξυπνα σπίτια και τις εξύπνες πόλεις όλη αυτή η συζήτηση γινέται με παρανομαστή τα ασύρματα δίκτυα αισθητήρων , Αλλα και σε πόλλα

ακόμα έργα όπως κτήρια , γέφυρες και δρόμους οπου τα δίκτυα μετράνε σε πραγματικό χρόνο την κατάσταση τους ενημερώνοντας μας έτσι για το αν είναι επικύνδινα ή οχι.

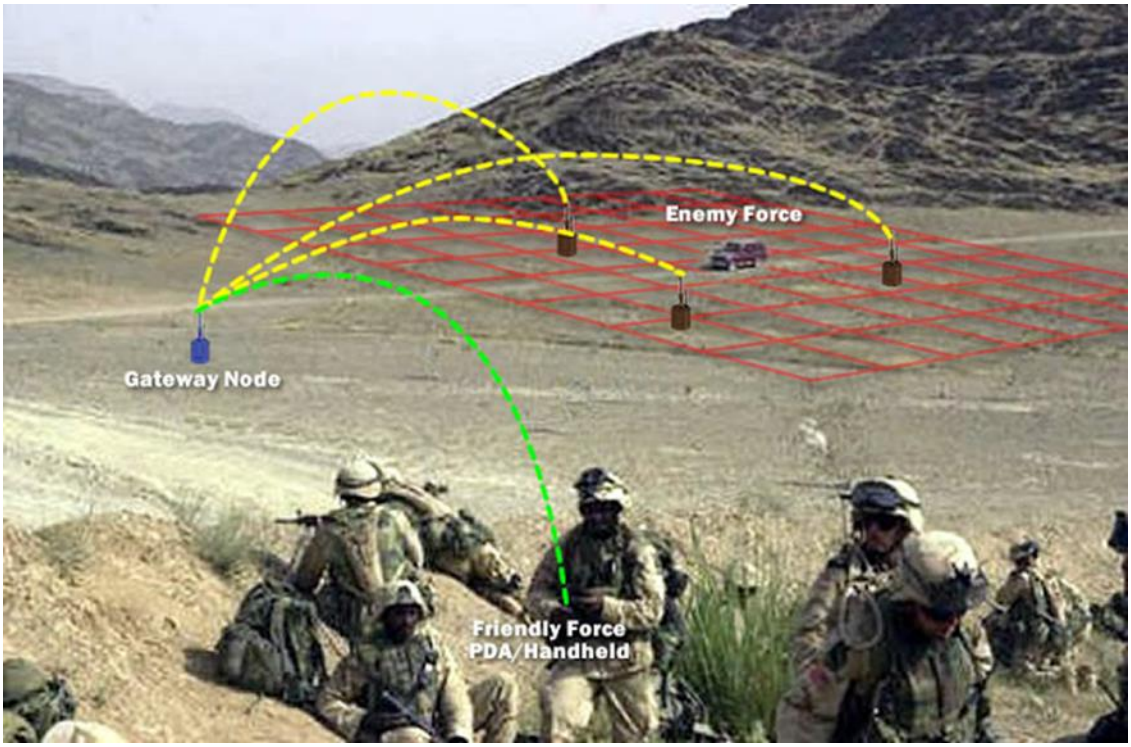
4)Υγεία:

Απαραίτητο κομμάτι τις ιατρικής είναι πλεον η τεχνολογία των ασύρματων δικτύων αισθητήρων και των υπηρεσιών που προσφέρει. Ένα απο τα πολλά παραδείγματα είναι το BSN (body sensor networks) που είναι σε θέση να παρακολουθήση ζωτικές λειτουργίες .

5) Περιβαλλοντική παρακολούθηση:

Η περιβαλλοντική παρακολούθηση είναι μια απο τις πιο συνηθισμένες αλλα και τις πιο σημαντικές εφαρμογές των ασύρματων δικτύων αισθητήρων.Περα τις ατμοσφαιρικής ρύπανσης που εξετάζουμε εμείς χρησιμοποιούνται για παρακολούθηση άγριων ζώων για ερευνιτικούς σκόπους, για την ανάπτυξη της γεωργίας κτλ.

Τα παραπάνω παραδείγματα είναι ενα μικρό δείγμα εφαρμογείς των δίκτυων καθώς πλεον χρησιμοποιούνται απο τα περισσότερα επαγγέλματα. Η τεχνολογία αυτή παρα την μικρή υπολογιστική τις δύναμη (στις περισσότερες περιπτώσης) δεν έχει όρια και επεκτύνεται συνεχώς.


Enemy Force
Gateway Node
Friendly Force
PDA/Handheld

7

8 ΚΕΦΑΛΑΙΟ 3

9 3.1 ΑΡΧΙΤΕΚΤΟΝΙΚΗ

Η αρχιτεκτονική των κόμβων σε ένα ασύρματο δίκτυο αισθητήρων δεν είναι ίδια σε κάθε περίπτωση, ανάλογα με την εφαρμογεί που πρέπει να υλοποιήσει αλλάζει η διαμόρφωση παρόλα αυτα τα δομικά στοίχεια μένουν τα ίδια.

Τα βασικά στοιχεία που χρειάζεται κάθε κόμβος ειναι:

1. Μικροελεγκτής (micro-controller):Ο μικροελεγκτής είναι το βασικότερο δομικό στοιχείο καθώς είναι απαραίτητο για τον συγχρονισμό και την εκτέλεση των λειτουργίων του συστήματος.Με βάση τον μικροελεγκή οι συσκευές επεξεργάζονται, στέλνουν και λαμβάνουν πληροφορία. Σε ορισμένες περιπτωσεις στην θέση του μικροελεγκτή συναντάμε μικροεπεξεργαστές γενικού σκοπού οπως FPGA ,DSP ,ASIC αλλα δεν αποτελούν την καλύτερη επιλογή οταν το σύστημα

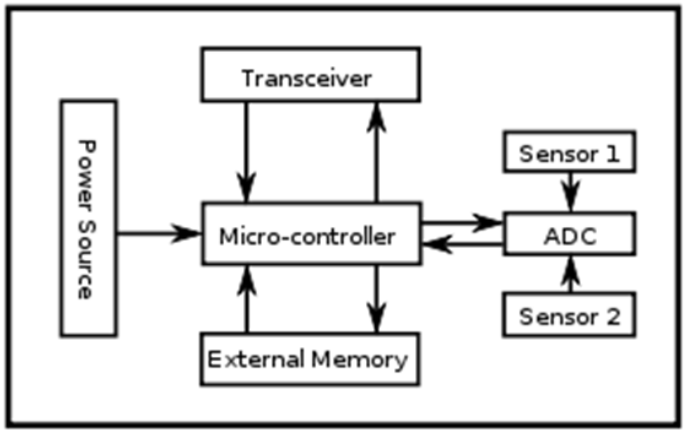
απαιτεί χαμηλή ενέργεια,χαμηλό κόστος , ευκολία προγραμματισμού και συνεργασία με το υπόλοιπο πρόγραμμα.

2. Μνήμη (external memory): Τις περισσότερες φορές επιλέγουν flash memory μαζί με την μνήμη του chip στο μικροελεγκτή με σκοπό την χαμηλή κατανάλωση . Άλλες περιπτώσεις ειναι η χρήση data logger ή καποια διαδικτυακή βάση δεδομένων.

3. Πομπός-δέκτης-Κεραία (transceiver):Είναι τα δομικά στοιχεία που χρησιμοποιούνται για την επικοινωνία μεταξύ των κόμβων ή με το base station.Οι μέθοδοι που βοήθουν στην επικοινωνία είναι το radio frequency (RF), optical communication (laser) και infrared (IR). Το πιο διαδεδομένο είναι το RF καθώς τα αλλα 2 δημιουργούν προβλήματα που δεν μπορούν να λυθούν όπως οπτική επαφή , κατάλληλες περιβαλλοντικές συνθήκες και έλλειψη ικανότητας για broadcast.

4. Πηγή ενέργειας (power source): Το σημαντικότερο ζήτημα στα ασύρματα δίκτυα αισθητήρων είναι η εξοικονόμηση και πηγή ενέργειας.Κάθε στοιχείο ενός κόμβου απαιτή ενέργεια που παρέχεται απο μπαταρίες ή αλλες ανανεώσιμες πηγές (πχ. Ηλιακό πανελ).Η περισσότερη ενέργεια καταναλώνετε κατα την αποστολή δεδομένων καθώς ο επεξεργαστής εκτελεί εκατομύρρια εντολές σε ελάχιστα δευτερόλεπτα.

Στην εφαρμογή μας χρησιμοποιούμε ενσύρματη επαφή αισθητήρων με arduino mini pro και η ασύρματη μετάδοση γίνεται με κεραία lora ra-02 με πηγή ενέργειας μπαταρίες 2 AA.



10 3.2 Δομή δικτύου

Τα ασύρματα δίκτυα αισθητήτρων αποτελούνται απο 2 βασικά δομικά στοιχεία , τα στοιχεία που παράγουν πληροφορία, όπως είναι ο κάθε κόμβος και ονομάζονται sources (πηγές) και απο τα στοιχεία που περισυλλέγουν πληροφορία απο τα sources τα sinks(αποδέκτες).Η τοπολογία του

κάθε δικτύου καθορίζεται απο τον τρόπο επικοινωνούν μεταξύ τους τα sources με τα sinks. Οι πιο δημογιλής τοπολογίες είναι 4.

1. Peer-to-Peer:Τα δίκτυα peer to peer επιτρέπουν στους κόμβους του δικτύου να μοιράζονται ισότιμα τους πόρους και την ίδια στιγμή χρησιμοποιεί την συνολική επεξεργαστική ισχύ, την μνήμη και το bandwidth για την λειτουργία του συστήματος.Μεταξύ τον κόμβων υπάρχει η λεγόμενη δικαιωσίνη αφου οι κόμβοι έχουν τα ίδια δικαιώματα στο δίκτυο και ακόμα όλοι οι κόμβοι εχουν πρόσβαση στους υπόλοιπους κόμβους. Τα peer to peer δίκτυα χωρίζονται σε 3 κατηγορίες

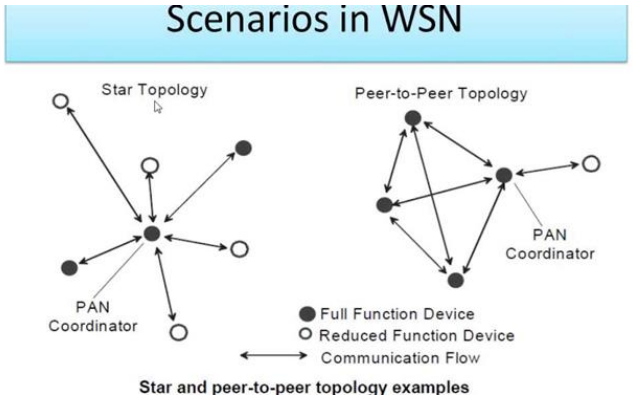
α. Συγκεντρωτικά peer-to-peer δίκτυα:Σε αυτή την κατηγορία υπάρχει ένας κεντρικός κοόμβος ο index server ο οποίος "θυμάται" την κατάσταση του κάθε κόμβου.Για παράδειγμα εάν κάποιος κόμβος θέλει μια πληροφορία απο κάποιον άλλον κόμβο θα το αιτηθεί στον index server οπου θα βρεί ποιος κόμβος έχει την πληροφορία και στην συνέχεια θα δημιουγήσει σύνδεση μεταξύ του πρώτου και του κόμβου που έχει το συγκεκριμένο δεδομένο.

β. Αποκεντρικά peer-to-peer δικτυα :Συνήθως κάθε κόμβος του δικτύου είναι servent(είναι κόμβοι που ταυτόχρονα είναι και clients και servers) αρα ταυτόχρονα εξυπηρετεί ή εξυπηρετήται .Εφόσον ισχύει κατι τέτοιο κάθε νέος κόμβος που εισέλθετε στο δίκτυο πρέπει να δηλώσει την παρουσία του σε όλους τους κόμβους που είναι κοντά και στην συνέχεια σε ολο το υπόλοιπο δικτύο.

γ. peer-to-peer δικτύα 3ης γενίας:Η φιλοσοφία αυτών των δικτύων είναι η ανωνυμία στον διαμοιρασμό πληροφορίας και στην κωδικοποίηση για να διαφυλάξει οτι δεν θα αποκτήσει άλλος κόμβος έλεγχο αν δεν έχει δικαιώματα.

2. Star : Σε κάθε star τοπολογία έχουμε έναν κεντρικό κόμβων ο οποίος είναι μεσολαβητής και διαβιβάζει τα μηνύματα μεταξύ των κόμβων γύρω απο αυτών.Η star τοπολογία μειώνει την πιθανότητα σφάλματος αφού ενώνει όλους τους κόμβους με τον κεντρικό ο οποίος είναι υπέθυνος για το broadcast οτι λαμβάνει για να το δούν όλοι οι κόμβοι αλλα είναι ευθύνη του λαβάνοντας κόμβου αν το αρχείο είναι δικο του και αν θα το αξιοποιήσει.Αν κάποιος απο τους κόμβους καταστραφεί εκτός απο τον κεντρικό κόμβο το σύστημα δεν παραλύει απλός απομονώνει τον συγκεκριμένο κόμβο . Τα πλεονεκτήματα τις συγκεκριμένης τοπολογίας είναι οτι έχουμε καλύτερη απόδοση καθώς για τη μεταφορά ενος μηνύματος είτε ενσύρματα είτε ασύρματα θα πρέπει να περάσει απο 3 συσκευές τον αποστολέα , τον κεντρικό κόμβο και τον παραλήπτη.Η τοπολογία με εναν κεντρικό κόμβο καθιστά απλή την επέκταση του δικτύου και εφόσον όλη η πληροφορία περνάει απο τον κεντρικό κόμβο είναι πιο εύκολο να ελέγξουμε το τι περνάει στο δίκτυο

μας.Επίσης σημαντικό πλεονέκτημα είναι η απλότητα του ως προς την δημιουργία τέτοιων δικτύων όπως και η συντήρηση τους.Τα μειωνεκτήματα αύτων των δικτύων είναι οτι όλο το δίκτυο βασίζεται σε έναν κόμβο οπότε η επέκταση του δικτύου γίνεται μέχρι το σημείο που μπορεί να εξυπηρετήση ο κεντρικός κόμβος.

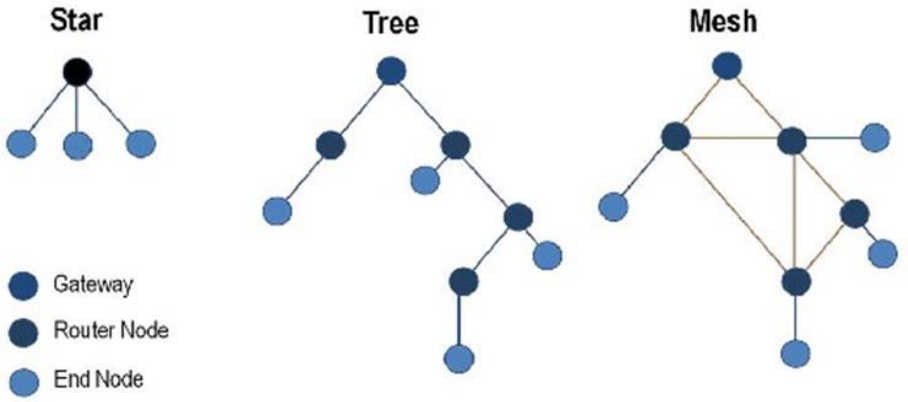


Star and peer-to-peer topology examples

3. Tree : Σε αυτή την τοπολογία έχουμε ιεραχία και πρώτο σε αυτή βρίσκεται το root note και στην συνέχεια λίγο πιο κάτω τα central hub όπου δημιουργούν το καθένα ξεχωριστά δική του τοπολογία τύπου star.Είναι ένας συνδιασμός τον 2 κατηγοριών που είδαμε και ονομάζεται hybrid.

Τα πλεονεκτήματα τις τοπολογίας tree είναι οτι σαν τοπολογία είναι πολυ δημοφιλής και υποστηρίζεται απο πολλούς καταστευαστές , μπορεί να γίνει σύνδεση 2 σημείων, όλοι οι κόμβοι έχουν πρόσβαση στο δικό τους δίκτυο αλλα και στο δίκτυο που υλοποείται απο τους "γονείς" τους.Τα μειωνεκτήματα είναι οτι αν ο κεντρικός κόμβος καταρρέυση ολο το δίκτυο θα καταστραφεί , είναι περίπλοκη η διαδικασία εγκατάστασης .

4. Mesh :Στην συγκεκριμένη τοπολογία οι κόμβοι θα πρέπει να συνεργαστούν αφού λειτουργούν σαν συνδετική κρίκοι για να υπάρξει συνολική μεταφορά πληροφορίας στο δίκτυο. Αυτό επιτυγχάνεται με 2 τρόπους καθορισμένη δρομολόγιση ή με πλημμυρισμα του δικτύου.Με την καθορισμένη δρομολόγηση τα δεδομένα ακολουθούν συγκεκριμένο μονοπάτι για να φτάσουν στον τελικό προορισμό ενδέχεται να χρειαστεί να περάσουν απο όλους τους κόμβους κάνοντας hops απο τον έναν στον άλλον.Για να πραγματοποιηθεί κατι τέτοιο θα πρέπει να τρέχουν συνεχώς αλγόριθμοι που θα βρίσκουν καινούργια μονοπάτια και κρατάνε το δικτυο λειτουργικό ακόμα και αν κάποιος κόμβος καταστραφεί.Στην τεχνική τις πλημμύρας ο κάθε κόμβος κάνει broadcast τα δεδομένα τους και στην συνέχεια οι παραλήπτες αναμεταδίδουν κατα αυτό τον τρόπο το δίκτυο γεμίζει με πληροφορία και καταλήγει στον επιθυμητό κόμβο.Τα mesh δίκτυα θεωρούνται ως ένα είδος ad hoc network.



11 3.3 Μοντέλο OSI

Μοντέλο OSI (Open Systems Interconnection) ή Μοντέλο επτά επιπέδων είναι ενα μοντέλο που ορίζει την διασύνδεση των δικτύων. Στα ασύρματα δίκτυα αισθητήρων απαίτειται η ύπαρξη των πρώτων 3 επιπέδων (φυσικού, ζεύξης δεδομένων,δικτύου) σε κάποιες περιπτώσεις και παραπάνω γιαυτό το λόγο θεωρήθηκε απαραίτητη η αναφορά στο μοντέλο OSI. Το συγκεκριμένο μοντέλο υποδιαιρεί τις λειτουργίες ενός τηλεπικοινωνιακού δικτύου σε μια κατακόυφη στοίβα επτά επιπέδων.Σε κάθε επίπεδο υπάρχει συγκεκριμένο πρωτόκολλο που θα πρέπει να παρέχει αναμενόμενη μορφή δεδομένων στο προηγούμενο και στο επόμενο επίπεδο.Πιο αναλυτικά :

1) Physical Layer (Φυσικό επίπεδο):

Είναι το χαμηλότερο επίπεδο του μοντέλου εκεί δηλαδή που γίνεται η δυαδική μετάδοση των δεδομένων.Στο φυσικό επίπεδο είναι το hardware ,συναντάμε συσκευές όπως repeaters ,hub, κάρτες δικτύου κτλ. Οι βασικές λειτουργίες του επιπέδου είναι :

1. Η έναρξη ή ο τερματισμός διασύνδεσης δυο επικοινωνιακών συσκευών.
2.Διαμόρφωση και αποδιαμόρφωση ψηφιακών δεδομένων.
3. Πολύπλεξη, οι συσκευές επικοινωνίας εξυπηρετούν παραπάνω απο ένα clients.

2) Data Link Layer(Επίπεδο Ζεύξης Δεδομένων) :

Το δεύτερο επίπεδο είναι για την αξιόπιστη μεταφορά δεδομένων στην καθορισμένη σύνδεση του πρώτου επιπέδου.Ονομάζεται και MAC layer .Οι διευθύνσεις των συσκευών είναι καθορισμένες εργοστασιακά και είναι φυσικές διευθύνσεις (MAC address).Στο συγκεκριμένο επίπεδο κάποια πρωτόκολλα μπορεί να υποδιαιρεθούν σεμικρότερα υποεπίδα:

1.Υποεπίπεδο MAC: γίνεται έλεγχος πρόσβασης στο κοινό μέσο.
2.Υποεπίπεδο LLC(logical link control): γίνεται έλεγχος λογικών συνδέσεων .

3) Network Layer (Επίπεδο δικτύου) :Ελέγχει τη λειτουργία του υποδικτύου.Οι λειουργίες που εκτελεί είναι :

1.Μεταγωγή στους κόμβους.

2.Δρομολόγηση.

3.Έλεγχος ροής.

4.Αποκατάσταση σφαλμάτων

4) Transport Layer (Επίπεδο μεταφοράς):Το επίπεδο μεταφοράς έχει τις εξής λειτουργίες:

1.Διαχείριση συνδέσεων.

2.Μεταβίβαση δεδομένων.

3.Έλεγχος ροής.

Αυτό το επίπεδο είναι υπέθυνο για να παρέχει αξιοπιστία στην μεταφορά δεδομένων στα παραπάνω επίπεδα και αυτό το καταφέρνει με τους εξής τρόπους :

1.Έλεγχος ροής .

2.Κατάτμηση .

3.Αποτμηματοποίηση.

4.Έλεγχος σφαλμάτων.

Ακόμα είναι σε θέση να γνωρίζει ποια πακέτα δεν παραδόθηκαν και να τα στείλει ξανα.

5) Session Layer (Επίπεδο Συνόδου):Το επίπεδο συνόδου υπεύθυνο για τον έλεγχος του διαλόγου μεταξύ των άκρων της επικοινωνίας. Επιτρέπει στους χρήστες να κάνουν συνόδους και να οργανώνουν-συγχρονίζουν την μεταφορά μηνυμάτων.Τα προβλήματα που καλείται να αντιμετωπίσει είναι:

1.FDX(full duplex) είναι όταν 2 συνομιλητές μιλάνε την ίδια στιγμή και δεσμέυουν δυο κανάλια.

2.HDX(half duplex) είναι όταν μόνο ένα κανάλι είναι διαθέσιμο και μιλάνε ένας ένας.

Το επίπεδο αυτό έχει τις εξής λειτουργίες:

1.Checkpoint (αποθηκέυη την κατάσταση)

2.Adjournment (αναβολή)

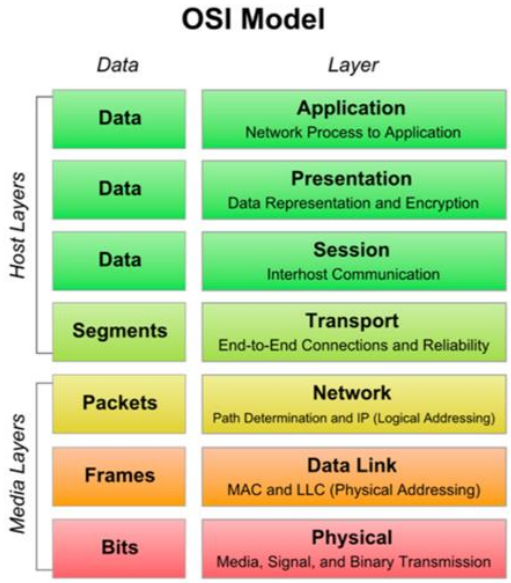
3.Termintation(τερματισμός)

4.Restart(επανεκκίνηση).

6) Presentation Layer (Επίπεδο παρουσίασης):Το επίπεδο παρυσίασης είναι υπέυθυνο για την αναπαράσταση δεδομένων και την κρυπτογράφηση.Τα δεδομένα επεξεγάζονται

(κρυπτογραφούνται- κωδικοποιούνται) σύμφωνα με το πρωτόκολλο τις κάθε εφαρμογής με τέτοιο τρόπο έτσι ώστε να είναι αναγνωρίσιμα απο τις εφαρμογές στο επίπεδο μεταφορών.

7) Application Layer (Επίπεδο μεταφορών): Είναι το ανώτερο επίπεδο του μοντέλου OSI και παρέχεται στις εφαρμογές πρόσβαση στο δίκτυο.



12 4.1 Ορισμοι:

Ενέργεια

Ο αριθμός των εφαρμογών που υποστηρίζονται από ασύρματα δίκτυα αισθητήρων είναι μεγάλος και έχει δημιουργήσει ακόμα μεγαλύτερο ενδιαφέρον από την ερευνητική κοινότητα. Διάφορες εφαρμογές από μικρού μεγέθους βιομηχανική παρακολούθηση έως μεγάλης κλίμακας περιβαλλοντική παρακολούθηση. Σε όλες τις περιπτώσεις, απαιτείται ένα λειτουργικό δίκτυο για την εκπλήρωση των αποστολών εφαρμογής. Επιπλέον, η κατανάλωση ενέργειας των κόμβων είναι ένα τεράστιο ζητούμενο για τη μεγιστοποίηση της διάρκειας ζωής του δικτύου και ίσως η μεγαλύτερη πρόκληση . Σε αντίθεση με άλλα δίκτυα, μπορεί να είναι επικίνδυνο, πολύ ακριβό ή ακόμη και αδύνατο να φορτιστεί ή να αντικατασταθούν εξαντλημένες μπαταρίες λόγω της εχθρικής φύσης του περιβάλλοντος. Οι ερευνητές καλούνται να σχεδιάσουν ενεργειακά αποδοτικά πρωτόκολλα επιτυγχάνοντας τις επιθυμητές λειτουργίες δικτύου.Η μεγαλύτερη ανησυχία στον σχεδιασμό τέτοιου δικτύου είναι πώς να εξοικονομήσετε ενέργεια κόμβου διατηρώντας

παράλληλα την επιθυμητή συμπεριφορά δικτύου.Ο στόχος είναι οποιασδήποτε ενεργειακά αποδοτική τεχνική για την μεγιστοποίηση της διάρκειας ζωής του δικτύου.

Ένα δίκτυο αισθητήρων μπορεί να συγκεντρώσει και να μεταδώσει δεδομένα για χρόνια ενω απαιτεί μικρή κατανάλωση ενέργειας απο τους κόμβους . Οι κόμβοι αισθητήρων πρέπει να εκμεταλλευτούν τη λειτουργική ποικιλομορφία, όπως οι μεγάλες περιόδους αδράνειας μεταξύ των μεταδόσεων μειώνοντας την κατανάλωση ενέργειας. Ο χρήστης πρέπει να καθορίσει με ακρίβεια την απόδοση του δικτύου και τις απαιτήσεις χρησιμοποιώντας μετρήσεις ακριβείας έτσι ώστε το δίκτυο να λειτουργεί σωστά και με αξιοπιστία για αρκετός υπολογισμός ώστε να ικανοποιήσει τις συγκεκριμένες απαιτήσεις του χρήστη.

Sleep mode

Το σημαντικότερο ζήτημα στα ασύρματα δίκτυα αισθητήρων είναι η εξοικονόμηση ενέργειας .Πλεον στις περισσότερες περιπτώσεις και όπου φυσικά το επιτρέπουν η συνθήκες χρησιμοποιούνται ανανεώσιμες πηγές ενέργειας(ηλιακά πάνελ , ανεμογεννήτριες κτλ) αλλά αυτό απο μόνο του δεν είναι αρκετό . Γιαυτό το λόγο δημιουργήθηκε η τεχνική sleep mode όπου θέτει τους αισθητήρες σε κατάσταση ύπνου τις χρονικές στιγμές κατά τις οποίες δεν λαμβάνουν μετρήσεις ή άλλα πακέτα μηνυμάτων από τους γύρω τους ετσι ώστε να μην καταναλώνουν ενέργεια.Το κυρίως πρόβλημα που συναντάμε σε αυτή την τεχνική το να μη γίνει λήψη κάποιου πακέτου όταν κάποιος κόμβος κοιμάται με αποτέλεσμα το εισερχόμενο πακέτο να χαθεί.Η τεχνική που καλείται για να αντιμετωπίσει κάτι τέτοιο λέγεται time synchronization, με αυτήν την τεχνική συγχρονίζονται ολα τα ρολόγια των αισθητήρων έτσι ώστε να ξυπνούν απο το sleep mode και να βρίσκονται σε κατάσταση listening την κατάλληλη χρονικά στιγμή για να λάβουν ένα πακέτο ή ξυπνάνε για να μεταδόσουν κάποιο πακέτο.Με λίγα λόγια στην κατάσταση sleep είναι σε αναμονή ενώ στην κατάσταση listen οι κόμβοι είναι ενεργοί.

Δομή Superframe

Superframe είναι η οριοθέτηση της διάρκειας πρόσβασης στο κανάλι το οποίο μεταδίδεται η πληροφορία απο τον διαχειριστή.Ο σκοπός του superframe είναι η δεσμευμένη απόδοση bandwidth και επίσης η χαμηλή καθυστέρηση στην επικοινωνία.Καθορίζεται με την μετάδοση ενός πλαισίου που περιλαμβάνει μια ενεργή και μια ανενεργή περιοχή.Είναι χωρισμένο σε 16 ίσες θυρίδες και το στέλνει ο διαχειριστής.Ανάμεσα στα πλαίσια υπάρχει Contention Access

Period(περίοδο ς πρόσβασης με διαμάχη) όπου όποια συσκευή θα προσπαθήσει να επικοινωνήσει κατα το Contention Access Period θα πρέπει να αναμετρηθεί με τις υπόλοιπες συσκευές χρησιμοποιόντας το CSMA-CA με χρονοθυρίδες.

GTS (Guaranteed Time Slots)

Όταν ο διαχειριστής χρησιμοποίει εφαρμογές συγκεκριμένου εύρους ή λανθάνουσας κατάστασης μπορεί να χρησιμοποιήσει τμήματα απο την ενεργή περιοχή του superframe που ονομάζονται GTS.

Αποτελούν την contention free period που βρίσκεται στο τέλος τις ενεργής περιοχής.Το GTS μπορεί να χρησιμοποιηθεί μονο απο τον διαχειριστή για την επικοινωνία του με άλλες συσκευές. Τα GTS χρησιμοποιούν παραπάνω απο μία χρονοθυρίδα αλλα πρέπει να έχει ολοκληρώσει τις λειτουργίες του πριν την contention free period και κάθε συσκευή η οποία μεταδίδει σε κάποιο GTS πρέπει να έχει ολοκληρώσει τις λειτουργίες του πριν την έναρξη κάποιου άλλου GTS ή της contention free period.Μπορούν να επεκταθούν παραπάνω απο το superframe που αντιστοιχή αρκει να αποθηκεσει την αρχική του θυρίδα,την κατεύθυνση του , το μήκος του και την διεύθυνση της συσκευής.

BER(Bit Error Rate)

Σε όλες τα δίκτυα επικοινωνιών υπάρχει ένας αριθμός πακέτων τα οποία φτάνουν στον παραλήπτη με λάθος τρόπο για διάφορους λόγους (π.χ. παρεμβολές , εξασθένιση) .Αυτός ο αριθμός λέγεται Bit Error Rate.Για να καταπολεμήσουμε αυτό το πρόβλημα προσθέτουμε επιπλέον bits ελέγχου στο πακέτο που στέλνουμε για να μπορεί ο δέκτης να εντοπίσει που σε ποία πακέτα υπάρχει λάθος και να ζητήσει την επανεκπομπή του πακέτου το ονομαζόμενο πρωτόκολλο AQR ή να τα διορθώνει στον δέκτη με την τεχνική Forward Error Correction.

13 4.2 ΠΡΩΤΟΚΟΛΛΑ MAC

Αρχές σχεδίασης MAC πρωτοκόλλων:

1. Αποφυγή συγκρούσεων.
2. Ελαχιστοποίηση κατανάλωσης ενέργειας.
3.Επεκρασιμότητα.
4.Προσαρμοστικότητα.

5.Βέλτιστη αξιοποίηση του καναλιού εκπομπής

6.Καθυστέρηση.

7.Δικαιοσύνη.

8.Διεκπεραίωση.

Κύριες αιτίες κατανάλωσης ενέργειας στα MAC πρωτόκολλα έχουμε:

1.Στις συγκρούσεις πακέτων.

2.Στην μακρόχρονη κατάσταση αναμονής λήψης δεδομένων(idle).

3.Κατά το φαινόμενο Overhearing.

4.Στο κόστος των πακέτων ελέγχου.

14 4.3 Πρωτόκολλο CSMA-CA

Η ανίσχευση συγκρούσεων απαιτεί full Duplex γραμμή.Στην περίπτωση που δεν ανιχνευτεί σύγκρουση στην περιοχή του αποστολέα δεν σημαίνει απαραίτητα οτι δεν έγινε σύγκρουση στην περιοχή του δέκτη γιαύτο χρησιμοποιείται το CSMA με επιβεβαίωση CSMA-CA και με τις τεχνικές RTS/CTS (Ready to send / Clear to send).Με αυτή την τεχνική κάθε κόμβος δήλωνει άμα μπορεί να λάβει πακέτο και έτσι αντιμετωπίζουμε την σύγκρουση πακέτων άρα και την κατανάλωση ενέργειας.

15 4.4 Contention - based protocols

MACA

MACA(Mutiple Access with Collision Avoidance) είναι το πρωτόκολλο λειτουργεί με τον μηχανισμό ανίχνευσης φέρουσας(πρώτα θα ακούσει για καθαρό μέσω) αλλά αυτό απο μόνο του δεν είναι αρκετό για να πετύχουμε καλη απόδοση χωρίς προβληματα(π.χ. συγκρούσεις πακέτων αναμεταδώσεις κτλ.).Για να μπορέσει να αντιμετωπίσει αυτά τα προβλήματα το MACA χρησιμοποιεί την τεχνική RTS/CTS.Πιο συγκεκριμένα ο κόμβος που θέλει να μεταδώσει ένα πακέτο σε έναν άλλον κόμβο στέλνει πρώτα ένα πακέτο RTS προς όλες τις κατευθύνσεις (broadcast) δηλώνοντας έτσι την επιθυμία του να μετάδοση σε συγκεκριμένο κόμβο σε όλους τους γείτονες.Όλοι οι γείτονες που λαμβάνουν το RTS εφόσον το πακέτο δεν απευθύνεται σε αυτούς

δεν απαντούν.Αν κάποιος απο τους υπόλοιπους κόμβους δεν μεταδίδει πακέτα στον κόμβο που δέχθηκε το RTS τότε ο κόμβος θα στείλει CTS και η μετάδοση θα γίνει κανονικά.Σε αντίθετη περίπτωση δηλαδή ο κόμβος που δέχεται το RTS πακέτο επικοινωνεί με άλλον κόμβο δεν θα στείλει CTS με αποτέλεσμα η μετάδοση να μην πραγματοποιηθεί και να αποφύγουμε την σύγκρουση πακέτων.

S-MAC

Στο S-MAC οι αισθητήρες βρίσκονται σε δύο καταστάσεις στο listening και στο sleep mode.Ο χρόνος που διαρκεί μια φάση listening συν τον χρόνο που διαρκεί μια φάση sleep ονομάζονται frame δηλαδή Tframe = Tlisten + Tsleep. Η αναλογία μεταξύ τις περιόδου listening και της περιόδου ενός frame ονομάζεται duty cycle άρα έχουμε Duty Cycle = Tlisten/ Tframe. Το πρόβλημα που συναντάμε στα S-MAC πρωτόκολλα είναι οτι κάθε κόμβος που θέλει να μεταδόση θα πρέπει να περιμένει να ξυπνήσει ο γείτονας αλλίως το πακέτο θα χαθεί.Αυτο προσθέτει καθυστέρηση στις μεταδόσεις αρα αυξάνει την σπατάλη ενέργειας. Οι τεχνική που καλείται να διορθώσει αυτό το πρόβλημα λέγεται virtual clustering (εικονική ομαδοποιηση).Με αυτή την τεχνική κάθε κόμβος αποφασίζει μόνος του πότε θα μπεί σε λειτουργία sleep mode και ενημερώνει και τους υπόλοιπους κόμβους με αποτέλεσμα όλοι οι γειτονικοί κομβοι να ακολουθούν το πρόγραμμα του και να ξυπνάνε-κοιμούνται τις ίδιες χρονικές στιγμές μειώνοντας τις καθυστερήσεις στο ελάχιστο δυνατόν. Αυτη η τεχνική απαιτεί περιοδικό συντονισμό των ρολογιών των κόμβων για να υπάχει συγχρονισμός όπως επίσης και συνοριακών κόμβων που βρίσκονται ανάμεσα στα virtual clustering για να ακολουθούν το ίδιο πρόγραμμα ύπνου ώστε να μην χάνεται η επαφή.

T-MAC

Το T-MAC πρωτόκολλο επιτυγχάνει πιο χαμηλή κατανάλωση σε σχέση με το S-MAC γιατί δεν έχει σταθερό duty cycle.Ο κόμβος μεταβαίνει σε κατάσταση ύπνου μετά από ένα χρονικό διάστημα Tact στο οποίο δεν έχει προκύψει κάποιο γεγονός. Το χρονικό διάστημα ‘Tact’ είναι το ελάχιστο χρονικό διάστημα idle listening, δηλαδή να ακούσει για τηλεπικοινωνιακή κίνηση όταν τίποτα δεν έχει σταλεί. Έτσι με το πρωτόκολλο T-MAC πετυχαίνουμε πολύ καλύτερη λιγότερη κατανάλωση ενέργειας με συνέπεια να έχουμε πιο μεγάλες καθυστερήσεις.

Preamble sampling

Στην Preamble sampling τεχνική δεν συχρονίζονται οι κόμβοι του δικτύου με ακρίβεια.Οι κόμβοι είναι σε sleep mode για συγκεκριμένο διάστημα , μόλις ολοκληρωθεί ξυπνούν και αφουγκράζονται το δίκτυο.Όταν κάποιος απο τους κόμβους επιθυμεί να στείλει ένα πακέτο , πρώτα στέλνει ένα preamble σε όλους τους κόμβους και τους ενημερώνει οτι θα γίνει αποστολή και να μείνουν ενεργοί δηλαδή να μην μπούνε σε sleep mode.Αν μετά απο ένα χρονικό διάστημα οι κόμβοι δεν λάβουν preamble μπαίνουν πάλι σε κατάσταση sleep και αυτό επαναλαμβάνεται συνεχώς όσο το δίκτυο είναι σε λειτουργία.

B-MAC

Το πρωτόκολλο B-MAC είναι ανταγωνιστικό πρωτόκολλο το οποίο ικανοποιεί κάποιες προδιαγραφές ώστε να χρησιμοποιείται σε ασύρματα δίκτυα
αισθητήρων όπως η χαμηλή κατανάλωση ενέργειας, η αποτελεσματική αποφυγή συγκρούσεων και η απλή υλοποίηση.Είναι βασισμένο στον μηχανισμό CSMA(Carrier Sense Multiple Access) για να αποφύγει τις συγκρούσεις πακέτων και στον αλγόριθμο οπισθοχώρησης (back-off).Το πρωτόκολλο χρησιμοποιεί μηχανισμό εκτίμησης ελευθέρων καναλιών, back-off πακέτα για την διαχείρισή τους και άκουσμα χαμηλής κατανάλωσης για επικοινωνία με χαμηλή ενεργειακή κατανάλωση και δεν διαθέτει μηχανισμό RTS/CTS.

PAMAS

PAMAS (Power Aware MultiAcces protocol with Sigaling) το πρωτόκολλο αποτελεί μια παραλλαγή του MACA και χρησιμοποιεί ξεχωριστό κανάλι για την σηματοδοσία για την αποστολή RTS/CTS και ξεχωριστό κανάλι για την ανταλλαγή πλαισίων δεδομένων.Το ξεχωριστό κανάλι για την σηματοδοσία δίνει την δυνατότητα στους κόμβους να αποφασίσουν την χρονική στιγμή και την χρονική διάρκεια που θα μεταβούν σε ανενεργή κατάσταση. Ένας κόμβος μπορεί να βρίσκεται σε μια από τις έξι παρακάτω καταστάσεις:

1.Ανενεργή (idle), είναι η κατάσταση που βρίσκεται ένας σταθμός όταν ένας σταθμός δεν μεταδίδει ή δεν λαμβάνει κάποιο πακέτο, ή δεν έχει κανένα πακέτο για μετάδοση, ή έχει αποθηκευμένα κάποια πακέτα για μετάδοση αλλά δεν μπορεί να τα μεταδώσει επειδή κάποιος γειτονικός σταθμός παραλαμβάνει κάποιο πακέτο.

2.Αναμονή για την παραλαβή ενός CTS πακέτου (AwaitCTS), μεταβαίνει σε αυτή την κατάσταση όταν θέλει να μεταδώσει ένα πακέτο, μεταδίδει πρώτα ένα RTS πλαίσιο.

3.Δυαδικής εκθετική οπισθοχώρησης (Binary Exponential Backoff), ο σταθμός μεταβαίνει σε αυτή την κατάσταση όταν το CTS πλαίσιο που αναμένει δεν το παραλάβει μέσα σε ένα συγκεκριμένο χρονικό διάστημα.

4.Αναμονής παραλαβής πακέτου (Await Packet), ο σταθμός μεταβαίνει σε αυτή την κατάσταση την στιγμή όπου ο παραλήπτης του RTS πλαισίου θα μεταδώσει το CTS πλαίσιο.

5.Παραλαβής πακέτου (Receive Packet), ο σταθμός μεταβαίνει σε αυτή την κατάσταση αν μέσα σε αυτό το χρονικό διάστημα ο παραλήπτης αρχίσει να λαμβάνει το πακέτο δεδομένων και μεταδίδει έναν παλμό busy πάνω από το κανάλι σηματοδοσίας.

6.Μετάδοσης πακέτου (Transmit Packet), ο σταθμός μεταβαίνει σε αυτή την κατάσταση όταν παραλάβει ένα CTS πλαίσιο, ο σταθμός ξεκινά την μετάδοση του πακέτου.

Σύγκριση contention-based πρωτοκόλλων

	MACA	S-MAC,T-MAC	B-MAC	PAMAS
Πλεονεκτήματα	Αξιόπιστη μετάδοση ακόμα και σε υποβρύχιες καταστάσεις κατα την μεταφορά bit.	Χαμηλή κατανάλωση ενέργειας.	Μικρό overhead όταν το δίκτυο είναι σε κατάσταση idle, απλή υλοποίηση και χαμηλή κατανάλωση ενέργειας.	Απλή υλοποίηση και επιτρέπει την εύκολη επέκταση του δικτύου (scalability).
Μειονεκτήματα	Επικεντρώνεται μόνο στα bit και όχι στην μεταφορά μεγαλύτερου επιπέδου πληροφορίας	Μεγάλη καθυστέρηση λόγου του περιοδικού ύπνου κάθε κόμβου.Πρόβλημα στην μετάδοση broadcast επειδή οι κόμβου δεν ακολουθούν τα ίδια προγράμματα.	Φαινόμενο overhearing, κακή απόδοση σε μεγάλη κίνηση και μεγάλη καθυστέρηση μετάδοσης.	Δεν έχει μηχανισμό επιβεβαίωσης RTS/CTS, έχει σχετικά μεγάλη κατανάλωση ενέργειας.

16 4.5 Schedule - based protocols

LEACH

Ένα απο τα πιο σημαντικά πρωτόκολλα επικοινωνίας στα ασύρματα δίκτυα αισθητήρων είναι το LEACH όπου ενδιαφέρεται κυρίως για την χαμηλή κατανάλωση ενέργειας.Στο LEACH οι κόμβοι χωρίζονται σε clusters (ομάδες) και κάθε cluster ορίζει έναν αρχηγό (cluster head).

Κάθε κόμβος της ομάδας επικοινωνεί μονο με τον αρχηγό τους είναι υπεύθυνος για την συγκέντρωση, την επεξεργασία και την αποστολή των δεδομένων στο επόμενο επίπεδο.Τα κριτήρια για να αποφασισθεί αν ένας κόμβος θα είναι cluster head είναι το προτεινόμενο ποσοστό cluster head για ένα δίκτυο και ο αριθμός των φορών που ένα κόμβος έχει γίνει ήδη αρχηγός ομάδας. Ο σκοπός είναι να διατηρείται σταθερό το ποσοστό των αρχηγών κάθε φορά που γίνεται επανάληψη και επίσης επιτυγχάνεται εξισορρόπηση της κατανάλωσης ενάργειας των κόμβων καθώς όλοι οι κόμβοι γίνονται αρχηγοί της ομάδας.

SMACS

Το πρωτόκολλο SMACS (Sensor Medium Access Control Protocol) επιτυγχάνει την έναρξη του δικτύου καθώς και την οργάνωση του επιπέδου ζεύξης δεδομένων και ο αλγόριθμος EAR (Energy Aware Routing) δίνει την δυνατότητα για διαφανή σύνδεση των ασύρματων κόμβων στο δίκτυο αισθητήρων. Το SMACS είναι ένα κατανεμημένο (πρωτόκολλο) χτισίματος δομής το οποίο δίνει την δυνατότητα στους κόμβους να ανακαλύψουν τους γείτονές τους και να προγραμματίσουν χρονικά την εκπομπή και την λήψη χωρίς την ανάγκη ύπαρξης κόμβων που θα παίζουν το ρόλο του κεντρικού οργανωτή, είτε σε τοπικό είτε σε καθολικό επίπεδο. Σε αυτό το πρωτόκολλο, η ανακάλυψη των γειτόνων και η ανάθεση των φάσεων του καναλιού συνδυάζονται έτσι ώστε από την ώρα που οι κόμβοι θα ακούσουν τους γείτονές τους θα έχουν σχηματίσει ένα ολοκληρωμένο δίκτυο. Ένας επικοινωνιακός δεσμός αποτελείται από ένα

ζευγάρι χρονοθυρίδων που λειτουργούν με την τυχαία επιλογή συχνότητας (σταθερής ή με αναπηδήσεις). Αυτό είναι εφικτό αφού το διαθέσιμο εύρος συχνοτήτων είναι πολύ μεγαλύτερο από τον αναμενόμενο ρυθμό μετάδοσης. Με τον τρόπο αυτό δεν είναι αναγκαίο να υπάρχει συγχρονισμός όλων των κόμβων του δικτύου αλλά μόνο αυτών που επικοινωνούν. Η διατήρηση της ενέργειας επιτυγχάνεται με την χρήση ενός τυχαίου προγράμματος ξυπνήματος κατά την φάση της σύνδεσης και με κλείσιμο του πομποδέκτη κατά την φάση των κενών χρονοθυρίδων. Το πρωτόκολλο EAR πρωτόκολλο προσπαθεί να προσφέρει συνεχή υπηρεσία στους κινούμενους κόμβους, είτε κάτω από συνθήκες κίνησης είτε σταθερότητας. Εδώ οι κινούμενοι κόμβοι έχουν τον πλήρη έλεγχο της επικοινωνίας και αποφασίζουν επίσης για το πότε να διακόψουν την σύνδεση μειώνοντας έτσι την επικεφαλίδα. Το EAR είναι διαφανές προς το SMACS και έτσι το τελευταίο είναι λειτουργικό μέχρι την είσοδο κινούμενων κόμβων στο δίκτυο. Σε αυτό το μοντέλο το δίκτυο υπολογίζεται να είναι γενικά στατικό, δηλ. κάθε κινούμενος κόμβος έχει ένα αριθμό στατικών σταθμών στην εμβέλειά του. Ένα μειονέκτημα ενός τέτοιου σχήματος ανάθεσης χρονοθυρίδων είναι η πιθανότητα μέλη που ανήκουν σε διαφορετικά υποδίκτυα να μην συνδεθούν ποτέ.

TRAMA

Το TRAMA είναι ένα πρωτόκολλο όπου οι κόμβοι συγχρονίζονται μεταξύ τους και ο χρόνος είναι μοιρασμένος με τυχαίο τρόπο σε αυτούς, ανταλλάσσουν πληροφορίες στους γείτονες για το πότε μεταδίδουν πακέτα.Το πρόβλημα επιλογής της κατάλληλης χρονοθυρίδας (timeslot) λύνεται με τον
υπολογισμό της προτεραιότητας που έχει ένας κόμβος για κάθε θυρίδα. Ως αποτέλεσμα, κάθε κόμβος θα μεταδίδει μόνο στις χρονικές θυρίδες που έχει την μέγιστη προτεραιότητα.

	LEACH	SMACS	TRAMA
Πλεονεκτήματα	Πλήρως κατανεμημένο πρωτόκολλο , αυξάνει την διάρκεια ζωής του δικτύου λόγο βέλτιστης κατανάλωσης ενέργειας και δεν χρειάζεται να γνωρίζουμε ολόκληρο το δίκτυο.	Μικρή καθυστέρηση στην μετάδοση, αποτελεσματική διαχείριση ενέργειας, επεκτασιμότητα (scalability).	Πολύ καλή ενεργειακή απόδοση γιατί αποφεύγονται οι συγκρούσεις, το περιοδικό listening και το φαινόμενο overhearing (κρυφάκουσμα).
Μειονεκτήματα	Δεν έχει καλή απόδοση σε δίκτυα μεγάλης κλίμακας και έχει επιπλέον overhead λόγο του dynamic clustering μηχανισμού.	Η πιθανότητα μέλη που ανήκουν σε διαφορετικά υποδίκτυα να μην συνδεθούν ποτέ.	Μεγάλη καθυστέρηση. Ιδανικό για εφαρμογές που απαιτούν ελάχιστη κατανάλωση ενέργειας αλλά δεν τις απασχολεί η καθυστέρηση.

17 ΚΕΦΑΛΑΙΟ 5

18 5.1 Ασφαλεια σε ασύρματα δίκτυα αισθητήρων

Το WSN είναι ένας ειδικός τύπος δικτύου. Μοιράζεται ορισμένες ομοιότητες με ένα τυπικό δίκτυο υπολογιστών, αλλά παρουσιάζει επίσης πολλά χαρακτηριστικά που είναι μοναδικά σε αυτό. Οι υπηρεσίες ασφαλείας σε ένα WSN πρέπει να προστατεύουν τις πληροφορίες που κοινοποιούνται μέσω του δικτύου και τους πόρους από επιθέσεις και κακή συμπεριφορά των κόμβων. Οι πιο σημαντικές απαιτήσεις ασφαλείας στο WSN : Εμπιστευτικότητα δεδομένων, ο

μηχανισμός ασφαλείας πρέπει να διασφαλίζει ότι κανένα μήνυμα στο δίκτυο δεν είναι κατανοητό από κανέναν εκτός από τον προοριζόμενο παραλήπτη. Σε ένα WSN, το ζήτημα της εμπιστευτικότητας πρέπει να καλύπτει τις ακόλουθες απαιτήσεις :

1) Ένας κόμβος αισθητήρα δεν θα πρέπει να επιτρέπει την πρόσβαση στις αναγνώσεις του από τους γείτονές του, εκτός εάν εξουσιοδοτηθούν να το πράξουν.

2) Ο βασικός μηχανισμός διανομής θα πρέπει να είναι εξαιρετικά ανθεκτικό.

3) Οι δημόσιες πληροφορίες όπως οι ταυτότητες αισθητήρων και τα δημόσια κλειδιά των κόμβων θα πρέπει επίσης να κρυπτογραφούνται σε ορισμένες περιπτώσεις για προστασία από επιθέσεις ανάλυσης κυκλοφορίας.

Ακεραιότητα δεδομένων: Ο μηχανισμός θα πρέπει να διασφαλίζει ότι κανένα μήνυμα δεν μπορεί να αλλάξει από μια οντότητα καθώς περνά από τον αποστολέα στον παραλήπτη.

Διαθεσιμότητα: Οι απαιτήσεις αυτές διασφαλίζουν ότι οι υπηρεσίες ενός ασύρματου δικτύου αισθητήρων θα πρέπει να είναι διαθέσιμες πάντα ακόμη και όταν υπάρχουν εσωτερικές ή εξωτερικές επιθέσεις, όπως μια επίθεση άρνησης υπηρεσίας (DoS).

Οι ερευνητές έχουν προτείνει διαφορετικές προσεγγίσεις για την επίτευξη αυτού του στόχου. Ενώ ορισμένοι μηχανισμοί χρησιμοποιούν πρόσθετη επικοινωνία μεταξύ κόμβων, άλλοι προτείνουν τη χρήση ενός κεντρικού συστήματος ελέγχου πρόσβασης για τη διασφάλιση επιτυχούς παράδοσης κάθε μηνύματος στον παραλήπτη του.

Data freshness: Αυτό σημαίνει ότι τα δεδομένα είναι πρόσφατα και διασφαλίζει ότι κανένας αντίπαλος δεν μπορεί να αναπαράγει παλιά μηνύματα. Αυτή η απαίτηση είναι ιδιαίτερα σημαντική όταν οι κόμβοι χρησιμοποιούν κοινόχρηστα κλειδιά για επικοινωνία μηνυμάτων,

όπου ένας πιθανός αντίπαλος μπορεί να ξεκινήσει μια επίθεση επανάληψης χρησιμοποιώντας το παλιό κλειδί καθώς το νέο κλειδί ανανεώνεται και διαδίδεται σε όλους τους κόμβους στο ασύρματο δίκτυο αισθητήρων.Μπορεί να προστεθεί ένας μετρητής σε κάθε πακέτο για να ελέγξετε το data freshness.

Αυτο-οργάνωση: Κάθε κόμβος σε ένα δίκτυο πρέπει να είναι αυτο-οργανωμένος και αυτοθεραπευόμενος. Αυτό θέτει επίσης μια μεγάλη πρόκληση για την ασφάλεια. Η δυναμική φύση ενός δικτύου τέτοιου τύπου καθιστά μερικές φορές αδύνατη την ανάπτυξη οποιουδήποτε προεγκατεστημένου μηχανισμού κοινόχρηστου κλειδιού μεταξύ των κόμβων και του σταθμού βάσης(base station). Έχουν προταθεί ορισμένα βασικά σχήματα προ-διανομής στο πλαίσιο της συμμετρικής κρυπτογράφησης . Ωστόσο, για την εφαρμογή κρυπτογραφικών τεχνικών δημόσιου κλειδιού ένας αποτελεσματικός μηχανισμός κατανομής κλειδιών είναι πολύ απαραίτητος. Είναι επιθυμητό οι κόμβοι να αυτο-οργανώνονται μεταξύ τους όχι μόνο για δρομολόγηση αλλά και για την πραγματοποίηση βασικής διαχείρισης και ανάπτυξης σχέσεων εμπιστοσύνης.

Ασφαλής εντοπισμός: Σε πολλές περιπτώσεις, είναι απαραίτητο να εντοπίζετε με ακρίβεια και αυτόματα κάθε κόμβος . Για παράδειγμα, ένα δίκτυο που έχει σχεδιαστεί για τον εντοπισμό σφαλμάτων απαιτεί ακριβείς τοποθεσίες κόμβων αισθητήρα για την αναγνώριση των βλαβών. Ένας δυνητικός αντίπαλος μπορεί εύκολα να χειριστεί και να παράσχει ψευδείς πληροφορίες τοποθεσίας αναφέροντας λάθος ισχύ σήματος(αναπαραγωγή μηνυμάτων κλπ.)εάν οι πληροφορίες τοποθεσίας δεν είναι σωστά ασφαλισμένες. Υπάρχει μια τεχνική που ονομάζεται verifiable multi-lateration (επαληθεύσιμη πολλαπλή καθυστέρηση). Σε πολλαπλές πλευρές, η θέση μιας συσκευής υπολογίζεται με ακρίβεια από μια σειρά γνωστών σημείων αναφοράς. Οι κατασκευαστες έχουν χρησιμοποιήσει έλεγχο ταυτότητας και οριοθέτηση απόστασης για να διασφαλίσουν την ακριβή τοποθεσία ενός κόμβου. Λόγω της χρήσης του ορίου απόστασης, ένας επιθετικός κόμβος μπορεί να αυξήσει μόνο την απόσταση από ένα σημείο αναφοράς. Ωστόσο, για να διασφαλιστεί η συνοχή της τοποθεσίας, ο εισβολέας θα πρέπει επίσης να αποδείξει ότι η

απόστασή του από άλλο σημείο αναφοράς είναι μικρότερη. Επειδή δεν είναι δυνατό να το αποδείξει είναι δυνατόν να εντοπιστεί ο εισβολέας.

Secure range-independentlocalization: Θεωρείται ότι οι εντοπιστές είναι αξιόπιστοι και δεν μπορούν να τεθούν σε κίνδυνο από οποιονδήποτε εισβολέα. Ένας αισθητήρας υπολογίζει τη θέση του ακούγοντας τις πληροφορίες φάρου που αποστέλλονται από κάθε εντοπιστή που περιλαμβάνει τις πληροφορίες θέσης του εντοπιστή. Τα μηνύματα beacon κρυπτογραφούνται χρησιμοποιώντας ένα κοινό καθολικό συμμετρικό κλειδί που είναι προδιανεμημένο στους κόμβους του αισθητήρα. Χρησιμοποιώντας τις πληροφορίες από όλους τους φάρους που λαμβάνει ένας κόμβος αισθητήρα, υπολογίζει την κατά προσέγγιση θέση του με βάση τις συντεταγμένες των εντοπιστών. Στη συνέχεια, ο κόμβος του αισθητήρα υπολογίζει μια επικαλυπτόμενη περιοχή κεραίας χρησιμοποιώντας ένα σχήμα πλειοψηφίας. Η τελική θέση του κόμβου αισθητήρα προσδιορίζεται με τον υπολογισμό του κέντρου βάρους της επικαλυπτόμενης περιοχής κεραίας.

Συγχρονισμός χρόνου: Οι περισσότερες εφαρμογές σε δίκτυα αισθητήρων απαιτούν συγχρονισμό χρόνου. Οποιοσδήποτε μηχανισμός ασφαλείας θα πρέπει επίσης να συγχρονίζεται με το χρόνο. Ένα συνεργατικό δίκτυο μπορεί να απαιτεί συγχρονισμό μεταξύ μιας ομάδας αισθητήρων.

Έλεγχος ταυτότητας: Διασφαλίζει ότι ο κόμβος επικοινωνίας είναι αυτός που ισχυρίζεται ότι είναι. Ένας αντίπαλος μπορεί όχι μόνο να τροποποιήσει πακέτα δεδομένων αλλά και να αλλάξει μια ροή πακέτων με την έγχυση πακέτων. Είναι επομένως απαραίτητο για έναν δέκτη να διαθέτει έναν μηχανισμό για να επαληθεύει ότι τα λαμβανόμενα πακέτα προέρχονται πράγματι από τον πραγματικό κόμβο αποστολέα. Σε περίπτωση επικοινωνίας μεταξύ δύο κόμβων, ο έλεγχος ταυτότητας δεδομένων μπορεί να επιτευχθεί μέσω ενός κωδικού ελέγχου ταυτότητας μηνυμάτων (MAC) που υπολογίζεται από το κοινό μυστικό κλειδί. Έχουν προταθεί από τους ερευνητές ορισμένα σχήματα ελέγχου ταυτότητας για ασύρματα δίκτυα αισθητήρων, τα περισσότερα από τα οποία προορίζονται για ασφαλή δρομολόγηση.

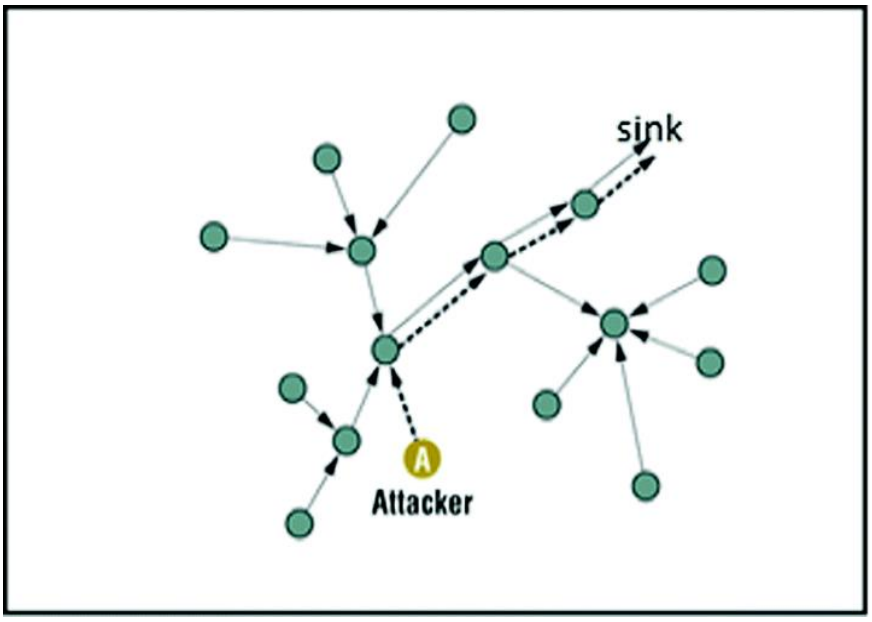
19 5.2 Ευπαθή σημεία στην ασφάλεια

Τα ασύρματα δίκτυα αισθητήρων είναι ευάλωτα σε διάφορους τύπους επιθέσεων. Αυτές οι επιθέσεις μπορούν να κατηγοριοποιηθούν ως εξής :

1) Επιθέσεις στο απόρρητο και στον έλεγχο ταυτότητας: οι τυπικές κρυπτογραφικές τεχνικές μπορούν να προστατεύσουν το απόρρητο και την αυθεντικότητα των καναλιών επικοινωνίας από εξωτερικές επιθέσεις όπως υποκλοπές, επιθέσεις αναπαραγωγής πακέτων και τροποποίηση ή πλαστογράφηση πακέτων.

2)Επιθέσεις στη διαθεσιμότητα δικτύου: οι επιθέσεις στη διαθεσιμότητα αναφέρονται συχνά ως επιθέσεις denial-of-service (DoS) . Οι επιθέσεις DoS ενδέχεται να στοχεύουν οποιοδήποτε επίπεδο δικτύου αισθητήρων.

3)Κρυφά επίθεση κατά της ακεραιότητας της υπηρεσίας: σε μια κρυφή επίθεση, ο στόχος του εισβολέα είναι να κάνει το δίκτυο να αποδεχτεί μια ψευδή τιμή δεδομένων. Για παράδειγμα, ένας εισβολέας θέτει σε κίνδυνο έναν κόμβο αισθητήρα και εισάγει μια ψευδή τιμή δεδομένων μέσω αυτού του κόμβου αισθητήρα. Σε αυτές τις επιθέσεις, είναι απαραίτητο να διατηρείται διαθέσιμο το δίκτυο αισθητήρων για την προβλεπόμενη χρήση του. Οι επιθέσεις DoS εναντίον στο δίκτυο ενδέχεται να επιτρέψουν πραγματική ζημιά στην υγεία και την ασφάλεια των ανθρώπων. Η επίθεση DoS συνήθως αναφέρεται στην προσπάθεια ενός αντιπάλου να διαταράξει, να ανατρέψει ή να καταστρέψει ένα δίκτυο. Ωστόσο, μια επίθεση DoS μπορεί να είναι οποιοδήποτε συμβάν που μειώνει ή εξαλείφει την ικανότητα ενός δικτύου να εκτελεί τις αναμενόμενες λειτουργίες του.



Επιθέσεις στο φυσικό επίπεδο

Το φυσικό επίπεδο είναι υπεύθυνο για την επιλογή συχνότητας, τη δημιουργία συχνότητας φορέα, την ανίχνευση σήματος, τη διαμόρφωση και την κρυπτογράφηση δεδομένων . Όπως συμβαίνει με οποιοδήποτε μέσο ραδιοεπικοινωνίας υπάρχει η πιθανότητα παρεμβολής στα ασύρματα δίκτυ αισθητήρων. Υπάρχουν δύο ευρείες κατηγορίες επίθεσης στο φυσικό επίπεδο: μπλοκαρίσματος και παραβίαση. Περιγράφονται ως εξής.

Μπλοκάρισμα: Είναι ένας τύπος επίθεσης που παρεμβαίνει στις ραδιοσυχνότητες που χρησιμοποιούν οι κόμβοι σε ένα δίκτυο για επικοινωνία . Μια πηγή μπλοκαρίσματος μπορεί να είναι αρκετά ισχυρή ώστε να διαταράξει ολόκληρο το δίκτυο. Ακόμη και με λιγότερο ισχυρές πηγές μπλοκαρίσματος, ένας αντίπαλος μπορεί δυνητικά να διακόψει την επικοινωνία σε ολόκληρο το δίκτυο, διανέμοντας στρατηγικά τις πηγές μπλοκαρίσματος. Μια διαλείπουσα παρεμβολή μπορεί επίσης να αποδειχθεί επιζήμια .

Παραβίαση: Τα δίκτυα αισθητήρων λειτουργούν συνήθως σε εξωτερικά περιβάλλοντα. Λόγω της απρόσκοπτης και κατανεμημένης φύσης, οι κόμβοι είναι πολύ ευαίσθητοι σε φυσικές επιθέσεις . Οι φυσικές επιθέσεις μπορεί να προκαλέσουν μη αναστρέψιμη βλάβη στους κόμβους. Ο αντίπαλος μπορεί να εξαγάγει κρυπτογραφικά κλειδιά από τον καταγεγραμμένο κόμβο, να παραβιάσει τα

κυκλώματά του, να τροποποιήσει τους κωδικούς προγράμματος ή ακόμα και να τον αντικαταστήσει με κακόβουλο αισθητήρα .

Επιθέσεις στο επίπεδο ζεύξης δεδομένων

Το επίπεδο ζεύξης δεδομένων είναι υπεύθυνο για την πολυπλεξία ροών δεδομένων, την ανίχνευση πλαισίου δεδομένων, τον έλεγχο μέσης πρόσβασης και τον έλεγχο σφαλμάτων . Οι επιθέσεις σε αυτό το επίπεδο περιλαμβάνουν σκόπιμα δημιουργημένες συγκρούσεις, εξάντληση πόρων και αδικία στην κατανομή. Μια σύγκρουση συμβαίνει όταν δύο κόμβοι προσπαθούν ταυτόχρονα να μεταδίδουν στην ίδια συχνότητα . Όταν συγκρούονται πακέτα, απορρίπτονται και πρέπει να μεταδοθούν ξανά. Ένας αντίπαλος μπορεί στρατηγικά να προκαλέσει συγκρούσεις σε συγκεκριμένα πακέτα, όπως μηνύματα ελέγχου ACK. Ένα πιθανό αποτέλεσμα τέτοιων συγκρούσεων είναι το δαπανηρό εκθετικό αποτέλεσμα. Ο αντίπαλος μπορεί απλώς να παραβιάζει το πρωτόκολλο επικοινωνίας και να μεταδίδει συνεχώς μηνύματα σε μια προσπάθεια δημιουργίας συγκρούσεων. Επαναλαμβανόμενες συγκρούσεις μπορούν επίσης να χρησιμοποιηθούν από έναν εισβολέα για να προκαλέσουν εξάντληση πόρων . Για παράδειγμα, μια εφαρμογή αφελής συνδέσμου μπορεί συνεχώς να προσπαθεί να αναμεταδώσει τα κατεστραμμένα πακέτα. Εάν δεν ανιχνευθούν νωρίς αυτές οι αναμεταδόσεις, τα επίπεδα ενέργειας των κόμβων θα εξαντληθούν γρήγορα. Ένας εισβολέας μπορεί να προκαλέσει ζημία χρησιμοποιώντας κατά διαστήματα τις επιθέσεις του επιπέδου συνδέσμου. Σε αυτήν την περίπτωση, ο αντίπαλος προκαλεί υποβάθμιση εφαρμογών σε πραγματικό χρόνο που εκτελούνται σε άλλους κόμβους, διακόπτοντας κατά διαστήματα τις μεταδόσεις καρέ τους.

Επιθέσεις στο επίπεδο δικτύου

Το επίπεδο δικτύου τ είναι ευάλωτο σε διαφορετικούς τύπους επιθέσεων όπως:

1) πλαστογραφημένες πληροφορίες δρομολόγησης.
2) επιλεκτική προώθηση πακέτων .
3) Sinkhole.
4) Sybil.
5) σκουληκότρυπα.
6) blackhole και Grayhole.
7) Πλημμύρα HELLO.

8) Βυζαντινή.

9) αποκάλυψη πληροφοριών.

10) Επίθεση εξάντλησης πόρων

11)Αναγνώριση πλαστογράφησης

1)Πληροφορίες δρομολόγησης πλαστών: η πιο άμεση επίθεση εναντίον πρωτοκόλλου δρομολόγησης είναι να στοχεύσετε τις πληροφορίες δρομολόγησης στο δίκτυο. Ένας εισβολέας μπορεί να πλαστογραφήσει, να τροποποιήσει ή να αναπαράγει πληροφορίες δρομολόγησης για να διαταράξει την κυκλοφορία στο δίκτυο. Αυτές οι διακοπές περιλαμβάνουν τη δημιουργία βρόχων δρομολόγησης, την προσέλκυση ή την απωθητική κίνηση του δικτύου από επιλεγμένους κόμβους, την επέκταση ή τη συντόμευση διαδρομών προέλευσης, τη δημιουργία ψευδών μηνυμάτων σφάλματος, την πρόκληση διαμερισμάτων δικτύου και την αύξηση της καθυστέρησης από άκρο σε άκρο.

2)Επιλεκτική προώθηση: σε ένα δίκτυο πολλαπλών hop όπως ένα ασύρματο δίκτυο αισθητήρων, για την επικοινωνία μηνυμάτων όλοι οι κόμβοι πρέπει να προωθούν τα μηνύματα με ακρίβεια. Ένας εισβολέας μπορεί να θέσει σε κίνδυνο έναν κόμβο με τέτοιο τρόπο ώστε να προωθεί επιλεκτικά ορισμένα μηνύματα και να ρίχνει άλλα .

3)Sinkhole: Σε μια επίθεση με sinkhole, ένας εισβολέας κάνει έναν συμβιβασμένο κόμβο να φαίνεται πιο ελκυστικός για τους γείτονές του σφυρηλατώντας τις πληροφορίες δρομολόγησης . Το αποτέλεσμα είναι ότι οι γειτονικοί κόμβοι επιλέγουν τον συμβιβασμένο κόμβο ως τον επόμενο κόμβο για να δρομολογήσουν τα δεδομένα τους. Αυτός ο τύπος επίθεσης καθιστά την επιλεκτική προώθηση πολύ απλή, καθώς όλη η κίνηση από μια μεγάλη περιοχή στο δίκτυο θα ρέει μέσω του συμβιβασμένου κόμβου.

4)Sybil: είναι μια επίθεση όπου ένας κόμβος παρουσιάζει περισσότερες από μία ταυτότητες σε ένα δίκτυο. Αρχικά περιγράφηκε ως επίθεση με σκοπό να νικήσει τον στόχο των μηχανισμών πλεονασμού σε κατανεμημένα συστήματα αποθήκευσης δεδομένων σε δίκτυα peer-to-peer . Εκτός από την ήττα των κατανεμημένων συστημάτων αποθήκευσης δεδομένων, η επίθεση Sybil είναι επίσης αποτελεσματική κατά των αλγορίθμων δρομολόγησης, της συγκέντρωσης

δεδομένων, της ψηφοφορίας, της δίκαιης κατανομής πόρων και της αποτροπής της ανίχνευσης κακής συμπεριφοράς. Ανεξάρτητα από τον στόχο (ψηφοφορία, δρομολόγηση, συγκέντρωση), ο αλγόριθμος Sybil λειτουργεί παρόμοια. Όλες οι τεχνικές περιλαμβάνουν τη χρήση πολλαπλών ταυτοτήτων. Για παράδειγμα, σε ένα σύστημα ψηφοφορίας δικτύου αισθητήρων, η επίθεση Sybil μπορεί να χρησιμοποιεί πολλαπλές ταυτότητες για να δημιουργήσει επιπλέον «ψήφους». Παρομοίως, για να επιτεθεί στο πρωτόκολλο δρομολόγησης, η επίθεση Sybil θα βασίζεται σε έναν κακόβουλο κόμβο που θα παίρνει την ταυτότητα πολλαπλών κόμβων, και έτσι θα δρομολογεί πολλαπλές διαδρομές μέσω ενός μόνο κακόβουλου κόμβου.

5)Σκουληκότρυπα: Η σκουληκότρυπα (wormhole) είναι ένας σύνδεσμος χαμηλού λανθάνοντος χρόνου μεταξύ δύο τμημάτων ενός δικτύου πάνω στο οποίο ένας εισβολέας αναπαράγει μηνύματα δικτύου . Αυτός ο σύνδεσμος μπορεί να δημιουργηθεί είτε μέσω ενός μηνύματος προώθησης ενός κόμβου μεταξύ δύο γειτονικών αλλά κατά τα άλλα μη γειτονικών κόμβων είτε από ένα ζεύγος κόμβων σε διαφορετικά μέρη του δικτύου που επικοινωνούν μεταξύ τους. Η τελευταία περίπτωση συνδέεται στενά με την επίθεση Sinkhole καθώς ένας επιθετικός κόμβος κοντά στο σταθμό βάσης μπορεί να παρέχει έναν σύνδεσμο απλής διαδρομής προς αυτόν τον σταθμό βάσης μέσω του άλλου κόμβου επίθεσης σε ένα μακρινό τμήμα του δικτύου.

6)Blackhole και Grayhole: στην επίθεση blackhole, ένας κακόβουλος κόμβος διαφημίζει ψευδώς καλές διαδρομές (π.χ. τη συντομότερη διαδρομή ή την πιο σταθερή διαδρομή) στον κόμβο προορισμού κατά τη διαδικασία εύρεσης διαδρομής (σε πρωτόκολλα αντιδραστικής δρομολόγησης) ή στην ενημέρωση διαδρομής μηνύματα (σε προληπτικά πρωτόκολλα δρομολόγησης). Ο σκοπός του κακόβουλου κόμβου θα μπορούσε να είναι η παρεμπόδιση της διαδικασίας εύρεσης διαδρομής ή η παρεμπόδιση όλων των πακέτων δεδομένων που αποστέλλονται στον σχετικό κόμβο προορισμού. Μια πιο ευαίσθητη μορφή αυτής της επίθεσης είναι γνωστή ως επίθεση γκρίζας τρύπας, όπου ο κακόβουλος κόμβος πέφτει περιοδικά πακέτα δεδομένων, καθιστώντας έτσι τον εντοπισμό του πιο δύσκολο.

7)Πλημμύρα HELLO: τα περισσότερα από τα πρωτόκολλα που χρησιμοποιούν πακέτα HELLO κάνουν την αφελής υπόθεση ότι η λήψη ενός τέτοιου πακέτου συνεπάγεται ότι ο αποστολέας βρίσκεται εντός του εύρους ραδιοφώνου του δέκτη. Ένας εισβολέας μπορεί να χρησιμοποιήσει

έναν πομπό υψηλής ισχύος για να ξεγελάσει έναν μεγάλο αριθμό κόμβων και να τους κάνει να πιστέψουν ότι βρίσκονται εντός της γειτονιάς του . Στη συνέχεια, ο κόμβος του εισβολέα μεταδίδει ψευδώς μια μικρότερη διαδρομή προς το σταθμό βάσης και όλοι οι κόμβοι που έλαβαν τα πακέτα HELLO προσπαθούν να μεταδώσουν στον κόμβο του εισβολέα. Ωστόσο, αυτοί οι κόμβοι βρίσκονται εκτός του ραδιοφωνικού εύρους του εισβολέα.

8)Βυζαντινή επίθεση: σε αυτήν την επίθεση, ένας συμβιβασμένος κόμβος ή ένα σύνολο συμβιβασμένων κόμβων λειτουργεί σε συνεργασία και εκτελεί επιθέσεις όπως δημιουργία βρόχων δρομολόγησης, προώθηση πακέτων σε μη βέλτιστες διαδρομές και επιλεκτική πτώση πακέτων. Οι βυζαντινές επιθέσεις είναι πολύ δύσκολο να εντοπιστούν, καθώς σε τέτοιες επιθέσεις τα δίκτυα συνήθως δεν παρουσιάζουν ανώμαλη συμπεριφορά.

9)Αποκάλυψη πληροφοριών: ένας παραβιασμένος κόμβος ενδέχεται να διαρρεύσει εμπιστευτικές ή σημαντικές πληροφορίες σε μη εξουσιοδοτημένους κόμβους σε ένα δίκτυο. Τέτοιες πληροφορίες μπορεί να περιλαμβάνουν πληροφορίες σχετικά με την τοπολογία του δικτύου, τη γεωγραφική θέση των κόμβων ή βέλτιστες διαδρομές προς εξουσιοδοτημένους κόμβους στο δίκτυο.

10)Επίθεση εξάντλησης πόρων: σε αυτόν τον τύπο επίθεσης, ένας κακόβουλος κόμβος προσπαθεί να εξαντλήσει πόρους άλλων κόμβων σε ένα δίκτυο. Οι τυπικοί πόροι που στοχεύονται είναι ισχύς μπαταρίας, εύρος ζώνης και υπολογιστική ισχύς. Οι επιθέσεις θα μπορούσαν να έχουν τη μορφή περιττών αιτημάτων για διαδρομές, πολύ συχνής δημιουργίας πακέτων φάρων ή προώθησης παλιών πακέτων σε άλλους κόμβους.

11)Αναγνώριση πλαστογράφησης: ορισμένοι αλγόριθμοι δρομολόγησης για ασύρματα δίκτυα αισθητήρων απαιτούν μετάδοση πακέτων αναγνώρισης. Ένας επιθετικός κόμβος μπορεί να ακούσει μεταδόσεις πακέτων από τους γειτονικούς κόμβους του και να πλαστογραφήσει τις επιβεβαιώσεις παρέχοντας έτσι ψευδείς πληροφορίες στους κόμβους . Με αυτόν τον τρόπο, ο εισβολέας είναι σε θέση να διαδώσει λανθασμένες πληροφορίες στο δίκτυο σχετικά με την κατάσταση των κόμβων, καθώς κάποια αναγνώριση μπορεί να φτάσει από κόμβους που δεν είναι στην πραγματικότητα.

Εκτός από τις παραπάνω κατηγορίες επιθέσεων, υπάρχουν διάφοροι τύποι πιθανών επιθέσεων στα πρωτόκολλα δρομολόγησης . Τα περισσότερα από τα πρωτόκολλα δρομολόγησης είναι ευάλωτα σε επιθέσεις όπως: υπερχείλιση πίνακα δρομολόγησης, δηλητηρίαση πίνακα δρομολόγησης, αναπαραγωγή πακέτων, δηλητηρίαση προσωρινής μνήμης διαδρομής, επιταχυνόμενες επιθέσεις κ.λπ.

Επιθέσεις στο επίπεδο μεταφοράς

Οι επιθέσεις που μπορούν να ξεκινήσουν στο επίπεδο μεταφοράς σε ένα ασύρματο δίκτυο αισθητήρων είναι επίθεση πλημμύρας και επίθεση αποσυγχρονισμού.

Πλημμύρας: Όποτε απαιτείται πρωτόκολλο για τη διατήρηση της κατάστασης και στα δύο άκρα μιας σύνδεσης, καθίσταται ευάλωτο στην εξάντληση της μνήμης μέσω πλημμύρας. Ένας εισβολέας μπορεί επανειλημμένα να υποβάλει νέο αίτημα σύνδεσης έως ότου εξαντληθούν οι πόροι που απαιτούνται από κάθε σύνδεση ή φτάσουν το μέγιστο όριο. Και στις δύο περιπτώσεις, θα παραβλεφθούν περαιτέρω νόμιμα αιτήματα.

Αποσυγχρονισμός: Ο αποσυγχρονισμός αναφέρεται στη διακοπή μιας υπάρχουσας σύνδεσης. Ένας εισβολέας μπορεί, για παράδειγμα, να πλαστογραφεί επανειλημμένα μηνύματα σε έναν τελικό κεντρικό υπολογιστή, προκαλώντας στον κεντρικό υπολογιστή να ζητήσει την αναμετάδοση των χαμένων πλαισίων. Εάν χρονομετρηθεί σωστά, ένας εισβολέας μπορεί να υποβαθμίσει ή ακόμη και να αποτρέψει την ικανότητα των τελικών κεντρικών υπολογιστών να ανταλλάσσουν επιτυχώς δεδομένα, προκαλώντας τους να σπαταλούν ενέργεια προσπαθώντας να ανακτήσουν από σφάλματα που δεν υπάρχουν ποτέ.

Επίπεδα	Επίθεση	Άμυνα
φυσικό επίπεδο	μπλοκαρίσματος και παραβίαση.	Spread-spectrum, μηνύματα προτεραιότητας, χαμηλότερος κύκλος λειτουργίας, χαρτογράφηση περιοχών, αλλαγή λειτουργίας
ζεύξης δεδομένων	Ανισότητα σύγκρουσης εξάντλησης	Κωδικός διόρθωσης σφαλμάτων Περιορισμός τιμών Μικρά κουφώματα

Δικτύου	Πληροφορίες πλαστογράφησης και επιλεκτική προώθηση Sinkhole Sybil Wormhole πλημμύρα HELLO	Φιλτράρισμα εξόδου έλεγχος ταυτότητας παρακολούθηση Έλεγχος πλεονασμού Έλεγχος ταυτότητας παρακολούθηση έλεγχος ταυτότητας έλεγχος ταυτότητας πακέτων με χρήση γεωγραφικών και χρονικών πληροφοριών
Μεταφοράς	πλημμύρα Αποσυγχρονισμός	Έλεγχος ταυτότητας Client puzzles

Επιθέσεις στο απόρρητο

Δεδομένου ότι τα ασύρματα δίκτυα αισθητήρων είναι ικανά για αυτόματη συλλογή δεδομένων μέσω αποτελεσματικής και στρατηγικής ανάπτυξης αισθητήρων, αυτά τα δίκτυα είναι επίσης ευάλωτα σε πιθανή κατάχρηση αυτών των τεράστιων δεδομένων πηγές. Η διατήρηση της ιδιωτικής ζωής των ευαίσθητων δεδομένων είναι ιδιαίτερα δύσκολη πρόκληση. Επιπλέον, ένας αντίπαλος μπορεί να συλλέξει φαινομενικά αθώα δεδομένα για να αντλήσει ευαίσθητες πληροφορίες εάν ξέρει πώς να συγκεντρώνει δεδομένα που συλλέγονται από πολλούς κόμβους αισθητήρων. Η διατήρηση της ιδιωτικής ζωής είναι ακόμη πιο δύσκολη, δεδομένου ότι αυτά τα δίκτυα καθιστούν ευρέως διαθέσιμους μεγάλους όγκους πληροφοριών μέσω μηχανισμών απομακρυσμένης πρόσβασης. Δεδομένου ότι ο αντίπαλος δεν χρειάζεται να είναι σωματικά παρών για τη διεξαγωγή της παρακολούθησης, η διαδικασία συλλογής πληροφοριών μπορεί να γίνει ανώνυμα με πολύ χαμηλό κίνδυνο. Επιπλέον, η απομακρυσμένη πρόσβαση επιτρέπει σε έναν μόνο αντίπαλο να παρακολουθεί ταυτόχρονα πολλούς ιστότοπους . Μερικές από τις κοινές επιθέσεις στο απόρρητο δεδομένων αισθητήρων είναι:

1)Παραβίαση και παθητική παρακολούθηση: Αυτή είναι η πιο κοινή και ευκολότερη μορφή επίθεσης στο απόρρητο των δεδομένων. Εάν τα μηνύματα δεν προστατεύονται από κρυπτογραφικούς μηχανισμούς, ο αντίπαλος θα μπορούσε εύκολα να κατανοήσει το περιεχόμενο. Τα πακέτα που περιέχουν πληροφορίες ελέγχου μεταφέρουν περισσότερες πληροφορίες από τις προσβάσιμες μέσω του διακομιστή τοποθεσίας. Η παρακολούθηση αυτών των μηνυμάτων αποδεικνύεται πιο αποτελεσματική για έναν αντίπαλο.

2) Ανάλυση κυκλοφορίας: Προκειμένου να γίνει αποτελεσματική επίθεση στην προστασία της ιδιωτικής ζωής, η υποκλοπή πρέπει να συνδυάζεται με ανάλυση κίνησης. Μέσω μιας αποτελεσματικής ανάλυσης της κίνησης, ένας αντίπαλος μπορεί να εντοπίσει ορισμένους κόμβους αισθητήρων με ειδικούς ρόλους και δραστηριότητες σε ένα ασύρματο δίκτυο αισθητήρων. Για παράδειγμα, μια ξαφνική αύξηση της επικοινωνίας μηνυμάτων μεταξύ ορισμένων κόμβων σημαίνει ότι αυτοί οι κόμβοι έχουν συγκεκριμένες δραστηριότητες και συμβάντα για παρακολούθηση.

3) Καμουφλάζ: Ένας αντίπαλος μπορεί να θέσει σε κίνδυνο έναν κόμβο αισθητήρα και αργότερα να χρησιμοποιήσει αυτόν τον κόμβο για να μεταμφιέσει έναν κανονικό κόμβο στο δίκτυο. Αυτός ο καμουφλαρισμένος κόμβος μπορεί στη συνέχεια να διαφημίσει ψευδείς πληροφορίες δρομολόγησης και να προσελκύσει πακέτα από άλλους κόμβους για περαιτέρω προώθηση. Αφού τα πακέτα αρχίσουν να φθάνουν στον συμβιβασμένο κόμβο, αρχίζει να τα προωθεί σε στρατηγικούς κόμβους όπου η ανάλυση απορρήτου στα πακέτα μπορεί να πραγματοποιείται συστηματικά. Τα δίκτυα αυτού του τύπου είναι ευάλωτα σε μια σειρά επιθέσεων σε όλα τα επίπεδα της στοίβας πρωτοκόλλων TCP / IP.

20 5.3 ΜΗΧΑΝΙΣΜΟΙ ΑΜΥΝΑΣ

Μηχανισμοί άμυνας στο φυσικό επίπεδο

Η επίθεση μπλοκαρίσματος μπορεί να υπερασπιστεί με τη χρήση παραλλαγών επικοινωνίας Spread-spectrum , όπως η μετάβαση συχνότητας και η διάδοση κώδικα . Το φάσμα εξάπλωσης συχνότητας (Frequency-hopping spread spectrum) είναι μια μέθοδος μετάδοσης σημάτων με γρήγορη εναλλαγή ενός φορέα μεταξύ πολλών καναλιών συχνοτήτων χρησιμοποιώντας μια ψευδο-τυχαία ακολουθία γνωστή τόσο στον πομπό όσο και στον δέκτη. Καθώς ένας δυνητικός εισβολέας δεν θα μπορούσε να προβλέψει την ακολουθία επιλογής συχνότητας, θα ήταν αδύνατο να μπλοκάρει τη συχνότητα που χρησιμοποιείται σε μια δεδομένη χρονική στιγμή. Η διάδοση κώδικα είναι μια άλλη τεχνική για την άμυνα από το μπλοκάρισμα. Ωστόσο, απαιτεί μεγαλύτερη πολυπλοκότητα και ενέργεια σχεδιασμού και συνεπώς δεν είναι πολύ κατάλληλο για τέτοια δίκτυα . Σε γενικές γραμμές, οι συσκευές αισθητήρων περιορίζονται σε χρήση μίας συχνότητας και είναι ιδιαίτερα ευαίσθητες σε επιθέσεις μπλοκαρίσματος. Μια προσέγγιση για την ανοχή κατά της επίθεσης μπλοκαρίσματος είναι να προσδιορίσετε το μπλοκαρισμένο τμήμα του δικτύου και

να το αποφύγετε αποτελεσματικά κάνοντας περιήγηση. Οι ειδικοί πρότειναν μια προσέγγιση όπου οι κόμβοι κατά μήκος της περιμέτρου μιας μπλοκαρισμένης περιοχής αναφέρουν την κατάστασή τους στους γείτονες και συλλογικά η προβληματική περιοχή εντοπίζεται και τα πακέτα δρομολογούνται γύρω από αυτήν.

Μηχανισμοί άμυνας στο επίπεδο ζεύξης

Μια τυπική άμυνα κατά της επίθεσης σύγκρουσης είναι η χρήση κωδικών διόρθωσης σφαλμάτων [. Οι περισσότεροι κωδικοί λειτουργούν καλύτερα με χαμηλά επίπεδα συγκρούσεων, όπως αυτά που προκαλούνται από περιβαλλοντικά ή πιθανολογικά σφάλματα. Ωστόσο, αυτοί οι κωδικοί προσθέτουν επιπλέον πρόσθετη επεξεργασία και γενική επικοινωνία. Είναι λογικό να υποθέσουμε ότι ένας εισβολέας θα είναι πάντα σε θέση να καταστρέψει περισσότερα από ότι μπορεί να διορθωθεί. Αν και είναι δυνατό να εντοπιστούν αυτές οι κακόβουλες συγκρούσεις, δεν υπάρχει κανένας πλήρης αμυντικός μηχανισμός εναντίον τους σήμερα. Μια πιθανή λύση για επίθεση ενεργειακής εξάντλησης είναι η εφαρμογή ενός ελέγχου περιορισμού ταχύτητας MAC. Αυτό θα επέτρεπε στο δίκτυο να αγνοήσει εκείνα τα αιτήματα που σκοπεύουν να εξαντλήσουν τα ενεργειακά αποθέματα ενός κόμβου. Μια δεύτερη τεχνική είναι η χρήση πολυπλεξίας διαίρεσης χρόνου όπου κάθε κόμβος εκχωρείται χρονοθυρίδα στην οποία μπορεί να μεταδώσει . Αυτό εξαλείφει την ανάγκη διαιτησίας για κάθε πλαίσιο και μπορεί να λύσει το πρόβλημα αόριστης αναβολής σε έναν αλγόριθμο back-off. Ωστόσο, εξακολουθεί να είναι ευαίσθητο σε συγκρούσεις. Η επίδραση της αδικίας που προκαλείται από έναν εισβολέα ο οποίος ξεκινά κατά διαστήματα επιθέσεις επιπέδου συνδέσμου μπορεί να μειωθεί με τη χρήση μικρών πλαισίων, καθώς μειώνει τον χρόνο που ένας εισβολέας έχει στη διάθεσή του για να συλλάβει το κανάλι επικοινωνίας . Ωστόσο, αυτή η τεχνική μειώνει συχνά την αποτελεσματικότητα και είναι επιρρεπής σε περαιτέρω αδικίες, όπως ένας εισβολέας που προσπαθεί να αναμεταδώσει γρήγορα αντί να καθυστερήσει τυχαία.

Μηχανισμοί άμυνας στο επίπεδο δικτύου

Ένα μέτρο κατά της πλαστογράφησης και της αλλοίωσης είναι η προσθήκη κωδικού ελέγχου ταυτότητας μηνύματος (MAC) μετά το μήνυμα. Προσθέτοντας ένα MAC στο μήνυμα, οι δέκτες μπορούν να επαληθεύσουν εάν τα μηνύματα έχουν πλαστογραφηθεί ή τροποποιηθεί. Για να υπερασπιστείτε τις πληροφορίες που αναπαράχθηκαν, οι μετρητές ή τα χρονικά σήματα μπορούν

να εισαχθούν στα μηνύματα . Μια πιθανή άμυνα κατά της επιλεκτικής επίθεσης προώθησης χρησιμοποιεί πολλαπλές διαδρομές για την αποστολή δεδομένων. Μια δεύτερη άμυνα είναι να εντοπιστεί ο κακόβουλος κόμβος ή να υποθέσει ότι έχει αποτύχει και να αναζητήσει μια εναλλακτική διαδρομή. Οι ειδικοί έχουν παρουσιάσει ένα συνεργατικό σύστημα ανίχνευσης για τον εντοπισμό κακόβουλων κόμβων αποστολής πακέτων σε ένα ad hoc δίκτυο.Εκμεταλλεύεται τον πλεονασμό στη δρομολόγηση πληροφοριών σε ένα ad hoc δίκτυο για να δημιουργήσει ένα ισχυρό πλαίσιο ανίχνευσης έτσι ώστε να λειτουργεί ακόμη και με την παρουσία παροδικών διαμερισμάτων δικτύου και βυζαντινής αποτυχίας κόμβων. Άλλη ερευνητές έχουν προτείνει έναν νέο και γενικό μηχανισμό που ονομάζεται πακέτο λουριά για την ανίχνευση και την άμυνα κατά των επιθέσεων σκουληκότρυπας . Σε μια επίθεση τύπου wormhole, ένας κακόβουλος κόμβος υποχωρεί σε μια σειρά πακέτων και, στη συνέχεια, τους συντονίζει μέσω μιας διαδρομής στο δίκτυο και τα επαναλαμβάνει. Αυτό γίνεται για να κάνουμε μια ψευδή αναπαράσταση της απόστασης μεταξύ των δύο κόμβων που συμπλέκονται. Χρησιμοποιείται επίσης, γενικότερα, για να διαταράξει το πρωτόκολλο δρομολόγησης παραπλανώντας τη διαδικασία ανακάλυψης του γείτονα , υπάρχει μηχανισμό που χρησιμοποιεί κατευθυντική κεραία για την καταπολέμηση της επίθεσης σκουληκότρυπας . Μια προσέγγιση που έχει χρησιμοποιηθεί είναι η οπτικοποίησης για την ανίχνευση σκουληκότρυπες . Στον μηχανισμό γίνεται μια εκτίμηση απόστασης μεταξύ όλων των κόμβων αισθητήρων σε μια γειτονιά. Χρησιμοποιώντας πολυδιάστατη κλίμακα, τότε υπολογίζεται μια εικονική διάταξη του δικτύου και χρησιμοποιείται μια στρατηγική εξομάλυνσης επιφανειών για την προσαρμογή των σφαλμάτων στρογγυλοποίησης. Εάν υπάρχει σκουληκότρυπα, το σχήμα του δικτύου θα λυγίσει και θα καμπυλωθεί προς την σκουληκότρυπα. Διαφορετικά, το δίκτυο θα εμφανίζεται επίπεδο. Άλλη μέθοδος είναι ένας μηχανισμό ασφαλείας που μπορεί να ανιχνεύσει συνεταιριστικές επιθέσεις σε ένα ασύρματο ad hoc και δίκτυο αισθητήρων, κάθε κόμβος παρακολουθεί τη συμπεριφορά προώθησης πακέτων καθενός από τους γείτονές του και χρησιμοποιείται ένας παγκόσμιος αλγόριθμος ανίχνευσης για την ανίχνευση τυχόν συμπεριφοράς δρομολόγησης.

Μηχανισμοί άμυνας στο επίπεδο Μεταφοράς

Ο τρόπος να υπερασπιστείς το σύστημα από τις πλημμύρες της επίθεσης DoS στο στρώμα μεταφοράς είναι με την χρήση παζλ πελατών (client puzzle), όπου κάθε πελάτης πρέπει να αποδείξει τη δέσμευσή του για τη σύνδεση λύνοντας ένα παζλ. Καθώς ένας εισβολέας δεν διαθέτει

άπειρο πόρο, θα είναι αδύνατο για αυτόν να δημιουργήσει νέες συνδέσεις αρκετά γρήγορα για να προκαλέσει λιμοκτονία πόρων στον κόμβο εξυπηρέτησης. Μια πιθανή άμυνα ενάντια στην επίθεση αποσυγχρονισμού είναι η επιβολή μιας υποχρεωτικής απαίτησης ελέγχου ταυτότητας όλων των πακέτων που επικοινωνούνται μεταξύ κόμβων . Εάν ο μηχανισμός ελέγχου ταυτότητας είναι ασφαλής, ένας εισβολέας δεν θα μπορεί να στείλει πλαστογραφημένα μηνύματα.

Ασφαλή πρωτόκολλα μετάδοσης και πολλαπλής διανομής

Οι τεχνικές πολλαπλής μετάδοσης και μετάδοσης χρησιμοποιούνται κυρίως για τη μείωση των γενικών εξόδων επικοινωνίας και διαχείρισης της αποστολής ενός μηνύματος σε πολλούς δέκτες. Προκειμένου να διασφαλιστεί ότι μόνο τα νόμιμα μέλη της ομάδας λαμβάνουν την επικοινωνία πολλαπλής διανομής και μετάδοσης, πρέπει να υπάρχουν κατάλληλοι μηχανισμοί ελέγχου ταυτότητας και κρυπτογράφησης. Για την αντιμετώπιση αυτού του προβλήματος, έχουν επινοηθεί διάφορα βασικά συστήματα διαχείρισης:

1) πρωτόκολλα κεντρικής διαχείρισης κλειδιών ομάδα.

2) αποκεντρωμένα πρωτόκολλα διαχείρισης κλειδιών.

3) κατανεμημένα πρωτόκολλα διαχείρισης κλειδιών.

Στην περίπτωση των κεντρικών πρωτοκόλλων διαχείρισης κλειδιών ομάδας, μια κεντρική αρχή χρησιμοποιείται για τη διατήρηση της ομάδας. Τα αποκεντρωμένα πρωτόκολλα διαχείρισης, ωστόσο, κατανέμουν το έργο της διαχείρισης ομάδων σε πολλούς κόμβους. Στα κατανεμημένα πρωτόκολλα διαχείρισης κλειδιών, η δραστηριότητα διαχείρισης κλειδιών κατανέμεται σε ένα σύνολο κόμβων και όχι σε έναν μόνο κόμβο. Σε ορισμένες περιπτώσεις, ολόκληρη η ομάδα κόμβων είναι υπεύθυνη για τη διαχείριση κλειδιών . Ένας αποτελεσματικός τρόπος διανομής κλειδιών σε ένα δίκτυο είναι να χρησιμοποιήσετε ένα λογικό δέντρο κλειδιών. Τέτοιες τεχνικές ανήκουν ουσιαστικά στην κατηγορία των κεντρικών πρωτοκόλλων διαχείρισης κλειδιών. Ενώ οι συγκεντρωτικές λύσεις δεν είναι πάντα οι πιο αποτελεσματικές, αυτοί οι μηχανισμοί μπορεί μερικές φορές να είναι πολύ αποτελεσματικοί καθώς οι βαρύτεροι υπολογισμοί μπορούν συνήθως να πραγματοποιούνται σε ισχυρούς σταθμούς βάσης. Στη λογική ιεραρχία, ένας κεντρικός διανομέας κλειδιού βρίσκεται στη ρίζα ενός δέντρου και οι κόμβοι στο δίκτυο είναι το επίπεδο των φύλλων. Οι εσωτερικοί κόμβοι του δέντρου περιέχουν κλειδιά που χρησιμοποιούνται στη διαδικασία εκ νέου πληκτρολόγησης. Η κατευθυνόμενη διάχυση είναι μια ενεργειακά αποδοτική τεχνική διάδοσης δεδομένων. Στην κατευθυνόμενη διάδοση, ένα ερώτημα μετατρέπεται σε

ενδιαφέρον και μετά διαχέεται σε όλο το δίκτυο. Στη συνέχεια, ο κόμβος προέλευσης ξεκινά τη συλλογή δεδομένων από το δίκτυο με βάση το ενδιαφέρον που διαδίδεται. Η τεχνική διάδοσης δημιουργεί επίσης ορισμένες κλίσεις που έχουν σχεδιαστεί για να προσελκύσουν γεγονότα προς το ενδιαφέρον. Τα δεδομένα που συλλέγονται στη συνέχεια αποστέλλονται πίσω στην πηγή κατά την αντίστροφη διαδρομή της διάδοσης ενδιαφέροντος. Το σχέδιο λογικής βασικής διάδοσης βασισμένης στη διάχυση επιτρέπει στους κόμβους να συμμετέχουν και να αποχωρούν από ομάδες. Η ιεραρχία κλειδιών χρησιμοποιείται για την αποτελεσματική αποκατάσταση κλειδιών για τους κόμβους κάτω από τον κόμβο που έχει αποχωρήσει από την ομάδα. Όταν ένας κόμβος δηλώνει την πρόθεσή του να συμμετάσχει σε μια ομάδα, δημιουργείται ένα σύνολο κλειδιών για τον νέο κόμβο βάσει των κλειδιών στην υπάρχουσα ιεραρχία κλειδιών.το πρόβλημα της διαχείρισης ομάδων πολλαπλής διανομής στο όπου οι κόμβοι σε ένα δίκτυο ομαδοποιούνται με βάση την τοποθεσία τους και κατασκευάζεται ένα δέντρο ασφαλείας στις ομάδες.

21 ΚΕΦΑΛΑΙΟ 6

Παραδείγματα εφαρμογής ασύρματων δικτύων αισθητήρων

Στο παρακάτω κεφάλαιο θα κάνουμε μια γρήγορη αναφορά σε πραγματικές περιπτώσεις μέτρησης ατμοσφαιρικής ρύπανσης με ασύρματα δίκτυα αισθητήρων.

22 6.1 Παρακολούθηση ατμοσφαιρικής ρύπανσης στο Πακιστάν

Στα περισσότερα από τα δίκτυα αισθητήρων λίγοι κόμβοι λειτουργούν ως ενδιάμεσοι ή κόμβοι συλλογής δεδομένων, που συλλέγουν τα δεδομένα και μεταφέρουν αυτά στον σταθμό βάσης για επεξεργασία. Υπάρχει η ανάγκη ενός αλγόριθμου δρομολόγησης έτσι ώστε τα δεδομένα να μπορούν να μεταδίδονται σε σταθμό βάσης σε μικρό χρονικό διάστημα. Λαμβάνοντας υπόψη την περίπτωση που έχει συγκεντρωθεί μεγάλο μέρος δεδομένων από τους αισθητήρες και ο αλγόριθμος δρομολόγησης δεν είναι φιλικός προς το περιβάλλον και όχι τόσο έξυπνος για την κατανομή του εύρους ζώνης με πιο αποτελεσματικό τρόπο, τότε το σύστημα δεν θα λειτουργήσει σωστά και αναμένεται να παραδώσει το λανθασμένες πληροφορίες. Η παρακάτω μεθοδολογία χρησιμοποιήθηκε στο πακιστάν κυρίως σε αστικά κέντρα και βιομηχανικές περιοχέςΟι ερευνητές από το πανεπιστήμιο της νότιας Φλόριντας έχουν προτείνει ένα μοντέλο που δεν απαιτεί τον περίπλοκο αλγόριθμο δρομολόγησης, αλλά οι κόμβοι αισθητήρων θα αναπτυχθούν και θα συνδεθούν με άλλους κόμβους αισθητήρα και κόμβο sink με πολύ πιο εύκολο τρόπο. Έχουν επίσης

προτείνει την τεχνική που χρησιμοποιήσαμε στο δίκτυο για τη συλλογή των δεδομένων. Υπάρχουν εσωτερικές και εξωτερικές μονάδες που δουλέυουν σε διαφορετικά πρωτόκολλα και στη συνέχεια συλλέγονται δεδομένα σε cloud για μεγάλα αναλυτικά δεδομένα. Για ορισμένες δοκιμές, έχουμε αναπτύξει κόμβους αισθητήρων κινητής τηλεφωνίας στα οχήματα μαζικών μεταφορών που ονομάζονται υπηρεσία λεωφορείων-μετρό που πραγματικά μετακινούνται στην πόλη και καλύπτουν όλες τις μεγάλες περιοχές της . Αυτά τα μέσα μαζικής μεταφοράς περνούν από διαφορετικές περιοχές στις οποίες η συγκέντρωση της ατμοσφαιρικής ρύπανσης διαφέρει μεταξύ τους. Επιπλέον, αυτές οι συσκευές αισθητήρων μπορούν επίσης να λάβουν τα δεδομένα άλλων περιβαλλοντικών παραμέτρων, συμπεριλαμβανομένων των πληροφοριών του επιβάτη, της έξυπνης μεταφοράς και πολλών άλλων χρήσιμων πληροφοριών. Για παράδειγμα, οι κόμβοι που χρησιμοποιούνται σε οχήματα. Για τη συλλογή δεδομένων καπνού, σκόνης και άλλων αερίων στο περιβάλλον που προκαλούν ατμοσφαιρική ρύπανση αυτοί οι κινητοί κόμβοι που έχουν αναπτυχθεί σε οχήματα δημοσίων μεταφορών συλλέγουν δεδομένα . Αυτή η τεχνολογία έχει αναπτυχθεί για τη μέτρηση της συγκέντρωσης της ατμοσφαιρικής ρύπανσης σε συγκεκριμένες περιοχές που η ατμοσφαιρική ρύπανση είναι μεγαλύτερη έτσι ώστε να ληφθούν τα απαραίτητα μέτρα.

Αρχιτεκτονική

Για τη συλλογή δεδομένων βασίζεται στο LTE-M, το οποίο είναι τεχνολογία προσανατολισμένη στο μέλλον, χαμηλή κατανάλωση ενέργειας ειδικά σχεδιασμένη για κάλυψη μεγάλης εμβέλειας και εκατομμύρια συνδέσεις διαθέσιμες για αρχιτεκτονική κινητικότητας και χαμηλό ρυθμό δεδομένων. Αυτή η τεχνολογία υπάρχει στις εξωτερικές μονάδες (λεωφορεία) που βασίζεται στην κινητικότητα και θα αναπτυχθεί σε κινούμενα λεωφορεία. Όταν τα λεωφορεία θα σταματήσουν στους σταθμούς όπου οι ασύρματοι αισθητήρες Zigbee ως σταθερό δίκτυο θα αναπτυχθούν τότε οι μονάδες του LTE-M θα συλλέγουν δεδομένα από τους ασύρματους αισθητήρες Zigbess και θα τα στείλουν στο cloud όπου θα αναλυθούν ανάλογα. Επιπλέον, η εσωτερική μονάδα που θα αναπτυχθεί στους σταθμούς λεωφορείων θα βασίζεται σε ασύρματους αισθητήρες Zigbee που θα συνδέονται με τις μονάδες LTE-M και τα δεδομένα θα συλλέγονται όταν κάθε λεωφορείο θα σταματήσει στο σταθμό . Αφού τα λεωφορεία των δημόσιων συγκοινωνιών φτάσουν στον προορισμό, μπορούμε να συλλέξουμε τα δεδομένα είτε χρησιμοποιώντας απευθείας USB είτε Ethernet που μας βοηθά να συνδεθούμε με τον διακομιστή που θα κάνει πραγματικά μια διαχείριση βάσης δεδομένων και καθιστά τα δεδομένα άμεσα διαθέσιμα για προβολή μέσω

Διαδικτύου χρησιμοποιώντας οποιοδήποτε διαδικτυακό συσκευή συνδεδεμένη στο Διαδίκτυο. Όποτε απαιτείται η ενημέρωση των δεδομένων, ο διακομιστής θα ζητά τα δεδομένα από τις συσκευές αισθητήρων και με αυτόν τον τρόπο μπορούμε να συλλέγουμε πιο εύκολο τρόπο.

23 6.2 Παρακολούθηση της ατμοσφαιρικής ρύπανσης στη Ζυρίχη

Στην Ζυρίχη της ελβετίας έχουν δημιουργήσει κάτι αντίστοιχο με το πακιστάν με σκοπό να μετρήσουν τα υπέρλεπτα σωματίδια (UFP) που βρίσκονται κυρίως στα αστικά κέντρα και είναι πολύ επιβλαβής για των ανθρώπινο οργανισμό. Στην συγκεκριμένη περίπτωση μας ενδιαφέρει ο αριθμός αυτών των σωματιδίων. Έχει προταθεί ένα κινητό σύστημα μέτρησης που απαρτίζετε απο 10 κόμβους αισθητήρων πάνω από τα μέσα μαζικής μεταφοράς τα οποία κάνουν δρομολόγια που καλύπτουν το τις περιοχές που μας απασχολούν σε τακτική βάση. Οι κόμβοι στο σύστημα διαθέτουν την τεχνολογία MiniDiSCs για την μέτρηση και την παρακολούθηση των υπέρλεπτων σωματιδίων. Τα τελευταία χρόνια που χρησιμοποιείτε το συγκεκριμένο σύστημα έχει γίνει λήψη πάνω από 50 εκατομμυρίων μετρήσεων και με βάση αυτές αναπτύχθηκαν μοντέλα παλινδρόμησης land-use regression (LUR). Τέτοιου είδους μοντέλα δημιουργούν επεξηγηματικές μεταβλητές για σημεία που δεν μετράνε οι αισθητήρες, αναλύουν τις μετρήσεις, κάνουν προβλέψεις σχετικά με τα επίπεδα μόλυνσης και όλα αυτά μεταφέρονται καταλήγουν στους χάρτες ρύπων προσπαθώντας να συμβουλέψουν τους πολίτες να ακολουθούν τον υγιεινό δρόμο ακόμα και αν αυτός είναι μακρύτερος. Οι χάρτες ρύπων έχουν 3 στάδια :

1)Statistical distribution-στατιστική διανομή.

2)Baselinesignal-σήμα της baseline.

3)Comparison to high-quality data sets-σύγκριση με σετ υψηλής ποιότητας δεδομένων.

24 6.3 Παρακολούθηση της ατμοσφαιρικής ρύπανσης στη Ναγκπούρ της Ινδίας

Αυτό το σύστημα περιβαλλοντικής παρακολούθησης της ατμοσφαιρικής ρύπανσης μετράει, RSPM (Αναπνεύσιμη αιωρούμενη σωματιδιακή ύλη), NOx (οξείδια του αζώτου) και S02 (διοξείδιο του θείου) και παρέχει:

1. Πληροφορίες σχετικά με τη σύνθεση του αέρα, με βάση τη θέση του χρήστη,
2. Ένα εύκολο στη χρήση περιβάλλον, διαθέσιμο στους χρήστες παντού.
3. Προειδοποιήσεις ρύπανσης μέσω SMS και ηλεκτρονικού ταχυδρομείου για εγγεγραμμένους χρήστες.
4. Οργανωμένο τρόπο προβολής πληροφοριών σχετικά με την εξέλιξη της ρύπανσης σε ορισμένες τοποθεσίες.
5. Ένα φτηνό και ισχυρό σύστημα παρακολούθησης της ατμοσφαιρικής ρύπανσης.

Πιο αναλυτικά:

Το επίπεδο ρύπανσης σε κάθε κόμβο αισθητήρα μπορεί να παρέχεται στους ανθρώπους χρησιμοποιώντας ηλεκτρονικό ταχυδρομείο, SMS ή μπορούμε να εμφανίσουμε τις πληροφορίες επιπέδων ρύπανσης σε μεγάλη οθόνη κοντά στην περιοχή. Όπως φαίνεται στο σχήμα, η κόκκινη κουκίδα δείχνει πολύ ρυπασμένη περιοχή, όπου η πράσινη κουκίδα δείχνει τα ανεκτά επίπεδα ρύπανσης. Οι άνθρωποι γενικά έχουν περισσότερες από μία εναλλακτικές διαδρομές για να φτάσουν στον ίδιο προορισμό εάν κάποιος γνωρίζει εκ των προτέρων τις πληροφορίες ρύπανσης, μπορεί να ακολουθήσει την ασφαλή διαδρομή.

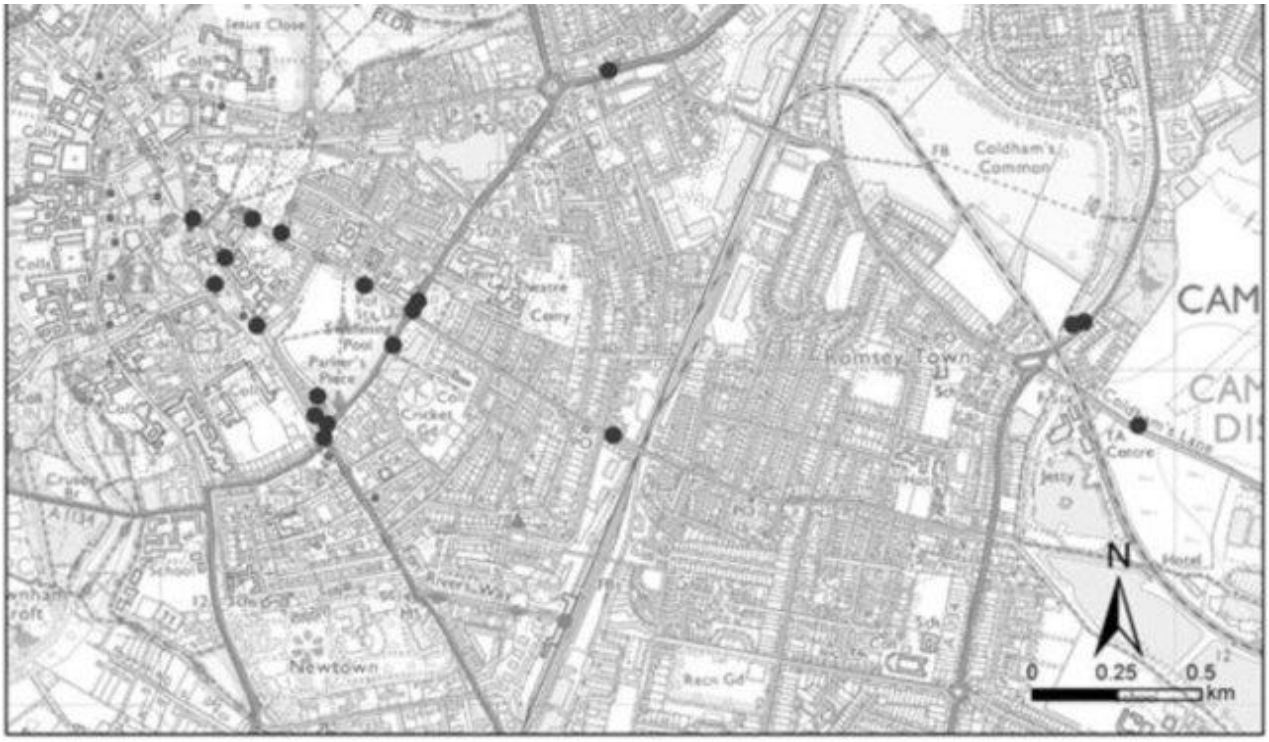
25

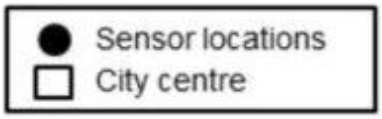
26

27 **6.4 Παρακολούθηση της ατμοσφαιρικής ρύπανσης στο Cambridge της Αγγλίας.**

Στο Cambridge της Αγγλίας δημιουργήθηκε ένα ασύρματο δίκτυο αισθητήρων χαμηλού κόστου στο οποίο χρησιμοποιήθηκαν 32 ηλεκτρομαγνητικοί κόμβοι αισθητήρων για την μέτρηση του μονοξειδίου του άνθρακα. Δημιουργήθηκαν 2 κόμβοι αισθητήρων ενας σε αστικό περιβάλλον και ένας σε αγροτικό ετσι ώστε να

γίνει αντιληπτή η διαφορά στην συχνότητα και στα επίπεδαα υψηλής ρύπανσης σε διαφορετικά





περιβάλλοντα καθώς υπήρχε αυτή γίνεται διάκριση μεταξύ των ρύπων που προκύπτουν από τοπικές εκπομπές και εκείνων που οφείλονται σε μη τοπικές ή περιφερειακές εκπομπές και αποδεικνύεται ότι η υψηλή χωρική πυκνότητα και η γρήγορη απόκριση των μετρήσεων από δίκτυα αισθητήρων χαμηλού κόστους μπορούν να διευκολύνουν αυτό τον διαχωρισμό.

28 6.5 COST Action TD1105 EuNetAir

TO/ COST Action TD1105 EuNetAir είναι το Ευρωπαϊκό δίκτυο για νέες τεχνολογίες αισθητήρων και είναι υπεύθυνο για τον έλεγχο τις ατμοσφαιρικής και περιβαλλοντικής ρυπανσης.

Αυτή η δράση επικεντρώνετε σε ένα νέο παράδειγμα ανίχνευσης που βασίζεται σε τεχνολογίες ανίχνευσης με χαμηλό κόστος για τον έλεγχο ποιότητας αέρα και θα δημιουργήσει ένα διεπιστημονικό συντονισμένο δίκτυο ανώτατου επιπέδου για τον καθορισμό καινοτόμων προσεγγίσεων σε νανοϋλικά αισθητήρων, αισθητήρες αερίου και συσκευές, ασύρματα συστήματα αισθητήρων, κατανεμημένους υπολογιστές , μεθόδους, μοντέλα, πρότυπα και πρωτόκολλα περιβαλλοντικής βιωσιμότητας εντός του Ευρωπαϊκού Χώρου Έρευνας . Η έρευνα σχετικά με καινοτόμες τεχνολογίες ανίχνευσης για τον έλεγχο ποιότητας αέρα βασίζεται σε προηγμένους χημικούς αισθητήρες και συστήματα αισθητήρων σε χαμηλό κόστος, συμπεριλαμβανομένων λειτουργικών υλικών και νανοτεχνολογιών για εφαρμογές οικολογικής αειφορίας, τον έλεγχο περιβάλλοντος εξωτερικού / εσωτερικού χώρου, οσφομετρία , η μοντελοποίηση της ποιότητας του αέρα, η πρόβλεψη των χημικών καιρικών συνθηκών και οι σχετικές μέθοδοι τυποποίησης εκτελούνται ήδη σε διεθνές επίπεδο, αλλά εξακολουθούν να χρειάζονται σοβαρές προσπάθειες συντονισμού για την ενίσχυση νέων παραγόντων ανίχνευσης για έρευνα και καινοτομία. Μόνο μια στενή πολυτομεακή συνεργασία θα εξασφαλίσει καθαρότερο αέρα στην Ευρώπη και θα μειώσει τις αρνητικές επιπτώσεις στην ανθρώπινη υγεία για τις μελλοντικές γενιές σε έξυπνες πόλεις, αποτελεσματική διαχείριση πράσινων κτιρίων με χαμηλές εκπομπές CO2 και βιώσιμη οικονομική ανάπτυξη. Ο στόχος της δράσης είναι η δημιουργία ενός συνεταιριστικού δικτύου για τη διερεύνηση νέων τεχνολογιών ανίχνευσης για τον έλεγχο της ρύπανσης της ατμόσφαιρας χαμηλού κόστους μέσω επιτόπιων μελετών και εργαστηριακών πειραμάτων για τη μεταφορά των αποτελεσμάτων σε προληπτικές πρακτικές ελέγχου σε πραγματικό χρόνο και την παγκόσμια βιωσιμότητα για την παρακολούθηση των κλιματικών αλλαγών και των εξωτερικών χώρων ή ενεργειακή απόδοση εσωτερικού χώρου. Η δημιουργία ενός τέτοιου ευρωπαϊκού δικτύου, με τη συμμετοχή βασικών εμπειρογνωμόνων εκτός COST, θα επιτρέψει στην ευρωπαϊκή ένωση να αναπτύξει παγκόσμιες δυνατότητες στην τεχνολογία αισθητικών πόλεων με βάση οικονομικά αποδοτικά νανοϋλικά και να συμβάλει στη διαμόρφωση μιας κρίσιμης μάζας ερευνητών

κατάλληλων για συνεργασία στην επιστήμη και την τεχνολογία, συμπεριλαμβανομένων κατάρτιση και εκπαίδευση.

29 ΚΕΦΑΛΑΙΟ 7

30 7.1 Πρόγραμμα ατμοσφαιρικής ρύπανσης

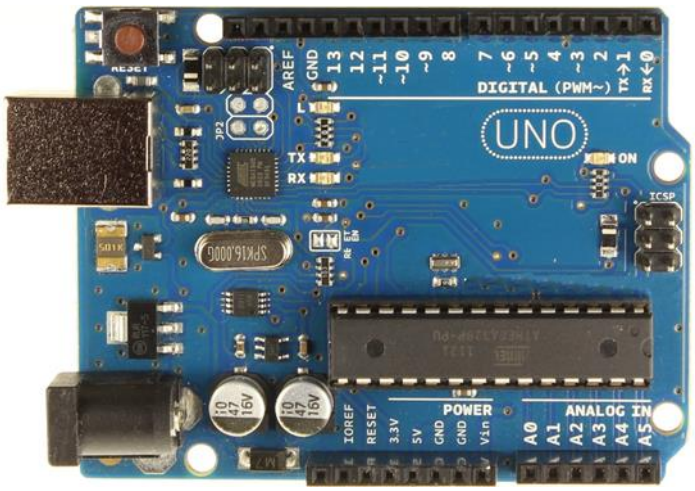
Το πρόγραμμα ατμοσφαιρικής ρύπανσης που δημιουργήσαμε σε αυτή την πτυχιακή εργασία είναι ανορθόδοξο σε σχέση με τα υπόλοιπα τέυοιου τύπου δίκτυα καθώς η δημιουργία και η εκτέλεση του δεν επιρρεάστικε απο άλλες παρόμοιες εφαρμογές και αποτελεί κατα το μεγαλύτερο βαθμό δίκια μου ιδέα ως προς την υλοποίηση.Στόχος είναι να μέτρησουμε την ατμοσφαίρικη ρύπανση καθώς επίσης να παρουσιάσουμε στον χρήστη ολα τα στοιχεία απο τις μετρήσεις ενημερώνοντας αν η περιοχή στην οποία κινήτε είναι επιβλαβείς για την υγεία του ή οχι . Θα μπορούσε να χρησιμοποιηθεί σε αστίκες περιόχες οπου η χρήση αυτοκινήτων γίνεται σε μεγάλο βαθμό ή σε πόλεις που υποφέρουν απο τους ατμοσφαιρικους ρύπους κυρίως απο εργοστάσια. Θα ειναι ιδανικό για ευπαθείς ομάδες , άτομα με αναπνευστικά προβλήματα και ηλικιμένους .Το σύστημα χρησιμοποιέι την τεχνική sleep mode για ακόμα χαμηλότερη κατανάλοση. Οι μετρήσεις γίνονται ανα 15 λέπτα οπου το σύστημα θα “ξυπνάει” θα στέλνει και θα “ξανακοιμάται”.
Τα δομικά στοιχεία είναι:

1) Arduino mini pro:To Arduino ini pro είναι μια πλακέτα μικροελεγκτή που βασίζεται στο ATmega328P.Διαθέτει 14 ψηφιακούς ακροδέκτες εισόδου / εξόδου (εκ των οποίων οι 6 μπορούν να χρησιμοποιηθούν ως έξοδοι PWM), 6 αναλογικές είσοδοι, ένα ενσωματωμένο resonator, ένα κουμπί επαναφοράς και οπές για την τοποθέτηση κεφαλίδων ακίδων. Μια κεφαλίδα έξι ακίδων

μπορεί να συνδεθεί σε ένα καλώδιο FTDI (στην συγκεκριμένη περίπτωση χρησιμοποιήθηκε το ftdi ft232rl) ή μια πλακέτα διάσπασης Sparkfun για να παρέχει ισχύ USB και επικοινωνία στον πίνακα.

Το Arduino Pro Mini προορίζεται για ημι-μόνιμη εγκατάσταση σε αντικείμενα ή εκθέσεις.Η πλακέτα έρχεται χωρίς προεγκατεστημένες κεφαλίδες, επιτρέποντας τη χρήση διαφόρων τύπων συνδετήρων ή απευθείας συγκόλληση καλωδίων.Η διάταξη του pin είναι συμβατή με το Arduino Mini.Υπάρχουν δύο εκδόσεις του Mini Pro. Το ένα τρέχει στα 3,3V και 8 MHz, το άλλο στα 5V και 16 MHz στην δίκια μας περίπτωση θα χρησιμοποιηθεί το arduino mini pro 3,3V 8 MHz για χαμηλότερη κατανάλωση.

2) Arduino Uno:To Arduino Uno είναι ένας πίνακας μικροελεγκτών που βασίζεται στο ATmega328P (φύλλο δεδομένων). Διαθέτει 14 ψηφιακούς ακροδέκτες εισόδου / εξόδου (εκ των οποίων οι 6 μπορούν να χρησιμοποιηθούν ως έξοδοι PWM), 6 αναλογικές είσοδοι, ένας κεραμικός συντονιστής 16 MHz (CSTCE16M0V53-R0), μια σύνδεση USB, μια υποδοχή τροφοδοσίας, μια κεφαλίδα ICSP και ένα κουμπί επαναφοράς . Περιέχει όλα όσα χρειάζονται για την υποστήριξη του μικροελεγκτή. Συνδέετε σε έναν υπολογιστή με καλώδιο USB ή τροφοδοτήτε τον με έναν προσαρμογέα AC-to-DC ή μια μπαταρία.



3) Lora ra-02:Ο όρος LoRa σημαίνει Long Range. Πρόκειται για μια ασύρματη τεχνολογία ραδιοσυχνοτήτων που εισήχθη από μια εταιρεία που ονομάζεται Semtech.Αυτή η τεχνολογία LoRa μπορεί να χρησιμοποιηθεί για τη μετάδοση αμφίδρομων πληροφοριών σε μεγάλες αποστάσεις χωρίς να καταναλώνει μεγάλη ισχύ. Αυτή η ιδιότητα μπορεί να χρησιμοποιηθεί από απομακρυσμένους αισθητήρες που πρέπει να μεταδίδουν τα δεδομένα τους λειτουργώντας σε μια μικρή μπαταρία.Συνήθως η Lora μπορεί να επιτύχει απόσταση 15-20km και μπορεί να λειτουργήσει με μπαταρία για χρόνια.Στην συγκεκριμένη περίπτωση χρησιμοποιούμε 2 lora ra 02 σαν πομπό- δέκτη αντίστοιχα.

4) MQ Sensors:Οι αισθητήρες σειράς MQ χρησιμοποιούν έναν μικρό θερμαντήρα στο εσωτερικό με έναν ηλεκτροχημικό αισθητήρα για τη μέτρηση διαφορετικών συνδυασμών αερίων. Μπορούν να βαθμονομηθούν, αλλά, για να γίνει αυτό, απαιτείται γνώση συγκέντρωσης του μετρημένου αερίου ή αερίων για αυτό. Για βιομηχανικούς σκοπούς, οι βαθμονομήσεις γίνονται σε ειδικά εργαστήρια μετρολογίας με ακριβείς ανιχνευτές και δοκιμές.Το ευαίσθητο υλικό του αισθητήρα σε όλους τους MQ αισθητήρες είναι το SnO2,.Οι αισθητήρες είναι απο την ίδια εταιρεία και ίδιου τύπου γιαυτό και τα χαρακτηριστικά τους είναι παρόμοια όπως θα δούμε και παρακάτω.

MQ-4: Όταν ανιχνέυση το εύφλεκτο αέριο, η αγωγιμότητα του αισθητήρα αυξάνεται μαζί με την αύξηση της συγκέντρωσης αερίου. Οι χρήστες μπορούν να μετατρέψουν την αλλαγή αγωγιμότητας ώστε να αντιστοιχεί στο σήμα εξόδου της συγκέντρωσης αερίου μέσω ενός απλού κυκλώματος. Ο αισθητήρας MQ-4 έχει υψηλή ευαισθησία το μεθάνιο, έχει επίσης αλκοόλη και άλλα αέρια.

Χαρακτηριστικά MQ-4

Technical Parameters **Stable.1**

Model			MQ-4
Sensor Type			Semiconductor
Standard Encapsulation			Bakelite, Metal cap
Target Gas			Methane
Detection range			300～10000ppm(CH_4)
Standard Circuit Conditions	Loop Voltage	V_c	≤24V DC
	Heater Voltage	V_H	5.0V±0.1V AC or DC
	Load Resistance	R_L	Adjustable
Sensor character under standard test conditions	Heater Resistance	R_H	26Ω±3Ω(room tem.)
	Heater consumption	P_H	≤950mW
	Sensitivity	S	Rs(in air)/Rs(in 5000ppmCH_4)≥5
	Output Voltage	Vs	2.5V～4.0V (in 5000ppm CH_4)
	Concentration Slope	α	≤0.6($R_{5000ppm}$/$R_{1000ppm}$ CH_4)
Standard test conditions	Tem. Humidity		20℃±2℃; 55%±5%RH
	Standard test circuit		Vc:5.0V±0.1V; V_H:5.0V±0.1V
	Preheat time		Over 48 hours

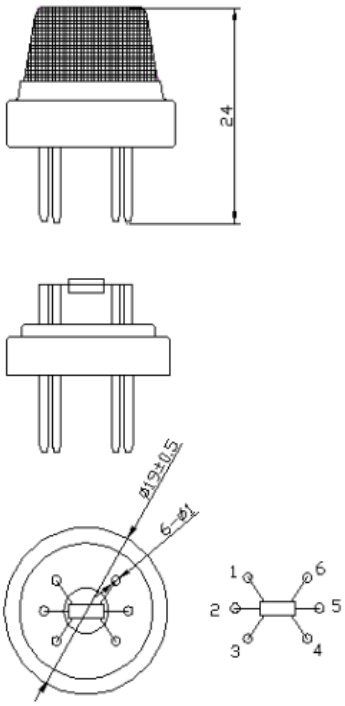


Fig1.Sensor Structure
Unit: mm

Η δομή και η διαμόρφωση του αισθητήρα αερίου MQ-4 παρουσιάζεται αισθητήρας που αποτελείται από κεραμικό σωλήνα micro AL2O3, ευαίσθητο στρώμα διοξειδίου κασσίτερου (SnO2), ηλεκτρόδιο μέτρησης και θερμαντήρας που στερεώνονται σε κρούστα από πλαστικό και δίχτυ από ανοξείδωτο χάλυβα. Ο θερμαντήρας παρέχει τις απαραίτητες συνθήκες εργασίας για την εργασία ευαίσθητων εξαρτημάτων. Το περίβλημα MQ-4 έχει 6 ακίδες, 4 από αυτά χρησιμοποιούνται για τη λήψη σημάτων και άλλα 2 χρησιμοποιούνται για παροχή ρεύματος θέρμανσης.

MQ-8: Όταν υπάρχει αέριο υδρογόνο, η αγωγιμότητα του αισθητήρα αυξάνεται καθώς αυξάνεται η συγκέντρωση του αερίου. Οι χρήστες μπορούν να μετατρέψουν την αλλαγή αγωγιμότητας ώστε να αντιστοιχεί στο σήμα εξόδου της συγκέντρωσης αερίου μέσω ενός απλού κυκλώματος. Ο αισθητήρας MQ-8gas έχει υψηλή ευαισθησία αέριο υδρογόνο, έχει επίσης αντι-παρεμβολές σε

άλλα αέρια. Αυτός ο αισθητήρας μπορεί να ανιχνεύσει υδρογόνο, ειδικά αέρια. Είναι ένα είδος αισθητήρας χαμηλού κόστους για είδη εφαρμογών.

Χαρακτηριστικά MQ-8

Technical Parameters **Stable.1**

Model			MQ-8
Sensor Type			Semiconductor
Standard Encapsulation			Bakelite, Metal cap
Target Gas			Hydrogen
Detection range			100～1000ppm(H_2 gas)
Standard Circuit Conditions	Loop Voltage	V_c	≤24V DC
	Heater Voltage	V_H	5.0V±0.1V AC or DC
	Load Resistance	R_L	Adjustable
Sensor character under standard test conditions	Heater Resistance	R_H	29Ω±3Ω(room tem.)
	Heater consumption	P_H	≤900mW
	Sensitivity	S	Rs(in air)/Rs(in 1000ppm H_2)≥5
	Output Voltage	Vs	2.5V～4.0V（in 1000ppm H_2）
	Concentration Slope	α	≤0.6($R_{1000ppm}$/R_{400ppm} H_2)
Standard test conditions	Tem. Humidity		20℃±2℃；55%±5%RH
	Standard test circuit		Vc:5.0V±0.1V； V_H:5.0V±0.1V
	Preheat time		Over 48 hours

NOTE: Output voltage (Vs) is V... in test environment

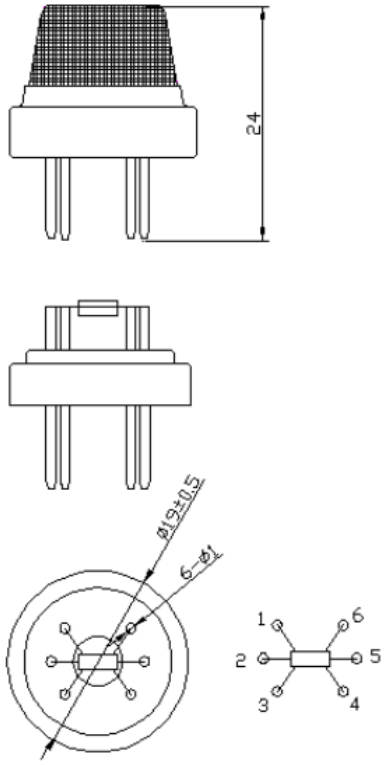
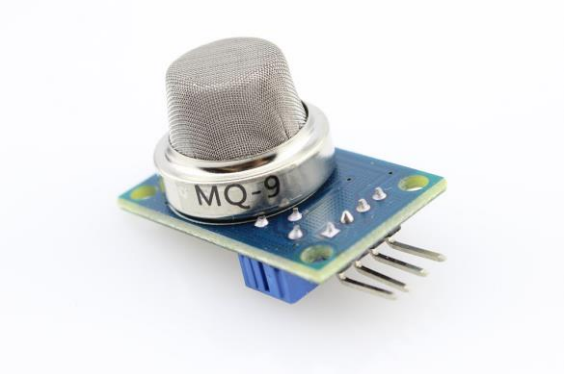


Fig1.Sensor Structure

Η δομή και διαμόρφωση του αισθητήρα αερίου MQ-8 αποτελείται από κεραμικό σωλήνα micro AL2O3, ευαίσθητο στρώμα διοξειδίου κασσίτερου (SnO2), ηλεκτρόδιο μέτρησης και θερμαντήρα

στερεώνονται σε κρούστα από πλαστικό και ανοξείδωτο δίχτυ. Ο θερμαντήρας παρέχει τις απαραίτητες συνθήκες εργασίας για την εργασία ευαίσθητων εξαρτημάτων. Το περίβλημα MQ-8 έχει 6 ακίδες, 4 από αυτά χρησιμοποιούνται για τη λήψη σημάτων και άλλα 2 χρησιμοποιούνται για παροχή ρεύματος θέρμανσης.

MQ-9: Κάνει ανίχνευση με μέθοδο κύκλου υψηλής και χαμηλής θερμοκρασίας, και ανιχνεύει CO όταν χαμηλή θερμοκρασία (θερμαίνεται κατά 1,5V). Η αγωγιμότητα του αισθητήρα είναι υψηλότερη μαζί με την αύξηση της συγκέντρωσης αερίου. Όταν η υψηλή θερμοκρασία (θερμαίνεται από 5,0 V), ανιχνεύει εύφλεκτο αέριο μεθάνιο, προπάνιο κ.λπ. και καθαρίζει τα άλλα αέρια που προσροφώνται σε χαμηλή θερμοκρασία. Χρησιμοποιήστε απλό ηλεκτρικό κύκλωμα και μετατροπή αλλαγής αγωγιμότητας για να αντιστοιχεί στο σήμα εξόδου της συγκέντρωσης αερίου. Ο αισθητήρας αερίου MQ-9 έχει υψηλή ευαισθησία σε μονοξείδιο του άνθρακα, μεθάνιο και υγραέριο. Ο αισθητήρας θα μπορούσε να χρησιμοποιηθεί για την ανίχνευση διαφορετικών αερίων που περιέχει CO και εύφλεκτα αέρια, είναι με χαμηλό κόστος και κατάλληλο για τέτοιου είδους εφαρμογές.



Χαρακτηριστικά MQ-9

Model No.			MQ-9
Sensor Type			Semiconductor
Standard Encapsulation			Bakelite
Detection Gas			CO and combustible gas
Concentration			10-1000ppm CO 100-10000ppm combustible gas
Circuit	Loop Voltage	V_c	≤10V DC
	Heater Voltage	V_H	5.0V±0.2V ACorDC（High） 1.5V±0.1V ACorDC（Low）
	Heater Time	T_L	60±1S（High）90±1S（Low）
	Load Resistance	R_L	Adjustable
Character	Heater Resistance	R_H	31Ω±3Ω（Room Tem.）
	Heater consumption	P_H	≤350mW
	Sensing Resistance	R_s	2KΩ-20KΩ(in 100ppm CO)
	Sensitivity	S	Rs(in air)/Rs(100ppm CO)≥5
	Slope	α	≤0.6(R_{300ppm}/R_{100ppm} CO)
Condition	Tem. Humidity		20℃±2℃; 65%±5%RH
	Standard test circuit		Vc:5.0V±0.1V; V_H（High）: 5.0V±0.1V; V_H（Low）: 1.5V±0.1V
	Preheat time		Over 48 hours

Η δομή και η διαμόρφωση του αισθητήρα αερίου MQ-9 είναι αισθητήρας που αποτελείται από κεραμικό σωλήνα micro AL2O3, ευαίσθητο στρώμα διοξειδίου κασσίτερου (SnO2), ηλεκτρόδιο μέτρησης και θερμαντήρα στερεώνονται σε κρούστα από πλαστικό και ανοξείδωτο δίχτυ. Ο θερμαντήρας παρέχει τις απαραίτητες συνθήκες εργασίας για την εργασία ευαίσθητων εξαρτημάτων. Το περίβλημα MQ-7 έχει 6 ακίδες, 4 από αυτά χρησιμοποιούνται για τη λήψη σημάτων και άλλα 2 χρησιμοποιούνται για την παροχή ρεύματος θέρμανσης.

MQ-135:ΤΣε μια ατμόσφαιρα όπου υπάρχει ρυπογόνο αέριο, η αγωγιμότητα του αισθητήρα αερίου αυξάνεται μαζί με τη συγκέντρωση του ρυπαντικού αερίου αυξάνεται. Το MQ-135 εκτελεί καλή ανίχνευση καπνού και άλλων επιβλαβών αερίων, ιδιαίτερα ευαίσθητο στην αμμωνία, το σουλφίδιο και τη βενζολοστεάμη. Η ικανότητά του να ανιχνεύει διάφορα επιβλαβή αέρια και χαμηλότερο κόστος καθιστά το MQ-135 ιδανική επιλογή για εφαρμογες ανίχνευσης αερίου.

Χαρακτηριστικά MQ-135

Technical Parameters **Stable.1**

Model			MQ135
Sensor Type			Semiconductor
Standard Encapsulation			Bakelite, Metal cap
Target Gas			ammonia gas, sulfide, benzene series steam
Detection range			10～1000ppm(ammonia gas, toluene, hydrogen, smoke)
Standard Circuit Conditions	Loop Voltage	V_c	≤24V DC
	Heater Voltage	V_H	5.0V±0.1V AC or DC
	Load Resistance	R_L	Adjustable
Sensor character under standard test conditions	Heater Resistance	R_H	29Ω±3Ω (room tem.)
	Heater consumption	P_H	≤950mW
	Sensitivity	S	Rs(in air)/Rs(in 400ppm H_2)≥5
	Output Voltage	Vs	2.0V～4.0V（in 400ppm H_2）
	Concentration Slope	α	≤0.6(R_{400ppm}/R_{100ppm} H_2)
Standard test conditions	Tem. Humidity		20℃±2℃； 55%±5%RH
	Standard test circuit		Vc:5.0V±0.1V； V_H: 5.0V±0.1V
	Preheat time		Over 48 hours

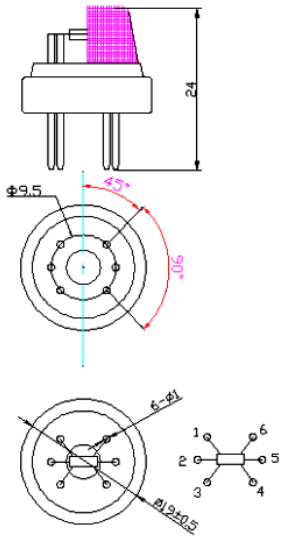


Fig1.Sensor Structure
Unit: mm

Η δομή και διαμόρφωση του αισθητήρα αερίου MQ-135 που αποτελείται από κεραμικό σωλήνα Micro AL2O3, ευαίσθητο στρώμα διοξειδίου κασσίτερου (SnO2), ηλεκτρόδιο μέτρησης και θερμαντήρα στερεώνονται σε ακροδέκτες από πλαστικό και ανοξείδωτο δίχτυ. Ο θερμαντήρας παρέχει τις απαραίτητες συνθήκες εργασίας για ευαίσθητες εργασίες συστατικά. Το περίβλημα MQ-135 έχει

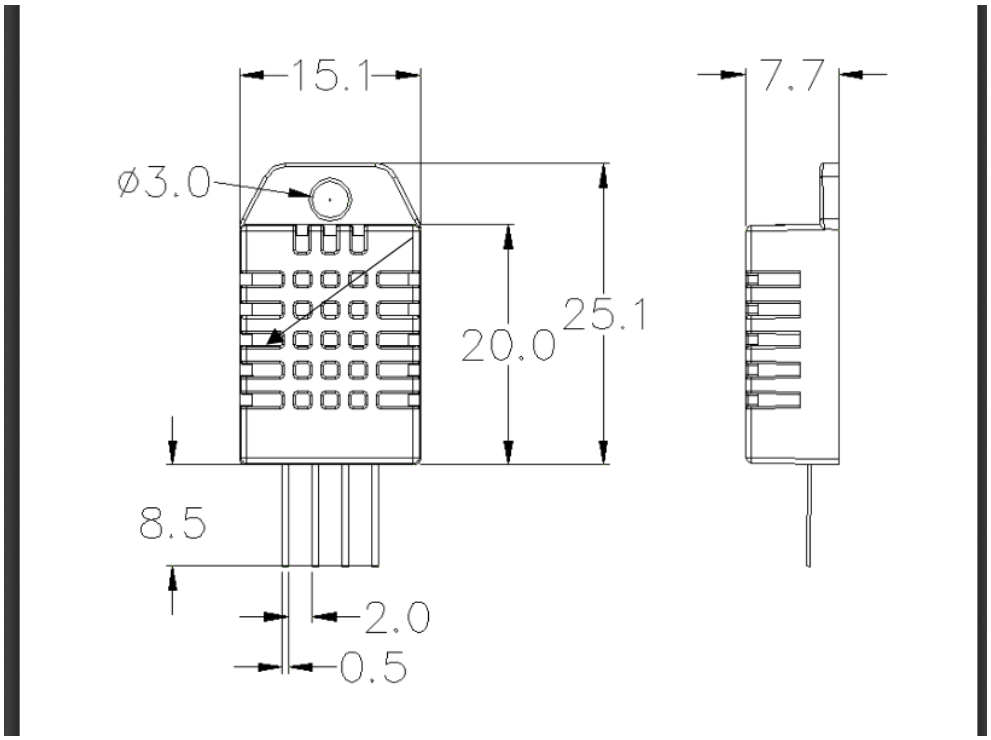
6 ακίδες, 4 από αυτά χρησιμοποιούνται για τη λήψη σημάτων και άλλα 2 χρησιμοποιούνται για την παροχή ρεύματος θέρμανσης.

5) DHT 22:Χρησιμοποιεί τεχνική συλλογής ψηφιακού σήματος και τεχνολογία ανίχνευσης υγρασίας, διασφαλίζοντας την αξιοπιστία και τη σταθερότητά του. Τα στοιχεία ανίχνευσής του συνδέονται με έναν ενιαίο υπολογιστή chip 8 bit. Κάθε αισθητήρας αυτού του μοντέλου αντισταθμίζεται από τη θερμοκρασία και βαθμονομείται σε θάλαμο ακριβούς βαθμονόμησης .Ο συντελεστής αποθηκεύεται σε τύπο προγράμματος στη μνήμη OTP, όταν ανιχνεύει ο αισθητήρας, θα έχει συντελεστή από τη μνήμη. Το μικρό μέγεθος και η χαμηλή κατανάλωση και η μεγάλη απόσταση μετάδοσης (20m) επιτρέπουν στο DHT22 να ταιριάζει σε όλα τα είδη σκληρών εφαρμογών, καθιστώντας τη σύνδεση πολύ βολική.

Χαρακτηριστικά DHT-22

Technical Specification:

Model	DHT22
Power supply	3.3-6V DC
Output signal	digital signal via single-bus
Sensing element	Polymer capacitor
Operating range	humidity 0-100%RH; temperature -40~80Celsius
Accuracy	humidity +-2%RH(Max +-5%RH); temperature <+-0.5Celsius
Resolution or sensitivity	humidity 0.1%RH; temperature 0.1Celsius
Repeatability	humidity +-1%RH; temperature +-0.2Celsius
Humidity hysteresis	+-0.3%RH
Long-term Stability	+-0.5%RH/year
Sensing period	Average: 2s
Interchangeability	fully interchangeable
Dimensions	small size 14*18*5.5mm; big size 22*28*5mm



6)<u>Solar power bank:</u>Είναι η συσκεύη που τροφοδοτεί το σύστημα και διατηρεί ενέργεια απο τον ήλιο για ακόμα μεγαλύτερη αυτονομία.

7.2 Συνδεσμολογία

<u>Πομπός:</u>

Ο πομπός έχει την μορφή ενός κούτιου (όπως φαίνεται και στην φωτογραφία παρακάτω) όπου περιέχει το ενα mini breadboard ,arduino mini pro, τους αισθητήρες και την κεραία lora ra-02.

Το arduino mini pro είναι πάνω στο breadboard ενώνοντας το vcc με την μπάρα + και το gnd(ground) με την μπάρα -.

Το lora ra 02 ειναι συνδεμένο ως εξής:

3.3V → + για να τροφοδοτήται
Gnd → - για να γειώνεται
Nss → D10
D100 → D2
SCK → D13
MISO → D12
MOSI → D11
RST → D9

Ο DHT 22 έχει ψηφιακή έξοδο και είναι συνδεμένο ως εξής:

3,3V → +
GND → -
*D4 → D3

Ο MQ4 συνδέεται ως εξής:

A0 → A0
VCC → +
GND → -

Ο MQ8 συνδέεται ως εξής:

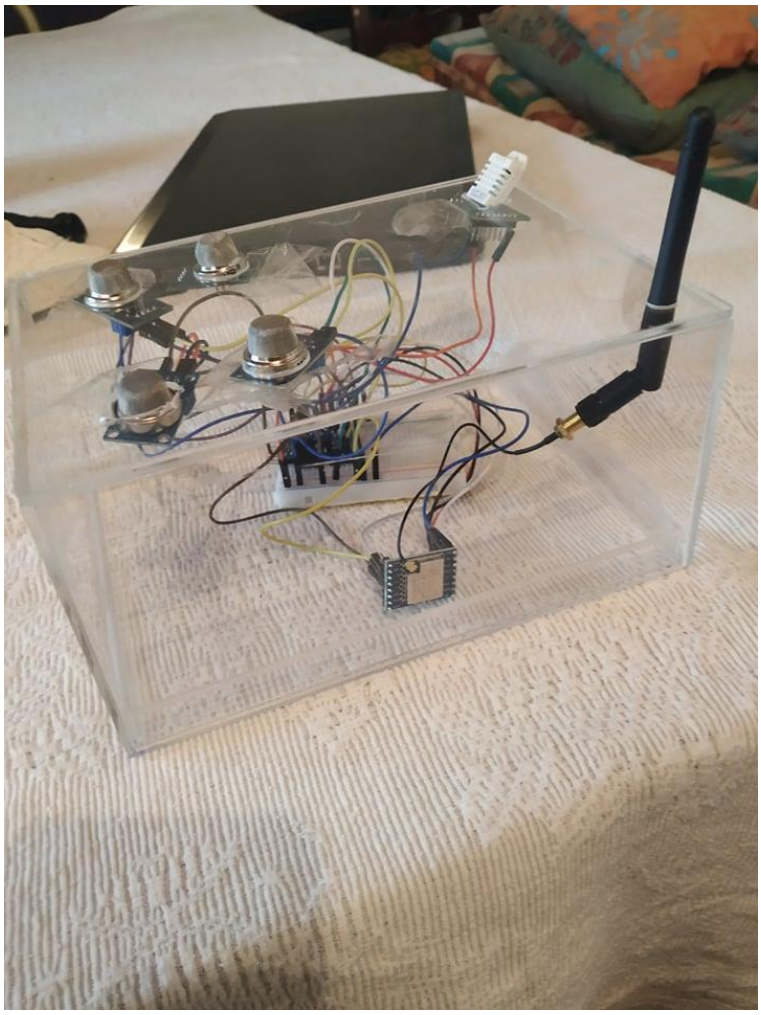
A0 → A3
VCC → +
GND → -

Ο MQ9 συνδέεται ως εξής:

A0 → A7
VCC → +
GND → -

Ο MQ135 συνδέεται ως εξής:

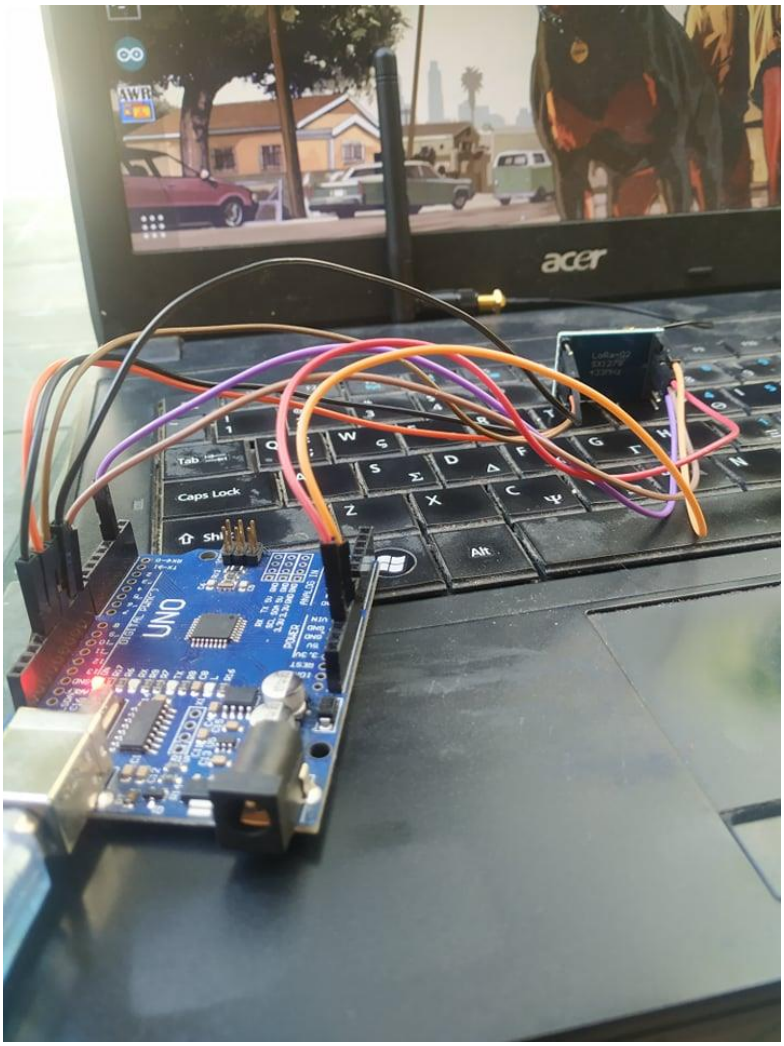
A0 → A6
VCC → +
GND → -



Δέκτης:

Ο δέκτης αποτελείται μόνο απο ένα arduino uno και το lora ra 02 το οποίο είναι συνδεμένο πάνω του ως εξής:
3,3V → 3,3V
GND → GND
NSS → D10
D100 → D2
SCK → D13
MISO → D12
MOSI → D11
RST → D9

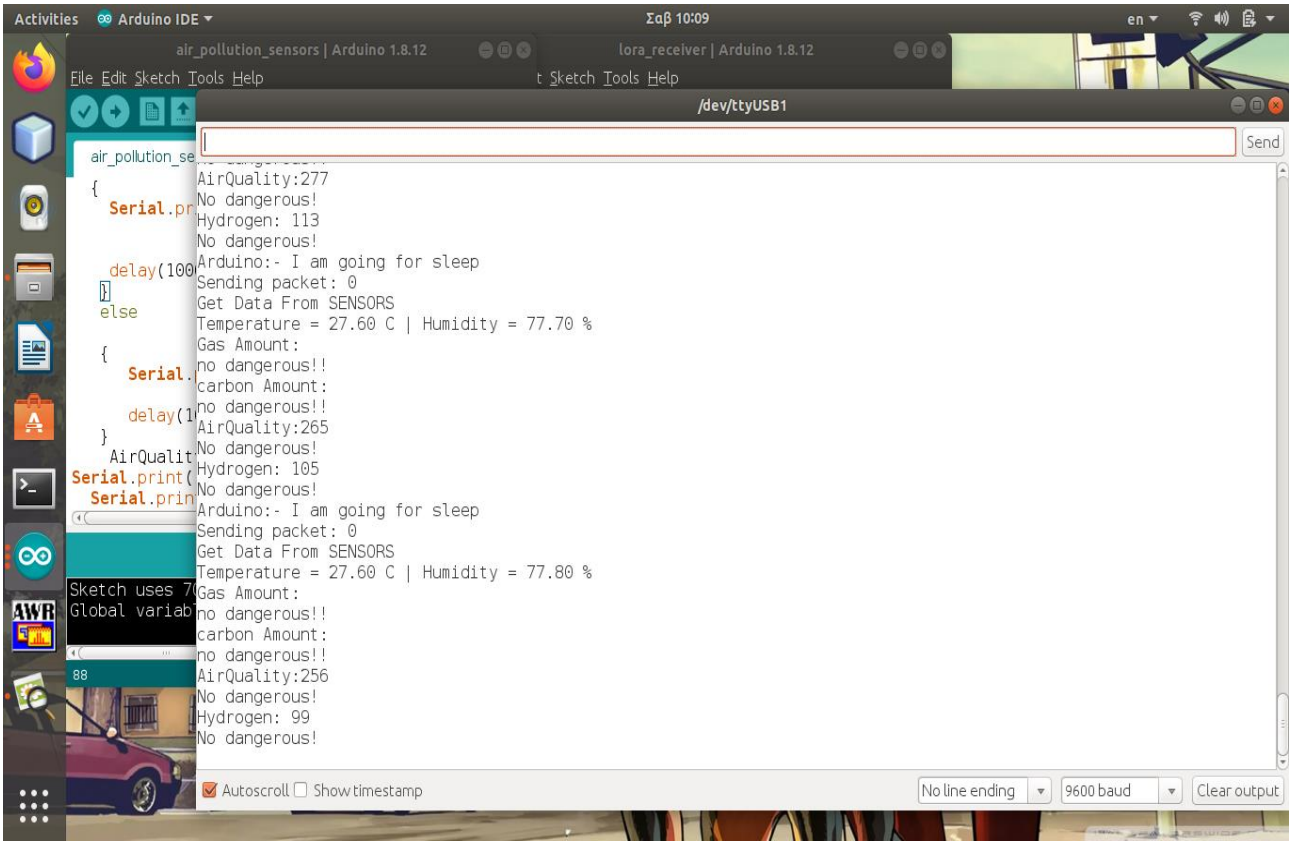
Το arduino uno είναι συνδεμένο με usb στον υπολογιστή ο οποίος μας δείχνει το αποτέλεσμα τον μετρήσεων real time αλλα και λειτουργεί σαν βάση δεδομένον κάθως αποθηκέυει τις τιμές σε ένα txt αρχείο.



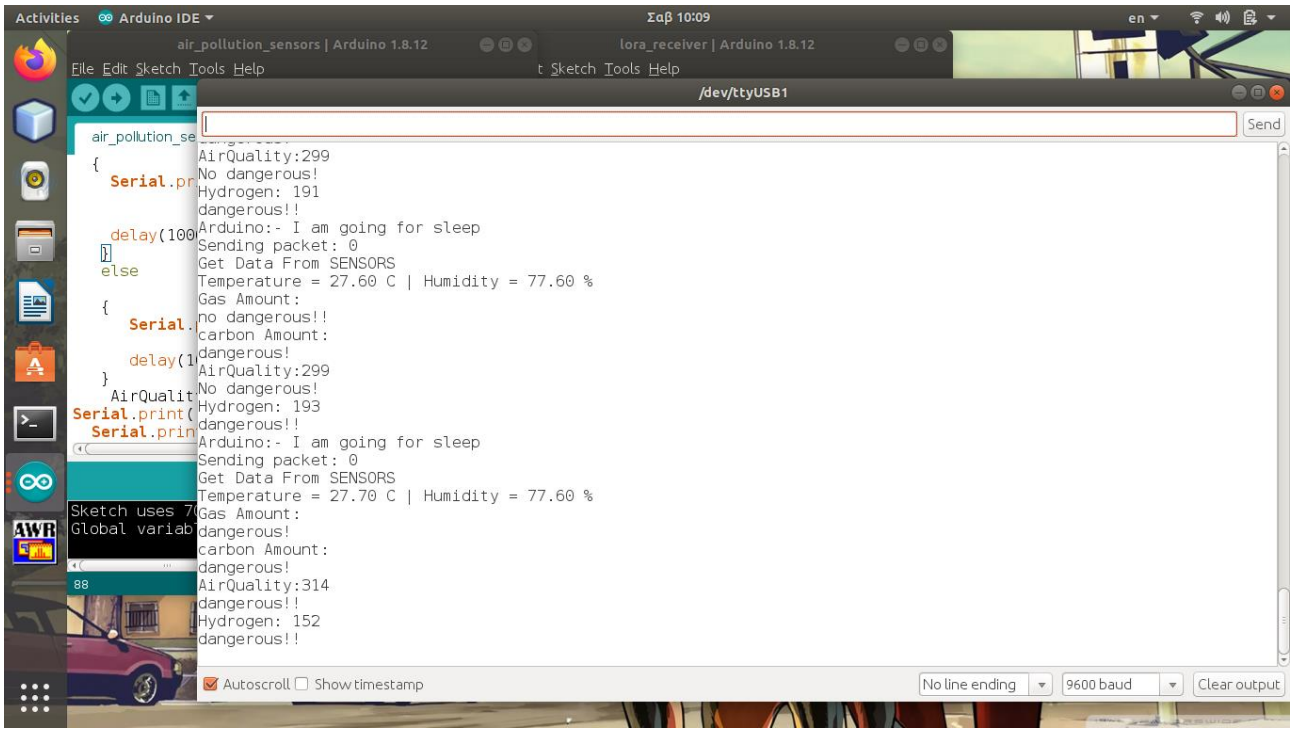
Εμφάνιση

Το πρόγραμμα τρέχει απο το Arduino IDE και η εμφάνιση των τιμών είναι στο serial monitor. Ας δούμε παρακάτω ένα παράδειγμα για το πως λειτουργεί.

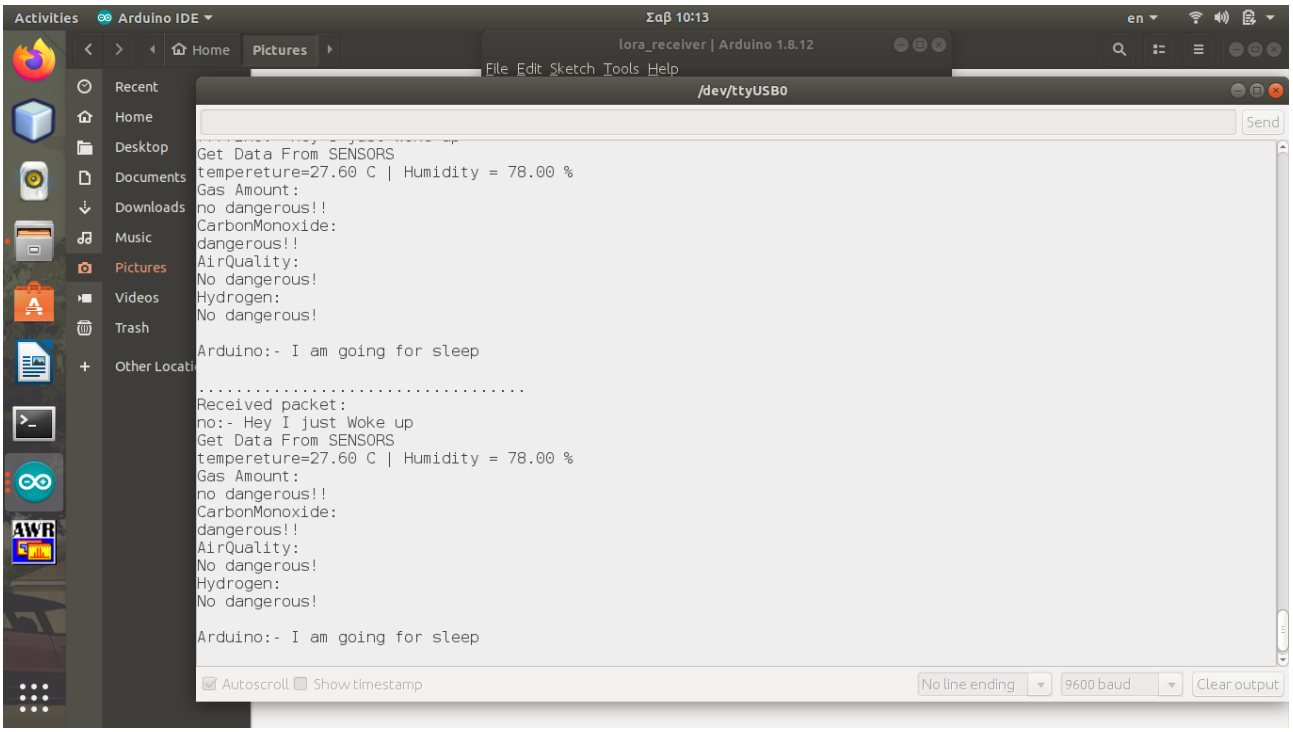
Αρχικά κάνουμε upload τον κώδικας μας στο arduino mini pro που λειτουργεί ως transmitter και τον κώδικα του receiver στο arduino uno.Συνδέουμε τις συσκευές με τον υπολογιστή και παίρνουμε τις αντίστοιχες τιμές.



Όπως παρατηρούμε το περιβάλλον είναι καθαρό και γιαυτό το πρόγραμμα μας δείχνει οτι δεν υπάρχει κίνδυνος.Την αμέσως επόμενη στιγμη περνάμε ενάν αναπτύρα με πατημένο το κουμπί του υγραερίου πάνω απο τους αισθητήρες μας.



Όπως παρατηρούμε απευθείας η τιμές έγιναν επικίνδυνες.Ας βγάλουμε τον trasmitter απο το port του υπολογιστή και ας τον τροφοδοτήσουμε με μπαταρία ετσι όπως θα λειτουργεί και μετα τον προγραμματισμό του . Ανοίγουμε το serial port του receiver.



Παρατηρούμε οτι όλες οι τιμές στέλνονται ασύρματα. Ο receiver λαμβάνει τα πακέτα του συστήματος μας και τα εμφανίζει real time. Όλες οι μετρήσεις αποθηκεύονται σε ένα txt αρχείο με την βοήθεια του προγράμματος PUTTY.

31 7.3 Κωδικοποίηση

Ο κώδικας του transmitter:

Αρχικοποιούμε τις βιβλιοθήκες

```
#include <SPI.h>
#include <LoRa.h>
#include <LowPower.h>
#include <time.h>
```

```
#include <MQUnifiedsensor.h>
#include <dht.h>
dht DHT;
```

Αρχικοποιούμε την θέση του DHT22 στο digital pin 3

```
#define DHT22_PIN 3
```

Αρχικοποιούμε τις τιμές

```
float hum;
float temp;
int gas;


int hydrogen;
int carbonMonoxide;
int AirQuality ;


int counter = 0;


void setup() {
```

Ορίζουμε braud

```
Serial.begin(9600);
```

Προγραμματίζουμε την κεραία Lora ra -02

```
while (!Serial);


Serial.println("LoRa Sender");


if (!LoRa.begin(433E6)) {
Serial.println("Starting LoRa failed!");
while (1);
}
```

```
}

void loop() {
```

Ορίζουμε τι θα εμφανίσει το serial port και τις διαχειριζόμαστε τις τίμες που μετράει ο κάθε αισθητήρας

```
Serial.print("Sending packet: ");
  Serial.println(counter);
  Serial.println("Get Data From SENSORS");
  delay(1000);
  int chk = DHT.read22(DHT22_PIN);

  float t = DHT.temperature;
  float h = DHT.humidity;

  Serial.print("Temperature = ");
  Serial.print(t);
  Serial.print(" C | ");

  Serial.print("Humidity = ");
  Serial.print(h);
  Serial.println(" % ");

gas=analogRead(0);
Serial.print("gas:");
Serial.println(gas, DEC);
 if(gas<400)
  {
    Serial.println("No dangerous!!");


   }
   else

   {
      Serial.println("dangerous!");
```

```
  }


hydrogen= analogRead(3);
Serial.print("Hydrogen: ");
Serial.print(hydrogen, DEC);
Serial.println("");

if(hydrogen<300)
 {
   Serial.println("No dangerous!!");


   delay(1000);
  }
  else
  {
    Serial.println(" dangerous!");

    delay(1000);
}



AirQuality = analogRead(6);
Serial.print("AirQuality:");
 Serial.println(AirQuality, DEC);
 if(AirQuality<300)
 {
   Serial.println("No dangerous!!");



  }
  else
  {
    Serial.println(" dangerous!");
```

```
  }

 carbonMonoxide = analogRead(7);

  Serial.print("Carbon Amount: " );
   Serial.println(carbonMonoxide, DEC);


   if(carbonMonoxide<300)
  {
    Serial.println("no dangerous!!");


    delay(1000);
   }
   else

   {
      Serial.println("dangerous!");


   }
delay(1000);
Serial.println("Arduino:- I am going for sleep");




  delay(200);
```

Ορίζουμε το τι θα μεταδόση η κεραία

```
   LoRa.beginPacket();
  LoRa.print("Sending paCket: ");
  LoRa.println(counter);
  LoRa.print("Arduino:- Hey I just Woke up");
  //delay (2000);
```

```
  LoRa.print('\n');
  LoRa.println("Get Data From SENSORS");
  //delay (2000);
  LoRa.print("tempereture=");
  LoRa.print( t);
  LoRa.print(" C | ");

  LoRa.print("Humidity = ");
  LoRa.print(h);
  LoRa.print(" % ");
  LoRa.print('\n');
  LoRa.print("gas:");
  LoRa.println(gas, DEC);
 if(gas<400)
  {
   LoRa.println("No dangerous!!");


   }
   else

   {
     LoRa.println("dangerous!");


   }

  LoRa.print("Hydrogen: ");
  LoRa.print(hydrogen, DEC);
  LoRa.println("");

if(hydrogen<300)
  {
    LoRa.println("No dangerous!!");



   }
   else
```

```
  {
    LoRa.println(" dangerous!");


}


 LoRa.print("AirQuality:");
 LoRa.println(AirQuality, DEC);

 if(AirQuality<300)
 {
   LoRa.println("No dangerous!!");



  }
 else
 {
     LoRa.println(" dangerous!");

 }
 LoRa.print("Carbon Amount: " );
 LoRa.println(carbonMonoxide, DEC);


   if(carbonMonoxide<300)
 {
  LoRa.println("no dangerous!!");



  }
 else

 {
    LoRa.println("dangerous!");
```

```
  }


  LoRa.println("Arduino:-sleep time");
  LoRa.endPacket();
  counter++;
  delay(200);
```

Λειτουργεία sleep mode

```
LowPower.idle(SLEEP_8S, ADC_OFF, TIMER2_OFF, TIMER1_OFF, TIMER0_OFF,
SPI_OFF, USART0_OFF, TWI_OFF);
Serial.println("Arduino:- Hey I just Woke up");
Serial.println("");
delay(2000);

}
```

Ο κώδικας του receiver :

Ορίζουμε την βιβλιοθήκη

```
#include <LoRa.h>


void setup()
{
Ορίζουμε το braud
Serial.begin(9600);
while (!Serial);
Serial.println("LoRa Receiver");
if (!LoRa.begin(433E6)) {
```

```
Serial.println("Starting LoRa failed!");
while (1);
}
}

void loop() {
Προσπαθεί να παραλάβει το πακέτο
int packetSize = LoRa.parsePacket();
Αμα λάβει λάβει το πακέτο
if (packetSize)
{
Serial.println("");
Serial.println(".....");
Serial.println("Received packet: ");

Διαβάζει το πακέτο
while (LoRa.available()) {
char incoming = (char)LoRa.read();
if (incoming == 'c')
{
Serial.print("Error");
}
else
{
Serial.print(incoming);
}
}
}
}
```

32 7.4 Προτάσεις για την βελτίωση του συστήματος

RTC:

Η σημαντικότερη έλλειψη του συστήματος μας είναι αυτή του RTC (Real Time Clocker). Ο λόγος που δεν χρησιμοποιήθηκε είναι γιατί οι 5 αισθητήρες και η κεραία Lora ra -02 δεσμεύουν σχεδόν όλα τα digital pins και δεν υπάρχουν τα 3pins που απαιτεί το RTC. Μπορούμε να το

παρακάμψουμε παίρνοντας ώρα απο τον υπολογιστή αλλά αυτό προϋποθέτει ότι το σύστημα θα είναι συνδεμένο μόνιμα. Άλλος τρόπος είναι να αφαιρεθούν 2 αισθητήρες και να δουλέψουμε με 3 αλλά μετά από πολύωρη σκέψη θεώρησα οτι είναι πιο σημαντικό σε ένα τέτοιο project να μπορούμε να συλλέγουμε και να μεταδίδουμε πληροφορία απο 5 αισθητήρες παρα την ώρα που είναι σχετικά απλή διαδικασία. Παραμένει όμως το βασικότερο ελάττωμα καθώς έλλειψη σηματοδοτεί άλλα προβλήματα όπως το να μην γνωρίζουμε αν το πακέτο μετρήθηκε αυτήν την χρονική στιγμή που στάλθηκε ή να μην γνωρίζουμε αν χάθηκε κάποιο πακέτο κτλ.

Zigbee:

Συνήθως τα ασύρματα δίκτυα αισθητήρων τέτοιου τύπου φτιάχνονται με Zigbee για αρκετούς λόγους (τυχαία διασπορά αισθητηρών κτλ.). Οι λόγοι που δεν χρησιμοποιήθηκε είναι αρχικά το κόστος θα ανέβαζε κατα πολύ την συνολική τιμή του συστήματος αλλά ένας λόγος είναι η απόσταση . Ενα σύστημα Zibgee έχει range μέχρι το πολύ 100 μέτρα ενώ με την τεχνολογία του Lora ra 02 που χρησιμοποιήθηκε φτάνει να μεταδώσει μέχρι και 15 χλμ γιαυτό και προτιμήθηκε.

Βίδες στους αισθητήρες:

Το κουτί που έφτιαξα για να προστατεύει την καλωδίωση είναι με το υλικό *plexiglass και σε πρώτη φάση η αισθητήρες στερεώθηκαν με σιλικόνη. Όμως ένα ανεπάντεχο πρόβλημα εμφανίστηκε καθώς οι αισθητήρες μετρούσανε τις βλαβερές ουσίες τις σιλικόνης ακόμα και αφού είχε στεγνώσει. Έτσι θα έπρεπε να αφαιρεθούν και να βρεθεί άλλος τρόπος, ο καλύτερος θα ήταν βίδες αλλά θα έκανε δύσκολη την αλλαγή κάποιου αισθητήρα όπως επίσης υπάρχει πολύ μεγάλος κίνδυνος να τραυματιστεί η πάνω πλευρά του κουτιού γιαυτό και προτιμήθηκε διάφανο tape.*

Database:

Μία ακόμα ιδέα που θα μπορούσε να βελτιώσει είναι να γίνονται upload οι μετρήσεις σε μια διαδικτυακή βάση δεδομένων για παράδειγμα στο drive ή στο firebase και να είναι εμφανείς στον χρήστη απο όπου και να βρίσκεται. Το συγκεκριμένο κομμάτι δεν πραγματοποιήθηκε λόγω έλλειψη hardware καθώς απαιτεί esp mcu 8266(το οποίο ενδέχεται θα έκανε παρεμβολές στην κεραία μας οπότε δεν συνιστάται) ή arduino uno wifi (και άλλες συσκευές με πρόσβαση στο internet). Μια άλλη ιδέα θα ήταν να μετατρέψουμε τα δεδομένα σε Json αρχεία και να τα αναρτήσουμε και με την βοήθεια τις python και τις μεθόδου mojo να τα αναρτούσαμε στο διαδίκτυο αλλά κάτι τέτοιο θα

ανέβαζε την πολυπλοκότητα του συστήματος και θα απευθυνόταν στον προγραμματιστικό κλάδο αλλά παραμένει καλή ιδέα μελοντικά.

LCD:

Τα δεδομένα απο τις μετρήσεις θα μπορούσαν να εμφανίζονται στην αρχή κάποιου δρόμου ή σε διασταυρώσεις οπού γίνονται οι μετρήσεις και θα εμφάνιζε στον χρήστη το αν είναι επικίνδυνη η διαδρομή σε πραγματικό χρόνο με την βοήθεια μιας μικρής lcd οθόνης έτσι ώστε να έχει ο καθένας πρόσβαση στις μετρήσεις των αισθητήρων και να αποφασίζει ποιόν δρόμο θα ακολουθήσει με κριτήριο την υγεία του.

Επίλογος

Ο κόσμος των αισθητήρων είναι ένας συναρπαστικός κόσμος χωρίς όρια καθώς φτάνει εκεί που φτάνει και η φαντασία του δημιουργού του. Πλέον υπάρχουν αμέτρητη αισθητήρες και ακόμα περισσότερες ιδέες για την χρήση τους . Με την ολοκλήρωση αυτής της πτυχιακής εργασίας επισημάνθηκαν πολλές από τις δυσκολίες που θα αντιμετωπίσει κάποιος που θα επιχειρήσει να δημιουργήσει ένα τέτοιο δίκτυο αλλά και το τι μπορείς να επιτύχεις μέσα από αυτά. Η τιμές που υπάρχουν στην αγορά είναι πολύ δελεαστικές να ασχοληθεί ο καθένας ακόμα και αν δεν είναι σχετικός με το αντικείμενο. Αυτή η εργασία έχει ως σκοπό την παρακολούθηση τις ατμοσφαιρικής ρύπανσης με σκοπό την προφύλαξη του ανθρώπου και του πλανήτη.

Ο πλανήτης μας είναι το σπίτι μας. Καθημερινά καταστρέφεται απο των άνθρωπο και απο δραστηριότητες του οι οποίες θα πρέπει να αντικατασταθούν απο πιο οικολογικές μεθόδους που θα προστατεύουν την γη ,των αέρα , το φυτικό και ζωικό βασίλειο αλλά και τον ανθρώπινο οργανισμό. Είμαστε υπεύθυνη να δώσουμε στην επόμενη γενιά έναν κόσμο με καθαρό ουρανό και αέρα αλλά επίσης την ανατροφή, την ευαισθησία και την αγάπη γι αυτόν έτσι ώστε να μην γυρίσουμε στις προηγούμενες και επιβλαβής και αντίξοες καταστάσεις. Στρέφοντας την ματιά μας στις ανανεώσιμες πήγες ενέργειας και στα βιοδιασπώμενα προϊόντα , θα πρέπει να χρησιμοποιούμε το αυτοκίνητο όπου είναι απαραίτητο να κινούμαστε στις μικρές αποστάσεις με τα πόδια , με ποδήλατα , με μέσα μαζικής μεταφοράς και με σκουτερς, να επιλέγουμε κατά την αγορά αυτοκίνητου υβριδικά και ηλεκτρικά οχήματα που πλέον δεν υστερούν σε τίποτα από τα βενζινοκίνητα και τα πετρελαιοκίνητα ενώ ακόμα μια πολύ καλή ιδέα για να καθαρίσει η ατμόσφαιρα , να γεμίσουν τα πνευμόνια μας οξυγόνο αλλά και για θέμα αισθητικής είναι να φυτέψουμε στην πόλη μας κήπους με λουλούδια και να στολίσουμε τους τοίχους μας με αναρριχόμενα φυτά μετατρέποντας την τσιμεντένια κόλαση σε έναν επίγειο φυσικό παράδεισο.

Μπορούμε όλοι μαζί με μικρές καθημερινές προσπάθειες να διορθώσουμε τα λάθη των προηγούμενων γενιών και να δημιουργήσουμε τον πλανήτη που μας αξίζει.

33 Βιβλιογραφία

https://ocw.aoc.ntua.gr/modules/document/file.php/CHEMENG134/Atmosfaira_Atmosfairikh%20kai%20rypansh.pdf

http://ebooks.edu.gr/ebooks/v/html/8547/2206/Chimeia_B-Gymnasiou_html-empl/index3_4.html

http://www.wwf.gr/images/pdfs/WWF%20Ellas_Odigos%20gia%20to%20perivallon_Aeras.pdf

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.421.5140&rep=rep1&type=pdf

https://ieeexplore.ieee.org/abstract/document/5199951

https://el.wikipedia.org/wiki/%CE%91%CF%83%CF%8D%CF%81%CE%BC%CE%B1%CF%84%CE%BF_%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF_%CE%B1%CE%B9%CF%83%CE%B8%CE%B7%CF%84%CE%AE%CF%81%CF%89%CE%BD

https://el.wikipedia.org/wiki/%CE%91%CE%B9%CF%83%CE%B8%CE%B7%CF%84%CE%AE%CF%81%CE%B1%CF%82

https://www.teilar.gr/dbData/ProfAnn/profann-e0af756b.pdf

http://nemertes.lis.upatras.gr/jspui/bitstream/10889/529/1/Nimertis_Gkamas.pdf

http://www.ijcse.com/docs/INDJCSE13-04-04-048.pdf

https://opencourses.ionio.gr/modules/document/file.php/DDI101/Chapter9.pdf

http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/6360/Nonis%2C%20P..pdf?sequence=2&isAllowed=y

https://eclass.upatras.gr/modules/document/file.php/EE602/%CE%A5%CE%BB%CE%B9%CE%BA%CF%8C%20%CE%94%CE%B9%CE%B1%CE%BB%CE%AD%CE%BE%CE%B5%CF%89%CE%BD%20-%20%CE%A3%CE%B7%CE%BC%CE%B5%CE%B9%CF%8E%CF%83%CE%B5%CE%B9%CF%82/MAC%20Protocols.ppt

file:///C:/Users/deigre/Downloads/Ergastirio_3.pdf

http://ikee.lib.auth.gr/record/114828/files/ptuxiaki1.pdf

https://www.ukessays.com/essays/information-technology/trama-in-wireless-sensor-networks-information-technology-essay.php

https://el.wikipedia.org/wiki/%CE%91%CE%B9%CF%83%CE%B8%CE%B7%CF%84%CE%AE%CF%81%CE%B1%CF%82#%CE%A7%CE%B1%CF%81%CE%B1%CE%BA%CF%84%CE%B7%CF%81%CE%B9%CF%83%CF%84%CE%B9%CE%BA%CE%AC_%CE%B1%CE%B9%CF%83%CE%B8%CE%B7%CF%84%CE%AE%CF%81%CF%89%CE%BD

https://el.wikipedia.org/wiki/%CE%91%CF%83%CF%8D%CF%81%CE%BC%CE%B1%CF%84%CE%BF_%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF_%CE%B1%CE%B9%CF%83%CE%B8%CE%B7%CF%84%CE%AE%CF%81%CF%89%CE%BD#%CE%95%CF%86%CE%B1%CF%81%CE%BC%CE%BF%CE%B3%CE%AD%CF%82

https://www.elprocus.com/architecture-of-wireless-sensor-network-and-applications/

https://ieeexplore.ieee.org/document/4956693

https://www.researchgate.net/publication/337048647_Lightweight_Energy_Efficient_Secure_Data_Transmission_in_WSN

https://www.researchgate.net/publication/335594390_Overhead_Assessment_in_WSN

https://www.researchgate.net/publication/322749839_Secure_Routing_for_Mobile_Ad_hoc_Networks

https://www.intechopen.com/books/smart-wireless-sensor-networks/security-of-wireless-sensor-networks-current-status-and-key-issues

http://ijcsit.com/docs/Volume%206/vol6issue04/ijcsit2015060490.pdf

https://www.winsen-sensor.com/d/files/PDF/Semiconductor%20Gas%20Sensor/MQ135%20(Ver1.4)%20-%20Manual.pdf

https://cdn.sparkfun.com/datasheets/Sensors/Biometric/MQ-4%20Ver1.3%20-%20Manual.pdf

https://cdn.sparkfun.com/datasheets/Sensors/Biometric/MQ-8%20Ver1.3%20-%20Manual.pdf

https://www.pololu.com/file/0J314/MQ9.pdf

https://www.sparkfun.com/datasheets/Sensors/Temperature/DHT22.pdf

https://store.arduino.cc/arduino-uno-rev3

https://www.arduino.cc/en/pmwiki.php?n=Main/ArduinoBoardProMini

http://wiki.ai-thinker.com/_media/lora/docs/c048ps01a1_ra-02_product_specification_v1.1.pdf

https://www.cost.eu/actions/TD1105/#tabs

https://www.sciencedirect.com/science/article/pii/S187770581502336X

https://www.researchgate.net/publication/228732543_Design_of_energy_aware_air_pollution_monitoring_system_using_WSW

https://www.researchgate.net/figure/WSN-Topologies-a-Star-topology-b-P2P-or-mesh-topology-c-Tree-topology_fig5_272497022