ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΣΤΕΡΕΑΣ ΕΛΛΑΔΑΣ

Σχολή Τεχνολογικών Εφαρμογών
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ Τ.Ε.

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΕΥΦΥΗΣ ΔΙΑΧΕΙΡΙΣΗ ΑΝΑΝΕΩΣΙΜΩΝ ΕΝΕΡΓΕΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ»

«Master of Science in Intelligent Management of Renewable Energy Systems»

«Ανάπτυξη σύνθετων μετρικών δρομολόγησης για το πρωτόκολλο RPL»

Διπλωματική Εργασία
που υποβλήθηκε στο Τμήμα Ηλεκτρολόγων Μηχανικών Τ.Ε. του Τ.Ε.Ι. Στερεάς Ελλάδας
ως μέρος των απαιτήσεων για την απόκτηση
Μεταπτυχιακού Διπλώματος Ειδίκευσης στην Ευφυή Διαχείριση Ανανεώσιμων Ενεργειακών Συστημάτων
από τον

ΙΩΑΝΝΗ ΒΟΥΓΙΟΥΚΑ του ΒΑΣΙΛΕΙΟΥ

Μάρτιος 2018

ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΣΤΕΡΕΑΣ ΕΛΛΑΔΑΣ

Σχολή Τεχνολογικών Εφαρμογών
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ Τ.Ε.
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΕΥΦΥΗΣ ΔΙΑΧΕΙΡΙΣΗ ΑΝΑΝΕΩΣΙΜΩΝ ΕΝΕΡΓΕΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ»

«Master of Science in Intelligent Management of Renewable Energy Systems»

«Ανάπτυξη σύνθετων μετρικών δρομολόγησης για το πρωτόκολλο RPL»

Διπλωματική Εργασία
που υποβλήθηκε στο Τμήμα Ηλεκτρολόγων Μηχανικών Τ.Ε. του Τ.Ε.Ι. Στερεάς Ελλάδας
ως μέρος των απαιτήσεων για την απόκτηση
Μεταπτυχιακού Διπλώματος Ειδίκευσης στην Ευφυή Διαχείριση Ανανεώσιμων Ενεργειακών Συστημάτων
από τον

ΙΩΑΝΝΗ ΒΟΥΓΙΟΥΚΑ του ΒΑΣΙΛΕΙΟΥ

Μάρτιος 2018

ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΣΤΕΡΕΑΣ ΕΛΛΑΔΑΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ Τ.Ε.

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ανάπτυξη σύνθετων μετρικών δρομολόγησης για το πρωτόκολλο RPL

Του

Ιωάννη Βουγιούκα

Επιβλέποντες: Δρ. Θεόδωρος Ζαχαριάδης, Καθηγητής ΤΕΙ Στερεάς Ελλάδας
Δρ. Λάμπρος Σαράκης, Επίκουρος Καθηγητής ΤΕΙ Στερεάς Ελλάδας

«Η παρούσα διπλωματική εργασία εγκρίθηκε ομόφωνα από την τριμελή εξεταστική επιτροπή η οποία ορίστηκε από την Γ.Σ.Ε.Σ. του Τμήματος Ηλεκτρολόγων Μηχανικών Τ.Ε. του Τ.Ε.Ι. Στερεάς Ελλάδας, σύμφωνα με το νόμο και τον εγκεκριμένο Οδηγό Σπουδών του ΠΜΣ «Ευφυής Διαχείριση Ανανεώσιμων Ενεργειακών Συστημάτων». Τα μέλη της Επιτροπής ήταν:

……..	……	…….
Δρ. Θεόδωρος Ζαχαριάδης	Δρ. Λάμπρος Σαράκης	Δρ. Χρήστος Μανασής
Καθηγητής	Επίκουρος Καθηγητής	Καθηγητής

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Ηλεκτρολόγων Μηχανικών Τ.Ε. του Τ.Ε.Ι. Στερεάς Ελλάδας, δεν υποδηλώνει αποδοχή των απόψεων του συγγραφέα.»

Μάρτιος 2018

Ευχαριστίες

Σε αυτό το σημείο θα ήθελα να εκφράσω την ευγνωμοσύνη μου στους επιβλέποντες καθηγητές μου, Δρ. Θεόδωρο Ζαχαριάδη και Δρ. Λάμπρο Σαράκη, για το πολύ ενδιαφέρον θέμα που μου εμπιστεύτηκαν καθώς και για την εποικοδομητική τους καθοδήγηση, υποστήριξη και εμπιστοσύνη καθ' όλη την διάρκεια της εκπόνησης της παρούσας διπλωματικής εργασίας.

Επίσης θα ήθελα να ευχαριστήσω το εκπαιδευτικό ίδρυμα για την ευκαιρία που μου προσέφερε να επεκτείνω τις γνώσεις μου καθώς και το διδακτικό και διοικητικό προσωπικό του Προγράμματος Μεταπτυχιακών Σπουδών (Π.Μ.Σ.) για την στήριξη και τις γνώσεις που μου μετέδωσαν.

Τέλος θα ήθελα ιδιαίτερα να ευχαριστήσω, την οικογένεια μου για την διαρκή υποστήριξη τους τόσο οικονομικά αλλά και ψυχολογικά σε όλη την διάρκεια των σπουδών μου, δείχνοντας μου κατανόηση και εμπιστοσύνη.

Ιωάννης Βουγιούκας

Περίληψη

Η κατανεμημένη φύση και η δυναμική τοπολογία των ασύρματων δικτύων αισθητήρων (WSNs) εισάγουν πολύ ειδικές απαιτήσεις σε πρωτόκολλα δρομολόγησης που πρέπει να πληρούνται. Μία από τις πιο σημαντικές απαιτήσεις για ένα πρωτόκολλο δρομολόγησης, προκειμένου αυτό να είναι αποτελεσματικό για (WSNs) είναι η αποδοτική διαχείριση της ενέργειας των κόμβων καθώς και η επέκταση διάρκειας ζωής του δικτύου.

Το πρωτόκολλο RPL (IPv6 Routing Protocol for Low- Power and Lossy Networks), το οποίο έχει τυποποιηθεί από τον οργανισμό IETF (Internet Engineering Task Force), προσφέρει δρομολόγηση βασισμένη στο IPv6 για ασύρματα δίκτυα αισθητήρων με περιορισμένους πόρους. Η παρούσα διπλωματική εργασία στοχεύει στην μελέτη των ήδη τυποποιημένων μετρικών δρομολόγησης καθώς στην ανάπτυξη σύνθετων μετρικών βασισμένων σε αθροιστικό συνδυασμό βασικών μετρικών και στην πειραματική αξιολόγηση της επίδοσης του πρωτοκόλλου RPL όπου η δρομολόγηση πραγματοποιείται με βάση την διαθέσιμη ενέργεια του κάθε κόμβου.

Η πειραματική αξιολόγηση της επίδοσης του πρωτοκόλλου RPL υλοποιείται στο λειτουργικό σύστημα Contiki. Το Contiki είναι ένα «ανοικτό» λειτουργικό σύστημα για το «Διαδίκτυο των Πραγμάτων» - Internet of Things. Επιπλέον το πρόγραμμα προσομοίωσης Cooja που χρησιμοποιείται, παρέχει ένα περιβάλλον προσομοίωσης που μας επιτρέπει να μελετάμε τις εφαρμογές (applications) που εκτελούνται σε δίκτυα μεγάλης κλίμακας. Επίσης χρησιμοποιείται ένας αναλυτής πακέτων δικτύου, το Wireshark, το οποίο είναι ένα ελεύθερο και ανοικτού κώδικα λογισμικό ανάλυσης πρωτοκόλλων δικτύου υπολογιστών όπου επιτρέπει την παρακολούθηση της κίνησης των πακέτων στο δίκτυο.

Λέξεις κλειδιά: Ασύρματα δίκτυα αισθητήρων (WSNs), πρωτόκολλο δρομολόγησης RPL, μετρικές δρομολόγησης, προσομοίωση, διαδίκτυο των πραγμάτων (Internet of Things)

Abstract

The distributed and dynamic topology of wireless sensor networks (WSNs) introduces very special requirements in routing protocols that should be met. One of the most important features of a routing protocol, in order for that to be efficient for WSNs, is the efficient management of the energy consumption and the extension of the network's lifetime.

The RPL protocol (IPv6 Routing Protocol for Low- Power and Lossy Networks), which has been standardized by the IETF (Internet Engineering Task Force), provides IPv6 based routing for wireless sensor networks with limited resources. This thesis aims to study the already standardized routing metrics, as well as the development of complex metrics based on an additive combination of fundamental metrics, and to experimentally evaluate the performance of the RPL protocol, in cases where the routing procedure takes into account the available energy of each node.

The experimental evaluation of RPL routing performance is implemented on the operating system Contiki. Contiki is an open source operating system for the "Internet of Things". Moreover, the simulator Cooja, which is used for this purpose, provides a simulation environment that enables us to monitor applications that are implemented on large scale networks. Furthermore, we are using Wireshark, which is a free and open source network protocol analyzer which monitors packet traffic in the network.

Keywords: Wireless sensor networks (WSNs), routing protocol RPL, routing metrics, simulation, Internet of Things (IoT)

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

1.1 Το Διαδίκτυο των Πραγμάτων

Το Διαδίκτυο των Πραγμάτων είναι μια έννοια που αφορά ένα δίκτυο αντικειμένων, συσκευών, οχημάτων, κτιρίων αλλά και άλλων αντικειμένων τα οποία περιέχουν ενσωματωμένα ηλεκτρονικά συστήματα, λογισμικά, αισθητήρες για την συλλογή δεδομένων και την ανάληψη κάποιας δράσης σε αυτά μέσα σε ένα δίκτυο. Το Διαδίκτυο των Πραγμάτων δίνει την δυνατότητα στα αντικείμενα αυτά να ελέγχονται απομακρυσμένα μέσω της υπάρχουσας δικτυακής υποδομής δημιουργώντας έτσι ευκαιρίες άμεσης ενσωμάτωσης του φυσικού κόσμου με τα υπολογιστικά συστήματα έχοντας σαν αποτέλεσμα την βελτίωση της αποτελεσματικότητας και της ακρίβειας αλλά και την μείωση κόστους. Κάθε αντικείμενο αναγνωρίζεται ξεχωριστά από το ενσωματωμένο σύστημα και μπορεί να λειτουργεί τόσο αυτόνομα όσο και σε συνεργασία με την υπόλοιπη διαδικτυακή υποδομή. Με απλά λόγια το Διαδίκτυο των Πραγμάτων είναι το τεχνολογικό μέλλον που θα κάνει την καθημερινότητα του ανθρώπου πιο εύκολη [4].

Το Διαδίκτυο των Πραγμάτων εξελίχθηκε με την γρήγορη διάδοση του ασύρματου Internet και των ενσωματωμένων αισθητήρων και έτσι οι άνθρωποι άρχισαν να αντιλαμβάνονται ότι η τεχνολογία θα μπορούσε να είναι επαγγελματικό εργαλείο αλλά και προσωπικό. Ο όρος “Internet of Things” (ή αλλιώς Διαδίκτυο των Πραγμάτων) επινοήθηκε στα τέλη της δεκαετίας του 1990 από τον επιχειρηματία Kevin Ashton. Ο Ashton ο οποίος είναι ένας από τους ιδρυτές του Auto-ID Center στο MIT (Massachusetts Institute of Technology), ήταν μέλος μιας ομάδας που ανακάλυψε τον τρόπο να συνδέσει τα αντικείμενα με το διαδίκτυο μέσω μιας ετικέτας RFID (Radio Frequency Identification). Έχει δηλώσει ότι χρησιμοποίησε πρώτη φορά την φράση “Internet of Things” σε μια παρουσίαση που έκανε το 1999 και ο όρος αυτός έχει παραμείνει από τότε.

Στις συζητήσεις γύρω από το IoT, έχει αναγνωριστεί από την αρχή ότι οι τεχνολογίες analytics είναι ζωτικής σημασίας για την μετατροπή αυτής της «πλημμύρας» streaming data σε κατατοπιστική και χρήσιμη γνώση. Στην παραδοσιακή ανάλυση, τα δεδομένα αποθηκεύονται και μετά αναλύονται. Ωστόσο στην περίπτωση των δεδομένων συνεχούς ροής (streaming data) όπως αυτά του IoT, τα μοντέλα και οι αλγόριθμοι είναι αυτοί που αποθηκεύονται και τα δεδομένα περνούν μέσα από αυτά για ανάλυση. Αυτό το είδος της ανάλυσης καθιστά δυνατό τον εντοπισμό και την εξέταση μοτίβων καθώς τα δεδομένα δημιουργούνται σε πραγματικό χρόνο. Έτσι πριν αποθηκευτούν τα δεδομένα στο cloud ή σε οποιοδήποτε άλλο χώρο αποθήκευσης υπόκειται σε επεξεργασία. Έπειτα, χρησιμοποιούνται analytics ώστε να αποκρυπτογραφηθούν τα δεδομένα, ενώ όλες οι συσκευές θα συνεχίσουν να εκπέμπουν και να λαμβάνουν δεδομένα.

Με τεχνικές advanced analytics, τα data stream analytics μπορούν να πάνε πέρα από την απλή παρακολούθηση των υπάρχων συνθηκών και την αξιολόγηση των κατώτατων ορίων στην πρόβλεψη μελλοντικών σεναρίων και στην εξέταση πολύπλοκων ερωτημάτων. Για να

εκτιμηθεί το μέλλον με την χρήση αυτών των ροών δεδομένων (data streams), θα πρέπει να υπάρχουν διαθέσιμες τεχνολογίες υψηλής απόδοσης που μπορούν να προσδιορίζουν μοτίβα στα δεδομένα της χρονικής στιγμής που αυτά δημιουργούνται. Μόλις ένα μοτίβο αναγνωρίζεται, μετρήσεις ενσωματωμένες στη ροή δεδομένων, οδηγούν στην αυτόματη προσαρμογή των συνδεδεμένων συστημάτων ή δημιουργούν ειδοποιήσεις για άμεσες δράσεις και λήψη καλύτερων αποφάσεων.

Επομένως, αυτό σημαίνει ότι μπορεί να προχωρήσει πέρα από την απλή παρακολούθηση συνθηκών και ορίων στην εκτίμηση πιθανών μελλοντικών γεγονότων και στον προγραμματισμό τους για αμέτρητα πολύπλοκα σενάρια. Υπάρχουν πολλά πράγματα που είναι συνδεδεμένα με το Διαδίκτυο και τα οικονομικά οφέλη που μπορεί να αποκομισθούν από την ανάλυση των data streams είναι αρκετά μεγάλα. Μερικά παραδείγματα των επιπτώσεων του Διαδικτύου των Πραγμάτων είναι τα παρακάτω:

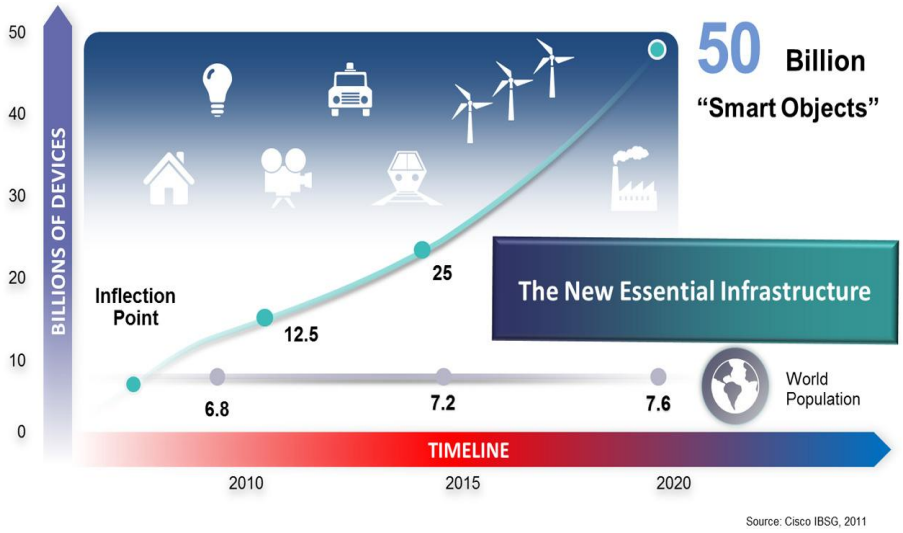
- Έξυπνες λύσεις μεταφοράς επιταχύνουν την ροή κυκλοφορίας, μειώνουν την κατανάλωση καυσίμων, δίνουν προτεραιότητα στα προγράμματα επισκευής οχημάτων και σώζουν ζωές.

- Έξυπνα ηλεκτρικά δίκτυα (smart electric grids) συνδέουν πιο αποτελεσματικά ανανεώσιμες πηγές ενέργειας, βελτιώνουν την αξιοπιστία του συστήματος και χρεώνουν τους καταναλωτές με βάση μικρότερες προσαυξήσεις.

- Μηχανές αισθητήρων παρακολούθησης πραγματοποιούν διαγνώσεις και προβλέπουν θέματα συντήρησης που εκκρεμούν, βραχυπρόθεσμα stock-out αποθεμάτων καθώς επίσης θέτουν προτεραιότητες στα προγράμματα του προσωπικού που είναι υπεύθυνο για τις επισκευές για να καλύψουν αποτελεσματικότερα τις ανάγκες επισκευής εξοπλισμού αλλά και περιφερειακές ανάγκες.

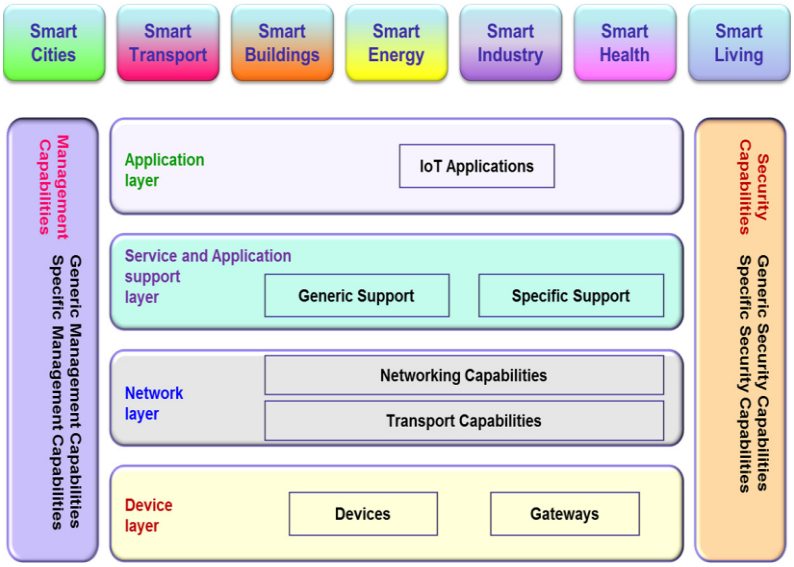
- Data-driven συστήματα, βασιζόμενα στις υποδομές των έξυπνων πόλεων (smart cities) καθιστούν ευκολότερο για τους δήμους των πόλεων να πραγματοποιούν διαδικασίες διαχείρισης αποθεμάτων, την επιβολή του νόμου και άλλα προγράμματα πιο αποτελεσματικά.

Το Διαδίκτυο των Πραγμάτων εξελίσσεται κάθε μέρα όλο και περισσότερο. Προσφέρει νέα αξία στις ζωές των καταναλωτών, πλεονεκτήματα και υπηρεσίες που καλύπτουν τις ανάγκες και τις επιθυμίες τους [4].



Εικόνα 1: Διαδικτυακές συσκευές & μελλοντική εξέλιξη (Πηγή: Cisco 2011)

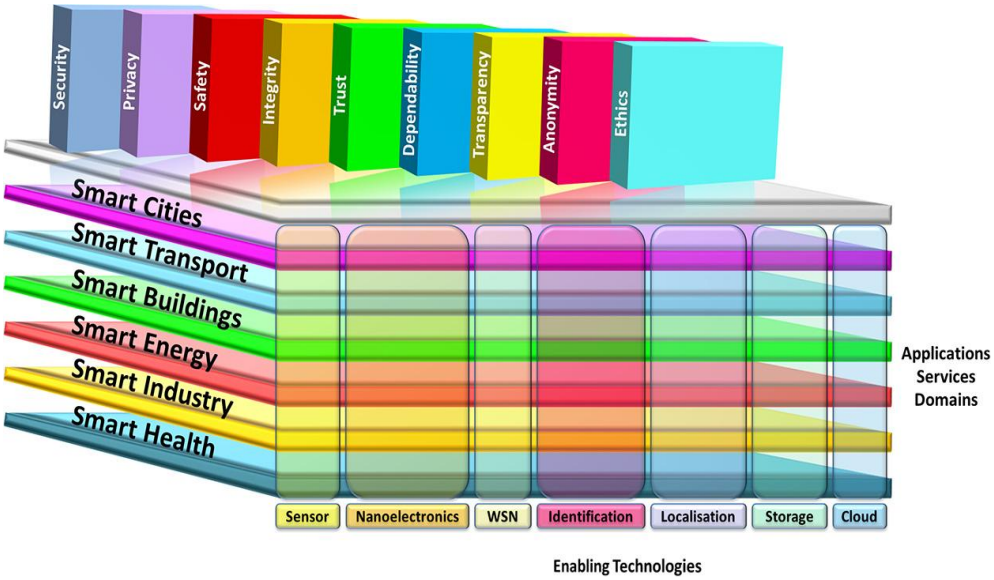
Όπως φαίνεται στην εικόνα 1, το IoT είναι η νέα βασική υποδομή που προβλέπεται να συνδέσει 50 δισεκατομμύρια έξυπνα αντικείμενα (smart objectives) έως το 2020, όταν ο παγκόσμιος πληθυσμός θα φθάσει τα 7,6 δισεκατομμύρια. Όπως πρότεινε η ITU (International Telecommunication Union), αυτή η βασική υποδομή θα οικοδομηθεί γύρω από μια πολύ- επίπεδη αρχιτεκτονική όπου τα έξυπνα αντικείμενα θα χρησιμοποιούνται για την παροχή διαφορετικών υπηρεσιών μέσω των τεσσάρων κύριων στρωμάτων όπως απεικονίζονται παρακάτω στην εικόνα 2.



Εικόνα 2: Αρχιτεκτονική Στρωμάτων IoT (Πηγή: ITU-T)

Στην εικόνα 2 απεικονίζεται ένα στρώμα συσκευής, ένα στρώμα δικτύου, ένα στρώμα υποστήριξης και το στρώμα εφαρμογής. Στο επίπεδο της διάταξης του στρώματος της συσκευής (αισθητήρες, συσκευές RFID) οι πύλες χρησιμοποιούνται για συλλογή μετρήσεων των αισθητήρων για περαιτέρω επεξεργασία. Το στρώμα δικτύου παρέχει τις απαραίτητες δυνατότητες μεταφοράς και δικτύωσης για δρομολόγηση και για επεξεργασία δεδομένων IoT. Το στρώμα υποστήριξης είναι ένα στρώμα middleware δηλαδή ένα ενδιάμεσο επίπεδο

μεταξύ εξυπηρετούμενων και άλλων επιπέδων του συστήματος, όπου λειτουργεί ως πλατφόρμα για διασυστημική λειτουργία και υψηλού επιπέδου application logic καθώς χρησιμεύει για να κρύψει την πολυπλοκότητα των κατώτερων στρωμάτων στο στρώμα εφαρμογής και να παρέχει ειδικές και γενικές υπηρεσίες όπως αποθήκευση σε διάφορες μορφές (συστήματα διαχείρισης βάσεων δεδομένων) και πολλές άλλες υπηρεσίες.



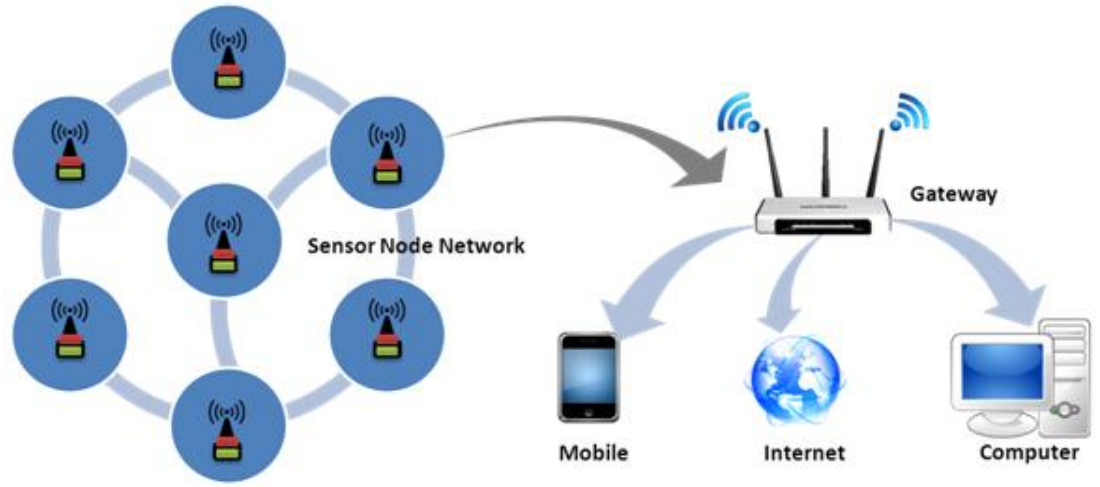
Εικόνα 3: IoT-3Dimentional View

Όπως δείχνει η εικόνα 3, το IoT μπορεί να θεωρηθεί ως μια υποδομή που οδηγεί σε πολλές εφαρμογές υπηρεσιών καθώς επιτρέπονται από μια σειρά τεχνολογιών. Οι υπηρεσίες εφαρμογών επεκτείνονται σε πολλούς τομείς όπως είναι οι έξυπνες πόλεις, οι έξυπνες μεταφορές, τα έξυπνα κτίρια, η έξυπνη ενέργεια, η έξυπνη βιομηχανία και η έξυπνη υγεία ενώ διατίθενται διάφορες τεχνολογίες όπως είναι η ανίχνευση, η νάνο-ηλεκτρονική, τα ασύρματα δίκτυα αισθητήρων (WSNs), RFID-ταυτοποίηση μέσω ραδιοσυχνοτήτων (Radio frequency Identification) και η αποθήκευση. Το επόμενο βήμα αυτής της τεχνολογικής επανάστασης είναι η σύνδεση των αντικειμένων σε ένα δίκτυο επικοινωνίας όπου αυτό το όραμα βασίζεται στο Διαδίκτυο των Πραγμάτων. Αυτό διευκολύνεται με την χρήση των Ασύρματων Δικτύων Αισθητήρων για την επέκταση των δυνατοτήτων επικοινωνίας και παρακολούθησης καθώς είναι πρώιμη μορφή πανταχού παρόντων δικτύων πληροφόρησης και επικοινωνίας. Είναι ένα από τα δομικά στοιχεία του Διαδικτύου των πραγμάτων.

1.2 Ασύρματα Δίκτυα Αισθητήρων (WSNs)

Ένα ασύρματο δίκτυο αισθητήρων αποτελείται από έναν μεγάλο αριθμό κόμβων αισθητήρων, οι οποίοι αναπτύσσονται είτε μέσα στο φαινόμενο ή πολύ κοντά σε αυτό. Η θέση των κόμβων δεν είναι πάντα προκαθορισμένη, υπάρχει όμως η απαίτηση το δίκτυο να αυτοσυντηρείται και να λειτουργεί για μεγάλα χρονικά διαστήματα χωρίς την ανθρώπινη παρέμβαση με ενέργεια από συσσωρευτές η άλλες αυτόνομες πηγές. Οι ιδιαιτερότητες αυτές των ασύρματων δικτύων αισθητήρων και η διαφοροποίησή τους από τα κλασικά δίκτυα υπολογιστών οδηγούν σε νέες προκλήσεις και αντικείμενα έρευνας με σκοπό την βελτιστοποίηση της απόδοσής τους [4].

Οι ενεργειακά αυτόνομοι κόμβοι «αισθάνονται», παρατηρούν φυσικά μεγέθη (θερμοκρασία, υγρασία, πίεση, κίνηση, εικόνα ήχο κ.τ.λ.) και μεταδίδουν την επεξεργασμένη (ή και όχι) μέτρησή τους, με τελική κατεύθυνση έναν σταθμό βάσης (base station). Η επικοινωνία των κόμβων είναι αμφίδρομη, δηλαδή όπως μεταδίδουν πληροφορίες στον σταθμό βάσης κάλλιστα μπορούν να δεχτούν πληροφορίες από αυτόν.



Εικόνα 4: Ασύρματο Δίκτυο Αισθητήρων (Πηγή: NS2 Projects)

Οι κόμβοι αισθητήρων είναι ουσιαστικά μικροί υπολογιστές με εξαιρετικά βασική λειτουργικότητα. Αποτελούνται από μια μονάδα επεξεργασίας με περιορισμένη υπολογιστική ισχύ και περιορισμένη μνήμη. Περιέχουν συσκευή ραδιοεπικοινωνίας (radio communication device), πηγή ενέργειας (μπαταρία) και έναν ή περισσότερους αισθητήρες. Η ενσωμάτωση αυτών των μικρών ηλεκτρικών συσκευών σε ποικίλα σενάρια εξασφαλίζει ένα ευρύ φάσμα εφαρμογών. Σε μία τυπική εφαρμογή ένα WSN όπου είναι διασκορπισμένο σε μια περιοχή προορίζεται να συλλέγει δεδομένα από τους κόμβους αισθητήρων [14].

Οι ασύρματοι κόμβοι αισθητήρων (βλέπε εικόνα 5) αποτελούνται από πέντε βασικά δομικά στοιχεία όπως φαίνεται παρακάτω:

1. **Επεξεργαστής (Processor):** Ο επεξεργαστής αποτελεί το κεντρικό δομικό στοιχείο κάθε “έξυπνης συσκευής” και είναι υπεύθυνος για τον συγχρονισμό και την εκτέλεση όλων των λειτουργιών του συστήματος. Μέσω αυτού οι συσκευές επεξεργάζονται, στέλνουν ή παραλαμβάνουν πληροφορίες. Ο επεξεργαστής μπορεί να “τρέξει” με διαφορετικές λειτουργίες όπως για παράδειγμα η λειτουργία κατάστασης ύπνωσης (sleep mode) όπου σε αυτήν την λειτουργία ο επεξεργαστής κατά το μεγαλύτερο μέρος του χρόνου παραμένει αδρανής για καλύτερη εξοικονόμηση ενέργειας. Επανέρχεται στην κατάσταση “on” όταν αποστέλλονται ή ανιχνεύονται δεδομένα από άλλους αισθητήρες.

2. **Πηγή Ενέργειας (Power Source):** Το κάθε δομικό στοιχείο του κόμβου χρειάζεται ενέργεια η οποία παρέχεται από μπαταρίες. Σε κάποιες εφαρμογές είναι δυνατόν να παρέχεται ενέργεια στην συσκευή με διάφορους μεθόδους - από τις συμβατικές μπαταρίες, την εκμετάλλευση της ηλιακής ενέργειας, τη διαφορά θερμοκρασίας, τις

δονήσεις της συσκευής και γενικά με οποιονδήποτε τρόπο μπορούμε να μετατρέψουμε ενέργεια από τον περιβάλλον σε ηλεκτρική μορφή. Οι κόμβοι αισθητήρων συνήθως διαθέτουν μικρή αποθήκευση ενέργειας, επομένως τα πρωτόκολλα δικτύωσης δίνουν έμφαση στην χαμηλή κατανάλωση ισχύος.

3. **Μνήμη (External Memory):** Συνήθως χρησιμοποιείται FLASH memory. Σε αρκετούς κόμβους γίνεται διαχωρισμός της περιοχής της μνήμης σε περιοχή όπου αποθηκεύονται προγράμματα και εφαρμογές του χρήστη και στην άλλη περιοχή αποθηκεύονται δεδομένα για την ομαλή λειτουργία του κόμβου (πχ. λειτουργικό σύστημα).

4. **Radio:** Οι συσκευές των ασύρματων δικτύων περιλαμβάνουν μία ασύρματη μικρής εμβέλειας επικοινωνία. Οι τυπικές τιμές είναι 10-100 Kbps (kilo bits per second) και η εμβέλεια είναι μικρότερη από 100 μέτρα. Η ράδιο-επικοινωνία είναι συχνά η πιο απαιτητική ενέργεια και γι' αυτό τον λόγο ενσωματώνονται ενεργειακά αποδοτικές λειτουργίες όπως για παράδειγμα η λειτουργία ύπνωσης (sleep mode) και αφύπνισης (wake-up mode).

5. **Αναλογικές/Ψηφιακές είσοδοι Αισθητήρες:** Αρκετές συσκευές έχουν ενσωματωμένους συγκεκριμένους αισθητήρες. Άλλες συσκευές πιο γενικού σκοπού έχουν αναλογικές (ή και ψηφιακές) εισόδους στις οποίες ο σχεδιαστής μπορεί να εφαρμόσει αναλογικούς ή και ψηφιακούς αισθητήρες και με κατάλληλες τροποποιήσεις στο λογισμικό (software) να μπορεί να συλλέξει πληροφορίες από το περιβάλλον.

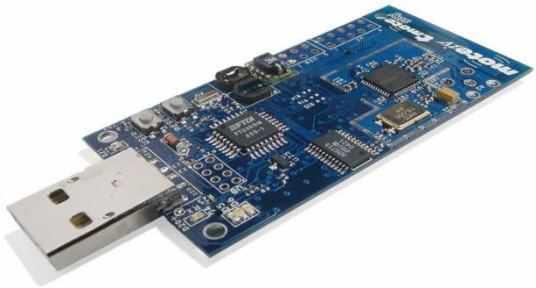
Ακολουθεί μια σύντομη περιγραφή των τεχνικών χαρακτηριστικών Ασύρματων Δικτύων Αισθητήρων που καθιστούν την τεχνολογία τους πολύ ελκυστική [7].

1. **Αυτόνομη και Προγραμματιζόμενη λειτουργία:** Ο κάθε κόμβος έχει την δυνατότητα να λειτουργήσει αυτόνομα, δηλαδή να ξέρει τι να κάνει (να παρέχει μετρήσεις), πότε να το κάνει (συχνότητα δειγματοληψίας), που θα στείλει την μέτρηση (πχ broadcasting σε όλους όσους είναι στην εμβέλεια του). Ταυτόχρονα έχει την δυνατότητα να προγραμματίζεται δυναμικά για παράδειγμα ο σταθμός βάσης να διαδώσει καινούργια δεδομένα λειτουργίας σε κάθε κόμβο με αποτέλεσμα τον δυναμικό επαναπρογραμματισμό του δικτύου.

2. **Χαμηλή Κατανάλωση:** Οι κόμβοι μπορεί να εγκατασταθούν σε απομακρυσμένες τοποθεσίες όπου δεν υπάρχουν διαθέσιμες πήγες ενέργειας. Τροφοδοτούνται συνήθως με μπαταρίες οι όποιες μετά από κάποιο χρονικό διάστημα θα αδειάσουν και αυτό έχει σαν αποτέλεσμα μετά από αυτό το χρονικό διάστημα το δίκτυο να αποκοπεί και να είναι πλέον άχρηστο. Επομένως για να λειτουργήσουν αρκετό χρονικό διάστημα οι κόμβοι χρησιμοποιούν χαμηλή ενεργειακή κατανάλωση (sleep mode) έτσι ώστε να μειώνεται το κόστος συντήρησης και να μεγαλώνει ο χρόνος διάρκειας ζωής τους. Σε αρκετά δίκτυα χρησιμοποιούνται ανανεώσιμες πηγές ενέργειας (πχ ηλιακή ενέργεια) όπου βέβαια μια τέτοια υλοποίηση εξαρτάται από την τοποθεσία και τις απαιτήσεις του κάθε δικτύου ξεχωριστά.

3. **Γρήγορη δημιουργία δικτύου:** Τα περισσότερα δίκτυα έχουν την δυνατότητα μέσα σε μερικά λεπτά να έχουν χαρτογραφήσει το δίκτυό τους και να ξεκινήσουν την προγραμματιζόμενη λειτουργία τους. Βέβαια αυτό είναι σχετικό διότι εξαρτάται αρκετά και από το μέγεθος του δικτύου και σίγουρα από το software/hardware των κόμβων.

4. **Προσαρμοστικότητα:** Βασικό χαρακτηριστικό τέτοιου είδους δικτύου είναι η ικανότητά τους να προσαρμόζονται στα νέα δεδομένα του δικτύου. Για παράδειγμα ένα κάποιοι κόμβοι σβήσουν τότε το δίκτυο θα δημιουργήσει νέα μονοπάτια δρομολόγησης.

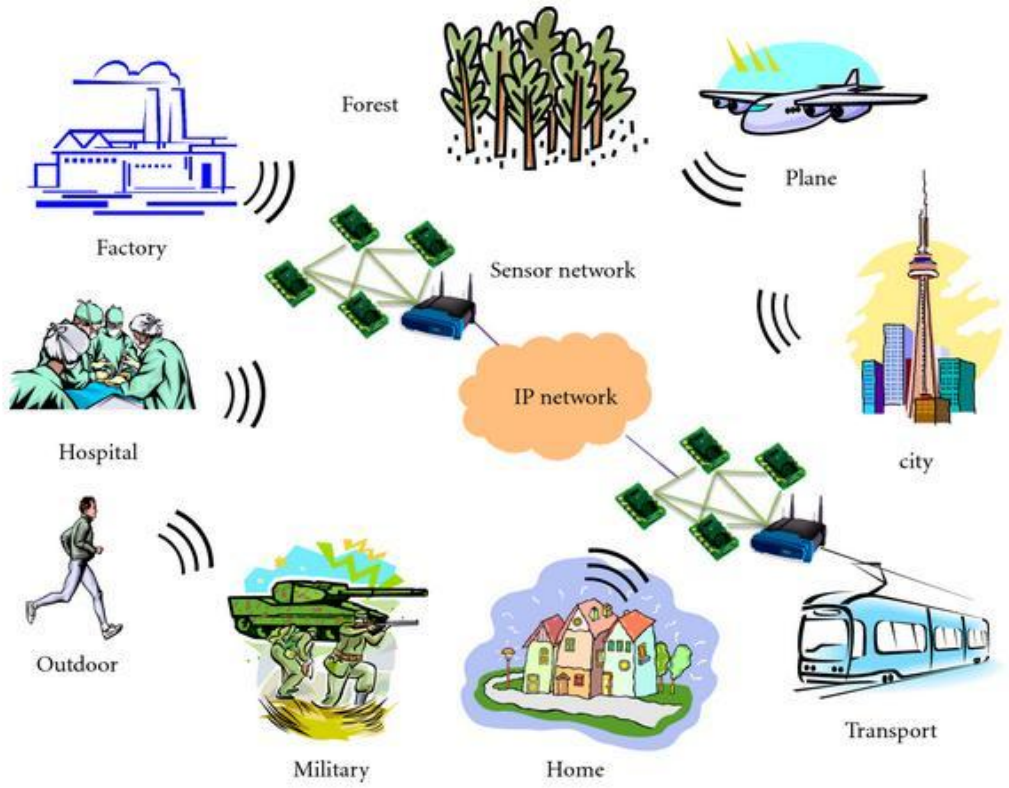


Εικόνα 5: Συσκευή Mote TelosB (Πηγή: Advanticsys)

1.3 Εφαρμογές Ασύρματων Δικτύων Αισθητήρων

Τα Ασύρματα Δίκτυα Αισθητήρων εφαρμόστηκαν αρχικά για τη «συλλογή δεδομένων» από περιβάλλοντα όπου ήταν δύσκολο να υφίσταται ανθρώπινη παρουσία και έπειτα χρησιμοποιήθηκαν για τον εντοπισμό συμβάντων ή θέσεων, όπως κινούμενων αντικειμένων ή σεισμικών δραστηριοτήτων [12]. Μεγάλη κινητικότητα παρατηρείται στην σημερινή εποχή γύρω από τις εφαρμογές των ασύρματων δικτύων αισθητήρων, λόγω των πλεονεκτημάτων που παρέχουν και των χαρακτηριστικών τους που τα κάνουν κατάλληλα για χρήση σε όλο και περισσότερους τομείς, όπου τα κλασσικά δίκτυα δεν μπορούν να ανταποκριθούν. Η σημασία και η χρησιμότητα των Ασύρματων Δικτύων Αισθητήρων φαίνεται από το τεράστιο φάσμα των τομέων στους οποίους μπορούν να εφαρμοστούν [14]. Όπως παρουσιάζονται και παρακάτω στην εικόνα 6, οι τομείς αυτοί είναι:

- Περιβαλλοντικές Εφαρμογές
- Οικιακοί Αυτοματισμοί
- Υγειονομικοί Περίθαλψη
- Βιομηχανικές Εφαρμογές
- Έλεγχος Μεταφορών και Συγκοινωνιών
- Στρατιωτικές Εφαρμογές



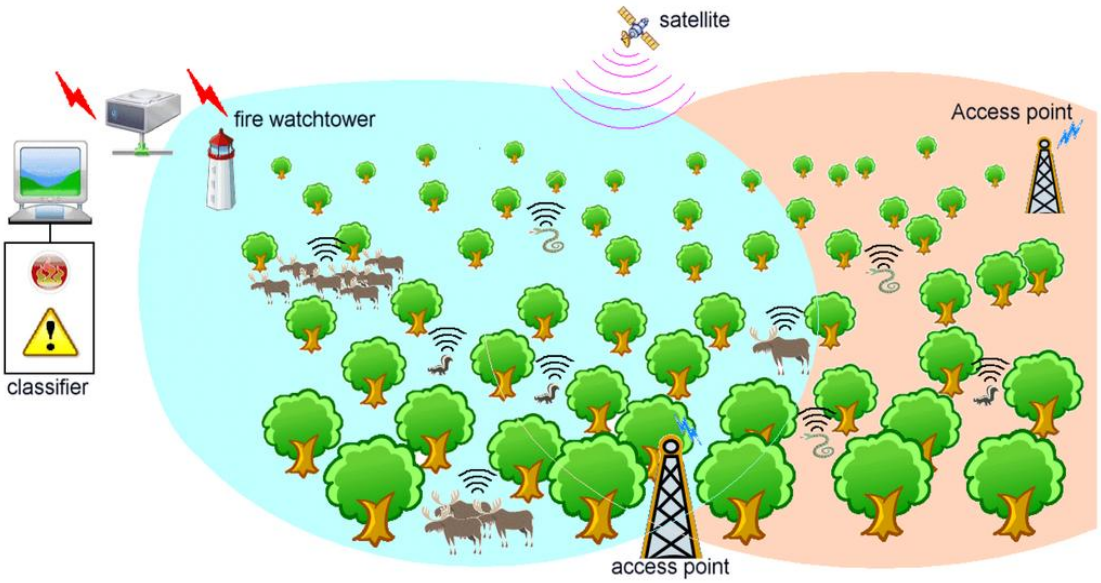
Εικόνα 6: Εφαρμογές Ασύρματων Δικτύων Αισθητήρων (Πηγή: ResearchGate)

1.3.1 Τομέας Περιβαλλοντικών Εφαρμογών

Η επίβλεψη και η ανίχνευση των περιβαλλοντικών συνθηκών γίνεται με την καταγραφή της εξέλιξης ενός οικοσυστήματος. Αυτό είναι δυνατό μέσω των ασύρματων δικτύων αισθητήρων, αφού μπορούν να επιβλέψουν ένα οικοσύστημα, να καταγράψουν τη βιοποικιλότητα, τη σύσταση του εδάφους, να κάνουν γεωφυσική μελέτη κ.ά. Υπάρχουν, συνεπώς, διάφορες εφαρμογές που σχετίζονται με το περιβάλλον και ανάλογα με την εφαρμογή διαφοροποιείται και ο τύπος του αισθητήρα που χρησιμοποιείται. Μερικές περιβαλλοντολογικές εφαρμογές των δικτύων αισθητήρων περιλαμβάνουν την παρακολούθηση των κινήσεων των πουλιών, μικρών ζώων, την παρακολούθηση περιβαλλοντολογικών συνθηκών που επηρεάζουν την χλωρίδα και την πανίδα, την εντολή σειράς ενεργειών για παρακολούθηση μεγάλης κλίμακας της γης και την εξερεύνηση του πλανήτη, την χημική βιολογική ανίχνευση, την ακριβή γεωργία καθώς και την βιολογική παρακολούθηση της θάλασσας, του εδάφους και του αέρα, την μετεωρολογική και γεωφυσική έρευνα, την μελέτη μολύνσεων και την παρακολούθηση πυρκαγιών στα δάση.

Για εφαρμογές μετεωρολογικής έρευνας και μελέτης της ρύπανσης, χρησιμοποιούνται αισθητήρες βροχόπτωσης, στάθμης νερού και αισθητήρες μέτρησης φυσικών παραμέτρων, όπως θερμοκρασία, ατμοσφαιρική πίεση, υγρασία και άλλες [14]. Στις περιβαλλοντολογικές εφαρμογές κυρίαρχο ρόλο διακατέχει η χρήση ειδικών προστατευτικών θηκών που βοηθούν στην τοποθέτηση των αισθητήρων σε ακραία και επικίνδυνα περιβάλλοντα όπου δεν θα

μπορούσε να βρεθεί ο άνθρωπος. Εξαιτίας του γεγονότος ότι οι κόμβοι των ασύρματων δικτύων μπορούν να καλύπτουν μεγάλες περιοχές και να εκτείνονται σε μεγάλος εύρος που είναι δύσβατες για τον άνθρωπο αλλά και για τα μέσα που χρησιμοποιεί για την πυρόσβεση, ενεργεί για την πρόσληψη και την άμεση ειδοποίηση των αρμόδιων αρχών.



Εικόνα 7: Υποδομή Συστημάτων Ανίχνευσης Πυρκαγιάς (Πηγή: dhsprojects)

1.3.2 Τομέας Οικιακών Αυτοματισμών

Ο σύγχρονος τρόπος ζωής δημιουργεί διαρκώς νέες ανάγκες, που απαιτούν την "έξυπνη διαχείρισή" τους. Άνεση, ασφάλεια, ενεργειακή διαχείριση, συστήματα ελέγχου εισόδου, διαχείριση περιεχομένων multimedia, έλεγχος και επίβλεψη από απόσταση είναι μερικές από τις βασικές ανάγκες. Στους οικιακούς αυτοματισμούς εντάσσονται οι "ευφυής μετρητές" όπου μπορούν να διαχειριστούν και να ελέγξουν έξυπνες οικιακές συσκευές. Οι αισθητήριοι κόμβοι ή αλλιώς έξυπνοι μετρητές μπορούν να παρέχουν πληροφορίες σχετικά με την ενεργειακή κατανάλωση των πελατών. Ο πάροχος έχει άμεση ενημέρωση της κατανάλωσης επομένως οι λογαριασμοί δεν είναι κατ' εκτίμηση και οι πελάτες έχουν μια γενική εικόνα της διαχείρισης της κατανάλωσής τους. Ο καταναλωτής ενημερωμένος από τις πληροφορίες του έξυπνου μετρητή μπορεί να επιλέξει να κάνει την διαχείριση αυτών των συσκευών με δική του πρωτοβουλία. Υπάρχουν αρκετά σύγχρονες ηλεκτρονικές συσκευές οι οποίες μπορεί να μετατρέψουν το σπίτι σε έξυπνο (smart) [14].

Εικόνα 8: Έλεγχος Έξυπνου Σπιτιού (Πηγή: consumers choice award)

1.3.3 Τομέας Εφαρμογών Υγείας και Περίθαλψης

Στον τομέα της υγείας και της περίθαλψης ένα ασύρματο δίκτυο αισθητήρων μπορεί να αναπτυχθεί με χαμηλό κόστος πάνω σε υπάρχοντες δομές. Τα δεδομένα συλλέγονται αυτόματα, επιτρέποντας καθημερινή φροντίδα και διαμήκη ιατρική παρακολούθηση και διάγνωση. Επίσης στον τομέα της Ιατρικής δεν χρησιμοποιείται ο όρος Wireless Sensor Network αλλά ο όρος Body Sensor Area Network (BSN) και αυτό συμβαίνει όχι μόνο λόγω της κατηγορίας των εφαρμογών αλλά επειδή υπάρχουν κάποιες διαφοροποιήσεις στα δίκτυα που σχετίζονται με τον τρόπο συγκρότησης τους.

Ένα τυπικό Body Sensor Area Network (BSN) αποτελείται από ένα αριθμό μικρών, οικονομικών, αισθητήρων όπου μπορούν είτε να φορεθούν είτε να εμφυτευθούν στο ανθρώπινο σώμα και να παρακολουθούν ζωτικές παραμέτρους του σώματος καθώς και κινήσεις. Τα δεδομένα που συγκεντρώνονται από το δίκτυο αισθητήρων μπορούν να αποθηκευτούν για ένα μεγάλο χρονικό διάστημα και μπορούν να χρησιμοποιηθούν για ιατρική έρευνα.

Εικόνα 9 : Εφαρμογές WSNs στον Τομέα της Υγείας (Πηγή: smart-labex)

1.3.4 Τομέας Βιομηχανικών Εφαρμογών

Στην Βιομηχανία τα ασύρματα δίκτυα αισθητήρων σε συνδυασμό με συστήματα ελέγχου μπορούν να εποπτεύουν όλη την γραμμή παραγωγής για την ορθή λειτουργία της καθώς και την ασφάλεια του προσωπικού. Το περιβάλλον στο οποίο βρίσκουν εφαρμογή μπορεί να είναι επικίνδυνο για τον άνθρωπο ή ακόμα να είναι αδύνατο να πάει. Υπάρχουν πολλά παραδείγματα βιομηχανικών εφαρμογών όπου σχετίζονται με δυσπρόσιτες παραγωγικές περιοχές όπου είναι δύσκολες για τον άνθρωπο όπως ο έλεγχος στο εσωτερικό των μηχανών και σε υπόγειες παραγωγικές διαδικασίες όπου είναι αρκετά επικίνδυνες και δύσκολες στον χειρισμό. Μερικές τέτοιες εφαρμογές μπορεί να είναι σε διυλιστήρια για την καταγραφή θερμότητας σε διάφορα στάδια της διεργασίας, όπου ο έλεγχος της παραγωγής γίνεται με την εκπομπή ειδικών σημάτων συναγερμών όταν η θερμοκρασία είναι εκτός επιθυμητού επιπέδου και υπάρχει κίνδυνος, καθώς και σε γεωτρήσεις για την μέτρηση των μη φυσιολογικών δονήσεων και την προειδοποίηση των μηχανών σε πιθανή επερχόμενη βλάβη του εξοπλισμού. Επίσης μια πολύ σημαντική εφαρμογή είναι ο έλεγχος των διάφορων υπόγειων αγωγών είτε πρόκειται για αποχετευτικούς είτε για υδρευτικούς.

1.3.5 Τομέας Συγκοινωνιών και Έλεγχος Μεταφορών

Στον τομέα των μεταφορών και των συγκοινωνιών τα δίκτυα αισθητήρων αποτελούν δυναμική παρουσία με έντονες αναπτυξιακές διαστάσεις που συνδυάζουν τις τεχνολογίες πληροφορικής και επικοινωνιών, παρέχοντας υψηλή προστιθέμενη αξία στους χρήστες των μεταφορικών μέσων και καθιστώντας τις μεταφορές στο σύνολο τους πιο ασφαλείς, αποτελεσματικές και φιλικές προς το περιβάλλον. Καθώς τα σύγχρονα μεταφορικά συστήματα εμφανίζουν σημαντικές απαιτήσεις ως προς την ασφάλεια, την οικονομία και την αποτελεσματικότητα στοχεύουν στην παροχή καινοτόμων υπηρεσιών που σχετίζονται με

τους διάφορους τρόπους μεταφοράς, όπως πχ την επιβολή των κανόνων και την διαχείριση της κυκλοφορίας καθώς και ελαχιστοποιούν τους κινδύνους ατυχημάτων, ενώ ταυτόχρονα επιτρέπουν στους χρήστες να ενημερώνονται καλύτερα και να κάνουν ασφαλέστερη και εξυπνότερη χρήση των μεταφορικών δικτύων και των διαθέσιμων πόρων.

Εικόνα 10 : Smart Transport (Πηγή: utexas edu)

1.3.6 Τομέας Στρατιωτικών Εφαρμογών

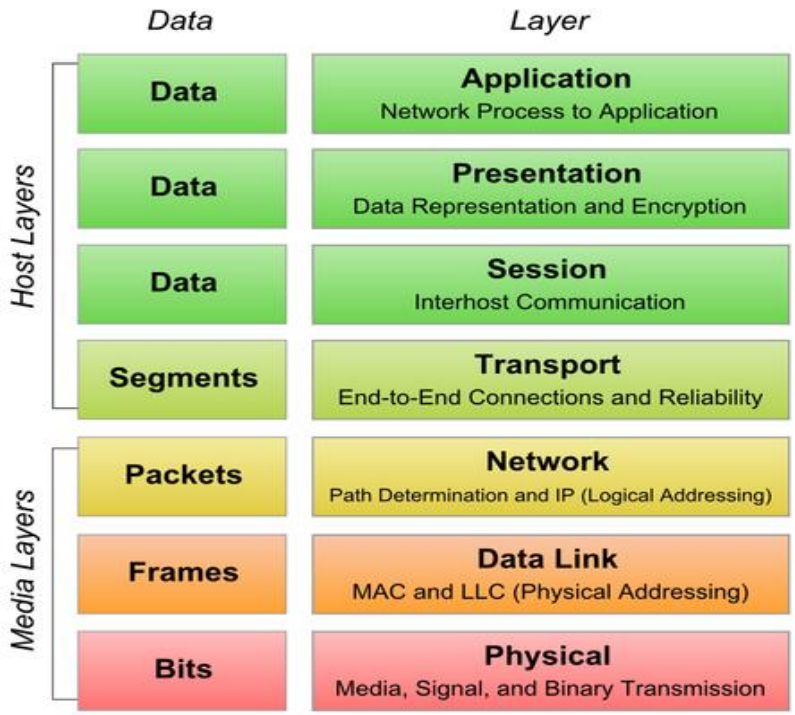
Τα ασύρματα δίκτυα αισθητήρων μπορούν να χρησιμοποιηθούν από τον στρατό για πολλούς σκοπούς, όπως η παρακολούθηση στρατιωτικής δραστηριότητας σε απομονωμένες περιοχές και η προστασία στρατιωτικών δυνάμεων. Καθώς τα δίκτυα αισθητήρων βασίζονται στην πυκνή χωρική εγκατάσταση η καταστροφή μερικών κόμβων από εχθρικές δυνάμεις δεν επηρεάζει μια στρατιωτική επιχείρηση σε τέτοιο βαθμό όσο η καταστροφή των παραδοσιακών αισθητήρων, κάνοντας την χρήση των δικτύων αισθητήρων ιδανική για τα πεδία των μαχών. Κάποιες από τις στρατιωτικές εφαρμογές είναι η παρακολούθηση των φιλικών δυνάμεων του εξοπλισμού και των πυρομαχικών τους καθώς και η αναγνώριση εχθρικών δυνάμεων και η αποτίμηση των ζημιών της μάχης.

ΚΕΦΑΛΑΙΟ 2

Τεχνολογίες και Τοπολογίες Δικτύων Αισθητήρων

2.1 Αρχιτεκτονική Ασύρματων Δικτύων Αισθητήρων

Η αρχιτεκτονική ενός ασύρματου δικτύου αισθητήρων βασίζεται στο μοντέλο αναφοράς OSI (μοντέλο αναφοράς ανοικτής διασύνδεσης συστημάτων – Open Systems Interconnection), επειδή αφορά ανοικτά συστήματα , δηλαδή συστήματα ανοικτά στην επικοινωνία με άλλα συστήματα. Το μοντέλο OSI αναπτύχθηκε μετά από πρόταση του Διεθνούς Οργανισμού Τυποποίησης (International Standards Organization) με στόχο την διεθνή τυποποίηση των πρωτοκόλλων που χρησιμοποιούνται στα επίπεδα σχεδίασης των δικτύων. Το μοντέλο αυτό έχει επτά στρώματα καθένα από τα οποία εκτελεί συγκεκριμένες λειτουργίες και επικοινωνεί με τα επίπεδα που είναι ακριβώς από πάνω του και από κάτω του. Τα ανώτερα επίπεδα ασχολούνται κυρίως με τις υπηρεσίες, εφαρμογές και δραστηριότητες χρηστών και τα κατώτερα στρώματα ασχολούνται κυρίως με την καθεαυτού μετάδοση δεδομένων [14].



Εικόνα 11 : Μοντέλο OSI (Πηγή: Tech-Faq)

Όπως φαίνεται από την εικόνα 11 οι λειτουργίες των τριών χαμηλότερων επιπέδων (Φυσικό, Σύνδεσης δεδομένων και Δικτύου) διενεργούν τον έλεγχο της μετάδοσης μηνυμάτων μέσα στο δίκτυο, ενώ οι λειτουργίες των υπόλοιπων ανώτερων επιπέδων (Μεταφοράς, Συνόδου, Παρουσίασης και Εφαρμογής) παρέχουν την αξιόπιστη μεταβίβαση της πληροφορίας από άκρο σε άκρο. Η λειτουργία ενός ασύρματου δικτύου καθορίζεται από τα πρωτόκολλα επικοινωνίας που εφαρμόζονται και αποτελούν την στοίβα πρωτοκόλλων (protocol stack).

Η εφαρμοζόμενη στοίβα πρωτοκόλλων επικοινωνίας πρέπει να είναι ενεργειακά αποδοτική και να υποστηρίζει την συνεργασία μεγάλου πλήθους κόμβων. Το μοντέλο OSI επηρέασε όχι

τόσο τον τρόπο με τον οποίο σχεδιάζουμε, αλλά πολύ περισσότερο τον τρόπο με τον οποίο κατανοούμε τα ασύρματα δίκτυα αισθητήρων.

2.2 Φυσικό Επίπεδο (Physical layer)

Το φυσικό επίπεδο μεταφέρει το bit stream μέσα στο δίκτυο σε επίπεδο ηλεκτρικό, οπτικό και ραδιοκυμάτων. Παρέχει τα μέσα hardware μέσω των οποίων στέλνονται και λαμβάνονται δεδομένα στο δίκτυο. Είναι υπεύθυνο για την επιλογή της συχνότητας, την παραγωγή συχνότητας μετάδοσης, την ανίχνευση σήματος, την διαμόρφωση του και για την κρυπτογράφηση των δεδομένων. Η διαμόρφωση και αποδιαμόρφωση του ψηφιακού σήματος εκτελείται από τον πομποδέκτη και δεν πρέπει να είναι ιδιαίτερα πολύπλοκη. Η ποιότητα του φυσικού επιπέδου σε ένα κόμβο εξαρτάται άμεσα από το κόστος και την κατανάλωση ενέργειας, γι’ αυτό και τα πρωτόκολλα σε αυτό το επίπεδο προσπαθούν να μειώσουν την κατανάλωση ενέργειας και το κόστος. Για την μετάδοση των σημάτων, ως επί το πλείστον χρησιμοποιούνται τεχνικές εξάπλωσης φάσματος, οι οποίες ονομάζονται έτσι επειδή το βασικό στοιχείο της λειτουργίας τους έγκειται στο γεγονός ότι οι εκπεμπόμενες κυματομορφές καταλαμβάνουν μεγαλύτερο εύρος ζώνης (bandwidth) από ότι πραγματικά χρειάζεται για την μετάδοση των δεδομένων [15].

Οι τεχνικές αυτές χρησιμοποιούνται για διάφορους λόγους και ο βασικότερος θεωρείται ότι είναι η μείωση των παρεμβολών από άλλα σήματα, καθώς το σήμα δεν μεταδίδεται σε μία μόνο συχνότητα. Άλλοι λόγοι για τους οποίους χρησιμοποιούνται τέτοιες τεχνικές είναι η ασφάλεια από υποκλοπές του σήματος, η αντίσταση στην εξασθένιση του σήματος, καθώς και η δυνατότητα χρήσης του μέσου από άλλες συσκευές ταυτόχρονα (multiple access). Το πρότυπο IEEE 802.15.4 είναι ευρέως χρησιμοποιούμενο σε WSNs δίκτυα με στόχο την επίτευξη χαμηλού κόστους πολυπλοκότητας και χαμηλής κατανάλωσης δικτύου. Το συγκεκριμένο πρότυπο αποτελεί την βάση για το πρότυπο ZigBee που παρέχει υπηρεσίες στα ανώτερα στρώματα αρχιτεκτονικής του WSN δικτύου.

2.3 Επίπεδο Ζεύξης Δεδομένων (Data Link Layer)

Το επίπεδο ζεύξης δεδομένων χρησιμοποιείται προκειμένου να μεταφέρει πακέτο επάνω σε μια ζεύξη. Ορίζει την μορφή των πακέτων που ανταλλάσσονται ανάμεσα στους κόμβους, στα άκρα της ζεύξης, καθώς και τις ενέργειες που γίνονται από αυτούς τους κόμβους όταν στέλνουν και λαμβάνουν αυτά τα πακέτα. Οι μονάδες δεδομένων που ανταλλάσσονται από ένα πρωτόκολλο επιπέδου ζεύξης ονομάζονται πλαίσια (frames) και συνεπώς οι ενέργειες που γίνονται από αυτά τα πρωτόκολλα κατά την αποστολή και λήψη τους είναι η ανίχνευση σφάλματος, η αναμετάδοση, ο έλεγχος ροής και η τυχαία πρόσβαση. Το επίπεδο ζεύξης δεδομένων είναι ένα ασύρματο multi-hop και αυτό-οργανούμενο δίκτυο αισθητήρων [15].

Έχει ως στόχο την δημιουργία της υποδομής του δικτύου και το δίκαιο και αποδοτικό διαχωρισμό των πόρων επικοινωνίας μεταξύ των κόμβων του δικτύου. Για την επίλυση των δυσχερειών που θέτουν σε κίνδυνο την αξιοπιστία του δικτύου έχει σχεδιαστεί το πρωτόκολλο MAC (Media Access Control) όπου είναι υπεύθυνο για την πρόσβαση στο μέσο της μετάδοσης και το LLC (Logical Link Control).

2.4 Επίπεδο Δικτύου (Network Layer)

Στο επίπεδο δικτύου καθορίζεται ο τρόπος δρομολόγησης των πακέτων (μονάδες δεδομένων) από τον αποστολέα στον παραλήπτη και ο έλεγχος συμφόρησης του δικτύου. Ως συμφόρηση ορίζεται εκείνη η κατάσταση του δικτύου όπου η εισερχόμενη κυκλοφορία είναι μεγαλύτερη από αυτή που μπορεί να εξυπηρετήσει απρόσκοπτα το δίκτυο. Ο αλγόριθμος δρομολόγησης των πακέτων μπορεί να είναι είτε στατικός είτε δυναμικός. Στην δεύτερη περίπτωση, κατά την επιλογή της διαδρομής διοχέτευσης της κυκλοφορίας μιας κλήσης λαμβάνεται υπόψη και ο φόρτος του δικτύου. Οι δυναμικοί αλγόριθμοι δρομολόγησης έχουν ως κύριο στόχο την γρήγορη εξάλειψη των περιστατικών συμφόρησης στο δίκτυο. Στα μελλοντικά δίκτυα υψηλής απόδοσης, όπου θα προσφέρονται υπηρεσίες πραγματικού χρόνου που θα απαιτούν εγγυημένη ποιότητα εξυπηρέτησης από το δίκτυο, οι αλγόριθμοι δρομολόγησης θα επιδιώκουν την αποφυγή των περιστατικών συμφόρησης. Σε αυτό το επίπεδο υλοποιείται το σχήμα διευθυνσιοδότησης του δικτύου [15].

Κάθε κόμβος που ανήκει σε ένα δίκτυο χαρακτηρίζεται μοναδικά από την διεύθυνση δικτύου. Η διεύθυνση δικτύου είναι μια παράμετρος του κόμβου, ορίζεται στο λογισμικό μέρος του και δεν συγχέεται με την φυσική διεύθυνση του. Η δρομολόγηση των πακέτων γίνεται με βάση την διεύθυνση δικτύου του παραλήπτη κόμβου. Το IP είναι το επίπεδο δικτύου για το διαδίκτυο (Internet) το οποίο ελέγχει την διευθυνσιοδότηση των κόμβων του δικτύου και την δρομολόγηση των πακέτων.

2.5 Επίπεδο Μεταφοράς (Transport Layer)

Στο επίπεδο μεταφοράς υλοποιείται το κανάλι επικοινωνίας μεταξύ των τερματικών κόμβων, μέσω του οποίου θα μεταβιβάζονται αξιόπιστα τα μηνύματα τους. Στον αποστολέα κόμβο τα μηνύματα που εισέρχονται από το ανώτερο Επίπεδο Συνόδου συνήθως διασπώνται σε πακέτα τα οποία αριθμούνται και προωθούνται για μετάδοση στο χαμηλότερο Επίπεδο Δικτύου. Αντίστοιχα στον παραλήπτη κόμβο τα αρχικά μηνύματα επανασυνθέτονται από τα εισερχόμενα πακέτα και προωθούνται προς επεξεργασία στο επίπεδο Συνόδου. Το Επίπεδο Μεταφοράς είναι υπεύθυνο για την εγκαθίδρυση, την συντήρηση και τον τερματισμό των καναλιών επικοινωνίας μεταξύ των τερματικών κόμβων. Σε αρκετές περιπτώσεις περισσότερα από ένα διαφορετικά μηνύματα χρησιμοποιούν το ίδιο κανάλι επικοινωνίας μεταξύ των τερματικών κόμβων. Σε άλλες περιπτώσεις ένα μήνυμα μπορεί να χρησιμοποιήσει περισσότερα από ένα κανάλια επικοινωνίας μεταξύ του αποστολέα και του προορισμού για να βελτιώσει τον ρυθμό εξυπηρέτησής του [15].

Επίσης διενεργείται και ο έλεγχος της ροής των δεδομένων μεταξύ των τερματικών κόμβων, έτσι ώστε να μη λαμβάνει ο παραλήπτης κόμβος περισσότερα δεδομένα από όσα μπορεί απρόσκοπτα να εξυπηρετήσει. Επειδή σε αυτό το επίπεδο ελέγχεται η από άκρο σε άκρο επικοινωνία, το επίπεδο μεταφοράς (και όλα τα ανώτερα από αυτό επίπεδα) υλοποιείται μόνο στους τερματικούς και όχι στους ενδιάμεσους κόμβους. Στο επίπεδο μεταφοράς αυτής της αρχιτεκτονικής βρίσκονται τα πρωτόκολλα TCP (Transmission Control Protocol – πρωτόκολλο ελέγχου μετάδοσης) και UDP (User Datagram Protocol – πρωτόκολλο αυτοδύναμων πακέτων χρήστη) τα οποία ελέγχουν την ανταλλαγή των πακέτων μεταξύ των τερματικών κόμβων, ρυθμίζοντας έτσι την από άκρο σε άκρο επικοινωνία.

2.6 Επίπεδο Συνόδου (Session Layer)

Στο επίπεδο συνόδου διενεργούνται όλες οι απαραίτητες λειτουργίες για την εγκαθίδρυση, την επίβλεψη και τον τερματισμό των συνόδων (sessions) μεταξύ των τελικών εφαρμογών. Πριν από την έναρξη της μετάδοσης δεδομένων οι τελικές εφαρμογές θα πρέπει να συμφωνήσουν εάν η επικοινωνία θα είναι αμφίδρομη (full duplex), εναλλακτικά αμφίδρομη (half duplex) ή μονόδρομη (simplex). Στην πρώτη περίπτωση τα δεδομένα μπορούν να μεταδίδονται και προς τις δύο κατευθύνσεις ταυτόχρονα, στην δεύτερη περίπτωση μπορούν να μεταδίδονται και προς τις δύο κατευθύνσεις αλλά όχι ταυτόχρονα, ενώ στην τρίτη περίπτωση τα δεδομένα μεταδίδονται μόνο προς μία κατεύθυνση. Αυτή η διαπραγμάτευση διενεργείται μεταξύ των ομότιμων οντοτήτων του επιπέδου συνόδου [14].

Επίσης από το επίπεδο συνόδου προσφέρεται και η υπηρεσία συγχρονισμού, η οποία χαρακτηρίζεται εξαιρετικά χρήσιμη για την αποτελεσματική αντιμετώπιση καταστάσεων κατάρρευσης της σύνδεσης. Στην ακολουθία δεδομένων εισάγονται κάποια προσυμφωνημένα σημεία συγχρονισμού πριν από την μετάδοσή τους. Εάν για κάποιο λόγο η σύνδεση καταρρεύσει, τότε θα επαναμεταδοθούν μόνο τα δεδομένα που εστάλησαν από το τελευταίο σημείο συγχρονισμού και μετά και όχι το σύνολο τους, κάτι που θα αποφέρει σημαντική εξοικονόμηση των πόρων του δικτύου.

2.7 Επίπεδο Παρουσίασης (Presentation Layer)

Το επίπεδο παρουσίασης ασχολείται με την αναπαράσταση των δεδομένων και έχει ως κύρια λειτουργία την εξασφάλιση της αναγνωσιμότητάς τους, ακόμα και μεταξύ κόμβων που χρησιμοποιούν διαφορετικές μορφές αναπαράστασης της πληροφορίας. Στην περίπτωση όπου ο αποστολέας κόμβος χρησιμοποιεί την κωδικοσειρά ASCII για την αναπαράσταση χαρακτήρων καθώς οι ακέραιοι αριθμοί εκφράζονται σαν συμπλήρωμα ως προς ένα και ο παραλήπτης κόμβος χρησιμοποιεί την κωδικοσειρά EBCDIC και οι ακέραιοι αριθμοί εκφράζονται σαν συμπλήρωμα ως προς δύο, για να μπορέσουν να επικοινωνήσουν οι δύο κόμβοι, θα πρέπει τα δεδομένα του αποστολέα να μετατραπούν στην μορφή δεδομένων που αναγνωρίζει ο παραλήπτης. Αυτή η μετατροπή διενεργείται στο επίπεδο παρουσίασης [15].

Επίσης στο επίπεδο παρουσίασης συμφωνείται η τεχνική συμπίεσης δεδομένων και το σχήμα κρυπτογράφησης της πληροφορίας που θα ακολουθούν ο αποστολέας και ο παραλήπτης κόμβος για την εξοικονόμηση των πόρων του δικτύου και την εξασφάλιση της μυστικότητας και της γνησιότητας της πληροφορίας, αντίστοιχα.

2.8 Επίπεδο Εφαρμογής (Application Layer)

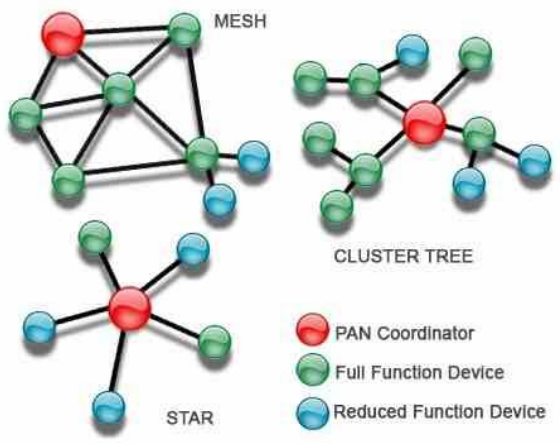
Το επίπεδο εφαρμογής παρέχει το λογισμικό της εφαρμογής, το οποίο είναι απαιτούμενο για να μορφοποιήσει τα δεδομένα σε μια κατανοητή μορφή για τον χειριστή, και ποικίλει αναλόγως των απαιτήσεων της εφαρμογής (π.χ. στρατιωτικής, ιατρικής περιβαλλοντικής κλπ.). Στο επίπεδο εφαρμογής τα πακέτα δεδομένων αναφέρονται ως μηνύματα (messages). Οι στόχοι που πρέπει να υλοποιούνται από το πρωτόκολλο του επιπέδου εφαρμογής κινούνται σε δύο άξονες. Στο πρώτο τίθεται το ερώτημα του τρόπου αποστολής εντολών ελέγχου από τον σταθμό βάσης προς τους κόμβους του δικτύου (downlink), και στο δεύτερο

τίθεται το ερώτημα της αντίστροφης αποστολής δεδομένων από τους κόμβους του δικτύου προς τον σταθμό βάσης.

Δηλαδή το επίπεδο εφαρμογής ορίζει τον τρόπο με τον οποίο ανταλλάσσουν μηνύματα τα δύο τερματικά συστήματα (σταθμός βάσης και κόμβοι) κατά τις διεργασίες της εφαρμογής. Αναλυτικά πρέπει να ορίζονται οι τύποι των μηνυμάτων που ανταλλάσσονται, η σύνταξη των μηνυμάτων (πεδία εντός των μηνυμάτων και διάκριση μεταξύ τους), η σημασία των πεδίων εντός των μηνυμάτων και ο καθορισμός για το πότε μια διεργασία λαμβάνει ή αποστέλλει μηνύματα [14].

2.9 Τοπολογίες Ασύρματων Δικτύων Αισθητήρων

Πολλές από τις σημερινές εφαρμογές αισθητήρων απαιτούν εναλλακτικές δικτύωσης που μειώνουν το κόστος και την πολυπλοκότητα ενώ βελτιώνει συνολικά την αξιοπιστία. Σε αυτό το σημείο θα αναφέρουμε τους βασικούς τύπους τοπολογίας σε ένα WSN [14].

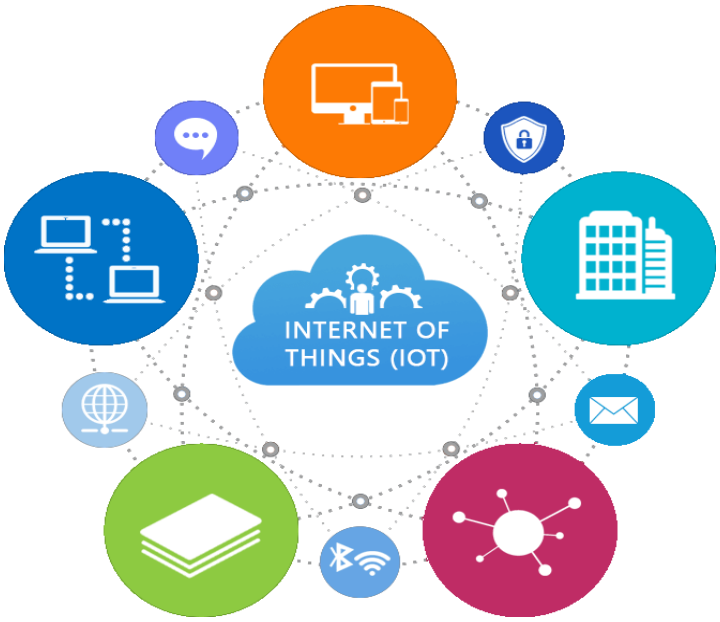


Εικόνα 12: Τοπολογίες WSNs (Πηγή: hlektrologia)

- **Τοπολογία αστέρα (Star):** Κάθε κόμβος δεν μπορεί να επικοινωνήσει απευθείας με άλλους, αλλά δρομολογεί δεδομένα μέσω ενός κεντρικού κόμβου. Οι κόμβοι (αισθητήρες) συλλέγουν την πληροφορία και την διοχετεύουν στο κεντρικό κόμβο, δηλαδή δεν υποστηρίζουν λειτουργία λήψης δεδομένων. Βασικό πλεονέκτημα είναι ότι η απώλεια κάποιου κόμβου πλην του κεντρικού δεν θέτει το δίκτυο WSN εκτός λειτουργίας. Μειονέκτημα της τοπολογίας είναι η κρισιμότητα του κεντρικού κόμβου, που καθιστά το δίκτυο α) λιγότερο ευέλικτο σε επέκταση, καθώς αυτή επηρεάζεται άμεσα από την ικανότητα του να εξυπηρετήσει νέους κόμβους και β) περισσότερο ευαίσθητο σε περίπτωση κατάρρευσης του κεντρικού κόμβου, καθώς ένα τμήμα του δικτύου τίθεται εκτός λειτουργίας.

- **Τοπολογία πλέγματος (mesh):** Τα δίκτυα πλέγματος επιτρέπουν στα δεδομένα να μεταβαίνουν από κόμβο σε κόμβο - αυτό επιτρέπει στο δίκτυο να είναι αυτό-διορθώσιμο. Κάθε κόμβος είναι τότε ικανός να επικοινωνεί με οποιονδήποτε άλλον καθώς τα δεδομένα δρομολογούνται από κόμβο σε κόμβο μέχρι να φτάσουν στην επιθυμητή τοποθεσία. Αυτό το είδος δικτύου είναι από τα πιο περίπλοκα, και οικονομικά μπορεί να κοστίσουν αρκετά για να αναπτυχθούν σωστά.

- **Τοπολογία δέντρου (tree):** Τα δίκτυα τοπολογίας δέντρου χρησιμοποιούν ένα κεντρικό hub που ονομάζεται κόμβος root ως τον βασικό δρομολογητή επικοινωνίας. Στην συνέχεια αυτό το επίπεδο σχηματίζει ένα δίκτυο αστέρα.



Εικόνα 13: Internet of Things (Πηγή: vidyatech)

ΚΕΦΑΛΑΙΟ 3

Πρωτόκολλα Στρώματος Δικτύου και Μεταφοράς

3.1 Πρωτόκολλα Δικτύων Επικοινωνίας

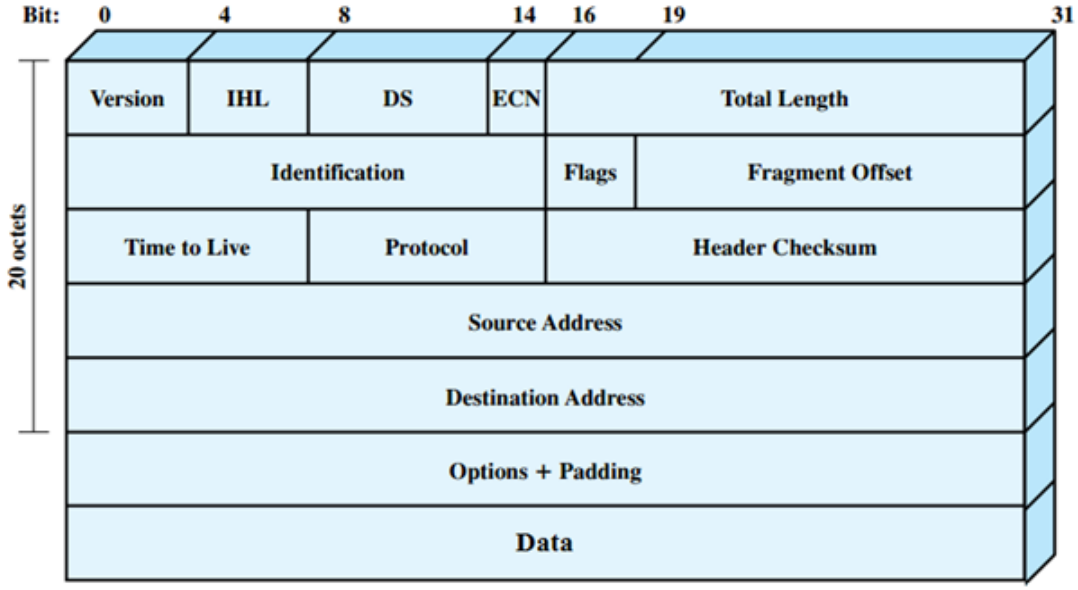
Στην καθημερινή ζωή, πρωτόκολλο είναι ένα σύνολο από συμβάσεις που καθορίζουν το πώς πρέπει να πραγματοποιηθεί κάποια διαδικασία. Στον κόσμο των δικτύων, πρωτόκολλο είναι ένα σύνολο από συμβάσεις που καθορίζουν το πώς ανταλλάσσουν μεταξύ τους δεδομένα οι υπολογιστές του δικτύου. Το πρωτόκολλο είναι αυτό που καθορίζει το πώς διακινούνται τα δεδομένα και το πώς γίνεται ο έλεγχος και ο χειρισμός των λαθών. Το Internet δεν είναι ένα απλό δίκτυο αλλά ένα διαδίκτυο. Χρειάζεται επομένως ένα σύνολο από συμβάσεις που να καθορίζουν το πώς ανταλλάσσουν μεταξύ τους δεδομένα οι υπολογιστές που μπορεί να είναι διαφορετικού τύπου και να ανήκουν σε διαφορετικά δίκτυα [15].

Οι αφηρημένες οντότητες που συνθέτουν τα επίπεδα σε ένα επικοινωνιακό σύστημα ονομάζονται πρωτόκολλα. Ένα πρωτόκολλο εκτελεί πρωτογενείς λειτουργίες και παρέχει συγκεκριμένες υπηρεσίες σε οντότητες υψηλότερου επιπέδου του ίδιου υπολογιστή (δηλαδή είτε σε άλλα πρωτόκολλα υψηλότερου επιπέδου είτε σε εφαρμογές τελικού χρήστη). Οι πρωτογενείς λειτουργίες που εκτελεί ένα πρωτόκολλο και οι υπηρεσίες που παρέχει σε οντότητες υψηλότερου επιπέδου καθορίζονται με σαφήνεια μέσω των σημείων επαφής υπηρεσίας του πρωτοκόλλου. Ένα πρωτόκολλο μπορεί να παρέχει πολλές διαφορετικές υπηρεσίες στις οντότητες των υψηλότερων επιπέδων. Οι οντότητες ενός πρωτοκόλλου επικοινωνούν με τις ομότιμες οντότητες του απομακρυσμένου υπολογιστή μέσω του σημείου επαφής πρωτοκόλλου, το οποίο καθορίζει τους κανόνες και τις συνθήκες αυτής της επικοινωνίας. Σκοπός αυτής της επικοινωνίας είναι η υλοποίηση των παρεχόμενων υπηρεσιών του πρωτοκόλλου.

Επιπρόσθετα σε κάποιο συγκεκριμένο επίπεδο μπορεί να υπάρχουν περισσότερα από ένα πρωτόκολλα, το καθένα από τα οποία παρέχει διαφορετικές υπηρεσίες. Επίσης, οι οντότητες ενός επιπέδου σε έναν υπολογιστή επικοινωνούν με τις αντίστοιχες οντότητες του ίδιου επιπέδου στον απομακρυσμένο υπολογιστή. Οι κανόνες και οι συνθήκες που χρησιμοποιούνται σε αυτήν την επικοινωνία ορίζουν το σημείο επαφής πρωτοκόλλου (protocol interface). Οι οντότητες του ίδιου επιπέδου συνήθως αναφέρονται ως ομότιμες οντότητες (peer objects). Στην πραγματικότητα, οι ομότιμες διεργασίες δεν επικοινωνούν απευθείας μεταξύ τους. Στον τοπικό υπολογιστή η τοπική διεργασία χρησιμοποιεί μια παρεχόμενη υπηρεσία του κατώτερου επιπέδου και αποστέλλει τις πληροφορίες στο χαμηλότερο επίπεδο. Το σύνολο των πρωτοκόλλων συνθέτουν την αρχιτεκτονική του δικτύου (network architecture). Τα σημεία επαφής υπηρεσίας και πρωτοκόλλου αποτελούν τις προδιαγραφές της αρχιτεκτονικής του δικτύου. Οι λεπτομέρειες υλοποίησης των πρωτοκόλλων αποκρύπτονται από τον εξωτερικό χρήστη και δεν αποτελούν μέρος της αρχιτεκτονικής του δικτύου.

3.2 Πρωτόκολλο Διαδικτύου IPv4

Το πρωτόκολλο IPv4 (Internet protocol version 4) χρησιμοποιεί 32 bit διευθύνσεις, χαρακτηριστικό το οποίο μας περιορίζει στον συνολικό αριθμό των 2^{32} διαφορετικών IPv4 διευθύνσεων. Το IPv4 είναι ακόμη το πιο ευρέως διαδεδομένο πρωτόκολλο του Internet Layer. Επίσης είναι ένα connectionless πρωτόκολλο για χρήση σε packet-switched Link Layer δίκτυα. Αναπτύσσει το καλύτερο δυνατό μοντέλο μεταφοράς ενός πακέτου, χωρίς να εγγυάται την παράδοση του, ούτε να διασφαλίζει την σωστή αλληλουχία του ή την αποφυγή της επαναποστολής του. Το μέγεθος διευθύνσεων που χρησιμοποιεί το πρωτόκολλο, το μεταβλητό μήκος της επικεφαλίδας του σε συνδυασμό με την ανάγκη για την δυνατότητα επισήμανσης ροών (flow labeling) αποτελούν τις κυριότερες αδυναμίες του πρωτοκόλλου, οι οποίες οδήγησαν και στον ορισμό του IPv6 [14].



Εικόνα 14: Μορφή Επικεφαλίδας IPv4 (Πηγή: bravelearn)

Επικεφαλίδα (Header): Η επικεφαλίδα αποτελείται από 14 πεδία, από τα οποία τα 13 είναι απαραίτητα. Το 14 πεδίο είναι προαιρετικό (options). Τα πεδία στην επικεφαλίδα πακετάρονται με το περισσότερο σημαντικό πεδίο εμπρός και για το διάγραμμα και την συζήτηση, τα περισσότερο σημαντικά bit βρίσκονται μπροστά. Έτσι το 0 είναι το περισσότερο σημαντικό bit, έτσι ώστε για παράδειγμα το πεδίο έκδοση (version) βρίσκεται στα 4 περισσότερο σημαντικά bit του πρώτου byte.

Έκδοση (Version): Το πρώτο πεδίο της επικεφαλίδας σε ένα IP πακέτο είναι το πεδίο της έκδοσης του πρωτοκόλλου, μήκους 4-bit. Για το IPv4 αυτό έχει την τιμή 4 (από όπου και αν προέρχεται το όνομα IPv4).

Μήκος Επικεφαλίδας (IHL, Internet Header Length): Το δεύτερο πεδίο (4-bits) είναι το μήκος της επικεφαλίδας. Αυτό μας δίνει το μήκος της επικεφαλίδας σε λέξεις των 32-bit. Επειδή η επικεφαλίδα του IPv4 μπορεί να περιέχει μεταβλητό αριθμό επιλογών, αυτό το πεδίο παρέχει το μήκος της επικεφαλίδας. Η μικρότερη τιμή του πεδίου είναι 5 (RFC 791), που σημαίνει ότι το μήκος είναι 5*32=160 bits =20 bytes. Επειδή το πεδίο είναι 4 bit, το μέγιστο μήκος είναι 2^4-1=15 λέξεις (15*32 bits) ή 480 bits=60 bytes.

Συνολικό Μήκος (Total length): Το πεδίο αυτό έχει μήκος 16-bits. Καθορίζει το συνολικό μήκος του κομματιού (fragment) σε bytes, συμπεριλαμβανομένων της επικεφαλίδας και των δεδομένων. Το ελάχιστο μήκος του πακέτου είναι 20 bytes (20 bytes επικεφαλίδα + 0 bytes δεδομένα) και το μέγιστο μήκος είναι 2^{16}-1=65535 bytes, καθότι το μήκος του πεδίου Συνολικό Μήκος είναι 16 bits.

Αναγνώριση (Identification): Το πεδίο αυτό είναι ένα πεδίο ταυτότητας και χρησιμεύει για τον μοναδικό προσδιορισμό των κομματιών (fragments) που ανήκουν στο ίδιο αρχικό IP αυτοδύναμο πακέτο.

Σημαίες (Flags): Αυτό είναι ένα πεδίο των τριών bit και χρησιμεύει να ελέγχει ή να προσδιορίζει τα κομμάτια. Αυτά είναι (κατά σειρά από το περισσότερο σημαντικό προς το λιγότερο): Bit 0 (δεσμευμένο, πρέπει να είναι 0), Bit 1 (απαγόρευσης διάσπασης του αυτοδύναμου πακέτου Don't Fragment), Bit 2 (ένδειξης ύπαρξης περισσοτέρων κομματιών More Fragments). Εάν η σημαία DF (Don't Fragment) έχει τεθεί στο 1 και για την δρομολόγηση του πακέτου είναι απαραίτητη η διάσπαση του, τότε το πακέτο απορρίπτεται. Σε πακέτα που δεν έχουν διασπαστεί η σημαία MF (More Fragments) είναι 0. Για διασπασμένα πακέτα όλα τα κομμάτια έχουν το MF=1, εκτός από το τελευταίο που έχει το MF=0. Το τελευταίο κομμάτι έχει μη μηδενικό πεδίο δείκτη εντοπισμού τμήματος, το οποίο το διακρίνει από ακομμάτιαστα πακέτα.

Δείκτης εντοπισμού τμήματος (Fragment Offset): Είναι 13-bit και απαριθμεί σε οκτάδες Byte. Προσδιορίζει την θέση ενός συγκεκριμένου κομματιού, από την αρχή του ακομμάτιαστου αυτοδύναμου πακέτου.

Χρόνος Ζωής (Time to Live): Το πεδίο αυτό οριοθετεί το χρόνο ζωής του αυτοδύναμου πακέτου. Έχει μήκος 8-bit και χρησιμεύει στο να καταστρέφονται αυτοδύναμα πακέτα. Δίνεται σε δευτερόλεπτα, αλλά χρόνοι μικρότεροι από 1s στρογγυλεύονται στο 1s. Στην πράξη έχει καταντήσει μετρητής αναπηδήσεων: όπου όταν ένα αυτοδύναμο πακέτο φτάσει σε ένα δρομολογητή, ο δρομολογητής μειώνει το πεδίο TTL κατά 1. Όταν μηδενιστεί ο δρομολογητής απορρίπτει το πακέτο και στέλνει ένα μήνυμα τέλους χρόνου του πρωτοκόλλου μηνυμάτων ελέγχου του Internet (ICMP Time Exceeded) μήνυμα στον αποστολέα.

Αριθμός Πρωτοκόλλου (Protocol): Το πεδίο αυτό προσδιορίζει την έκδοση του πρωτοκόλλου IP που χρησιμοποιείται από το αυτοδύναμο πακέτο. Η Internet Assigned Numbers Authority διατηρεί έναν κατάλογο αριθμών πρωτοκόλλου IP, ο οποίος αρχικά είχε καθοριστεί στο RFC 790.

Άθροισμα Ελέγχου Επικεφαλίδας (Header Checksum): Τα 16-bits άθροισμα ελέγχου της επικεφαλίδας, χρησιμοποιείται για έλεγχο σφαλμάτων της επικεφαλίδας. Μόλις ένα πακέτο φτάσει σε έναν δρομολογητή, ο δρομολογητής υπολογίζει το άθροισμα ελέγχου της επικεφαλίδας και το συγκρίνει με το πεδίο αθροίσματος ελέγχου της επικεφαλίδας. Εάν δεν ταιριάζουν, τότε ο δρομολογητής απορρίπτει το πακέτο.

IP Διεύθυνση Πηγής (Source Address): Αυτό το πεδίο είναι η IPv4 διεύθυνση του αποστολέα του πακέτου. Η διεύθυνση αυτή μπορεί να αλλάξει κατά την διέλευση από μια συσκευή μετάφρασης διεύθυνσης δικτύου (NAT).

IP Διεύθυνση Προορισμού (Destination Address): Αυτό το πεδίο είναι η IPv4 διεύθυνση του παραλήπτη του πακέτου. Η διεύθυνση αυτή μπορεί να αλλάξει κατά την διέλευση από μια συσκευή μετάφρασης διεύθυνσης δικτύου (NAT).

Δεδομένα (Data): Το τμήμα δεδομένων του πακέτου, δεν συμπεριλαμβάνεται στο άθροισμα ελέγχου, το οποίο και γι' αυτό αποκαλείται άθροισμα ελέγχου επικεφαλίδας. Ο τρόπος αναπαράστασης των περιεχομένων του βασίζεται στην τιμή που υπάρχει στο πεδίο «αριθμός πρωτοκόλλου» της επικεφαλίδας.

3.3 Πρωτόκολλο Διαδικτύου IPv6

Το IPv6 (Internet Protocol version 6) είναι η πιο πρόσφατη αναθεώρηση του πρωτοκόλλου Internet (IP), του βασικού πρωτοκόλλου επικοινωνίας πάνω στο οποίο έχει χτιστεί ολόκληρο το διαδίκτυο όπου πρόκειται να αντικαταστήσει το παλιότερο IPv4. Το IPv6 αναπτύχθηκε από την *Τακτική Δύναμη Μηχανικών του Internet (Internet Engineering Task Force,* IETF*)*, για να ασχοληθεί με το επί μακρόν αντιμετωπιζόμενο πρόβλημα της εξάντλησης των διευθύνσεων του IPv4. Το IPv6 χρησιμοποιεί διευθύνσεις 128 bit, το οποίο επιτρέπει 2^{128} δηλαδή 3,4*10^38 διαφορετικές IPv6 διευθύνσεις. Τα δύο πρωτόκολλα δεν έχουν σχεδιαστεί ώστε να μπορούν να συνεργάζονται, δυσκολεύοντας έτσι την μετάβαση στο IPv6. Οι διευθύνσεις IP του πρωτοκόλλου IPv6, αποτελούνται από 8 ομάδες των τεσσάρων δεκαεξαδικών ψηφίων, χωρισμένων με άνω και κάτω τελεία. Ένα παράδειγμα ρεαλιστικής διεύθυνσης IPv6 μπορεί να είναι: 2001:0db8:4004:0010:0000:0000:6543:0ffd [4].

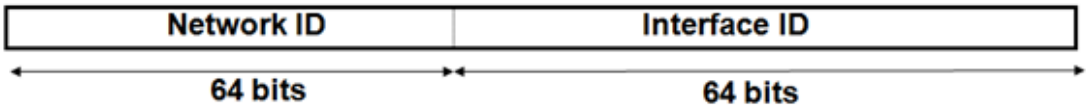
3.3.1 Το IPv6 σε σύγκριση με το IPv4

Το IPv6 καθορίζει μια νέα μορφή πακέτου, σχεδιασμένη για να ελαχιστοποιεί την επεξεργασία των πακέτων από τους δρομολογητές. Επειδή οι επικεφαλίδες των πακέτων του IPv4 και IPv6 διαφέρουν σημαντικά, τα δύο πρωτόκολλα δεν μπορούν να συνεργαστούν. Όμως από τις περισσότερες πλευρές το IPv6 είναι μία συντηρητική επέκταση του IPv4. Τα περισσότερα πρωτόκολλα του επιπέδου μεταφοράς και εφαρμογής, χρειάζονται λίγη ή και καθόλου μετατροπή για να δουλέψουν πάνω στο IPv6. Εξαίρεση αποτελούν τα πρωτόκολλα εφαρμογών, τα οποία ενσωματώνουν διευθύνσεις του επιπέδου του Internet, όπως το FTP.

3.3.2 Ανεπίσημη Αυτόματη Απόδοση Διευθύνσεων (SLAAC)

Οι συσκευές που συνδέονται σε ένα δίκτυο IPv6 μπορούν να αποδώσουν αυτόματα στον εαυτό τους μια IPv6 διεύθυνση, χρησιμοποιώντας το πρωτόκολλο Neighbor Discovery Protocol (Πρωτόκολλο Ανακάλυψης Γειτόνων). Αυτό το πετυχαίνουν χρησιμοποιώντας Μηνύματα Ανακάλυψης Δρομολογητών του Πρωτοκόλλου Μηνυμάτων Ελέγχου του Internet, έκδοσης 6 (Internet Control Message Protocol version 6). Με τα πακέτα αυτά οι συσκευές ζητούν από τους δρομολογητές να τους στείλουν τις παραμέτρους διαμόρφωσης τους. Οι δρομολογητές ανταποκρίνονται σε αυτήν την αίτηση με ένα πακέτο διαφήμισης του δρομολογητή, το οποίο περιέχει τις παραμέτρους διαμόρφωσης του επιπέδου του Internet (Layer Internet). Εάν η ανεπίσημη αυτόματη απόδοση (stateless address autoconfiguration) διευθύνσεων IPv6 είναι ακατάλληλη για μια εφαρμογή, τότε ένα δίκτυο μπορεί να χρησιμοποιεί επίσημη διαμόρφωση (stateful configuration) χρησιμοποιώντας το Πρωτόκολλο Δυναμικής Απόδοσης Διευθύνσεων, έκδοσης 6 (Dynamic Host Configuration Protocol version

6) ή ακόμη μπορεί να αποδοθεί στην συσκευή χειροκίνητα μια διεύθυνση IPv6 (στατική διεύθυνση) [4].



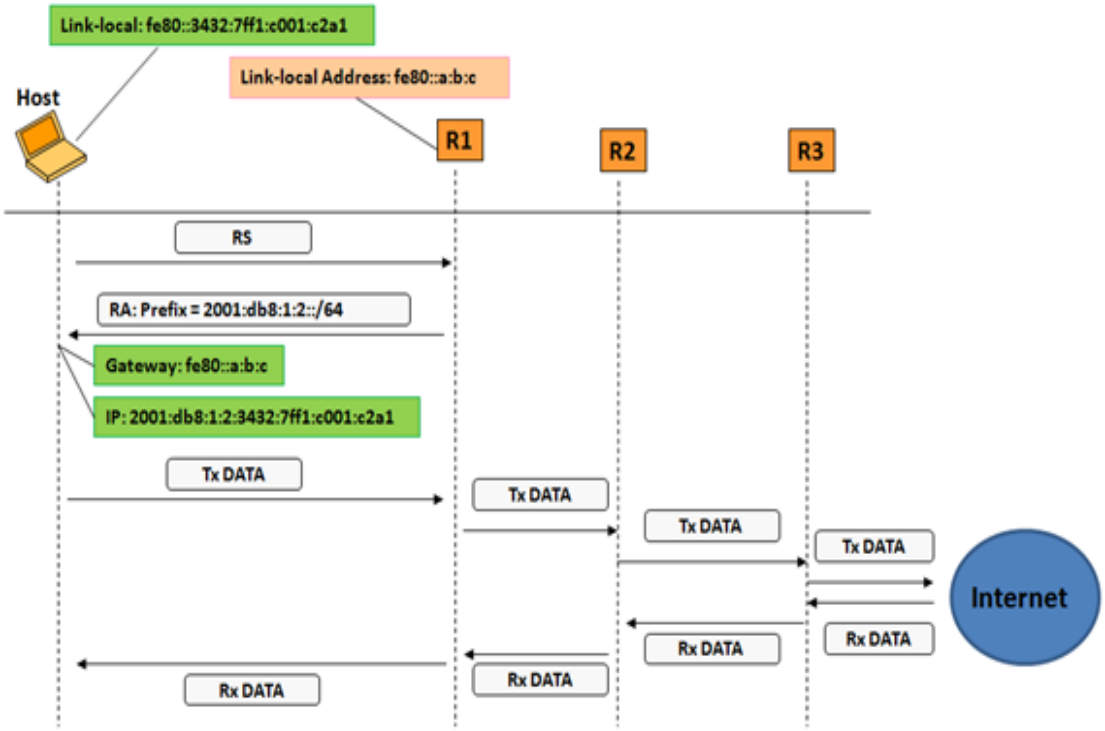
Εικόνα 15: IPv6 Address Interface Identifier (Πηγή: IoT in 5 days)

Η εικόνα 15 δείχνει τα δεξιά 64 bits που ονομάζεται διεπαφή αναγνώρισης (Interface Identifier) επειδή αναγνωρίζουν μοναδικά την διασύνδεση του κεντρικού υπολογιστή στο τοπικό δίκτυο.

Τα πλεονεκτήματα του SLAAC είναι ότι απλοποιεί την διαμόρφωση των «χαλαρών» συσκευών, όπως αισθητήρες, κάμερες ή οποιαδήποτε άλλη συσκευή με χαμηλή ισχύ επεξεργασίας. Επίσης απλοποιεί την υποδομή του δικτύου που απαιτείται για την κατασκευή ενός δικτύου IPv6 επειδή δεν χρειάζεται πρόσθετη συσκευή/διακομιστής. Χρησιμοποιείται ο ίδιος δρομολογητής που χρειάζεται για να σταλθούν τα πακέτα έξω από το δίκτυο ώστε να ρυθμιστούν οι παράμετροι των συσκευών IP.

Ένα τοπικό δίκτυο LAN (Local Area Network) το οποίο είναι συνδεδεμένο με ένα δρομολογητή, ο δρομολογητής αυτός είναι υπεύθυνος για την αποστολή όλων των απαραίτητων πληροφοριών, στους κεντρικούς υπολογιστές χρησιμοποιώντας ένα μήνυμα διαφήμισης δρομολόγησης (Router Advertisement). Ο δρομολογητής στέλνει περιοδικά μηνύματα διαφήμισης (RAs), αλλά για να επιταχυνθεί η διαδικασία ένας κεντρικός υπολογιστής μπορεί να στείλει ένα μήνυμα RS (Router Solicitation) όταν συνδεθεί με το δίκτυο. Ο δρομολογητής θα στείλει αμέσως ένα RA μήνυμα σαν απάντηση του RS.

Η εικόνα 16 που φαίνεται παρακάτω δείχνει την ανταλλαγή των πακέτων μεταξύ ενός κεντρικού υπολογιστή που μόλις συνδέθηκε με ένα τοπικό δίκτυο και μερικώς IPv6 προορισμοί στο διαδίκτυο.



Εικόνα 16: Packet exchange & IPv6 destination (Πηγή: IoT in 5 days)

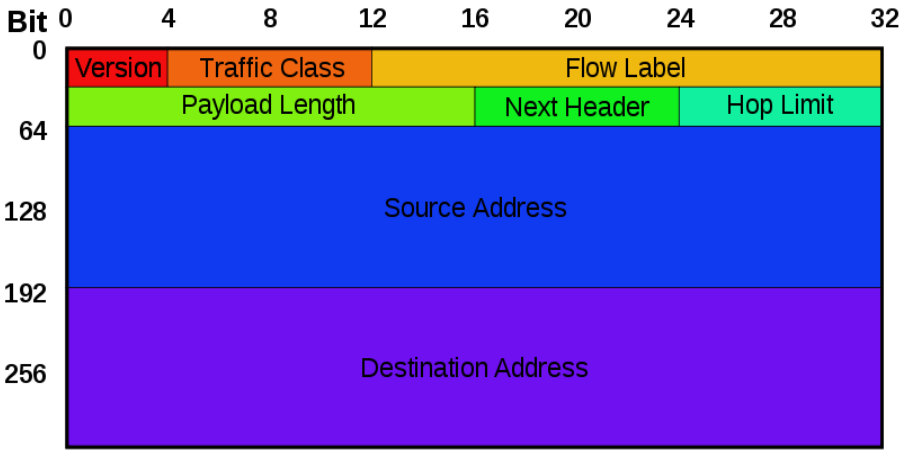
Σύμφωνα με την εικόνα 16 ο R1 δρομολογητής συνδέεται σε έναν κεντρικό υπολογιστή (host) στο τοπικό δίκτυο (LAN) και στέλνει RAs μηνύματα. Τόσο ο R1 όσο και κεντρικός υπολογιστής στις μεταξύ τους συνδέσεις διαθέτουν μία τοπική διεύθυνση σύνδεσης (link-local-address) που συνδέονται στο LAN, όπου η διεύθυνση αυτή διαμορφώνεται αυτόματα. Ο κεντρικός υπολογιστής δημιουργεί την τοπική διεύθυνση σύνδεσης συνδυάζοντας τα «αριστερά» 64bits (64 leftmost bits) του τοπικού συνδέσμου (fe80::/64) και τα «δεξιά» 64bits (64 rightmost bits) του αναγνωριστικού σύνδεσης IID (Interface Identifier) [4].

Οι κεντρικοί υπολογιστές χρειάζονται δύο βασικά πράγματα για να μπορούν να στέλνουν πακέτα σε άλλα δίκτυα. Το πρώτο είναι μια παγκόσμια διεύθυνση IPv6 (Global IPv6 Address) και το δεύτερο είναι η διεύθυνση μια πύλης (Gateway Address) ενός δρομολογητή στον οποίο θα σταλούν τα πακέτα που θέλει για να μεταφερθούν εκτός δικτύου. Παρόλο που ο R1 στέλνει RA μηνύματα περιοδικά (συνήθως κάθε κάποια δευτερόλεπτα) όταν κεντρικός υπολογιστής συνδεθεί και έχει διαμορφώσει την διεύθυνση της τοπικής σύνδεσης στέλνει ένα RS μήνυμα στον οποίο ο R1 ανταποκρίνεται άμεσα με ένα RA μήνυμα. Μόλις ρυθμιστεί η διεύθυνση πύλης καθώς και η παγκόσμια διεύθυνση IPv6 ο κεντρικός υπολογιστής μπορεί να λάβει ή να στείλει πληροφορίες. Στην εικόνα 16 φαίνεται ότι στέλνει Tx δεδομένα (Tx data) σε ένα κεντρικό υπολογιστή στο Internet.

Επομένως δημιουργεί ένα πακέτο IPv6 με την διεύθυνση προορισμού του κεντρικού υπολογιστή του παραλήπτη. Ο κεντρικός υπολογιστής προορισμού απαντά με Rx δεδομένα (Rx data).

3.3.3 Μορφή Επικεφαλίδας IPv6

Ένα πακέτο IPv6 αποτελείται από την επικεφαλίδα και από τα δεδομένα. Η επικεφαλίδα αποτελείται από ένα σταθερό τμήμα με την ελάχιστη λειτουργικότητα που είναι απαραίτητη για όλα τα πακέτα και μπορεί να ακολουθείται από προαιρετικές επεκτάσεις, που υλοποιούν ειδικά χαρακτηριστικά. Το σταθερό μέρος της επικεφαλίδας καταλαμβάνει τις πρώτες 40 οκτάδες (320bits) του πακέτου. Στην εικόνα 17 παρακάτω φαίνεται η επικεφαλίδα πακέτου IPv6 [28].



Εικόνα 17: Μορφή Επικεφαλίδας IPv6 (Πηγή: Wikimedia Commons)

Τα πεδία της IPv6 κεφαλίδας πιο αναλυτικά είναι:

Έκδοση (Version): Η έκδοση του πρωτοκόλλου, έχει την τιμή έξι, αφού είναι IPv6.

Κλάση κίνησης (Traffic Class): Το πεδίο traffic class (8bits) αντικαθιστά το πεδίο Type of Service, και επιτρέπει στο τερματικό πηγή ή σε ένα δρομολογητή να αναγνωρίζει την κλάση ή την προτεραιότητα του πακέτου.

Ετικέτα ροής (Flow label): Το πεδίο Ετικέτα ροής (20bits) επιτρέπει στο τερματικό πηγή να μαρκάρει μια σειρά από πακέτα (π.χ. μια ροή), η οποία απαιτεί ειδική μεταχείριση από τους ενδιάμεσους δρομολογητές, όταν ένα πακέτο μεταφέρεται από την πηγή στον προορισμό.

Μήκος ωφέλιμου φορτίου (Payload Length): Το Payload Length είναι το μεταβλητό μήκος των δεδομένων που το πακέτο IPv6 μεταφέρει μετά την επικεφαλίδα.

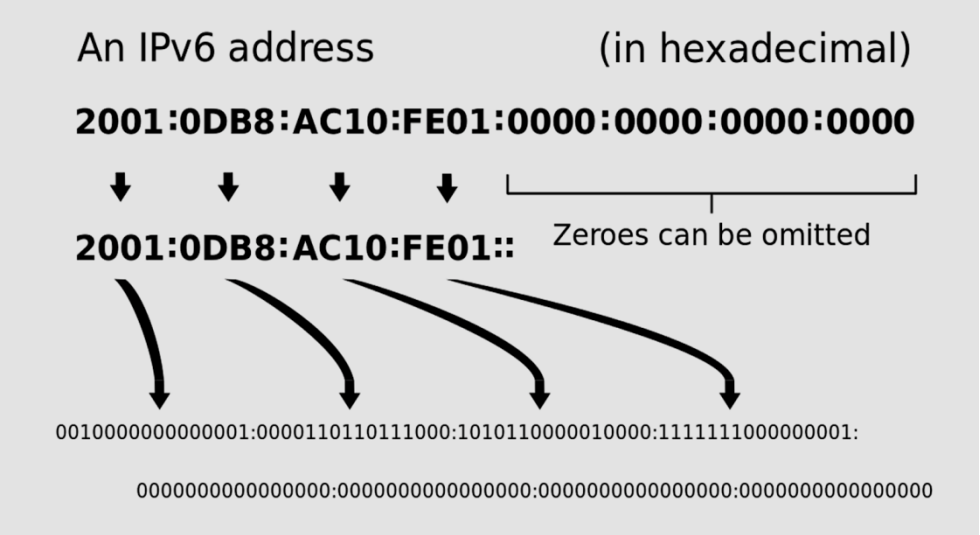
Next Header: Το πεδίο Next Header (8bits) προσδιορίζει τον τύπο της επικεφαλίδας που ακολουθεί την επικεφαλίδα IPv6.

Αριθμός κόμβων (Hop Limit): Το πεδίο αριθμός κόμβων (8bits) εκφράζει τον χρόνο ζωής ενός πακέτου. Χρησιμοποιείται για να αποτρέπει την επ΄ αόριστον ύπαρξη πακέτων σε ένα δίκτυο. Ορίζεται ως ο αριθμός των κόμβων που μπορεί να διαβαστεί ένα πακέτο.

Διεύθυνση Πηγής (Source Address): Η IP Διεύθυνση (128bits) του αποστολέα του πακέτου.

Διεύθυνση Προορισμού (Destination Address): Η IP Διεύθυνση (128bits) του προορισμού του πακέτου.

Οι διευθύνσεις διαφέρουν σημαντικά στην σημειολογία, στην σημασία και στην δομή. Το μήκος τους είναι 128bits και γράφονται με δεκαεξαδική μορφή σαν 8 ακέραιοι των 16bits χωρισμένα με άνω κάτω τελεία (“:”).



Εικόνα 18: IPv6 διεύθυνση στο δυαδικό αριθμητικό σύστημα (Πηγή: Wikipedia)

Οι διευθύνσεις IPv6 ταξινομούνται με βάση τις μεθόδους διευθυνσιοδότησης και δρομολόγησης. Έτσι έχουμε διευθύνσεις unicast, διευθύνσεις anycast και διευθύνσεις multicast [28].

Μια διεύθυνση unicast προσδιορίζει μια συγκεκριμένη διασύνδεση δικτύου. Το πρωτόκολλο Internet παραδίδει τα πακέτα που στέλνονται σε μια unicast διεύθυνση, μόνο στην συγκεκριμένη διεύθυνση δικτύου.

Μια διεύθυνση anycast αποδίδεται σε μια ομάδα διασυνδέσεων, που συνήθως ανήκουν σε διαφορετικούς κόμβους. Ένα πακέτο που στέλνεται σε μία διεύθυνση anycast παραδίδεται μόνο σε μία από τις διασυνδέσεις της ομάδας, τυπικά στην πλησιέστερη, σύμφωνα με τον ορισμό της απόστασης που χρησιμοποιεί το πρωτόκολλο δρομολόγησης.

Μια διεύθυνση multicast χρησιμοποιείται από πολλές διασυνδέσεις. Αυτές παίρνουν την multicast διεύθυνση συμμετέχοντας σε πρωτόκολλα διανομής διευθύνσεων multicast ανάμεσα στους δρομολογητές του δικτύου.

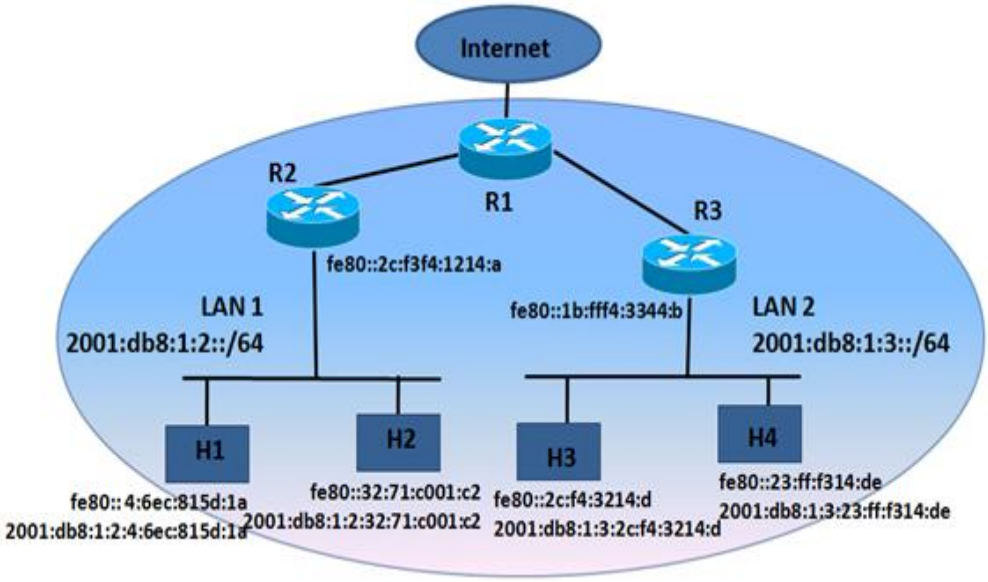
Ένα πακέτο το οποίο στέλνεται σε μια διεύθυνση multicast, διανέμεται σε όλες τις διασυνδέσεις που συμμετέχουν στην αντίστοιχη multicast ομάδα. Το πρωτόκολλο IPv6 δεν υλοποιεί διευθύνσεις τύπου broadcast. Ο παραδοσιακός ρόλος των broadcast διευθύνσεων, υλοποιείται με το multicast group ff02::1 (the all-nodes link-local multicast group ff02::1). Όμως η χρήση του all-nodes link-local multicast group δεν συνίσταται και τα περισσότερα IPv6 πρωτόκολλα χρησιμοποιούν μια ειδική link local multicast ομάδα, για να αποφευχθεί η ενόχληση όλων των διασυνδέσεων του δικτύου.

3.3.4 Ασφάλεια Επιπέδου Δικτύου & Κινητικότητα

Αρχικά για την ασφάλεια στο IPv6, είχε αναπτυχθεί το πρωτόκολλο Internet Protocol Security (IPsec). Το πρωτόκολλο όμως αυτό χρησιμοποιήθηκε ευρέως και στο IPv4, αφού βέβαια τροποποιήθηκε κατάλληλα. Στην αρχή το IPsec ήταν βασικό χαρακτηριστικό του IPv6, αλλά στην συνέχεια έγινε προαιρετικό. Αντίθετα με το κινητό IPv4, το κινητό IPv6 αποφεύγει την τριγωνική δρομολόγηση (triangular routing) και για αυτό είναι το ίδιο αποτελεσματικό με το σταθερό IPv6. Οι δρομολογητές του IPv6, επιτρέπουν να μετακινηθούν ολόκληρα υποδίκτυα σε άλλους δρομολογητές, χωρίς επαναρίθμηση [4].

3.3.5 Παράδειγμα Δικτύου IPv6

Παρακάτω η εικόνα 19 δείχνει πως μοιάζει ένα απλό δίκτυο IPv6 για όλες τις συσκευές δικτύου.



Εικόνα 19: IPv6 Network Example (Πηγή: IoT in 5 days)

Σύμφωνα με το παράδειγμα της εικόνας 19 υπάρχουν τέσσερις συσκευές (π.χ. αισθητήρες) και δύο από αυτές τις συσκευές τοποθετούνται σε δύο διαφορετικά σημεία, όπως για παράδειγμα σε δύο ορόφους ενός κτιρίου. Υπάρχουν τέσσερις συσκευές IP, αλλά μπορεί να είναι συνδεδεμένες μέχρι 2^{64} συσκευές στο ίδιο τοπικό δίκτυο (LAN). Δημιουργούνται δύο τοπικά δίκτυα με έναν δρομολογητή σε κάθε ένα από αυτά καθώς και οι δύο δρομολογητές είναι συνδεδεμένοι σε ένα κεντρικό δρομολογητή R1 ο οποίος είναι συνδεδεμένος στο Internet.

Το τοπικό δίκτυο 1 (LAN1) εξυπηρετείται από τον κεντρικό δρομολογητή R2 (μαζί με την τοπική διεύθυνση σύνδεσης fe80::2c:f3f4:1214:a σε αυτό το LAN) και χρησιμοποιεί την διεύθυνση 2001:db8:1:2::/64 όπου έχει ανακοινωθεί από την ανεπίσημη αυτόματη απόδοση διευθύνσεων (SLAAC). Επίσης το τοπικό δίκτυο LAN2 εξυπηρετείται από τον R3 (με την

διεύθυνση τοπικού συνδέσμου fe80::1b:fff4:3344:b στο LAN) και χρησιμοποιεί την 2001:db81:3::/64 όπου και αυτή έχει δοθεί από την SLAAC. Ο κάθε κεντρικός υπολογιστής ρυθμίζει την πύλη (gateway) χρησιμοποιώντας την διεύθυνση τοπικού συνδέσμου (link-local address) που χρησιμοποιείται από τον δρομολογητή για το RA (Router Advertisement). Η τοπική διεύθυνση σύνδεσης μπορεί να χρησιμοποιηθεί για επικοινωνία μεταξύ των υπολογιστών εντός τοπικού δικτύου, αλλά για επικοινωνία με άλλα τοπικά δίκτυα ή γενικά με άλλα δίκτυα απαιτείται μια παγκόσμια IPv6 διεύθυνση (global IPv6 address).

3.4 Το Πρότυπο 6LoWPAN

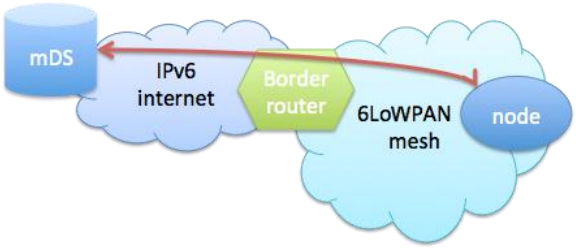
Το 6LoWPAN είναι ένα πρωτόκολλο συμπληρωματικό του IPv6 σε ασύρματα δίκτυα χαμηλής κατανάλωσης. Είναι ένα σύνολο προτύπων που καθορίζονται από την Ομάδα Μηχανικών Διαδικτύου (IETF), η οποία δημιουργεί και διατηρεί όλα τα βασικά πρότυπα καθώς και την αρχιτεκτονική. Ένας τεχνικός ορισμός του 6LoWPAN είναι:

Το πρότυπο 6LoWPAN επιτρέπει την αποδοτική χρήση του IPv6 μέσω χαμηλής κατανάλωσης ενέργειας ασύρματων δικτύων σε απλές ενσωματωμένες συσκευές μέσω ενός στρώματος προσαρμογής και βελτιστοποίησης του σχετικών πρωτοκόλλων.

Η ομάδα 6LoWPAN έχει ορίσει μηχανισμούς συμπίεσης κεφαλίδων που επιτρέπουν την αποστολή και λήψη πακέτων IPv6 μέσω δικτύων που βασίζονται στο IEEE 802.15.4. Οι συσκευές IEEE 802.15.4 παρέχουν δυνατότητα επικοινωνίας στον τομέα της ασύρματης επικοινωνίας. Ωστόσο, οι εγγενείς φύσεις των δικτύων είναι διαφορετικές. Η βασική προδιαγραφή που αναπτύχθηκε από την ομάδα 6LoWPAN IETF είναι το RFC 4944 (ενημερώθηκε από το RFC 6282 με συμπίεση κεφαλίδας και από το RFC 6775 με βελτιστοποίηση εντοπισμού γείτονα). Το έγγραφο δήλωσης προβλήματος είναι RFC 4919. Το IPv6 μέσω Bluetooth χαμηλής ενέργειας ορίζεται από το RFC 7668. Ο στόχος για δικτύωση IP, ραδιοεπικοινωνία χαμηλής ισχύος είναι εφαρμογές που χρειάζονται ασύρματη σύνδεση με χαμηλές ταχύτητες δεδομένων για συσκευές με περιορισμένο συντελεστή μορφής [1].

3.4.1 Επισκόπηση των LoWPANs

Τα δίκτυα χαμηλής κατανάλωσης (LLNs) είναι ο όρος που χρησιμοποιείται συνήθως για να αναφέρεται σε δίκτυα που είναι κατασκευασμένα από πολύ περιορισμένους κόμβους (περιορισμένη CPU, μνήμη, ισχύς) που συνδέονται σε μια ποικιλία συνδέσμων “lossy” (ραδιοεπικοινωνία χαμηλής ισχύος). Χαρακτηρίζονται από χαμηλή ταχύτητα, χαμηλή απόδοση, χαμηλό κόστος και ασταθή συνδεσιμότητα.



Εικόνα 20: Overview of the 6LoWPAN Network (Πηγή: arm MBED)

Όπως φαίνεται και από την εικόνα 20 συνήθως το δίκτυο 6LoWPAN αποτελείται από έναν γειτονικό δρομολογητή (border router) και από πολλούς κόμβους χαμηλής ισχύος. Οι κόμβοι συνδέονται από μια υπηρεσία cloud για την τροφοδοσία του αισθητήρα ή των δεδομένων ελέγχου. Τα τυπικά χαρακτηριστικά ενός LoWPAN είναι τα εξής:

1. **Περιορισμένη δυνατότητα επεξεργασίας (Limited processing capability):** διαφορετικοί τύποι και επεξεργαστές ταχύτητας ρολογιού ξεκινώντας από τα 8bit.
2. **Μικρή χωρητικότητα μνήμης (small memory capacity):** λίγα kilobytes της μνήμης RAM και ROM/flash αναμένεται να αναπτυχθεί στο μέλλον και γίνεται προσπάθεια να δημιουργηθεί η ελάχιστη απαραίτητη μνήμη.
3. **Χαμηλή Ισχύ (Low Power):** της τάξης των milliamperes.
4. **Σύντομη Εμβέλεια (Shorty Range):** ο προσωπικός χώρος λειτουργίας (personal operating space) ορίζεται από το IEEE 802.15.4 δίνει εύρος εμβέλειας 10 μέτρα. Για πραγματικές εφαρμογές μπορεί να φτάσει και πάνω από τα 100 μέτρα.
5. **Χαμηλό Κόστος (Low Cost):** αυτό οδηγεί σε ορισμένα από τα άλλα χαρακτηριστικά όπως χαμηλή επεξεργασία, χαμηλή μνήμη κλπ.

Όλοι αυτοί οι περιορισμοί που περιλαμβάνουν τους κόμβους αναμένεται στο μέλλον καθώς εξελίσσεται η τεχνολογία να αλλάξουν, αλλά σε σύγκριση με άλλα πεδία τα δίκτυα LoWPAN θα χρησιμοποιούν πάντα πολύ περιορισμένες συσκευές για να πετύχουν χαμηλές τιμές και μεγάλη διάρκεια ζωής [1].

Παρακάτω προσδιορίζονται τα χαρακτηριστικά των δικτύων LoWPANs όπου είναι οι περιορισμοί που καθοδηγούν των σύνολο των τεχνικών εργασιών. Αυτά είναι:

1. **Μικρό μέγεθος πακέτου (Small packet size):** δεδομένου ότι το μέγιστο πλαίσιο φυσικού στρώματος είναι 127 bytes, το μέγιστο μέγεθος πλαισίου στο επίπεδο ελέγχου πρόσβασης πολυμέσων είναι 102 octets. Η ασφάλεια στρώματος συνδέσμου επιβάλει μέγιστο 81 octets για τα πακέτα δεδομένων.
2. **Το IEEE 802.15.4 ορίζει διάφορες λειτουργίες διευθύνσεων:** επιτρέπει την χρήση των 64bit διευθύνσεων ή των 16bit μοναδικών διευθύνσεων στο προσωπικό δίκτυο (Personal Area Network).
3. **Χαμηλό εύρος ζώνης (Low bandwidth):** τα ποσοστά δεδομένων για κάθε ένα από τα φυσικά στρώματα που ορίζονται σήμερα είναι 250 kbps, 40 kbps, και 20kbps (2.4GHz, 915MHz και 868 MHz αντίστοιχα).
4. **Μεγάλος αριθμός συσκευών** αναμένεται να αναπτυχθεί κατά την διάρκεια της ζωής της τεχνολογίας. Η τοποθεσία των συσκευών δεν είναι συνήθως προκαθορισμένη, καθώς τείνουν να αναπτυχθούν κατά ad hoc τρόπο.
5. **Λειτουργία ύπνωσης (Sleeping mode):** οι συσκευές ενδέχεται να είναι σε κατάσταση “sleep” για μεγάλες χρονικές περιόδους προκειμένου να εξοικονομούν ενέργεια.

3.4.2 Η Χρήση του IP σε δίκτυα LoWPANs

Η χρήση του IP και συγκεκριμένα του IPv6, υιοθετείται ευρέως επειδή προσφέρει πολλά πλεονεκτήματα. Τα 6LoWPAN είναι δίκτυα LoWPAN που βασίζονται στο IPv6. Η εφαρμογή της τεχνολογίας IP και ειδικότερα η δικτύωση IPv6 θεωρείται ότι παρέχει τα ακόλουθα πλεονεκτήματα για το LoWPAN:

1. Οι τεχνολογίες που βασίζονται στην τεχνολογία IP ήδη υπάρχουν, είναι γνωστές, αποδεδειγμένα λειτουργούν και διατίθενται ευρέως. Αυτό επιτρέπει μία καλή λειτουργικότητα και εύκολη ανάπτυξη του επιπέδου εφαρμογής.
2. Οι συσκευές που βασίζονται στην τεχνολογία IP μπορούν εύκολα να συνδεθούν σε άλλα δίκτυα IP, χωρίς να χρειάζονται ενδιάμεσες οντότητες όπως πύλες μετάφρασης πρωτοκόλλων.
3. Η χρήση του IPv6 επιτρέπει μια τεράστια ποσότητα διευθύνσεων και παρέχει εύκολη αυτόματη διαμόρφωση παραμέτρων δικτύου (SLAAC). Αυτό είναι σημαντικό για τα δίκτυα 6LoWPAN όπου πρέπει να υποστηρίζεται από ένα μεγάλο αριθμό συσκευών.

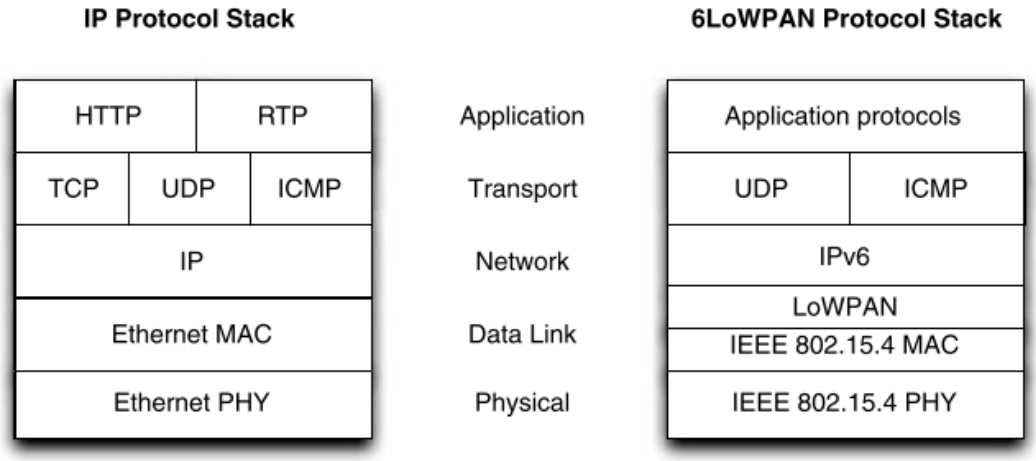
Χρησιμοποιώντας την επικοινωνία IP σε LoWPAN, δημιουργούνται ορισμένα ζητήματα που πρέπει να ληφθούν υπόψη. Αυτά είναι:

1. **Περιορισμένο μέγεθος πακέτου (Limited packet size):** οι εφαρμογές στο LoWPAN αναμένεται να δημιουργήσουν μικρά πακέτα. Η προσθήκη όλων των επιπέδων για συνδεσιμότητα IP θα πρέπει να επιτρέπει την μετάδοση σε ένα πλαίσιο, χωρίς να υπάρχει υπερβολικός κατακερματισμός και επανασυναρμολόγηση.
2. **Τοπολογίες (Topologies):** τα LoWPANs υποστηρίζουν διάφορες τοπολογίες όπως mesh, star. Οι τοπολογίες mesh δηλώνουν την δρομολόγηση multi-hop σε ένα επιθυμητό προορισμό Σε αυτήν την περίπτωση, οι ενδιάμεσες συσκευές δρουν ως προωθητές πακέτων στο στρώμα σύνδεσης. Οι τοπολογίες star περιλαμβάνουν την παροχή ενός υποσυνόλου συσκευών με λειτουργίες προώθησης πακέτων. Εάν εκτός από το IEEE 802.15.4 οι συσκευές αυτές χρησιμοποιούν άλλα είδη συνδέσεων δικτύου όπως το Ethernet ή το IEEE 802.11, ο στόχος είναι η ομαλή ενσωμάτωση των δικτύων που έχουν δημιουργηθεί πάνω σε αυτές τις διαφορετικές τεχνολογίες. Αυτό φυσικά είναι ένα κίνητρο για την χρήση της IP.
3. **Ανακάλυψη υπηρεσίας (Service discovery):** τα LoWPANs απαιτούν απλά πρωτόκολλα δικτύου για την εύρεση και τον έλεγχο των υπηρεσιών που παρέχονται από τις συσκευές.
4. **Ασφάλεια (Security):** το IEEE 802.15.4 επιβάλει την ασφάλεια του link-layer που βασίζεται στο AES (Advanced Encryption Standard) αλλά παραλείπει κάθε λεπτομέρεια σχετικά με θέματα όπως η διαχείριση κλειδιών καθώς και την ασφάλεια στα υψηλότερα επίπεδα. Φυσικά, μια ολοκληρωμένη λύση ασφαλείας για συσκευές LoWPAN για τις ανάγκες εφαρμογής πρέπει να εξεταστεί πολύ προσεκτικά.

3.4.3 Η Στοίβα Πρωτοκόλλου 6LoWPAN

Παρακάτω το σχήμα της εικόνας 21 δείχνει την στοίβα των πρωτοκόλλων IPv6 με 6LoWPAN σε σύγκριση με μια τυπική στοίβα πρωτοκόλλου IP και τα αντίστοιχα πέντε επίπεδα του Μοντέλου Διαδικτύου. Το Μοντέλο Διαδικτύου καθώς και το πρωτόκολλα Διαδικτύου συνδέει μια μεγάλη ποικιλία τεχνολογιών στρώματος συνδέσμων με πολλαπλά πρωτόκολλα

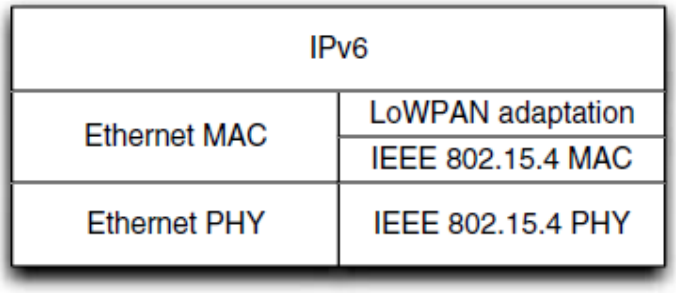
μεταφοράς και εφαρμογής. Μια απλή στοίβα πρωτοκόλλων IPv6 με 6LoWPAN είναι σχεδόν ίδια με μια κανονική στοίβα IP με κάποιες διαφορές.



Εικόνα 21: 6LoWPAN Protocol Stack (Πηγή: Research Gate)

Στην πράξη οι υλοποιήσεις της στοίβας 6LoWPAN σε ενσωματωμένες συσκευές συχνά εφαρμόζουν το στρώμα προσαρμογής LoWPAN μαζί με το IPv6, έτσι ώστε να μπορούν να παρουσιαστούν μαζί ως μέρος του στρώματος δικτύου (network layer). Το πιο συνηθισμένο πρωτόκολλο μεταφοράς που χρησιμοποιείται μαζί με το 6LoWPAN είναι το πρωτόκολλο User Datagram Protocol (UDP) [RFC 768] το οποίο μπορεί επίσης να συμπιεστεί χρησιμοποιώντας την μορφή LoWPAN. Η προσαρμογή μεταξύ του IPv6 και του LoWPAN εκτελείται από δρομολογητές που ονομάζονται δρομολογητές των «άκρων» (edge routers) [1].

Η προσαρμογή του LoWPAN σε ένα δρομολογητή άκρων τυπικά εκτελείται ως μέρος της σύνδεσης του δικτύου 6LoWPAN. Η εικόνα 22 απεικονίζει μια υλοποίηση ενός δρομολογητή άκρων με υποστήριξη 6LoWPAN. Μέσα στο LoWPAN, οι κεντρικοί υπολογιστές και οι δρομολογητές δεν χρειάζεται να λειτουργούν με πλήρεις μορφές κεφαλίδων IPv6 ή UDP σε οποιοδήποτε σημείο καθώς όλα τα συμπιεσμένα πεδία είναι γνωστά από κάθε κόμβο [3].

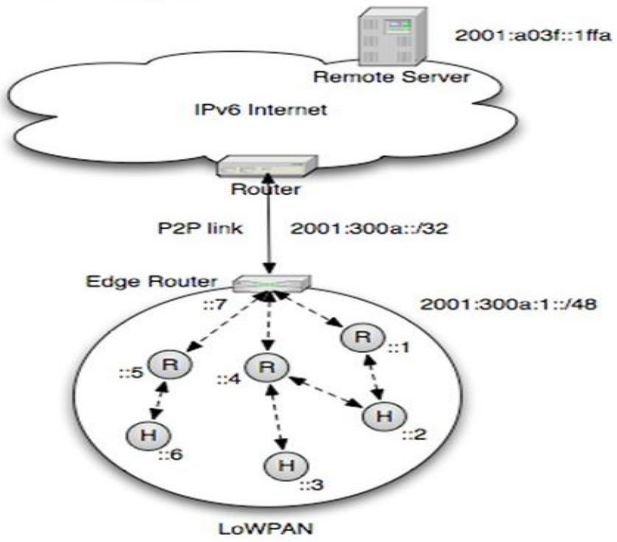


Εικόνα 22: IPv6 edge router with 6LoWPAN support (Πηγή: Research Gate)

3.4.4 Διευθυνσιοδότηση 6LoWPAN

Η διεύθυνση του 6LoWPAN διαφέρει από αυτήν του IPv6. Ουσιαστικά οι διευθύνσεις IPv6 συμπιέζονται για τους σκοπούς του 6LoWPAN. Έτσι το LoWPAN λειτουργεί με την ύπαρξη ενός επίπεδου χώρου διευθύνσεων, όπου αυτό σημαίνει ότι μέσα σε ένα ασύρματο δίκτυο υπάρχει μόνο ένα υποδίκτυο IPv6 εντός του οποίου υπάρχουν μοναδικές διευθύνσεις ελέγχου πρόσβασης πολυμέσων. Αυτές οι διευθύνσεις είναι των 64bit [3].

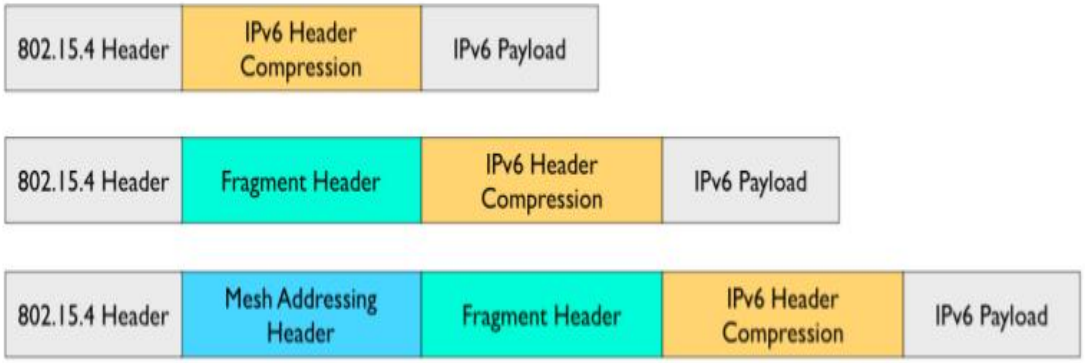
Η συμπίεση των διευθύνσεων IPv6 γίνεται με την παράδοση του προθέματος IPv, με την συμπίεση του IID (Interface Identifier) και την συμπίεση των διευθύνσεων multicast. Ουσιαστικά το παγκόσμιο πρόθεμα (global prefix) είναι γνωστό από όλους τους κόμβους του δικτύου. Στην εικόνα 23 παρουσιάζεται ένα παράδειγμα διευθυνσιοδότησης, όπου υπάρχει συνδεδεμένο ένα δίκτυο Internet IPv6 συνδεδεμένο μέσω ενός δρομολογητή και ενός δρομολογητή edge που υποστηρίζει το 6LoWPAN. Από αυτό το σημείο ασχολείται με την διευθυνσιοδότηση του δικτύου καθώς επίσης η διεύθυνση του δρομολογητή edge είναι κοινή σε ολόκληρο το δίκτυο του 6LoWPAN [1].



Εικόνα 23: 6LoWPAN addressing (Πηγή: Research Gate)

3.4.5 Στοίβες Επικεφαλίδας 6LoWPAN

Το 6LoWPAN πρωτόκολλο χρησιμοποιεί τρείς μορφές κεφαλίδας (όπως παρουσιάζονται στην εικόνα 24). Αυτές είναι: αποστολής (dispatch), πλέγματος (mesh), και κατακερματισμού (fragmentation). Η μορφή της κεφαλίδας προσδιορίζεται από το πεδίο 802.15.4 στην αρχή κάθε κεφαλίδας. Μειώνοντας το μέγεθος της κεφαλίδας, επιτυγχάνεται η εξοικονόμηση ενέργειας ανά πακέτο, η αύξηση της ωφέλιμης πληροφορίας και ο μέγιστος δυνατός περιορισμός του κόστους του κατακερματισμού [4].

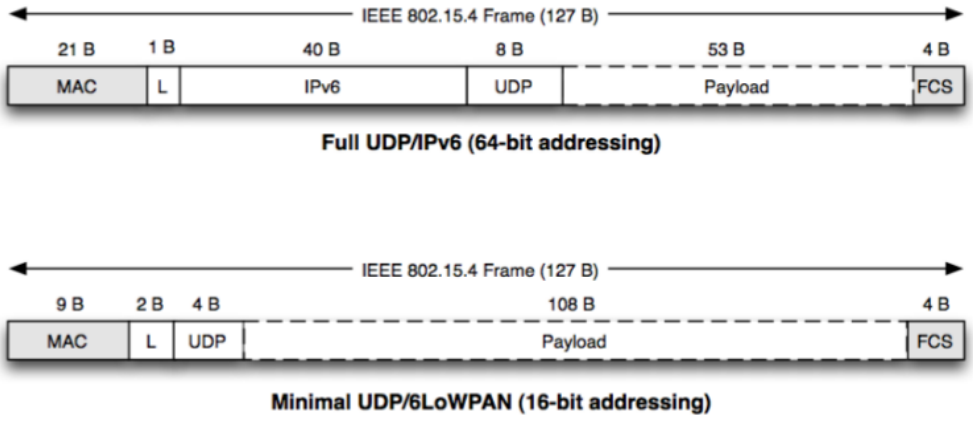


Εικόνα 24: 6LoWPAN Header Stacks (Πηγή: Research Gate)

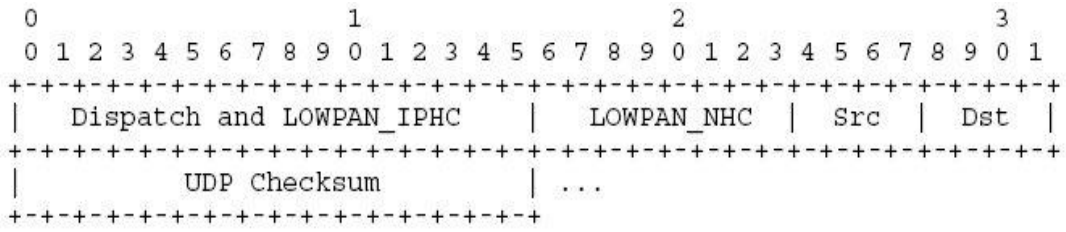
3.4.6 Μορφή Επικεφαλίδας 6LoWPAN

Η κύρια λειτουργία του 6LoWPAN είναι το στρώμα προσαρμογής LoWPAN, το οποίο επιτρέπει την συμπίεση του IPv6 καθώς και την παρακολούθηση των κεφαλίδων όπως το UDP (User Datagram Protocol) μαζί με τα χαρακτηριστικά κατακερματισμού και διευθυνσιοδότησης πλέγματος. Οι κεφαλίδες του 6LoWPAN ορίζονται στο [RFC 4944] το οποίο βελτιώθηκε και επεκτάθηκε αργότερα από το [ID-6Lowpan-hc]. Η συμπίεση 6LoWPAN είναι απλή και αξιόπιστη. Στηρίζεται σε κοινές πληροφορίες που είναι γνωστές σε όλους τους κόμβους που συμμετέχουν στο LoWPAN δίκτυο και στον χώρο διευθύνσεων IPv6 [3].

Η επικεφαλίδα LoWPAN αποτελείται από μια τιμή αποστολής που προσδιορίζει τον τύπο της επικεφαλίδας, ακολουθούμενη από ένα byte συμπίεσης επικεφαλίδας IPv6 που υποδεικνύει ποια πεδία είναι συμπιεσμένα. Εάν για παράδειγμα οι επικεφαλίδες επέκτασης UDP ή IPv6 ακολουθούν το IPv6 τότε αυτές οι επικεφαλίδες μπορεί επίσης να συμπιεστούν χρησιμοποιώντας την συμπίεση next-header [ID-6LoWPAN-hc]. Ένα παράδειγμα συμπιέσεως 6LoWPAN παρουσιάζεται στην εικόνα 25 όπου στο άνω πακέτο περιλαμβάνεται μια τιμή αποστολής LoWPAN για να υποδείξει το πλήρες IPv6 μέσω του IEEE 802.15.4 . Η εικόνα 26 παρουσιάζει ένα παράδειγμα 6LoWPAN/UDP με μία τιμή αποστολής και συμπίεση κεφαλίδας IPv6 (LOWPAN_NHC) σύμφωνα με το [ID-6LoWPAN-hc] (2bytes) [1].



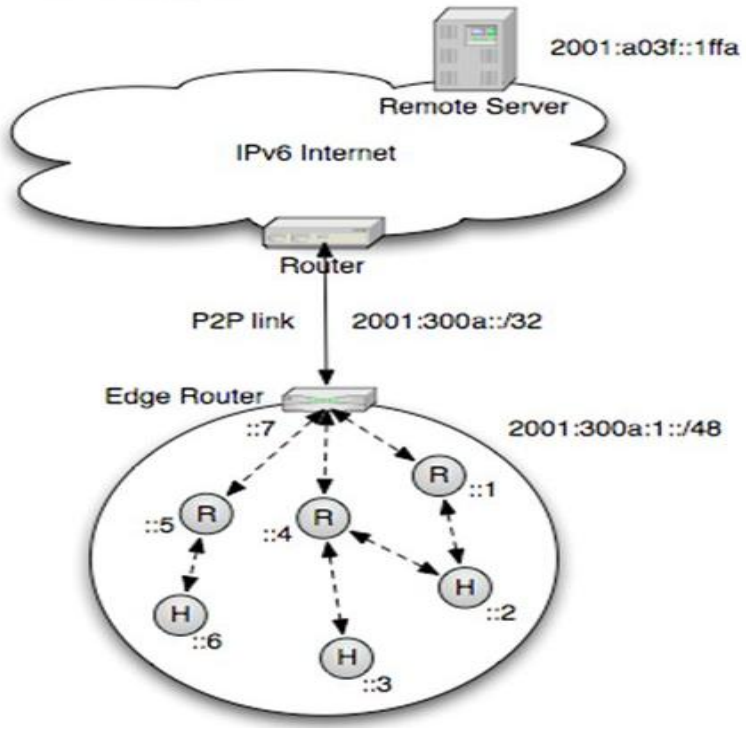
Εικόνα 25: 6LoWPAN Header Compression example (Πηγή: Research Gate)



Εικόνα 26: 6LoWPAN/UDP compressed headers (Πηγή: 6LoWPAN the wireless embedded internet)

3.4.7 Παράδειγμα 6LoWPAN Δικτύου

Σε αυτήν την ενότητα δίνεται ένα σύντομο παράδειγμα το πώς λειτουργεί ένα 6LoWPAN δίκτυο στην πράξη, εστιάζοντας στα βασικά πράματα που συμβαίνουν κατά την εκκίνηση και την λειτουργία. Η εικόνα 27 δείχνει ένα παράδειγμα ανάπτυξης ενός απλού δικτύου LoWPAN που συνδέεται μέσω μιας backhaul σύνδεσης στο internet IPv6. Το δίκτυο LoWPAN αποτελείται από έναν edge δρομολογητή, από τρεις (R) δρομολογητές και από τρεις δρομολογητές host (H). Επιπλέον υπάρχει ένας απομακρυσμένος διακομιστής στο Internet. Το δίκτυο LoWPAN βασίζεται πάνω στο IEEE 802.15.4 και χρησιμοποιεί την δρομολόγηση IP. Επίσης οι διευθύνσεις των κόμβων που περιλαμβάνονται στο σχήμα είναι ψεύτικες για να γίνει πιο κατανοητό το παράδειγμα (στην πραγματικότητα οι διευθύνσεις είναι πολύ μεγαλύτερες).

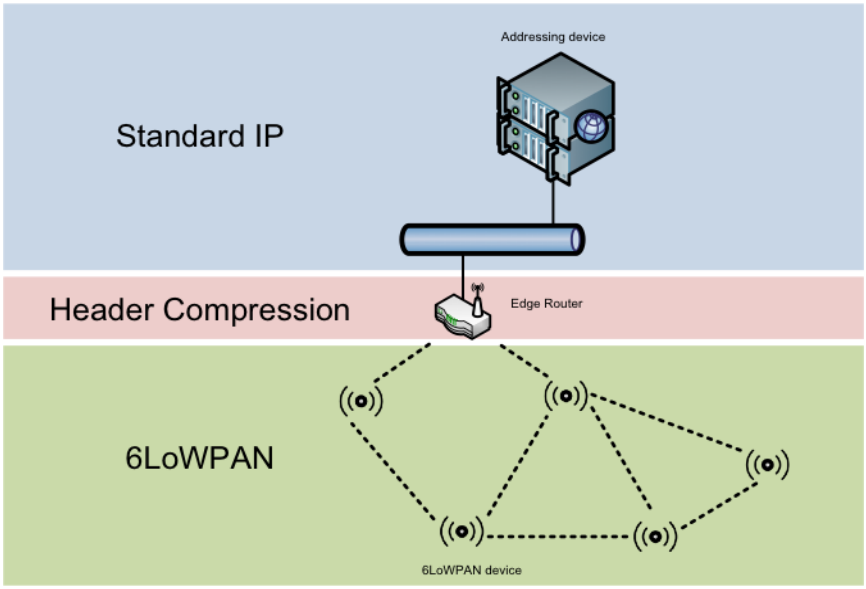


Εικόνα 27: 6LoWPAN Network Example (Πηγή: 6LoWPAN the wireless embedded internet)

Ο δρομολογητής στο internet διαφημίζει το πρόθεμα (prefix) IPv6 2001:300a::/48 στην ασύρματη σύνδεση IEEE 802.15.4. Σημειώνεται ότι η σύνδεση LoWPAN και backhaul βρίσκονται σε διαφορετικά υποδίκτυα καθώς χρησιμοποιείται το μοντέλο simple LoWPAN. Οι ασύρματες συσκευές IEEE 802.15.4 αναλαμβάνουν προεπιλεγμένες ρυθμίσεις καναλιού και κλειδιού ασφαλείας. Ο δρομολογητής edge ξεκινάει την διαφήμιση του προθέματος IPv6 το οποίο χρησιμοποιείται από τρείς δρομολογητές για την πραγματοποίηση της ανεπίσημης αυτόματης απόδοσης διεύθυνσης (SLAAC) για να εγγραφεί στον δρομολογητή edge χρησιμοποιώντας το 6LoWPAN-ND.

Κάθε κόμβος του LoWPAN δικτύου έχει μια διεύθυνση με ένα IID (Interface Identifier) 64bit και επιπλέον λαμβάνει μια διεύθυνση IPv6 που έχει παραχθεί με ένα IID 16bit από τον edge δρομολογητή κατά την εγγραφή του. Το τμήμα IID της διεύθυνσης IPv6 φαίνεται στην εικόνα 27, όπως για παράδειγμα, ::1 το οποίο έχει μια πλήρη διεύθυνση IPv6 του 2001:300a:1::1 . Στην πραγματικότητα, τα IID κατασκευάζονται από 16bit τυχαίους αριθμούς. Με την σειρά τους οι δρομολογητές διαφημίζουν το ίδιο πρόθεμα στους τρεις κεντρικούς υπολογιστές (hosts) οι οποίοι επίσης εγγράφονται στον δρομολογητή edge. Η τοπολογία του LoWPAN μπορεί να αλλάξει χωρίς να επηρεάζει τις IPv6 διευθύνσεις των κόμβων.

Η κίνηση του Neighbor Discovery (εντοπισμός γείτονα) χρησιμοποιείται για την προετοιμασία του αλγόριθμου δρομολόγησης και για την διαφήμιση των κόμβων. Στην εικόνα 27 οι διαδρομές δρομολόγησης φαίνονται με διακεκομμένες γραμμές. Οι διευθύνσεις προέλευσης και προορισμού IPv6 των κόμβων LoWPAN διευρύνονται κατά την διάρκεια της επικοινωνίας. Ένα πακέτο που αποστέλλεται σε ένα κόμβο στον ίδιο σύνδεσμο (π.χ. ::6 έως ::5) δεν απαιτεί καθόλου διευθύνσεις IPv6, καθώς η επικεφαλίδα στρώματος συνδέσμου περιέχει ήδη τις διευθύνσεις IEEE 802.15.4 προέλευσης και προορισμού. Όταν κάποιο πακέτο προωθείται σε πολλαπλά hops (multiple hops) τότε μόνο οι διευθύνσεις πηγής και προορισμού (π.χ. ::3 έως ::7) χρησιμοποιούνται για την δρομολόγηση του πακέτου. Τα πακέτα που προορίζονται εκτός από το LoWPAN δίκτυο περιλαμβάνουν είτε μια διεύθυνση προορισμού IPv6 είτε μια συμπιεσμένη διεύθυνση εάν το πλαίσιο συμπίεσης για αυτήν την διεύθυνση διαφημίζεται στο LoWPAN δίκτυο. Για παράδειγμα ο εξυπηρετητής LoWPAN host 2001:300a:1::6 μπορεί να στείλει ένα πακέτο στον απομακρυσμένο διακομιστή το 2001:a03f::1ffa. Ο δρομολογητής edge επεκτείνει τις συμπιεσμένες κεφαλίδες LoWPAN και IPv6 σε μια πλήρη κεφαλίδα IPv6 μαζί με την κεφαλίδα UDP. Τα εισερχόμενα πακέτα που επεξεργάζονται από τον δρομολογητή edge συμπιέζουν όσο το δυνατόν περισσότερο τις κεφαλίδες IPv6 και UDP.



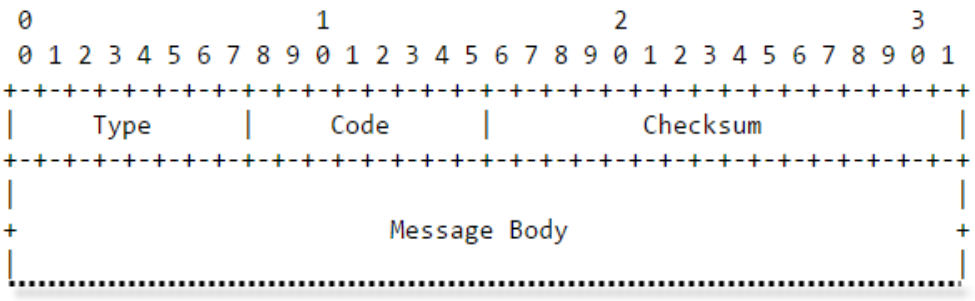
Εικόνα 28: 6LoWPAN Topology (Πηγή: embedded)

3.5 Το Πρωτόκολλο ICMPv6

Το πρωτόκολλο Μηνυμάτων Ελέγχου Διαδικτύου έκδοση 6 (Internet Control Message Protocol version 6, ICMPv6) αποτελεί αναπόσπαστο κομμάτι της IPv6 αρχιτεκτονικής και εκτελεί λειτουργίες αναφορών και διαγνωστικών σφαλμάτων (π.χ. ping) καθώς ορίζεται στο RFC 4443. Τα ICMPv6 μηνύματα μεταφέρονται μέσω IPv6 πακέτων που μπορούν να περιλάβουν και extended κεφαλίδες. Το ICMPv6 πρωτόκολλο προσφέρει μια ολοκληρωμένη λύση, προσφέροντας όλες τις διαφορετικές λειτουργίες των ICMP, ARP (Address Resolution Protocol) και IGMP (Internet Group Membership Protocol) πρωτοκόλλων, απλοποιώντας μάλιστα, την διαδικασία επικοινωνίας μέσω της εξάλειψης παλιών μηνυμάτων [1].

Το ICMPv6 πρωτόκολλο χρησιμοποιείται για πολλαπλές λειτουργίες, όπως για αναφορά σφαλμάτων σε επεξεργασία πακέτων, για αναφορά IPv6 multicast membership και για τις Neighbor Discovery λειτουργίες. Τα μηνύματα ICMPv6 χρησιμοποιούνται από το ping (packet internet gopher) πρωτόκολλο για τον έλεγχο επικοινωνίας. Τα μηνύματα ICMPv6 μπορούν να ταξινομηθούν σε δύο κατηγορίες:

1) **Μηνύματα Σφάλματος:** Τα ICMPv6 μηνύματα σφάλματος χωρίζονται σε τέσσερις κατηγορίες: αδυναμία πρόσβασης σε κάποιο προορισμό (Destination Unreachable), χρονικό όριο (Time Exceeded), πρόβλημα παραμέτρων (Parameter Problem) και πακέτο μεγάλο μεγέθους (Packet Too Big).
2) **Μηνύματα Πληροφοριών:** Τα ICMPv6 μηνύματα πληροφοριών χωρίζονται σε τρεις κατηγορίες: μηνύματα διάγνωσης, Neighbor Discovery μηνύματα και μηνύματα διαχείρισης των multicast μονάδων.



Εικόνα 29: ICMPv6 Πακέτο (Πηγή: IETF Tools, RFC 4443)

Τα πεδία του ICMPv6 πακέτου πιο αναλυτικά:

Τύπος: Δηλώνει το είδος του μηνύματος. Τιμές από 0-127 υποδεικνύει μήνυμα λάθους, ενώ από 128-255 υποδεικνύει μήνυμα ενημέρωσης.

Code: Εξαρτάται από τον τύπο του μηνύματος.

Checksum: Βοηθά στην ανίχνευση σφαλμάτων στο ICMPv6 μηνυμάτων.

Όταν ένα ICMPv6 μήνυμα συμπεριλαμβάνεται σε ένα IPv6 πακέτο, δεικνύεται με την τιμή 58 στο πεδίο Next Header της IPv6 κεφαλίδας. Στην εικόνα 30 παρουσιάζεται η λίστα με τους κωδικούς για κάθε τύπο ICMPv6 μηνυμάτων.

Type	Meaning	Type	Meaning
1	Destination Unreachable	138	Router Renumbering
2	Packet Too Big	139	ICMP Node Info. Query
3	Time Exceeded	140	ICMP Node Info. Response
4	Parameter Problem	141	Inverse Neighbor Solicitation
128	Echo Request	142	Inverse Neighbor Advertise.
129	Echo Reply	143	Multicast Listener Reports
130	Multicast Listener Query	144	Home Agent Request
131	Multicast Listener Report	145	Home Agent Reply
132	Multicast Listener Done	146	Mobile Prefix Solicitation
133	Router Solicitation (NDP)	147	Mobile Prefix Advertisement
134	Router Advertise. (NDP)	148	Certification Path Solicitation
135	Neighbor Solicitation (NDP)	149	Certification Path Advertise.
136	Neighbor Advertise. (NDP)	151	Multicast Router Advertise.
137	Redirect Message		

Εικόνα 30: ICMPv6 Τύποι Μηνυμάτων (Πηγή: Cisco Certification kits)

Όταν ένας κόμβος ICMPv6 λαμβάνει ένα πακέτο, αναλαμβάνει ενέργειες που εξαρτώνται από τον τύπο του μηνύματος. Το πρωτόκολλο ICMPv6 περιορίζει τον αριθμό των μηνυμάτων σφάλματος που στέλνονται στον ίδιο προορισμό για να αποφευχθεί η υπερφόρτωση δικτύου. Για παράδειγμα αν ένας κόμβος συνεχίζει να στέλνει εσφαλμένα πακέτα, το ICMP θα σηματοδοτήσει το σφάλμα στο πρώτο πακέτο και στην συνέχεια θα το κάνει περιοδικά, με μια καθορισμένη ελάχιστη περίοδο.

3.6 Το Πρωτόκολλο UDP

Το πρωτόκολλο Πακέτων Χρήστη (User Datagram Protocol, UDP) επιτρέπει στις εφαρμογές TCP/IP να ανταλλάσσουν μονοσήμαντα ανεξάρτητα μηνύματα πληροφορίας πάνω από ένα δίκτυο σε ένα περιβάλλον πολυεπεξεργασίας. Το πρωτόκολλο UDP προσφέρει μια μη αξιόπιστη υπηρεσία μεταφοράς χωρίς σύνδεση, χρησιμοποιώντας το πρωτόκολλο IP για την μεταφορά των μηνυμάτων. Δεν χρησιμοποιεί επιβεβαιώσεις, δεν αριθμεί τα μηνύματα και δεν ελέγχει την ροή τους. Έτσι ένα μήνυμα UDP μπορεί να χαθεί ή να φτάσει σε δύο αντίγραφα ή τα μηνύματα UDP να φτάσουν σε λανθασμένη σειρά. Επιπλέον τα μηνύματα UDP μπορεί να φθάσουν σε μια διεργασία συχνότερα από ότι αυτή μπορεί να τα επεξεργαστεί. Όλα τα παραπάνω σημαίνουν ότι μια εφαρμογή που χρησιμοποιεί το πρωτόκολλο UDP θα πρέπει η ίδια να λύσει το πρόβλημα της αξιοπιστίας.

Επίσης, ειδικά σε μεγάλα δίκτυα, είναι αρκετά πιθανό να συμβεί αναπάντεχος τερματισμός της σύνδεσης. Η έλλειψη των μηχανισμών αυτών το πρωτόκολλο UDP το καθιστά αρκετά πιο γρήγορο και αποτελεσματικό, τουλάχιστον για τις εφαρμογές εκείνες που δεν απαιτούν αξιόπιστη επικοινωνία.

Οι εφαρμογές audio και video streaming χρησιμοποιούν πακέτα UDP διότι είναι σημαντικό τα πακέτα να παραδοθούν στον παραλήπτη σε σύντομο χρονικό διάστημα ώστε να μην υπάρχει διακοπή στην ροή του ήχου ή της εικόνας. Επίσης το UDP υποστηρίζει broadcasting, δηλαδή την αποστολή ενός πακέτου σε όλους τους υπολογιστές ενός δικτύου καθώς και multicasting, δηλαδή την αποστολή ενός πακέτου σε κάποιους συγκεκριμένους υπολογιστές ενός δικτύου [12].

3.6.1 Διαφορές μεταξύ UDP και TCP

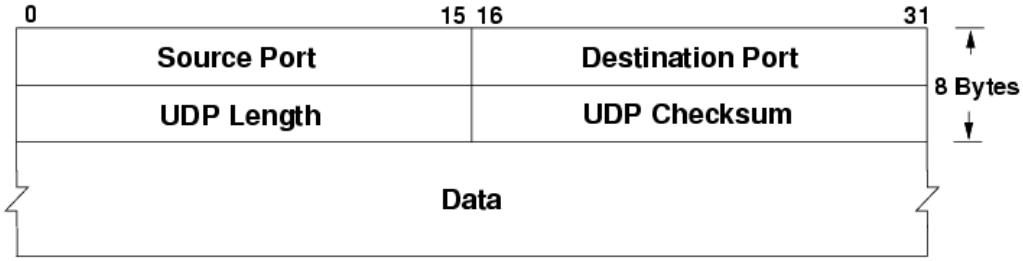
Αν και τα μειονεκτήματα του πρωτοκόλλου UDP είναι αρκετά όπως είδαμε παραπάνω, για αρκετές εφαρμογές το UDP θεωρείται καταλληλότερο από το TCP, για τους εξής λόγους:

- Δεν παρέχει εγκατάσταση σύνδεσης. Σε αντίθεση με την διαδικασία εγκατάστασης σύνδεσης που λαμβάνει χώρα στο TCP, το UDP απλά στέλνει απευθείας τα δεδομένα, χωρίς να προηγηθούν ειδικές διαδικασίες. Με αυτόν τον τρόπο το UDP δεν εισάγει καμία καθυστέρηση στην εγκατάσταση της σύνδεσης.
- Δεν διατηρεί κατάσταση σύνδεσης. Σε αντίθεση με το TCP που διατηρεί κατάσταση σύνδεσης στα τελικά συστήματα (ενταμιευτές αποστολής/λήψης, παράμετροι ελέγχου συμφόρησης και αριθμοί ακολουθίας και επιβεβαίωσης), το UDP δεν διατηρεί καμία κατάσταση. Για τον λόγο αυτό, κάποιος εξυπηρετητής υπεύθυνος για μια εφαρμογή μπορεί να εξυπηρετήσει πολλούς παραπάνω ενεργούς clients όταν η εφαρμογή τρέχει πάνω από UDP σε σχέση με το αν έτρεχε πάνω από το TCP.
- Έχει μικρή επικεφαλίδα. Το TCP segment έχει επικεφαλίδα των 20 bytes, ενώ το UDP χρησιμοποιεί μόνο 8 bytes για την επικεφαλίδα.
- Ο ρυθμός μετάδοσης δεν περιορίζεται ούτε επιβαρύνει λόγω ελέγχου των πακέτων. Το TCP έχει ένα μηχανισμό ελέγχου συμφόρησης, ο οποίος περιορίζει τον ρυθμό μετάδοσης, όταν παρατηρηθεί συμφόρηση σε κάποια ζεύξη μεταξύ αποστολέα και παραλήπτη. Ο περιορισμός αυτός μπορεί να έχει σοβαρές επιπτώσεις σε εφαρμογές πραγματικού χρόνου, οι οποίες είναι ανεκτικές σε απώλειες ορισμένων πακέτων,

αλλά απαιτούν ένα ελάχιστο ρυθμό μετάδοσης. Από την άλλη πλευρά, ο ρυθμός μετάδοσης στο UDP περιορίζεται μόνο από τον ρυθμό με τον οποίο η εφαρμογή παράγει δεδομένα, τις δυνατότητες της πηγής και το διαθέσιμο εύρος ζώνης. Ένα σημαντικό μέρος των δεδομένων UDP μπορεί να έχουν χαθεί λόγω υπερχείλισης.

3.6.2 Δομή UDP Πακέτου

Η δομή ενός πακέτου UDP περιγράφεται αναλυτικά στο αντίστοιχο πρότυπο IETF RFC 768. Στην στοίβα πρωτοκόλλων του διαδικτύου, το UDP βρίσκεται ανάμεσα στο επίπεδο δικτύου (network layer) και στο επίπεδο συνόδου (session layer) ή εφαρμογών (application layer). Παρακάτω στην εικόνα 31 φαίνονται τα πεδία της κεφαλίδας του UDP [17].



Εικόνα 31: Η επικεφαλίδα του πακέτου UDP (Πηγή: Wikimedia)

Ακολουθεί μια συνοπτική εξήγηση των πεδίων:
Source Port: η πόρτα του αποστολέα από την οποία προήλθε το πακέτο. Εάν ο παραλήπτης επιθυμεί να στείλει κάποια απάντηση, θα πρέπει να την στείλει στην πόρτα αυτήν. Το συγκεκριμένο πεδίο δεν είναι υποχρεωτικό και στις περιπτώσεις που δεν χρησιμοποιείται παίρνει την τιμή 0.
Destination Port: Η πόρτα του παραλήπτη στην οποία θα πρέπει να παραδοθεί το πακέτο.
Length: Το πεδίο length δηλώνει το μήκος του segment σε bytes μαζί με τη επικεφαλίδα
Checksum: Το πεδίο checksum είναι προαιρετικό και όταν χρησιμοποιείται εφαρμόζεται μόνο στην επικεφαλίδα IP και όχι στο πεδίο δεδομένων, το οποίο σε αυτήν την περίπτωση αποτελείται από την επικεφαλίδα UDP και τα δεδομένα του χρήστη.

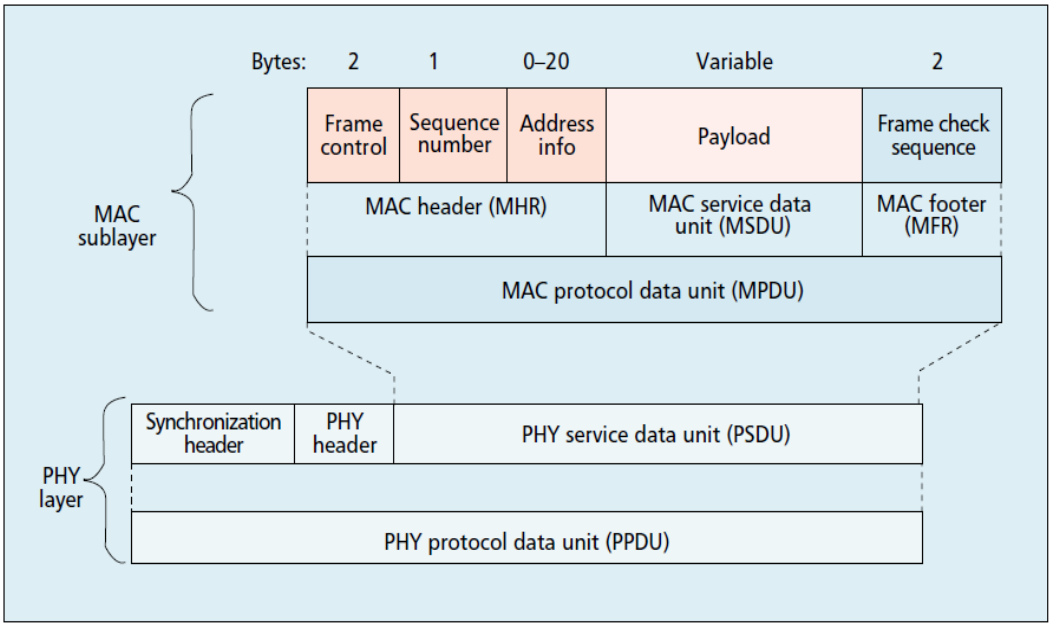
3.7 IEEE 802.15.4

Το IEEE 802.15.4 πρωτόκολλο καθορίζει τα physical και media access control (MAC) στρώματα για χαμηλού ρυθμού ασύρματων δικτύων προσωπικής περιοχής (LR-WPAN). Ένα LR-WPAN δίκτυο είναι ένα απλό, χαμηλού κόστους ασύρματης επικοινωνίας δίκτυο βελτιστοποιημένο για χρήση σε εφαρμογές με περιορισμένη ισχύ και περιορισμένες απαιτήσεις απόδοσης. Τα LR-WPAN δίκτυα σκοπεύουν την χαμηλή κατανάλωση ενέργειας και το χαμηλό κόστος, διατηρώντας παράλληλα αξιόπιστη μεταφορά δεδομένων, μικρής εμβέλειας σύνδεση, καθώς και απλό και ευέλικτο πρωτόκολλο. Ένα LR-WPAN δίκτυο μπορεί να λειτουργεί, είτε σε peer-to-peer τοπολογία, είτε σε star τοπολογία. Στην περίπτωση της peer-to-peer τοπολογίας, η

επικοινωνία μεταξύ δύο κόμβων είναι δυνατή εφόσον βρίσκονται εντός εμβέλειας. Αυτή η τοπολογία προσφέρει μεγαλύτερη ευελιξία από την star τοπολογία [11].

Η τοπολογία peer-to-peer χρειάζεται ένα PAN (Personal Area Network) συντονιστή. Είναι πιθανή η ζήτηση ενός κατάλληλου πρωτοκόλλου δρομολόγησης με πολλά άλματα σε περίπτωση που δύο κόμβοι δεν είναι στην σειρά. Στην περίπτωση star τοπολογίας η επικοινωνία όλων των συσκευών γίνεται μέσω του κεντρικού κόμβου ο οποίος είναι ένας PAN συντονιστής.

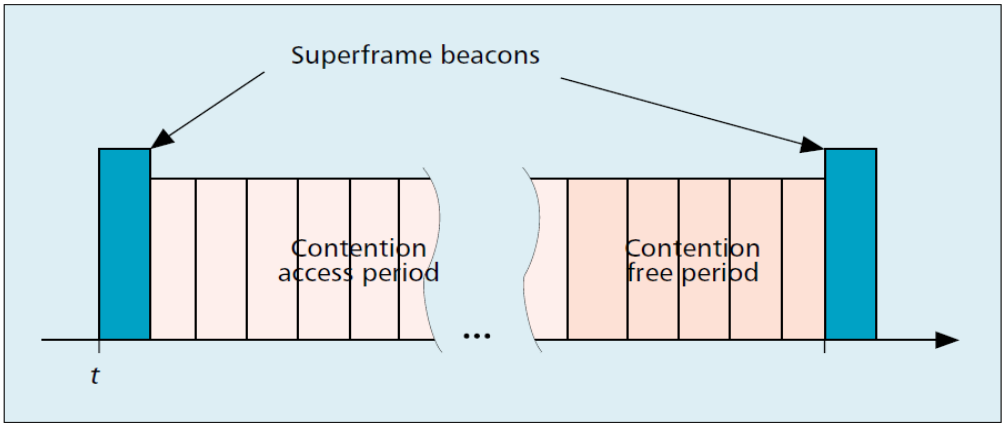
Η δομή του πλαισίου MAC είναι πολύ ευέλικτη για να ικανοποιεί τις ανάγκες των διαφορετικών εφαρμογών και τοπολογιών του δικτύου. Παρακάτω στην εικόνα 32 παρουσιάζεται η γενική μορφή πλαισίου MAC.



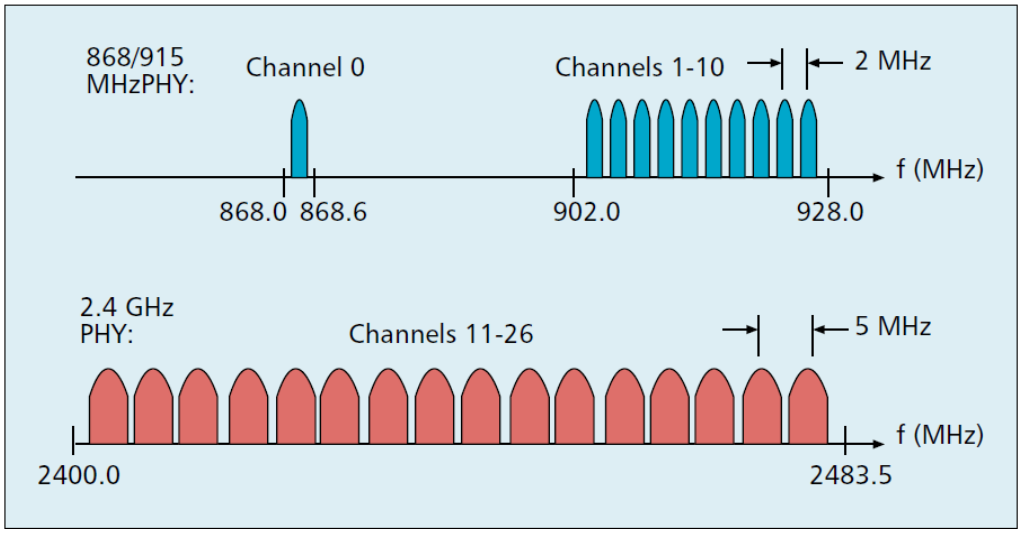
Εικόνα 32: Η γενική μορφή πλαισίου MAC (Πηγή: IEEE Communication Magazine, August 2002)

Το πλαίσιο MAC ονομάζεται μονάδα δεδομένων πρωτοκόλλου MAC (protocol data unit, MPDU) και αποτελείται από την κεφαλίδα (header) MAC (MHR), την μονάδα δεδομένων υπηρεσίας (MSDU) και από το footer MAC (MFR). Το πρώτο πεδίο της κεφαλίδας MAC είναι το πεδίο ελέγχου πλαισίου (frame control field) όπου δείχνει τον τύπο του πλαισίου MAC που μεταδίδεται, καθώς καθορίζει την μορφή του πεδίου διεύθυνσης και ελέγχει την επιβεβαίωση. Το μέγεθος του πεδίου διεύθυνσης μπορεί να κυμαίνεται από 0-20 bytes. Για παράδειγμα, ένα πλαίσιο δεδομένων μπορεί να περιέχει πληροφορίες πηγής και προορισμού, ενώ το πλαίσιο επιβεβαίωσης επιστροφής δεν περιέχει καθόλου πληροφορίες διεύθυνσης. Από την άλλη πλευρά ένα πλαίσιο beacon μπορεί να περιέχει μόνο πληροφορίες διεύθυνσης πηγής. Επιπλέον μπορεί να χρησιμοποιηθούν σύντομες διευθύνσεις συσκευών 8-bit ή διευθύνσεις συσκευών IEEE 64-bit. Το πεδίο ωφέλιμου φορτίου (payload field) είναι μεταβλητό σε μήκος. Ωστόσο, το πλήρες πλαίσιο MAC δεν μπορεί να υπερβαίνει τα 127-bytes σε μήκος. Τα δεδομένα που περιέχονται στο ωφέλιμο φορτίο εξαρτώνται από τον τύπο του πλαισίου.

Το IEEE 802.15.4 MAC έχει τέσσερις διαφορετικούς τύπους πλαισίων. Αυτά είναι το πλαίσιο beacon, το πλαίσιο δεδομένων (data frame), το πλαίσιο επιβεβαίωσης (acknowledgment frame) και το πλαίσιο εντολών MAC. Μόνο το πλαίσιο δεδομένων και beacon περιέχουν πληροφορίες που στέλνονται από ανώτερα στρώματα. Άλλα πεδία σε ένα πλαίσιο MAC είναι ο αριθμός ακολουθίας (sequence number) και η ακολουθία ελέγχου πλαισίου (Frame Check Sequence). Ο αριθμός ακολουθίας στην κεφαλίδα MAC αντιστοιχεί στο πλαίσιο επιβεβαίωσης με την προηγούμενη μετάδοση. Η συναλλαγή θεωρείται επιτυχής μόνο όταν το πλαίσιο επιβεβαίωσης περιέχει τον ίδιο αριθμό ακολουθίας με το προηγούμενο μεταδιδόμενο πλαίσιο. Το FCS συμβάλει στην επαλήθευση της ακεραιότητας του πλαισίου MAC. Ορισμένες εφαρμογές ενδέχεται να απαιτούν αποκλειστικό εύρος ζώνης για να πετύχουν χαμηλές περιόδους λειτουργίας. Για να γίνει αυτό το IEEE 802.15.4 LR-WPAN μπορεί να λειτουργήσει σε μια προαιρετική λειτουργία superframe, όπου ο συντονιστής δικτύου PAN μεταδίδει superframe beacons σε προκαθορισμένα χρονικά διαστήματα [11].



Εικόνα 33: Η δομή superframe ενός LR-WPAN (Πηγή: IEEE Communication Magazine, August 2002)



Εικόνα 34: Η δομή καναλιού του IEEE 802.15.4 (Πηγή: IEEE Communication Magazine, August 2002)

Όπως φαίνεται στην εικόνα 34 είκοσι επτά κανάλια συχνότητας είναι διαθέσιμα στις τρεις ζώνες. Το PHY 868/915 MHz υποστηρίζει ένα μόνο κανάλι μεταξύ 868,0 και 868,6 MHz και

δέκα κανάλια μεταξύ 902,0 και 928,0 MHz. Λόγω της περιφερειακής υποστήριξης για αυτές τις δύο ζώνες, είναι απίθανο ένα και μόνο δίκτυο να χρησιμοποιεί πάντα και τα έντεκα κανάλια. Ωστόσο οι δύο ζώνες θεωρούνται αρκετά κοντά στην συχνότητα, που αυτό σημαίνει ότι παρόμοιο, αν όχι ταυτόσημο υλικό μπορεί να χρησιμοποιηθεί και για τις δύο (ζώνες), μειώνοντας έτσι το κόστος κατασκευής. Το PHY 2,4 GHz υποστηρίζει 16 κανάλια μεταξύ 2,4 και 2,4835 GHz με επαρκή απόσταση καναλιών (5 MHz) που στοχεύει στην διευκόλυνση των απαιτήσεων φιλτραρίσματος και μετάδοσης.

3.7.1 Τεχνολογία ZigBee

Το ZigBee στα ασύρματα δίκτυα προσωπικού χώρου (WPANs) είναι μία τεχνολογία που προέκυψε από την εταιρία ZigBee Alliance και την επιτροπή IEEE 802.15.4. Η σύνδεση των συσκευών πραγματοποιείται με χαμηλό κόστος, χαμηλή κατανάλωση ενέργειας και απευθύνεται σε εφαρμογές όπου γίνεται απομακρυσμένος έλεγχος. Η τεχνολογία ZigBee δεν χρησιμοποιεί υψηλές ταχύτητες μεταφοράς δεδομένων, όπως για παράδειγμα η τεχνολογία Bluetooth. Εφαρμόζεται σε ραδιοσυχνότητες (RF) που απαιτούν χαμηλό αριθμό μεταφοράς δεδομένων και προσφέρει μεγάλη διάρκεια ζωής στις μπαταρίες από 2 έως 5 έτη, με εξασφαλισμένη δικτύωση. Οι ZigBee ασύρματοι κόμβοι μεταδίδουν σε εμβέλεια από 10 έως 75 μέτρα, εξαρτώμενη από την κατανάλωση ισχύος που χρειάζεται κάποια εφαρμογή. Τέτοιου τύπου κόμβοι που δεν χρειάζονται άδεια λειτουργίας εκπέμπουν στις εξής συχνότητες: 2.400-2.484 GHz, 902-928 MHz και 868.0-868.6 MHz. Ένα ZigBee δίκτυο χρησιμοποιεί ψηφιακούς πομπούς για την δυνατότητα επικοινωνίας μεταξύ των διαφόρων κόμβων που βρίσκονται διάσπαρτες σε ένα χώρο. Ένας από τους κόμβους αυτούς δουλεύει ως συντονιστής, γνωρίζοντας όλους τους κόμβους του συγκεκριμένου δικτύου και διαχειρίζεται τα πακέτα που ανταλλάσσονται μεταξύ των κόμβων. Τα ZigBee δίκτυα έχουν δύο λειτουργίες: την λειτουργία περιοδικής εκπομπής ενός σήματος συντονισμού και την λειτουργία μη εκπομπής. Στην περίπτωση της λειτουργίας περιοδικής εκπομπής ο κόμβος συντονιστής αφυπνίζει όλους τους κόμβους του δικτύου, οι οποίοι πρέπει να τον ενημερώσουν αν υπάρχει μήνυμα για προώθηση, στέλνοντας περιοδικά μηνύματα. Στην περίπτωση της λειτουργίας μη εκπομπής, όταν δεν στέλνονται περιοδικά μηνύματα αφύπνισης από τον κόμβο συντονιστή, το δίκτυο είναι λιγότερο συντονισμένο, καθώς κάθε κόμβος εκπέμπει ένα σήμα το οποίο πρέπει να παραδοθεί στον συντονιστή κόμβο μέσω των ενδιάμεσων κόμβων στο δίκτυο. Έτσι ο συντονιστής πρέπει να είναι σε συνεχή λειτουργία για να είναι έτοιμος να ανταποκριθεί σε οποιοδήποτε σήμα, έχοντας αυξανόμενη κατανάλωση ενέργειας. Σε όλες τις περιπτώσεις που ένα δίκτυο αποτελείται από κόμβους που ενσωματώνουν το IEEE 802.15.4 πρωτόκολλο διατηρείται χαμηλή κατανάλωση ισχύος, λόγω της πλειοψηφίας των κόμβων του δικτύου που παραμένουν σε κατάσταση ύπνου (sleep mode) για μεγάλα χρονικά διαστήματα. Αξιολογώντας την τεχνολογία ZigBee, παρουσιάζονται πολλά πλεονεκτήματα, με κύριο πλεονέκτημα την ικανότητα ρύθμισης ενός δικτύου πλέγματος με τους ασύρματους κόμβους του να είναι βιώσιμοι μόνο με μπαταρία για μερικά χρόνια. Ένα από τα σημαντικά στοιχεία είναι ότι σε σχέση με την τεχνολογία Bluetooth, έχει καλύτερη διαχείριση ενέργειας υποστηρίζει περισσότερους κόμβους και επιτρέπει στις συσκευές να ενώνονται πιο γρήγορα στο δίκτυο. Επίσης η τεχνολογία ZigBee για τα WPAN-LR δίκτυα έχει μέγιστο ρυθμό μετάδοσης δεδομένων 250Kbps [11].

ΚΕΦΑΛΑΙΟ 4

Βασικές Αρχές του Πρωτοκόλλου RPL

4.1 Αρχικοί Στόχοι της ομάδας Εργασίας ROLL

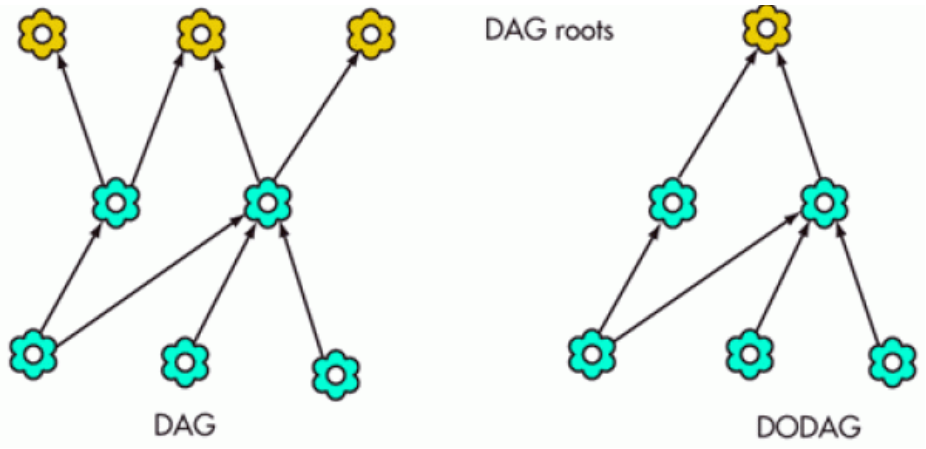
Το πρωτόκολλο RPL έχει φτιαχτεί για την αντιμετώπιση του θέματος δρομολόγησης ασύρματων αισθητήρων όπου δημιουργήθηκε από την ομάδα εργασίας (Routing over Low-power and Lossy networks) για να καθορίσει ένα ολοκληρωμένο πρωτόκολλο δρομολόγησης το οποίο θα μπορούσε να δρομολογήσει αποτελεσματικά τα δεδομένα μέσω των LLNs δικτύων [9]. Η ομάδα ROLL επικεντρώθηκε κυρίως στον καθορισμό των απαιτήσεων δρομολόγησης για τα ακόλουθα σενάρια δημιουργώντας παράλληλα το πρωτόκολλο RPL. Τα σενάρια αυτά είναι βιομηχανικά, οικιακά ή κτιριακά και αστικά συνδεδεμένα δίκτυα αισθητήρων. Ορισμένα από τα βασικά χαρακτηριστικά που έλαβε υπόψη η ομάδα αυτή ήταν η υψηλή αξιοπιστία, επιτρέποντας λειτουργία χαμηλής ισχύος με πολύ μέτρια μνήμη σε δίκτυα που ενδεχομένως περιλαμβάνουν πολύ μεγάλο αριθμό (αρκετές χιλιάδες) κόμβων. Στην προσπάθεια για δημιουργία απαιτητικής δρομολόγησης η ομάδα ROLL εξέτασε κάποιες πτυχές κινητικότητας μέσα σε ένα LLN δίκτυο. Η δρομολόγηση για ασφάλεια και διαχειρισιμότητα ήταν σημαντική, όπως και τα χαρακτηριστικά μεταφοράς που θα αντιμετωπίσουν τα μηνύματα ελέγχου (control messages) [8].

4.2 Το Πρωτόκολλο RPL

Για την δρομολόγηση σε περιβάλλοντα με περιορισμένη ενέργεια-LLNs χρειάζεται ειδική μεταχείριση αφού τα είδη υπάρχοντα πρωτόκολλα μπορεί να μην καλύπτουν τις απαιτήσεις. Γι’ αυτό τον λόγο αναπτύχθηκε το πρωτόκολλο RPL (IPv6 Routing Protocol for LLNs) το οποίο χαρακτηρίζεται ως distance vector (χρήση Bellman-Ford αλγόριθμου), λειτουργεί με IPv6 και πρέπει να έχει χαμηλή κατανάλωση, κάτι το οποίο έρχεται σε αντίθεση με την ανάγκη διάδοσης πληροφοριών δρομολόγησης σε ταχύ χρόνο.

Βασικό χαρακτηριστικό του πρωτοκόλλου είναι η δυνατότητα ανάκαμψης από συνδέσεις που δεν είναι πλέον διαθέσιμες, το οποίο μπορεί να συμβεί σε περιβάλλοντα με δύσκολες συνθήκες και παρεμβολές. Αυτό γίνεται για επίτευξη αξιοπιστίας και υλοποιείται διατηρώντας πολλές διαδρομές για έναν προορισμό αντί για έναν [2].

Επιπλέον, σε αντίθεση με άλλα πρωτόκολλα, το RPL δεν υπολογίζει τα κόστη των διαδρομών στατικά αλλά περιλαμβάνει δυναμικές μετρικές συνδέσμων για τον καθορισμό της αξιοπιστίας (όπως μέγιστο αριθμό μεταδόσεων). Το πρωτόκολλο RPL υποστηρίζει τον υπολογισμό και εγκατάσταση μονοπατιών δρομολόγησης ενώ οι κόμβοι που το χρησιμοποιούν μπορούν να ανακαλύπτουν, να υπολογίζουν και να εγκαθιστούν διαδρομές (routes) αυτόνομα. Οι κόμβοι σχηματίζουν Directed Acyclic Graphs (DAGs), δηλαδή γράφους που δεν σχηματίζουν κύκλους, οι οποίοι επιτρέπουν σε κάθε κόμβο να επιλέγει και να διατηρεί άλλους κόμβους ως πιθανούς πατέρες (fathers) στο δένδρο (μπορεί και περισσότερους του ενός) για την δρομολόγηση μέσα στο RPL δίκτυο προς την ρίζα του δικτύου (root).



Εικόνα 35: Destination oriented direct acyclic graph (Πηγή: Electronic Design)

Το RPL υποστηρίζει τρία πρότυπα κίνησης:

1) **Multipoint-to-point (MP2P):** Κίνηση πληροφοριών μεταξύ πολλών κόμβων προς την ρίζα του γράφου.
2) **Point-to-multipoint (P2MP):** Κίνηση μεταξύ ενός κόμβου και πολλών.
3) **Point-to-point (P2P):** Κίνηση που ανταλλάσσεται μεταξύ δύο κόμβων.

Στα LLNs δίκτυα είναι πολύ συνηθισμένο όταν πρόκειται για M2P και P2MP η κίνηση προς και από ένα σημείο εξόδου. Κόμβοι που έχουν το ρόλο του Low Power and lossy network Border Router (LBR) μπορούν τυπικά να αποτελούν τη ρίζα σε ένα τέτοιο δίκτυο [8].

4.3 Εφαρμογές Ανοικτού Κώδικα του RPL

Υπάρχουν ορισμένες εφαρμογές ανοικτού κώδικα του RPL, όπου υλοποιούν διάφορες λειτουργίες, και δίνουν στον χρήστη την ελευθερία να τρέξει πολλά πράματα για οποιονδήποτε σκοπό, να μελετήσει και να τροποποιήσει το λογισμικό έχοντας πρόσβαση στον πηγαίο κώδικα του και να διανέμει αντίγραφα του προγράμματος είτε είναι τροποποιημένο είτε όχι [3].

Μερικά πλεονεκτήματα ανοικτού κώδικα είναι η σταθερότητα και η αξιοπιστία που αναφέρεται στο διάστημα που μεσολαβεί μεταξύ δύο αποτυχιών του συστήματος. Όσο μεγαλύτερο το διάστημα, τόσο πιο αξιόπιστο είναι το σύστημα. Επίσης σημαντικό πλεονέκτημα είναι η ασφάλεια λόγω της δυνατότητας για ελεύθερη πρόσβαση, διόρθωση λαθών και σφαλμάτων όπου μπορεί να εντοπίσουν κάποιοι χρήστες. Εφόσον ο κώδικας είναι ανοικτός δίνεται η δυνατότητα τροποποίησης, βελτίωσης και επέκτασής του. Ορισμένες εφαρμογές ανοικτού κώδικα του RPL διατυπώνονται παρακάτω.

4.3.1 Tiny OS

Το Tiny OS είναι ίσως το πρώτο λειτουργικό σύστημα όπου βασίζεται σε ένα event-driven μοντέλο προγραμματισμού αντί multithreading. Τα Tiny OS προγράμματα αποτελούνται από μηχανισμούς χειρισμού συμβάντων και εργασιών με run-to-completion σημασιολογία. Όταν ένα εξωτερικό συμβάν όπως ένα εισερχόμενο πακέτο δεδομένων ή μια ανάγνωση του αισθητήρα, το Tiny OS σηματοδοτεί τον κατάλληλο χειρισμό συμβάντων ώστε να χειριστούν

την εκδήλωση. Οι χειριστές των συμβάντων μπορούν να δημοσιεύσουν εργασίες που έχουν προγραμματιστεί από τον πυρήνα (core) του Tiny OS. Λαμβάνοντας υπόψη τις νέες προκλήσεις που θέτουν τα δίκτυα χαμηλής κατανάλωσης ενέργειας το Tiny OS υποστηρίζει το πρωτόκολλο δρομολόγησης RPL με την πλατφόρμα Tiny RPL που βρίσκεται στο αρχείο tos/lib/rpl [9].

4.3.2 Contiki OS

Το Contiki OS είναι ελαφρύ λειτουργικό σύστημα σχεδιασμένο για περιβάλλοντα με συσκευές περιορισμένης ενέργειας. Υποστηρίζει τα τυποποιημένα πρωτόκολλα IETF καθώς επίσης και το πρωτόκολλο δρομολόγησης RPL όπου βρίσκεται στο αρχείο contiki/core/net/rpl. Μπορεί να υποστηρίξει preemptive multithreading ανά διαδικασία (ως βιβλιοθήκη όπου είναι απαραίτητο). Είναι φτιαγμένο σε event-driven πυρήνα και πάνω του μπορούν να τρέχουν προγράμματα με νήματα χωρίς την ανάγκη για μνήμη (στοίβα) ανά νήμα, λόγω των Protothreads. Αποτελείται από τον πυρήνα (core), τις βιβλιοθήκες (libraries), τον φορτωτή προγραμμάτων και τις διαδικασίες. Ο πυρήνας (core) αποτελείται από τις βασικές υπηρεσίες και τα φορτωμένα προγράμματα [5].

Στον πυρήνα τα προγράμματα που εκτελούνται ενεργοποιούνται είτε από γεγονότα που αποστέλλονται από τον πυρήνα είτε μέσω του μηχανισμού polling. Ο πυρήνας υποστηρίζει σύγχρονα και ασύγχρονα γεγονότα. Ο μηχανισμός polling αφορά στα γεγονότα με υψηλή προτεραιότητα τα οποία θέτονται ανάμεσα στα ασύγχρονα γεγονότα. Ο πυρήνας χρησιμοποιεί μία μόνο μοιρασμένη στοίβα για όλες τις διεργασίες που εκτελούνται. Το υπόλοιπο σύστημα εκτός του πυρήνα αποτελείται από βιβλιοθήκες συστήματος που συνδέονται προαιρετικά με προγράμματα. Τα προγράμματα μπορούν να συνδέονται με βιβλιοθήκες με 3 διαφορετικούς τρόπους: 1) στατική σύνδεση με βιβλιοθήκες που είναι μέρος του πυρήνα, 2) στατική σύνδεση με βιβλιοθήκες που είναι μέρος ενός προγράμματος που μπορεί να φορτωθεί και 3) τα προγράμματα μπορεί να είναι υπηρεσίες που υλοποιούν μια συγκεκριμένη βιβλιοθήκη. Όταν ένα πρόγραμμα φορτώνεται στο σύστημα, ο φορτωτής προγραμμάτων υλοποιεί την κατανομή επαρκούς μνήμης σε αυτό και αν αυτή η διαδικασία αποτύχει, το πρόγραμμα δεν φορτώνεται.

Αν τελικά φορτωθεί, ο φορτωτής καλεί την μέθοδο έναρξης του προγράμματος η οποία μπορεί να εκκινήσει ή να αντικαταστήσει μια ή περισσότερες διαδικασίες. Το Contiki είναι ένα λογισμικό ανοικτού κώδικα με ενεργή κοινότητα, διαρκή εξέλιξη και έτοιμα παραδείγματα. Επίσης κάνει χρήση προτύπων όπως IPv6, IPv4, 6LoWPAN και RPL. Επιπλέον παρέχει στον χρήστη περιβάλλον εξομοίωσης το οποίο επιτρέπει την δημιουργία κώδικα χωρίς την ανάγκη υλικού, άρα με μηδενικό κόστος. Η φορητότητα είναι βασικό χαρακτηριστικό του συγκεκριμένου συστήματος αφού μπορεί να τρέξει σε πληθώρα συστημάτων και πλατφόρμων. Κατά την εκτέλεση κώδικα στην διάρκεια των πειραμάτων είναι δυνατή η αλλαγή παραμέτρων, ακόμα και η προσθαφαίρεση κόμβων, χωρίς να υπάρχει ανάγκη επανέναρξης του πειράματος [9].

Οι διαδικασίες του Contiki είναι τα Protothreads και χρησιμοποιείται από το Contiki σαν μια μέση διαδρομή μεταξύ των event-driven και των preemptive-multithreading συστημάτων. Έτσι αποφεύγεται η δέσμευση μνήμης του preemptive-multithreading, χρησιμοποιούνται event-handlers (δείγμα event-driven συστήματος) αλλά και επιτρέπεται η υλοποίηση while() βρόχων και if(). Όλες οι διαδικασίες μοιράζονται τον ίδιο χώρο διευθύνσεων και κάθε

διαδικασία ορίζεται από μια event handler μέθοδο και μια poll handler μέθοδο. Η κατάσταση της διαδικασίας κρατείται στην ιδιωτική μνήμη της και ο πυρήνας απλώς διατηρεί ένα δείκτη στην κατάσταση αυτή. Η επικοινωνία μεταξύ των διαδικασιών γίνεται με γεγονότα μέσω του πυρήνα. Οι εφαρμογές που χρησιμοποιούν μια υπηρεσία χρησιμοποιούν μια βιβλιοθήκη (stub library) η οποία χρησιμοποιεί το στρώμα υπηρεσιών για να βρει την διαδικασία υπηρεσίας.

Το Cooja είναι το περιβάλλον εξομοίωσης ασύρματων δικτύων αισθητήρων που υποστηρίζει το Contiki. Κατά την εκτέλεσή του, το περιβάλλον αυτό μπορεί να εμφανίζει το δίκτυο αισθητήρων που εξομοιώνεται, τα γεγονότα επικοινωνίας της εξομοίωσης στην μονάδα του χρόνου και τις εκτυπώσεις των συριακών θυρών από όλους τους αισθητήρες. Στα πλεονεκτήματα χρήσης του τοποθετείται η δυνατότητα μελέτης και συμπεριφοράς ενός συγκεκριμένου συστήματος και η παρακολούθηση πιθανών αλληλεπιδράσεων σε ασφαλές περιβάλλον. Σημαντικό πλεονέκτημα είναι πως μπορεί να εξομοιωθεί λογισμικό που με τοποθέτηση υλικού μπορεί να τρέξει με τον ίδιο ακριβώς τρόπο, ενώ ο χρήστης έχει δυνατότητα να φορτώσει σε κάθε κόμβο όποιο κώδικα επιθυμεί (ή σε πολλούς κόμβους τον ίδιο κώδικα, αν πρόκειται για ομάδα αισθητήρων που μετρούν το ίδιο μέγεθος). Κάθε φορά που ο χρήστης επιθυμεί την μεταγλώττιση κάποιου κώδικα, η μεταγλώττιση διεξάγεται για την πλατφόρμα που διαλέγει, με την συγκεκριμένη αρχιτεκτονική και φορτώνεται τελικά στον κόμβο.

Τέλος στο Contiki μπορεί να χρησιμοποιηθεί το ελεύθερο και ανοικτού κώδικα λογισμικό ανάλυσης πρωτοκόλλων δικτύου το Wireshark, όπου παρατηρείται η ακολουθία των μηνυμάτων που ανταλλάσσουν μεταξύ τους οι κόμβοι στην εξομοίωση. Ο packet sniffer αποτελεί το βασικό εργαλείο για την παρατήρηση αυτών των μηνυμάτων καθώς αποθηκεύει και απεικονίζει τα περιεχόμενα διάφορων πεδίων πρωτοκόλλων που περιέχονται στα μηνύματα που συλλαμβάνονται από τους κόμβους.

4.4 Τοπολογία RPL

4.4.1 DODAG

Οι κόμβοι του πρωτοκόλλου RPL χρησιμοποιούν την DODAG (Destination-oriented directed acyclic graph) όπου αυτή είναι μια DAG τοπολογία με ρίζες (roots) προς μια κατεύθυνση. Η ρίζα DODAG μπορεί να λειτουργήσει σαν border router για την τοπολογία DODAG. Ειδικότερα μπορεί να συγκεντρώνει τις διαδρομές DODAG και να τις μοιράζει σε άλλα πρωτόκολλα δρομολόγησης. Η κατασκευή του γράφου αρχίζει από τον sink (ρίζα του γράφου). Ο sink αρχικά θα στείλει ένα μήνυμα τύπου DIO σε όσους κόμβους βρίσκονται στην εμβέλειά του. Ένας κόμβος που θα λάβει το μήνυμα DIO, θα αποφασίσει με βάση την objective function αν θα ενταχθεί στον γράφο ή όχι. Όταν ο κόμβος ενταχθεί στον γράφο, τότε θα έχει ένα μονοπάτι προς τον sink, ο οποίος αποτελεί τον γονέα του. Ακολούθως, ο κόμβος θα υπολογίσει τον βαθμό (rank) που έχει στον γράφο. Αφού γίνει ο υπολογισμός του rank, ο κόμβος θα στείλει μήνυμα DIO σε όσους κόμβους βρίσκονται στην εμβέλεια του διαφημίζοντας τον γράφο. Όταν η κατασκευή του γράφου ολοκληρωθεί, κάθε κόμβος θα έχει ορισμένο έναν γονέα και έτσι θα μπορεί να στείλει πακέτα στον sink προωθώντας τα στον γονέα του [12].

4.4.2 Rank

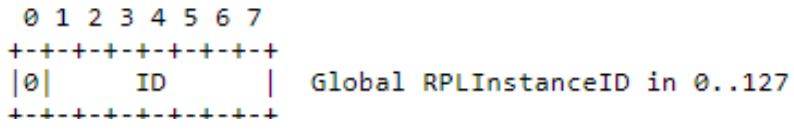
Το Rank ενός κόμβου καθορίζει την μεμονωμένη θέση (του κόμβου) σε σχέση με άλλους κόμβους, καθώς επίσης και την σχέση με την ρίζα DODAG. Το Rank του κάθε κόμβου αυξάνεται προς την κάτω (Down) κατεύθυνση (δηλαδή μακριά από την ρίζα του δέντρου) και μειώνεται προς την πάνω (Up) κατεύθυνση (δηλαδή κοντά στην ρίζα του δέντρου). Ο ακριβής τρόπος υπολογισμού του Rank εξαρτάται από την αντικειμενική συνάρτηση (objective function) του DAG. Το Rank εκφράζεται σαν βαθμός της μεταξύ τους απόστασης των κόμβων του δέντρου δρομολόγησης [2].

4.4.3 RPL Instances

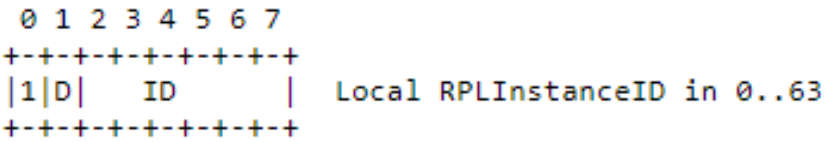
Ο γράφος DODAG που κτίζεται αποτελεί μια λογική τοπολογία δρομολόγησης πάνω στο φυσικό δίκτυο. Στο ίδιο δίκτυο μπορούν να υπάρξουν πολλοί γράφοι για εξυπηρέτηση διαφορετικών απαιτήσεων. Ένας κόμβος του δικτύου που έχει την δυνατότητα να συμμετέχει σε ένα ή περισσότερους γράφους αναφέρονται ως RPL παρουσίες (RPL Instances). Κάθε RPL Instance λειτουργεί ανεξάρτητα και υλοποιεί διαφορετική αντικειμενική συνάρτηση (objective function) σε σχέση με άλλα RPL Instances [22].

4.4.4 RPL Instance ID

Μία global RPL Instance ID πρέπει να είναι μοναδική μέσα σε ένα LLN δίκτυο. Μπορεί να υπάρχουν πάνω από 128 global Instances (παρουσίες) σε ένα ολόκληρο δίκτυο. Οι τοπικές παρουσίες (local instances) χρησιμοποιούνται πάντοτε σε συνδυασμό με ένα DODAG ID και μπορεί να υποστηρίξει μέχρι και 64 τοπικές παρουσίες ανά DODAG ID. Οι τοπικές παρουσίες κατανέμονται και διαχειρίζονται από τον κόμβο που διαθέτει το DODAG ID.



Εικόνα 36: RPL Instance ID field format for global instances (Πηγή: RFC 6550)



Εικόνα 37: RPL Instance ID field format for local instances (Πηγή: RFC 6550)

Η σημαία “D” σε μια local instance ID είναι πάντα ρυθμισμένη στο 0 στα μηνύματα ελέγχου του RPL. Χρησιμοποιείται σε πακέτα δεδομένων για να υποδείξει εάν το DODAG ID είναι η πηγή ή ο προορισμός του πακέτου. Εάν η σημαία “D” έχει οριστεί στο 1 τότε η διεύθυνση προορισμού του IPv6 πακέτου πρέπει να είναι το DODAG ID.

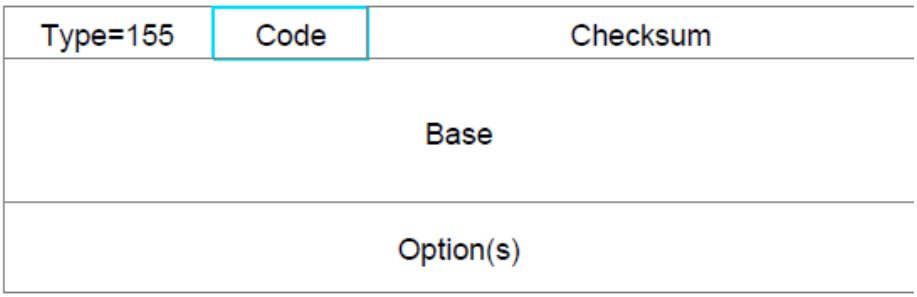
4.5 Trickle Timers

Αφού οι περισσότερες συσκευές που σχηματίζουν το δίκτυο κάνουν χρήση μπαταριών ως πηγή ενέργειας, είναι ζωτικής σημασίας να περιοριστεί ο αριθμός των μηνυμάτων ελέγχου στο δίκτυο. Όσον αφορά την συντήρηση (maintenance) του δικτύου, το πρωτόκολλο RPL χρησιμοποιεί τα χρονόμετρα trickle (trickle timers). Τα χρονόμετρα αυτά ελέγχουν την συχνότητα των μηνυμάτων DIO. Το χρονικό διάστημα που στέλνονται τα μηνύματα DIO ξεκινά από μια αρχική τιμή Tmin και αυξάνεται όσο το δίκτυο σταθεροποιείται. Επομένως, μειώνεται ο αριθμός των μηνυμάτων DIO που στέλνονται στο δίκτυο. Το χρονικό διάστημα μπορεί να αυξηθεί μέχρι μια σταθερή τιμή Tmax [12].

Όταν εντοπιστεί μια ασυνέπεια (inconsistency) στο δίκτυο τότε το χρονόμετρο επαναφέρεται (reset) στην αρχική τιμή Tmin για να σταλούν πιο συχνά τα μηνύματα DIO και να διορθωθεί η ασυνέπεια. Ως ασυνέπεια θεωρείται ο εντοπισμός κύκλου (loop) στον γράφο, η είσοδος ενός νέου κόμβου στον γράφο και η μετακίνηση ενός κόμβου στο δίκτυο. Επίσης, το χρονόμετρο γίνεται reset όταν παραληφθεί ένα μήνυμα τύπου DIS.

4.6 Μηνύματα Ελέγχου στο RPL

Το RPL καθορίζει ένα σύνολο από νέα ICMPv6 μηνύματα ελέγχου (control messages) για να γίνεται η ανταλλαγή πληροφοριών του γράφου DODAG στο δίκτυο [8].



Εικόνα 38: RPL Control Message (Πηγή: RFC 6550)

Το πεδίο code προσδιορίζει τον τύπο των μηνυμάτων ελέγχου RPL, όπως φαίνεται παρακάτω στην εικόνα 39.

Code: Identify the type of control message

0x00 → DODAG Information Solicitation (DIS)

0x01 → DODAG Information Object (DIO)

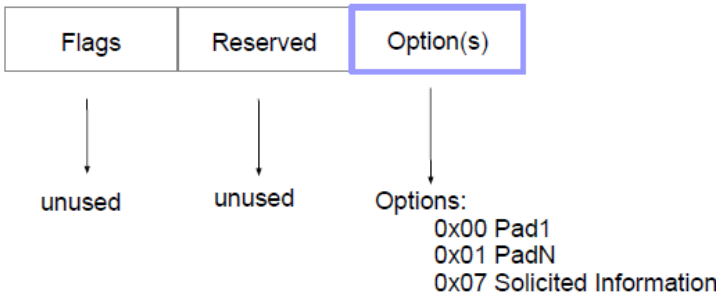
0x02 → Destination Advertisement Object (DAO)

0x03 → DAO-ACK

Εικόνα 39: RPL Control Messages Types (Πηγή: RFC 6550)

4.6.1 DODAG Information Solicitation (DIS)

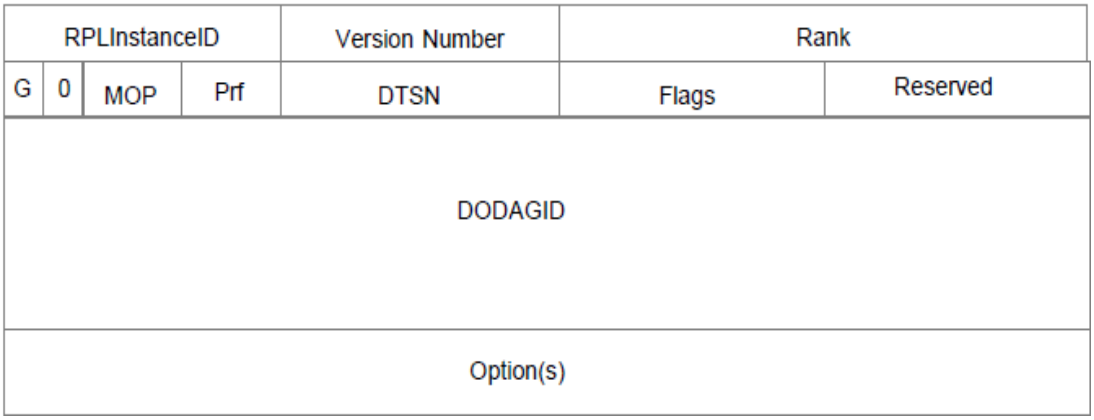
Το μήνυμα DIS στέλνεται στους γείτονες ενός κόμβου ως αίτημα για πληροφορίες δρομολόγησης και για ανίχνευση γράφων. Συγκεκριμένα, ένας κόμβος που ενεργοποιείται σε περιβάλλον όπου υπάρχει ήδη γράφος αποστέλλει μήνυμα DIS προκειμένου να ζητήσει πληροφορία σχετικά με τον γράφο από τους γονείς του, οι οποίοι ενδεχομένως ανταποκριθούν με μηνύματα DIO.



Εικόνα 40: The DIS Base Object (Πηγή: RFC 6550)

4.6.2 DODAG Information Object (DIO)

Είναι η κύρια πηγή των πληροφοριών δρομολόγησης. Χρησιμοποιείται κατά την κατασκευή του DODAG και για διαφήμιση διάφορων πληροφοριών σχετικά με τον γράφο. Περιέχει μεταξύ άλλων τον βαθμό ενός κόμβου (rank), το RPL Instance και την διεύθυνση της ρίζας.

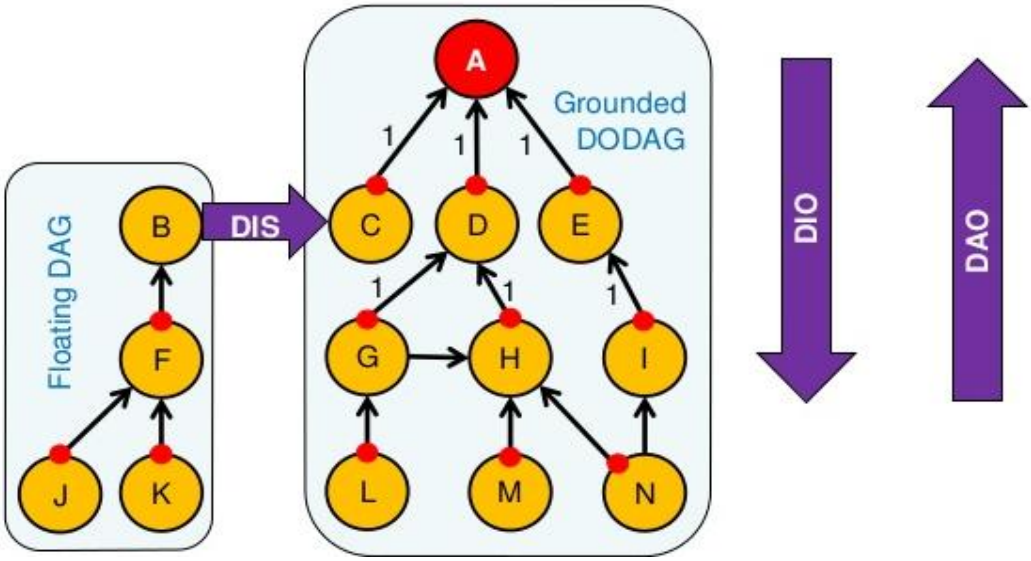


Εικόνα 41: DIO Base Object (Πηγή: RFC 6550)

Grounded (G): Η σημαία G δείχνει αν το DODAG που διαφημίζεται μπορεί να ικανοποιήσει τον καθορισμένο από την εφαρμογή στόχο.
Mode of Operation (MOP): Το πεδίο αυτό προσδιορίζει τον τρόπο λειτουργίας του RPL Instance που παρέχεται και διανέμεται από την ρίζα του DODAG.
DODAG Preference (Prf): Είναι ένας μη προσημασμένος ακέραιος αριθμός των 3-bit που καθορίζει τον τρόπο προτίμησης της ρίζας του DODAG καθώς συγκρίνεται και με άλλες ρίζες. Το DAG Preference κυμαίνεται από 0x00 δηλαδή λιγότερο προτιμώμενο έως 0x07 περισσότερο προτιμώμενο. Η προεπιλογή είναι 0 (λιγότερο προτιμώμενο).

Version Number: Αριθμός έκδοσης. Είναι ένας μη προσημασμένος ακέραιος αριθμός των 8-bit που ορίζεται από την ρίζα DODAG στο DODAG Version number.
Rank: Μη προσημασμένος ακέραιος αριθμός των 16-bit που δείχνει το rank του DODAG του κόμβου στέλνοντας ένα DIO μήνυμα.
RPL Instance ID: Πεδίο των 8-bit που ορίζεται από την ρίζα DODAG.
Destination Advertisement Trigger Sequence Number (DTSN): Μη προσημασμένος ακέραιος αριθμός των 8-bit που έχει οριστεί από τον κόμβο που εκδίδει το μήνυμα DIO.
Flags: Αχρησιμοποίητο πεδίο των 8-bit που προορίζεται για σημαίες.
Reserved: Αχρησιμοποίητο πεδίο των 8-bit.
DODAG ID: Διεύθυνση IPv6 των 128-bit που έχει καθοριστεί από μια ρίζα DODAG που είναι μοναδική [21].

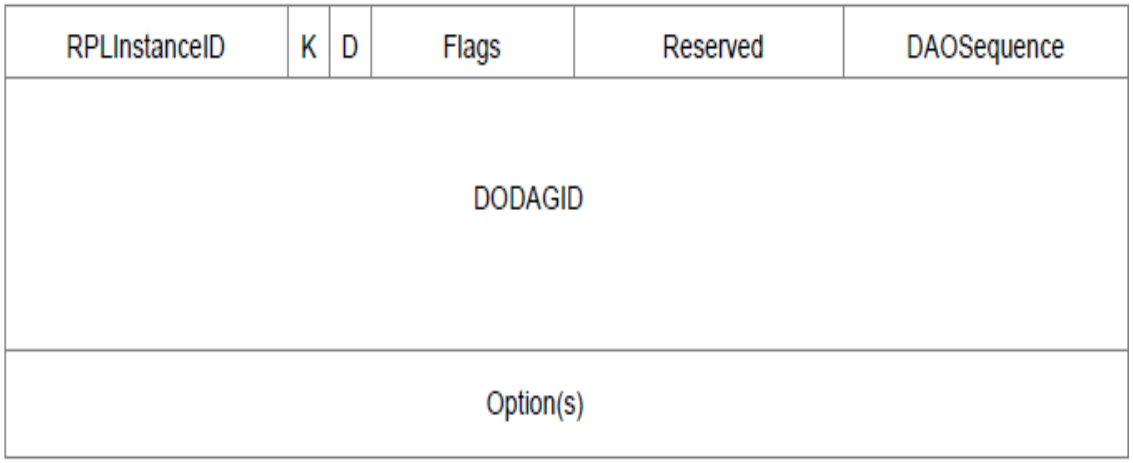
Επίσης το μήνυμα DIO φέρει κάποιες επιλογές (**options**). Παρακάτω φαίνονται οι επιλογές του μηνύματος DIO:
0x00 Pad 1
0x01 Pad 2
0x02 DAG Metric Container
0x03 Routing Information
0x04 DODAG Configuration
0x08 Prefix Information



Εικόνα 42: Messages for Routing (Πηγή: Cisco)

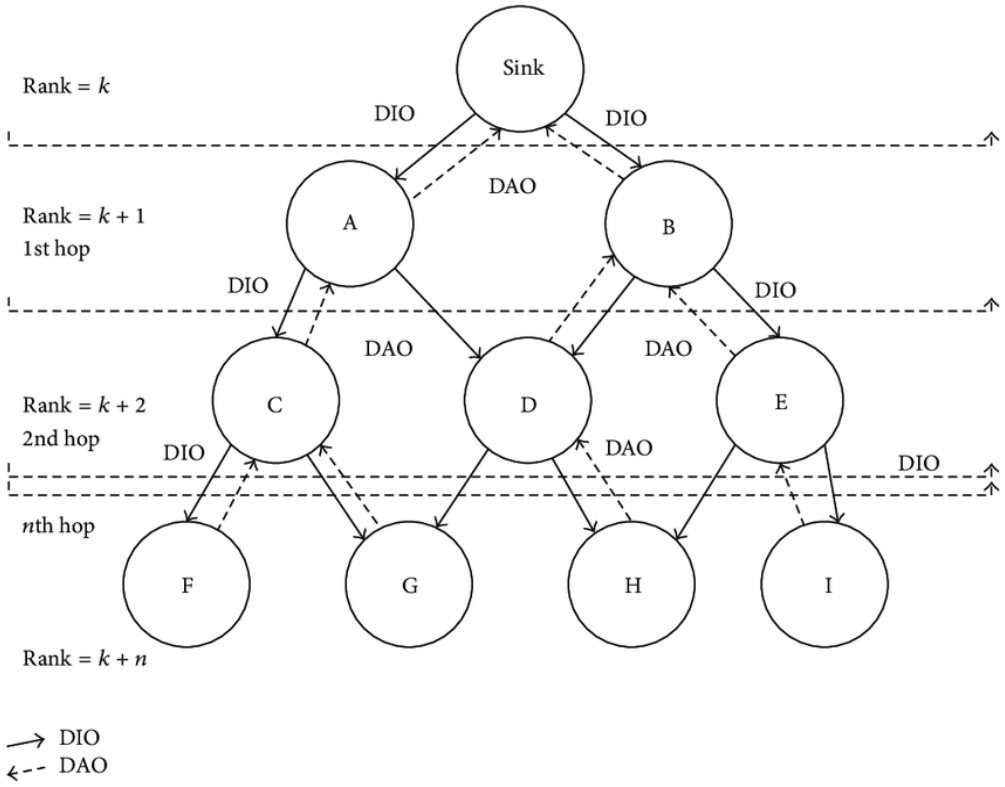
4.6.3 DODAG Destination Advertisement Object (DAO)

Το μήνυμα DAO, στέλνεται από τους κόμβους στο κάτω μέρος του γράφου, προς την πάνω κατεύθυνση του γράφου (προς τον sink) μεταφέροντας πληροφορίες δρομολόγησης. Κάθε κόμβος στέλνει μήνυμα DAO στον γονέα (parent) του. Με αυτόν τον τρόπο, υποστηρίζεται η δρομολόγηση προς την κάτω κατεύθυνση του γράφου (Point to Multipoint). Ο κόμβος που λαμβάνει ένα μήνυμα DAO, το χρησιμοποιεί για να ενημερώσει τον πίνακα δρομολόγησης του [21].



Εικόνα 43: DAO Base Object (Πηγή: RFC 6550)

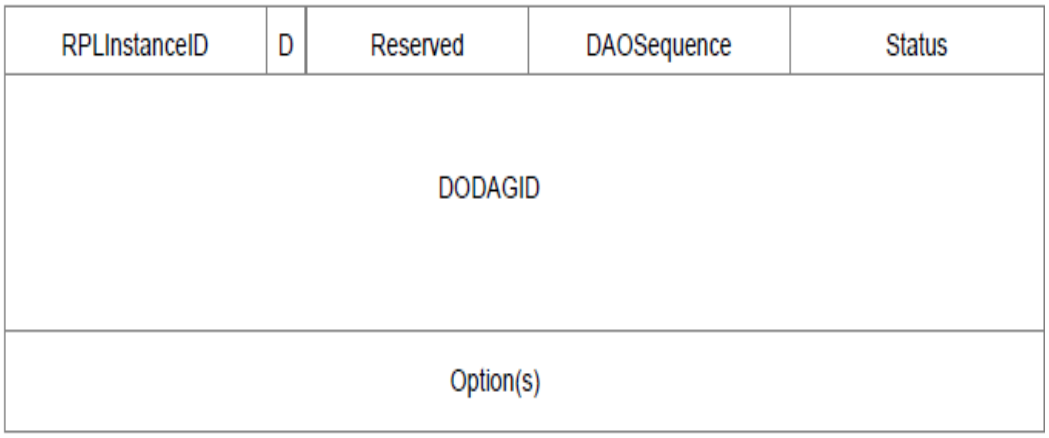
RPL Instance ID: Πεδίο των 8-bit που δηλώνει το Instance της τοπολογίας που συνδέεται με το DODAG.
K: Η σημαία "K" δηλώνει ότι ο παραλήπτης αναμένεται να στείλει ένα μήνυμα DAO-ACK πίσω.
D: Η σημαία "D" δηλώνει ότι υπάρχει πεδίο DODAG ID.
Flags: Αχρησιμοποίητο πεδίο των 6-bits για σημαίες.
Reserved: Αχρησιμοποίητο πεδίο των 8-bits.
DAO Sequence: Αυξανόμενο σε κάθε μοναδικό μήνυμα DAO από έναν κόμβο.
DODAG ID: Μη προσημασμένος ακέραιος αριθμός των 128-bit που ορίζεται από μια ρίζα DODAG. Αυτό το πεδίο λειτουργεί μόνο όταν η σημαία "D" έχει οριστεί. Αυτό το πεδίο είναι συνήθως ενεργό μόνο όταν ένα RPL Instance ID είναι σε χρήση.
Κάποιες επιλογές (**options**) του μηνύματος DAO είναι οι εξής:
0x00 Pad 1
0x01 Pad N
0x05 RPL Target
0x06 Transmit Information
0x09 RPL Target Descriptor
Εμφανίζεται μια ειδική περίπτωση του μηνύματος DAO, που ονομάζεται No-Path, που χρησιμοποιείται στο Storing Mode για να "καθαρίσει" την κατάσταση δρομολόγησης προς τα κάτω.



Εικόνα 44: Flow of DIO and DAO message in RPL network (Πηγή: Research Gate)

4.6.4 DAO-ACK

Το μήνυμα DAO-ACK στέλνεται ως απάντηση σε ένα μήνυμα τύπου DAO επιβεβαιώνοντας την παραλαβή του.



Εικόνα 45: The DAO ACK Base Object (Πηγή: RFC 6550)

RPL Instance ID: Πεδίο των 8-bit που δηλώνει το Instance της τοπολογίας που συνδέεται με το DODAG.
D: Η σημαία "D" δηλώνει ότι υπάρχει πεδίο DODAG ID.
Reserved: Αχρησιμοποίητο πεδίο των 7-bits.

DAO Sequence: Χρησιμοποιείται για την συσχέτιση ενός μηνύματος DAO και ενός μηνύματος DAO-ACK και δεν πρέπει συσχετίζεται με την πληροφορία μεταφοράς (Transmit Information) της λειτουργίας Path Sequence.
DODAG ID: Μη προσημασμένος ακέραιος αριθμός των 128-bit που ορίζεται από μια ρίζα DODAG. Αυτό το πεδίο λειτουργεί μόνο όταν η σημαία "D" έχει οριστεί. Αυτό το πεδίο είναι συνήθως ενεργό μόνο όταν ένα RPL Instance ID είναι σε χρήση.

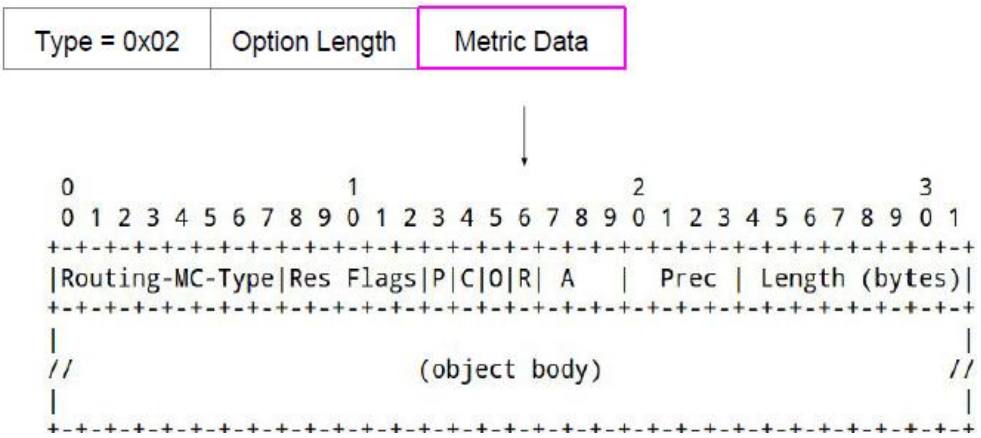
4.6.5 DAG Metric Container

Ο DAG Metric Container μπορεί να υπάρχει στα μηνύματα DIO ή DAO. Χρησιμοποιείται για την αναφορά μητρικών (metrics) κατά μήκος του DODAG. Επίσης μπορεί να περιέχει έναν αριθμό από κόμβους, μητρικές μονοπατιών (path metrics) και περιορισμών (constraints) που καθορίζονται στο RFC 6551. Επίσης μπορεί να εμφανίζεται περισσότερες από μια φορές στο ίδιο μήνυμα ελέγχου RPL (RPL control message). Η επεξεργασία και η διάδοση του DAG metric container διέπεται από συγκεκριμένες λειτουργίες εκτέλεσης. Όπως φαίνεται παρακάτω στην εικόνα 46 σύμφωνα με το format του DAG Metric Container υπάρχουν κάποια πεδία και αυτά είναι:

Option Type: 0x02

Option Length: Περιέχει το μήκος των Μετρικών Δεδομένων (Metric Data) σε οχτάδες (octets).

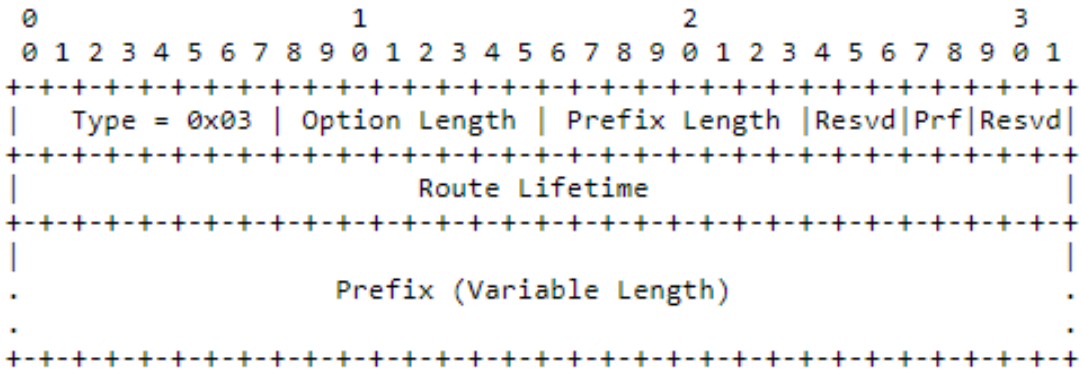
Metric Data: Είναι η σειρά, το περιεχόμενο και η κωδικοποίηση των δεδομένων του DAG Metric Container [22].



Εικόνα 46: Format of the DAG Metric Container Option (Πηγή: RFC 6550)

4.6.6 Route Information

Η επιλογή πληροφορίας διαδρομής (Route Information Option) μπορεί να υπάρχει στα μηνύματα DIO και να φέρει τις ίδιες πληροφορίες για την εύρεση γειτόνων IPv6 (Neighbor Discovery) όπως ορίζεται στο RFC 4191.



Εικόνα 47: Format of the Route Information Option (Πηγή: RFC 6550)

Το RIO χρησιμοποιείται για να δηλώσει ότι η σύνδεση με το πρόθεμα (prefix) του προορισμού είναι διαθέσιμη από την ρίζα DODAG. Σε περίπτωση όπου ένα μήνυμα ελέγχου RPL χρειαστεί να καθορίσει την σύνδεση σε περισσότερους από έναν προορισμούς τότε μπορεί να επαναληφθεί το RIO. Οι περιγραφές των πεδίων εξηγούνται παρακάτω:

Option length: Μεταβλητή, μήκος σε οκτάδες (octets) εξαιρουμένων των πεδίων τύπος (Type) και μήκος (Length).

Θα πρέπει να σημειωθεί ότι το μήκος εκφράζεται σε μονάδες οκτάδων, σε αντίθεση με το IPv6 ND.

Prefix Length: Μη προσημασμένος ακέραιος αριθμός των 8-bit. Η τιμή του κυμαίνεται από 0 έως 128. Το πεδίο πρόθεμα έχει τον αριθμό byte που συνάγεται από το πεδίο Option Length. Θα πρέπει να σημειωθεί ότι στο RPL το Prefix Length μπορεί να έχει διαφορετικό μήκος από 0, 8 ή 16.

PrF: Μη προσημασμένος ακέραιος αριθμός των 2-bit. Η προτίμηση διαδρομής (Route Preference) δείχνει αν υπάρχει προτιμώμενος δρομολογητής που σχετίζεται με το πρόθεμα έναντι άλλων, όταν έχουν ληφθεί πολλά ταυτόσημα προθέματα (για διαφορετικούς δρομολογητές).

Route Lifetime: Μη προσημασμένος ακέραιος αριθμός των 32-bit. Το χρονικό διάστημα σε δευτερόλεπτα (σε σχέση με τον χρόνο αποστολής του πακέτου) ότι το πρόθεμα είναι έγκυρο για τον προσδιορισμό της διαδρομής.

Prefix: Πεδίο μεταβλητού μήκους που περιέχει μια διεύθυνση IP ή ένα πρόθεμα μιας διεύθυνσης IPv6. Το πεδίο του προθέματος περιέχει τον αριθμό των έγκυρων δυαδικών ψηφίων. Τα δυαδικά ψηφία του προθέματος πρέπει να οριστούν στο μηδέν από τον αποστολέα και να αγνοηθούν από τον δέκτη [24].

4.7 Objective Function (OF)

Η λειτουργία της αντικειμενικής συνάρτησης (Objective Function) ορίζει τον τρόπο με τον οποίο επιλέγουν οι κόμβοι και βελτιστοποιούν τις διαδρομές ενός RPL δικτύου. Η αντικειμενική συνάρτηση αναγνωρίζεται από ένα κωδικό σημείο (Objective Code Point). Μια αντικειμενική συνάρτηση καθορίζει τον τρόπο με τον οποίο οι κόμβοι μεταφράζουν μία ή περισσότερες μητρικές. Επίσης καθορίζει τον τρόπο με τον οποίο οι κόμβοι επιλέγουν τους γονείς του δέντρου δρομολόγησης [22].

4.7.1 Objective Function Zero (OF0)

Η λειτουργία της Objective Function Zero έχει σχεδιαστεί για να βρίσκει την πλησιέστερη ρίζα. Αυτό μπορεί να επιτευχθεί όταν το Rank ενός κόμβου είναι πολύ κοντά στην συνάρτηση απόστασης από την ρίζα. Η OF0 επιλέγει ένα προτιμώμενο γονέα και έναν εφικτό διάδοχο (feasible successor) εάν είναι διαθέσιμος. Όλη η προς τα πάνω κίνηση (upward traffic) δρομολόγησης κατευθύνεται κανονικά μέσω του προτιμώμενου γονέα. Εάν οι συνθήκες σύνδεσης δεν αφήνουν ένα πακέτο να πάει προς τα πάνω μέσω του προτιμώμενου γονέα, τότε το πακέτο αυτό μεταβιβάζεται στον εφικτό διάδοχο. Ένας κόμβος RPL παρακολουθεί τις συνδέσεις μεταξύ των γειτονικών κόμβων και μπορεί να χρησιμοποιήσει την OF0 για να εκχωρήσει ένα rank_increase σε κάθε σύνδεση. Η OF0 υπολογίζει μια μεταβλητή step_of_rank που σχετίζεται με τον γονέα και τις μητρικές συνδέσμων.
Το step_of_rank χρησιμοποιείται για να υπολογίσει το ποσό με το οποίο θα αυξηθεί το rank κατά μήκος ενός συγκεκριμένου συνδέσμου. Η OF0 αλληλοεπιδρά για την διαχείριση και τις λειτουργίες με τους παρακάτω τρόπους:
Processing DIO: Όταν λαμβάνεται ένα νέο DIO η αντικειμενική συνάρτηση που αντιστοιχεί στο Objective Code Point ενεργοποιείται με το περιεχόμενο του DIO. Η OF0 αναγνωρίζεται από το Objective Code Point 0 (μηδέν).
Providing DAG Information: Η OF0 παρέχει μια διεπαφή που επιστρέφει πληροφορίες σχετικά με το instance. Περιλαμβάνει υλικό από την κεφαλίδα DIO, τον ρόλο (δρομολογητή) και το rank του κόμβου.
Providing a Parent list: Η OF0 παρέχει μια διεπαφή που επιστρέφει τον κατάλογο των γονέων και τους εφικτούς διαδόχους για ένα συγκεκριμένο instance στον πυρήνα του RPL.
Triggered Updates: Η OF0 παρέχει κάποιες εκδηλώσεις για να ενημερώσει οτιδήποτε αλλαγή στις πληροφορίες του DAG ή στην λίστα των γονέων. Αυτό μπορεί να οφείλεται στην αλληλεπίδραση με άλλα στοιχεία του συστήματος όπως για παράδειγμα η διαμόρφωση (configuration) και οι χρονοδιακόπτες (timers).

Η Objective Function Zero χρησιμοποιεί τις ακόλουθες μεταβλητές:
step_of_rank (strictly positive integer): είναι ένας ενδιάμεσος υπολογισμός που βασίζεται στις ιδιότητες σύνδεσης με έναν συγκεκριμένο γείτονα.
rank_increase (strictly positive integer): δέλτα (delta) μεταξύ του rank του προτιμώμενου γονέα και του ίδιου.

4.7.2 MRHOF

Η αντικειμενική συνάρτηση MRHOF (Minimum Rank with Hysteresis Objective Function), έχει σχεδιαστεί για να βρίσκει τα μονοπάτια ή αλλιώς διαδρομές δρομολόγησης με το μικρότερο κόστος. Αυτό γίνεται με δύο μηχανισμούς. Ο πρώτος μηχανισμός βρίσκει την ελάχιστη διαδρομή κόστους, δηλαδή την διαδρομή δρομολόγησης με το μικρότερο Rank. Ο δεύτερος μηχανισμός είναι η υστέρηση (hysteresis), όπου το πακέτο το οποίο δρομολογείται, μεταβαίνει στην ελάχιστη διαδρομή κόστους εάν και μόνο εάν είναι μικρότερη (από άποψη κόστους διαδρομής) από την τρέχουσα διαδρομή στην οποία βρίσκεται, τουλάχιστον με ένα δεδομένο όριο. Η MRHOF μπορεί να χρησιμοποιηθεί με οποιαδήποτε μετρική, εφόσον όμως ο στόχος δρομολόγησης είναι να ελαχιστοποιήσει την μετρική δρομολόγησης. Ο κόμβοι στο δέντρο δρομολόγησης πρέπει να υποστηρίζουν τουλάχιστον μία από αυτές τις μετρικές όπως: hop count, latency ή ETX [26].

Οι κόμβοι της ρίζας ρυθμίζουν την μεταβλητή cure_min_path_cost στην τιμή της μετρικής που υπολογίζει το Rank του Min Hop Rank Increase. Αν ένας κόμβος ο οποίος δεν ανήκει στην ρίζα και δεν διαθέτει μετρικές για να υπολογίσει το κόστος διαδρομής μεταξύ των γειτονικών κόμβων, τότε ο κόμβος αυτός πρέπει να προσχωρήσει στους γειτονικούς κόμβους ως RPL Leaf.

Το κόστος διαδρομής ενός γειτονικού κόμβου αντιπροσωπεύει το κόστος της διαδρομής από την άποψη της επιλεγμένης μετρικής, από έναν κόμβο στην ρίζα του DODAG μέσω αυτού του γείτονα. Ένας κόμβος πρέπει να υπολογίσει το κόστος διαδρομής για την διαδρομή μέσω του υποψήφιου γείτονα που είναι προσβάσιμος. Αν ένας κόμβος δεν μπορεί να υπολογίσει το κόστος της διαδρομής που ενώνει τον υποψήφιο γειτονικό κόμβο, τότε ο κόμβος αυτός δεν μπορεί να τον επιλέξει σαν προτιμώμενο γονέα του, τον γειτονικό κόμβο αυτό. Ωστόσο αν ο κόμβος δεν μπορεί να υπολογίσει το κόστος διαδρομής μέσω οποιοδήποτε γείτονα, τότε μπορεί να ενταχθεί στον υποψήφιο γείτονα ως Leaf.

Η MRHOF πρέπει να εκτελεί την επιλογή γονέων κάθε φορά, που το κόστος της διαδρομής για έναν υποψήφιο γείτονα συμπεριλαμβανομένου και του προτιμώμενου γονέα αλλάζει. Εάν η μετρική για ένα link (σύνδεσμο) είναι μεγαλύτερη από το MAX_LINK_METRIC τότε ο κόμβος θα πρέπει να αποκλείσει αυτό το link (σύνδεσμο) για την επιλογή γονέα. Ένας κόμβος πρέπει να επιλέξει τον υποψήφιο γείτονα με το χαμηλότερο κόστος διαδρομής ως προτιμώμενο γονέα του. Αν υπάρχουν πολλοί γείτονες που μοιράζονται το μικρότερο κόστος διαδρομής, τότε ο κόμβος μπορεί να χρησιμοποιήσει διαφορετικά κριτήρια επιλογής για να επιλέξει ποιος από τους γείτονες θα πρέπει να θεωρηθεί ότι έχει το χαμηλότερο κόστος. Μόλις επιλεγεί ο προτιμώμενος γονέας, τότε ο κόμβος ορίζει την μεταβλητή cur_min_path_cost στο κόστος της διαδρομής που αντιστοιχεί στον προτιμώμενο γονέα. Η τιμή του cur_min_path_cost μεταφέρεται στον metric container που αντιστοιχεί στην επιλεγμένη μετρική όταν αποστέλλονται τα DIO μηνύματα.

Οι ρίζες DAG θέτουν το Rank τους στο Min Hop Rank Increase. Μόλις ο κόμβος (ο οποίος δεν ανήκει στην ρίζα) επιλέξει το σύνολο των γονέων, μπορεί να χρησιμοποιήσει τον παρακάτω πίνακα για να καλύψει το κόστος διαδρομής ενός γονέα, σε μια τιμή Rank.

Node/link Metric	Rank
Hop-Count	Cost
Latency	Cost/65536
ETX	Cost

Εικόνα 48: Conversion Metric to Rank (Πηγή: RFC 6719)

Η MRHOF χρησιμοποιεί την τιμή του Rank για να υπολογίσει την διαδρομή κάθε μέλους από το σύνολο των γονέων. Το Rank που σχετίζεται με το μονοπάτι ενός μέλους από το σύνολο των γονέων είναι το μέγιστο των δύο τιμών. Η πρώτη είναι η αντίστοιχη τιμή Rank που υπολογίζεται από τον παραπάνω πίνακα της εικόνας 48. Η δεύτερη είναι ότι οι κόμβοι διαφημίζονται με Rank plus Min Hop Rank Increase. Μόλις επιλεγεί ο προτιμώμενος γονέας, ο κόμβος ρυθμίζει την μεταβλητή cur_min_path_cost στο κόστος του μονοπατιού που αντιστοιχεί στον προτιμώμενο γονέα.
Στην συνέχεια υπολογίζει την μετρική που θα διαφημίσει στο metric container. Αυτή η τιμή είναι το κόστος μονοπατιού του μέλους από το σύνολο των γονέων με το υψηλότερο κόστος μονοπατιού. Έτσι, ενώ το cure_min_path_cost είναι το κόστος μέσω του προτιμώμενου γονέα, ένας κόμβος διαφημίζει το μονοπάτι υψηλότερου κόστους από τον κόμβο στην ρίζα μέσω ενός μέλους που ανήκει στο σύνολο των γονέων. Η τιμή του μονοπατιού με το υψηλότερο κόστος μεταφέρεται στον metric container όταν αποστέλλονται τα μηνύματα DIO.

Η MRHOF χρησιμοποιεί την μεταβλητή:
cur_min_path_cost: Το κόστος του μονοπατιού από έναν κόμβο μέσω του προτιμώμενου γονέα προς την ρίζα.
Επίσης η MRHOF χρησιμοποιεί τις παρακάτω παραμέτρους:
MAX_LINK_METRIC: Μέγιστη επιτρεπόμενη τιμή για την μετρική του link του μονοπατιού.
MAX_PATH_COST: Μέγιστη επιτρεπόμενη τιμή για την μετρική του μονοπατιού.
PARENT_SWITCH_THRESHOLD: Η διαφορά μεταξύ του κόστους του μονοπατιού μέσω του προτιμώμενου γονέα και του ελάχιστου κόστους του μονοπατιού προκειμένου να ενεργοποιηθεί ένας νέος προτιμώμενος γονέας.
PARENT_SET_SIZE: Ο αριθμός των υποψηφίων γονέων, συμπεριλαμβανόμενου και του προτιμώμενου γονέα μέσα στο σύνολο των γονέων.
ALLOW_FLOATING_ROOT: Αν είναι ρυθμισμένο στο 1 τότε ο κόμβος μπορεί να γίνει floating root.
Οι τιμές των παραμέτρων καθορίζονται ανάλογα με την μετρική δρομολόγησης. Οι καλύτερες τιμές για αυτές τις παραμέτρους καθορίζονται από τις απαιτήσεις της λειτουργίας του RPL. Για παράδειγμα εάν χρησιμοποιήσουμε την μετρική ETX και το UDP ως πρωτόκολλο μεταφοράς, τότε θα πρέπει να χρησιμοποιηθεί ένα μικρό MAX_LINK_METRIC έτσι ώστε οι αναμεταδόσεις του link στρώματος να είναι αρκετές ώστε να υπάρχει καλή πιθανότητα και αξιοπιστία μεταφοράς των πακέτων [26].

4.8 Μετρικές δρομολόγησης RPL

Η δυναμική φύση του RPL μέσα σε ένα ασύρματο δίκτυο αισθητήρων, επιβάλει την συνεχή παρακολούθηση διάφορων πτυχών της λειτουργίας του. Χρησιμοποιώντας δυναμικές πληροφορίες για τις μεταβολές της δομής του δικτύου, για την ποιότητα των ζεύξεων και των δίαυλων, την αξιοπιστία και την ενέργεια των κόμβων καθίσταται δυνατή η προσαρμογή της λειτουργίας του δικτύου στις αλλαγές, επιδιώκοντας την βελτιστοποίηση του, όπως αυτή εκφράζεται από τον σχεδιαστή του δικτύου και μπορεί να αναφέρεται σε ελάχιστα σφάλματα, μέγιστη διάρκεια ζωής κ.λπ. Οι διαφορετικές πτυχές λειτουργίας ελέγχονται μέσω διαφορετικών μετρικών. Οι πληροφορίες που αντλούνται μέσω μιας μετρικής ενσωματώνονται στο πρωτόκολλο δρομολόγησης RPL, συμμετέχοντας στην διαμόρφωση της τιμής της αντικειμενικής συνάρτησης (objective function), ενώ η επιλογή της καλύτερης τιμής γίνεται με βάση τις απαιτήσεις βέλτιστης λειτουργίας [2].

Η χρήση μιας μεμονωμένης μετρικής, ωστόσο, ενώ εποπτεύει αποτελεσματικά το χαρακτηριστικό που εστιάζει, δεν αποτυπώνει άλλα, επίσης σημαντικά στοιχεία του δικτύου. Συνεπώς, η χρησιμοποίηση πολλαπλών μετρικών είναι επιβεβλημένη. Παρόλα αυτά, η σύνθεση μετρικών απαιτεί πολύ καλή μελέτη, καθώς καλείται να εξυπηρετήσει δύο, συχνά αντικρουόμενες ανάγκες. Πρώτον, η σύνθεση πρέπει να γίνει κατά τέτοιο τρόπο, ώστε να πληρούνται βασικές απαιτήσεις του πρωτοκόλλου δρομολόγησης του RPL και έτσι να εξυπηρετείται ο πρωταρχικός σκοπός του, που είναι η πρόσβαση στον προορισμό. Δεύτερον, οι μετρικές πρέπει να συντίθενται κατά τέτοιο τρόπο, ώστε να μην αλλοιώνονται, αλλά να διατηρούν τις ιδιότητές τους και να μπορούν να συλλάβουν τις μεταβολές της λειτουργίας, την οποία στοχεύουν [10].

4.8.1 Node Energy Object

Μερικές φορές αποφεύγεται η επιλογή ενός κόμβου με χαμηλό υπόλοιπο ενέργειας ως επιλεγμένος δρομολογητής. Επομένως απαιτείται υποστήριξη για δρομολόγηση βάση κάποιων περιορισμών. Σε τέτοιες περιπτώσεις, ο μηχανισμός πρωτοκόλλου δρομολόγησης μπορεί να υπολογίσει μια μεγαλύτερη διαδρομή (με βάση τον περιορισμό) για την κίνηση πακέτων δρομολόγησης, προκειμένου να αυξηθεί η διάρκεια ζωής του δικτύου [12].

Η ισχύς η ενέργεια είναι σαφώς κρίσιμοι πόροι στα LLNs δίκτυα. Μέχρι σήμερα δεν υπάρχει κάποια λύση που να καλύπτει επαρκώς το ευρύ φάσμα πηγών ενέργειας και συσκευών αποθήκευσης ενέργειας που χρησιμοποιούνται σε κόμβους των LLNs δικτύων. Οι μπαταρίες που χρησιμοποιούνται, μερικές φορές υποβαθμίζονται εάν η μέση κατανάλωση ρεύματος υπερβαίνει ένα μικρό κλάσμα του μέγιστου ρεύματος που μπορούν να αποδώσουν. Επειδή υπάρχει πολυπλοκότητα στην αντιμετώπιση κάποιων περιορισμών έχουν ορισθεί κάποια επίπεδα λύσεων [6]. Η απλούστερη λύση βασίζεται σε τρεις τύπους πηγών ενέργειας: “powered”, “battery”, “scavenger”. Η Μέση ενέργεια (average power) σχετίζεται με τον χρόνο εκφόρτωσης της μπαταρίας του κόμβου. Για συσκευές αποθήκευσης ενέργειας όπως είναι η μπαταρία η εξίσωση της ενέργειας δίνεται από τον τύπο:

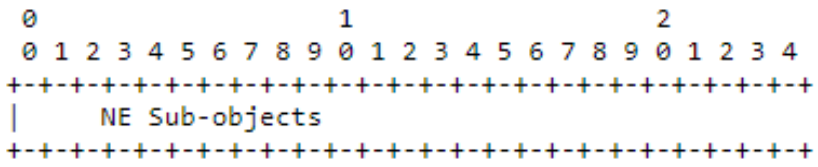
$$EE = \frac{Power_{now}}{Power_{max}} \times 100 \qquad (4.1)$$

Όπου:

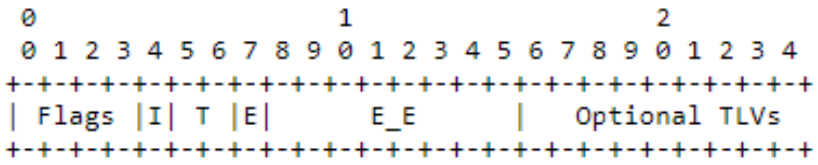
$Power_{now}$ η υπολειπόμενη ενέργεια
$Power_{max}$ η εκτιμώμενη ενέργεια

Το αντικείμενο της ενέργειας του κόμβου (Node Energy Object) χρησιμοποιείται για παροχή πληροφοριών σχετικά με την ενέργεια του κόμβου και μπορεί να χρησιμοποιηθεί σαν μετρική ή σαν περιορισμός (constraint).

Το NE object μπορεί να υπάρξει στον metric container του DAG. Δεν πρέπει όμως να υπάρχουν περισσότερα από ένα NE object ως περιορισμοί στον metric container του DAG.



Εικόνα 49: NE Sub-Object Format (Πηγή: RFC 6551)

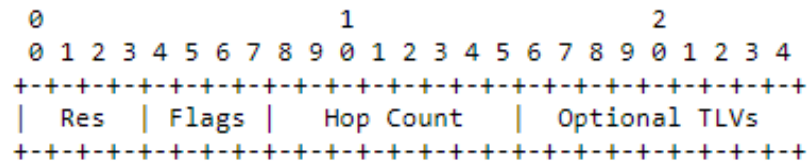


Εικόνα 50: NE Sub-Object Format (Πηγή: RFC 6551)

Flags field (8-bits): Οι ακόλουθες σημαίες έχουν οριστεί ως
I (Include): το "I" του bit έχει σημασία μόνο όταν ο τύπος του κόμβου χρησιμοποιείται σαν περιορισμός (constraint).
T (node type): πεδίο των 2-bit που δείχνει τον τύπο του κόμβου. Αν το T ισούται με 1 (T=1) σημαίνει ότι η ενέργεια του κόμβου τροφοδοτείται από την μπαταρία.
E (Estimation): όταν το bit "E" έχει οριστεί ως μετρική, το εκτιμώμενο ποσοστό της υπολειπόμενης ενέργειας στον κόμβο υποδεικνύεται στο πεδίο EE των 8-bit.
EE (Estimated-Energy): μη προσημασμένος ακέραιος αριθμός των 8-bit που δείχνει ένα εκτιμώμενο ποσοστό της υπολειπόμενης ενέργειας [21].

4.8.2 Hop Count Object

Το Hop Count (HP) object χρησιμοποιείται για την αναφορά αριθμού των κόμβων κατά μήκος του μονοπατιού στο δέντρο δρομολόγησης. Το HP object μπορεί να υπάρχει στον metric container του DAG. Επίσης περιέχει ένα σύνολο από TLVs που χρησιμοποιούνται για την μετάδοση διάφορων χαρακτηριστικών του κόμβου.



Εικόνα 51: Hop Count Object Body Format (Πηγή: RFC 6551)

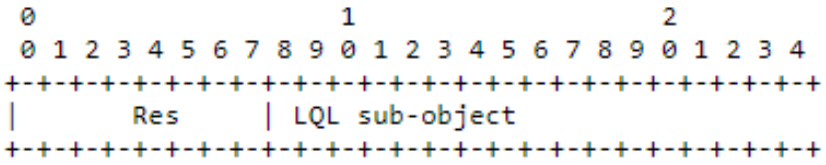
Res flags (4 bits): Δεσμευμένο πεδίο. Αυτό το πεδίο πρέπει να ρυθμιστεί στο μηδέν κατά την μετάδοση και πρέπει να αγνοηθεί κατά την παραλαβή.

No flag is currently defined: Μη προσημασμένα bits που θεωρούνται δεσμευμένα. Το HP object μπορεί να χρησιμοποιηθεί ως περιορισμός ή ως μετρική. Όταν χρησιμοποιηθεί ως περιορισμός η ριζά DAG υποδεικνύει τον μέγιστο αριθμό hops στο μονοπάτι δρομολόγησης.

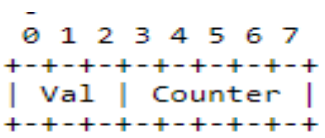
4.8.3 Μετρική Link Quality Level

Το επίπεδο ποιότητας ζεύξης του αντικειμένου (Link Quality Level) object χρησιμοποιείται για την αξιοπιστία των ζεύξεων στο δέντρο δρομολόγησης. Χρησιμοποιείται μια τιμή από 0 έως 7, όπου το 0 δηλώνει το άγνωστο επίπεδο ποιότητας ζεύξης και το 1 δηλώνει το υψηλότερο επίπεδο ποιότητας ζεύξης. Το LQL μπορεί να χρησιμοποιηθεί είτε ως μετρική είτε ως περιορισμός. Επίσης ο metric container του DAG μπορεί να ζητήσει από όλους τους κόμβους του δέντρου δρομολόγησης να καταγράψουν το LQL. Στην συνέχεια κάθε κόμβος μπορεί να χρησιμοποιήσει το LQL για να επιλέξει τον γονέα του με βάση βέβαια ορισμένους κανόνες που ορίζονται από τον χρήστη. Για παράδειγμα ένας κανόνας που μπορεί να ορίζεται από τον χρήστη είναι να επιλέξει την διαδρομή με τις περισσότερες ζεύξεις (links) που αναφέρονται στην τιμή LQL [13].

Οι μετρητές (containers) χρησιμοποιούνται για την συμπίεση πληροφοριών δηλαδή, για κάθε τιμή LQL, όπου αναφέρεται μόνο ο αριθμός των ζεύξεων. Επίσης το LQL object μπορεί να υπάρχει στον metric container του DAG. Το LQL object πρέπει να περιέχει ένα ή περισσότερα υπό αντικείμενα (sub-object) που χρησιμοποιούνται για τον αριθμό των ζεύξεων [21].



Εικόνα 52: LQL Object Body Format (Πηγή: RFC 6551)



Εικόνα 53: LQL Type 1 Sub-Object Format (Πηγή: RFC 6551)

Res Flags (8 bits): Δεσμευμένο πεδίο
Val: Η τιμή LQL από 0 έως 7 όπου 0 σημαίνει απροσδιόριστο και 1 σημαίνει υψηλή ποιότητα ζεύξης.
Counter: Ο αριθμός των ζεύξεων με αυτήν την τιμή.

4.8.4 Μετρική ETX

Η ασφάλεια και η αξιοπιστία των ζεύξεων επηρεάζει σημαντικά την ποιότητα υπηρεσίας (Quality of Service-QoS) που αντιλαμβάνεται ο χρήστης, επομένως είναι σημαντική η σύνθεση μετρικών αξιοπιστίας ζεύξης και εμπιστοσύνης. Ο όρος «αξιοπιστία ζεύξης» νοείται η δυνατότητα παράδοσης πακέτων σε σχέση με την ποιότητα διαύλου ή την δυνατότητα πρόσβασης του γειτονικού κόμβου που επιλέγεται [13].

Η επιλογή και η σύνθεση μετρικών είναι κρίσιμη για την απρόσκοπτη λειτουργία του δικτύου. Οι απαιτήσεις σύγκλισης, βέλτιστης διαδρομής και χωρίς βρόχους δεν ικανοποιούνται απαραίτητα από κάθε μετρική εμπιστοσύνης. Όταν πρόκειται να συνδυαστούν με άλλες μετρικές όπως για παράδειγμα αξιοπιστία ζεύξης, είναι σημαντικό να λαμβάνονται υπόψη οι ιδιότητές του από κοινού. Για να αποδειχθεί αποδοτική μια τέτοια σύνθεση μετρικών, οι ιδιότητες και οι στόχοι των θεωρούμενων μετρικών πρέπει να συμβαδίζουν μεταξύ τους, για παράδειγμα είναι ανούσιο η σύνθεση μιας μετρικής της οποίας θεωρείται βέλτιστη η μέγιστη τιμή για μια μετρική, η οποία είναι επιθυμητό να ελαχιστοποιηθεί.

Στην συνέχεια ορίζεται μια μετρική δρομολόγησης όπου στοχεύει στην εξασφάλιση αξιοπιστίας των θεωρούμενων ζεύξεων. Συγκεκριμένα ορίζεται η μετρική ETX (Expected Transmission Time) δηλαδή ο προσδοκητός χρόνος μετάδοσης και εξετάζεται ως προς τις αλγεβρικές του ιδιότητες και του τρόπου σύνθεσής του. Η μετρική ETX επιτρέπει τον εύκολο συνδυασμό είτε μέσω αθροιστικής είτε μέσω λεξικογραφικής μεθόδου. Αξιοποιείται ευρέως ως μετρική αξιοπιστίας των ζεύξεων κατά την δρομολόγηση. Η τιμή ETX μπορεί να υπολογίζεται από τον κόμβο y_i για τον κόμβο y_j ορίζεται ως το αντίστροφο γινόμενο της πιθανότητας άφιξης πακέτων από τον κόμβο y_i στον κόμβο y_j επί την πιθανότητα αποστολής επιβεβαίωσης επιτυχούς λήψης πακέτου (acknowledgement) από τον κόμβο y_j στον κόμβο y_i ως εξής:

$$ETX_{ij} = \frac{1}{p_r^{ij} \times p_s^{ij}} \qquad (4.2)$$

όπου p_r^{ij} είναι η μετρηθείσα πιθανότητα επιτυχούς άφιξης ενός πακέτου από τον κόμβο y_i στον κόμβο y_j (ευθύς προσανατολισμός), ενώ p_s^{ij} η μετρηθείσα πιθανότητα ότι ένα πακέτο επιβεβαίωσης (ACK) θα φτάσει επιτυχώς στον κόμβο y_i (αντίστροφος προσανατολισμός). Χρησιμοποιώντας το αντίστροφο του γινομένου τους, ο υπολογισμός του ETX αποδίδει ένα κόστος ελάχιστου βάρους στις αξιόπιστες ζεύξεις. Σύμφωνα με τον μαθηματικό του ορισμό, το ETX εκφράζει τον προσδοκητό αριθμό μεταδόσεων που απαιτούνται προκειμένου ένα πακέτο να φτάσει στον προορισμό του, όταν οι χαμηλής ποιότητας ζεύξεις εισάγουν αποτυχίες μεταδόσεων. Το ETX αποτελεί μία από τις συνηθέστερες μετρικές δρομολόγησης η οποία εφαρμόζεται σε διάφορα πρωτόκολλα δρομολόγησης όπως το RPL. Η απλότητα και η αποτελεσματικότητα του αποδεικνύεται σε πληθώρα εφαρμογών, ενώ έχει εκτενώς μελετηθεί, συνδυαστεί και τροποποιηθεί προκειμένου να εντοπίσει συγκεκριμένα χαρακτηριστικά του δικτύου και να οδηγήσει σε βελτιωμένη απόδοση του δικτύου. Ένα πρωτόκολλο δρομολόγησης όπως το RPL που χρησιμοποιεί το ETX μπορεί να περιγραφεί από την αλγεβρική πλειάδα:

$$(L_{ETX}\ , \Sigma_{ETX}\ , W_{ETX}, f_{ETX}, +, \leq) \qquad (4.3)$$

Όπου L_{ETX} το σύνολο των ετικετών των ζεύξεων ή αλλιώς οι τιμές ETX των ζεύξεων που ορίζονται στο διάστημα $[1, +\infty]$, Σ_{ETX} το σύνολο των υπογραφών ή οι τιμές ETX των μονοπατιών που ορίζονται επίσης στο διάστημα $[1, +\infty]$, W_{ETX} το σύνολο των βαρών των μονοπατιών που προκύπτουν εφαρμόζοντας την συνάρτηση f_{ETX} στις υπογραφές, το σύμβολο + υποδεικνύει ότι οι ετικέτες και οι υπογραφές προστίθενται προκειμένου να προκύψει η υπογραφή του μονοπατιού, ενώ η σχέση διάταξης είναι $\leq$. Το σύνολο W_{ETX} συνδέεται στενά με την επιλογή της συνάρτησης f_{ETX} . Ο υπολογισμός του βάρους των μονοπατιών βάσει της άθροισης των τιμών ETX των επιμέρους ζεύξεων στηρίζεται στη ρεαλιστική υπόθεση ότι το σύστημα υποστηρίζει αναμεταδόσεις του στρώματος ζεύξης δεδομένων. Δηλαδή, κάθε κόμβος που ανήκει στο μονοπάτι θα μεταδίδει εκ νέου ένα πακέτο, για το οποίο δεν έχει λάβει επιβεβαίωση, προκειμένου η λήψη του τελικά να είναι εγγυημένη.

4.9 Σύνθεση Μετρικών Δρομολόγησης

Οι μετρικές δρομολόγησης στοχεύουν στην ανίχνευση συγκεκριμένων συμπεριφορών ή χαρακτηριστικών των ζεύξεων. Κάποιες διαφορετικές μετρικές εξυπηρετούν διαφορετικούς σκοπούς. Μια μετρική μπορεί να παρατηρεί μια συγκεκριμένη συμπεριφορά, αλλά μπορεί να αδυνατεί να αποφύγει κάποιες διαφοροποιημένες συμπεριφορές. Σε πραγματικές εφαρμογές μπορεί να αποφευχθούν διάφοροι τύποι συμπεριφορών, επομένως μία μεμονωμένη μετρική δεν είναι κατάλληλη για να καλύψει μια λίστα από απαιτήσεις. Επομένως, η χρήση πολλαπλών μετρικών πολλές φορές επιβάλλεται. Η σύνθεση πολλαπλών μετρικών είναι αναγκαία, εφόσον απαιτείται και ικανοποίηση των απαιτήσεων δρομολόγησης. Η σύνθεση είναι σημαντική για την εξασφάλιση της ορθής λειτουργίας κάθε μεμονωμένης μετρικής και για την κάλυψη των απαιτήσεων του πρωτοκόλλου δρομολόγησης. Δύο κύριες εναλλακτικές μέθοδοι συνδυασμού πολλαπλών μετρικών είναι η λεξικογραφική σύνθεση μετρικών και η αθροιστική σύνθεση μετρικών [13]. Παράδειγμα αθροιστικής σύνθεσης μετρικών παρουσιάζεται παρακάτω στο κεφάλαιο 5 όπου σαν μετρικές αθροίζονται το hop count και το κόστος της ποσοστιαίας ενέργειας της μπαταρίας.

ΚΕΦΑΛΑΙΟ 5

Αποτίμηση της Επίδοσης του Πρωτοκόλλου RPL

5.1 Πειραματισμός και Εξαγωγή Αποτελεσμάτων

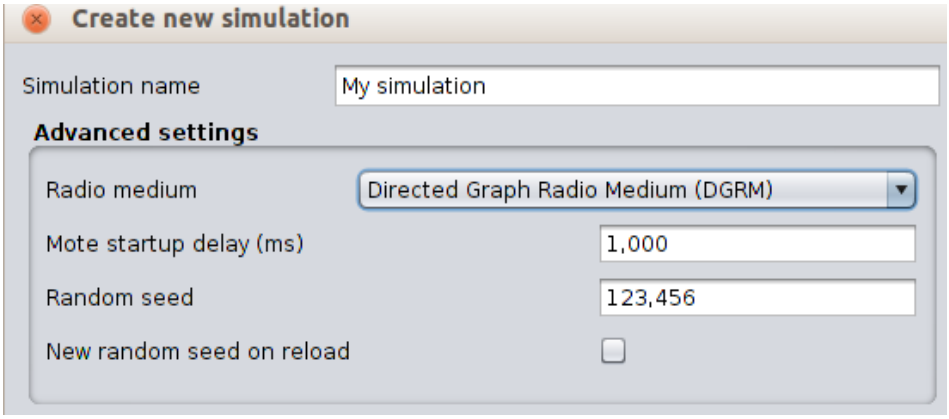
Για την μελέτη των ήδη τυποποιημένων μετρικών δρομολόγησης και την πειραματική αξιολόγηση της επίδοσης του πρωτοκόλλου RPL, καθώς επίσης και για την διεξαγωγή προσομοιώσεων κάποιων σεναρίων χρησιμοποιήθηκε το λειτουργό σύστημα Contiki 3.0. Το σύστημα αυτό είναι γραμμένο σε γλώσσα προγραμματισμού C και μπορεί να τρέξει σε μια ποικιλία από πλατφόρμες συμπεριλαμβανομένου και προσωπικών υπολογιστών μέσω του περιβάλλοντος Ubuntu [19]. Επίσης στην παρούσα διπλωματική εργασία χρησιμοποιήθηκε το εργαλείο προσομοίωσης Cooja όπου οι προσομοιώσεις μπορεί να γίνουν σε δίκτυα μεγάλου μεγέθους και βοηθά στην αξιολόγηση και στην αποσφαλμάτωση του κώδικα [18].

Ο προσομοιωτής (simulator) βρίσκεται στον φάκελο contiki/tools/cooja και το ανοίγουμε από το terminal πατώντας την εντολή ant run [20]. Εάν έχουμε εκτελέσει πολλές προσομοιώσεις καλό είναι να καθαρίζουμε τον φάκελο του Cooja εκτελώντας στο terminal την εντολή: contiki /tools/cooja ant clean και αν θέλουμε να την εκτελέσουμε ως administrator contiki/tools/cooja sudo ant clean. Για την παρακολούθηση των πακέτων χρησιμοποιήθηκε το πρόγραμμα Wireshark. Όλα τα αποτελέσματα που φαίνονται στο παρόν κεφάλαιο έχουν ληφθεί με χρήση του προσομοιωτή Contiki Cooja προκειμένου να είναι εύκολη η μεταφορά του κώδικα σε πραγματικές συσκευές αισθητήρων.

5.2 ETX (Expected Transmission Count)

5.2.1 Σενάριο 1

Για την επίδειξη της χρήσης της μετρικής ETX χρησιμοποιήθηκε το αρχείο contiki/examples/ipv6/simple-udp-rpl που αποτελεί εφαρμογή αποστολής δεδομένων μέσω μιας σύνδεσης UDP από τους clients (κόμβους) στην πηγή. Αφού ανοίξουμε το Cooja, εκτελούμε κάποιες ενέργειες.



Εικόνα 54: Δημιουργία Προσομοίωσης Contiki-Cooja

Σύμφωνα με την εικόνα 54, η πειραματική μας τοπολογία επιλέγουμε να είναι Directed Graph Radio Medium, δηλαδή κατευθυνόμενος γράφος. Στην συνέχεια όπως φαίνεται και

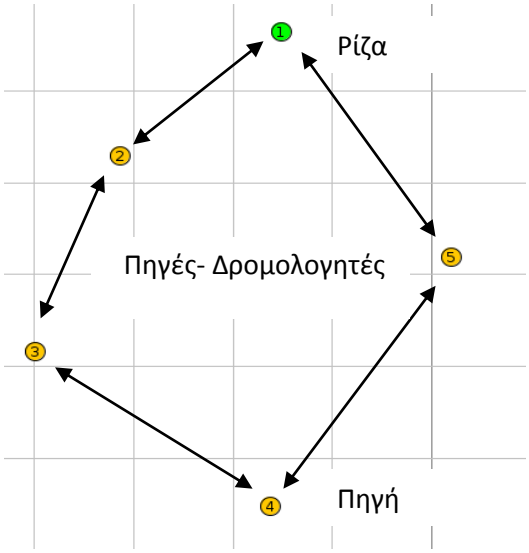
παρακάτω στην εικόνα 55, στο DGRM Configurator ορίζουμε τις πιθανότητες επιτυχίας προώθησης του πακέτου μεταξύ των κόμβων και παρατηρούμε ότι οι πιθανότητες αυτές μεταξύ των κόμβων είναι μη συμμετρικές.

DGRM Configurator

Source	Destination	RX Ratio	RSSI	LQI	Delay
Contiki 1	Contiki 2	100.0%	-10.0	105	0 ms
Contiki 2	Contiki 1	100.0%	-10.0	105	0 ms
Contiki 2	Contiki 3	100.0%	-10.0	105	0 ms
Contiki 3	Contiki 2	100.0%	-10.0	105	0 ms
Contiki 3	Contiki 4	100.0%	-10.0	105	0 ms
Contiki 4	Contiki 3	100.0%	-10.0	105	0 ms
Contiki 4	Contiki 5	40.0%	-10.0	105	0 ms
Contiki 5	Contiki 4	40.0%	-10.0	105	0 ms
Contiki 5	Contiki 1	40.0%	-10.0	105	0 ms
Contiki 1	Contiki 5	40.0%	-10.0	105	0 ms

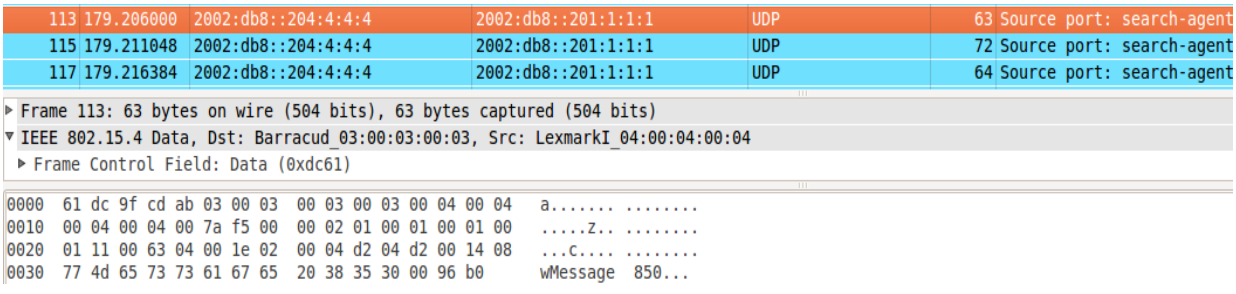
Εικόνα 55: DGRM Configurator Contiki-Cooja

Στην συνέχεια δημιουργήσαμε την τοπολογία του δικτύου μας που απαρτίζεται από 5 κόμβους. Ο κόμβος 4 στέλνει πακέτα προς την ρίζα τον 1 (end to end) δηλαδή από άκρη σε άκρη. Οι κόμβοι 2,3,5 είναι πηγές – δρομολογητές. Εξετάζουμε ότι ο κόμβος 4 που είναι η πηγή, διαλέγει το μονοπάτι με την καλύτερη ποιότητα ζεύξης, καθώς και τον προτιμώμενο γονέα (preferred parent) που θα στείλει τα πακέτα.

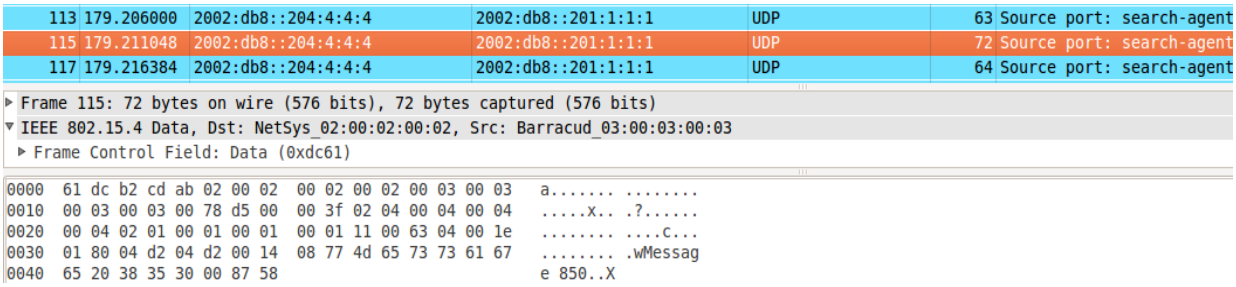


Εικόνα 56: Τοπολογία Δικτύου (από Contiki-Cooja)

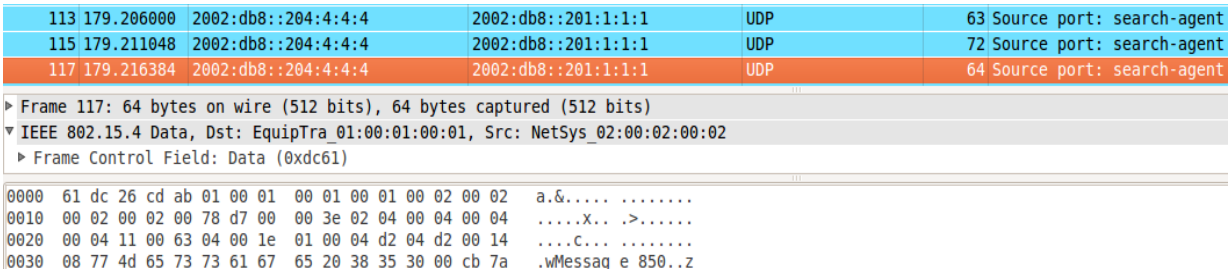
Στην συνέχεια με την βοήθεια του Wireshark παρατηρούμε την δρομολόγηση του πακέτου μέσα από τους κόμβους του δικτύου.



Εικόνα 57: Διαδρομή Πακέτου (από Wireshark)

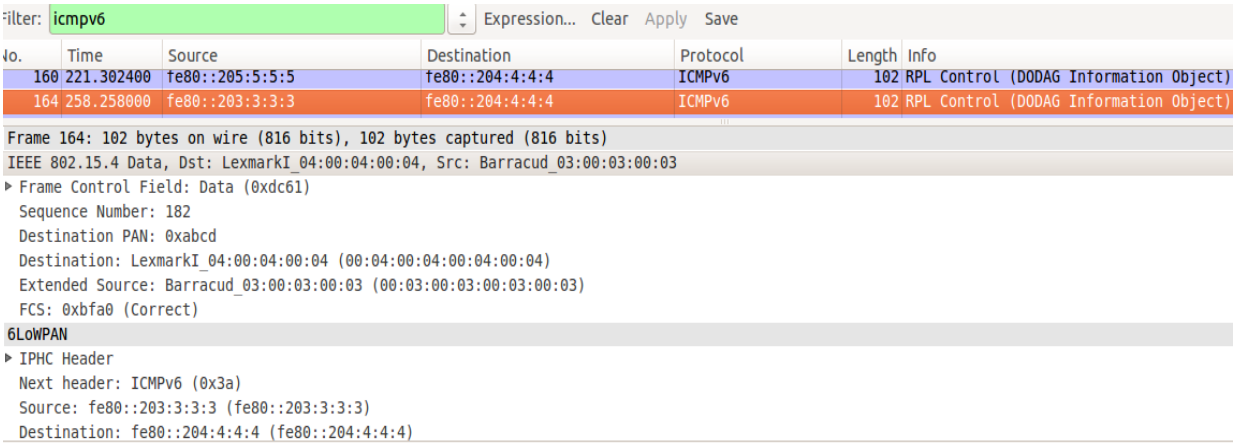


Εικόνα 58: Διαδρομή Πακέτου (από Wireshark)



Εικόνα 59: Διαδρομή Πακέτου (από Wireshark)

Επομένως από τις εικόνες 57 έως 59 παρατηρούμε ότι ο κόμβος 4 που είναι η πηγή στέλνει UDP μήνυμα προς την ρίζα (κόμβος 1). Το πακέτο αυτό από ότι παρατηρείται είναι το μήνυμα με αύξοντα αριθμό 850 και δεν αλλάζει. Ο κόμβος 4 διαλέγει σαν προτιμώμενο γονέα (preferred parent) τον κόμβο 3 για να στείλει το πακέτο του στην ρίζα. Στη συνέχεια το πακέτο "ταξιδεύει" από τον 4 μέσω του 3 στην συνέχεια μέσω του 2 με τελικό προορισμό τον 1.



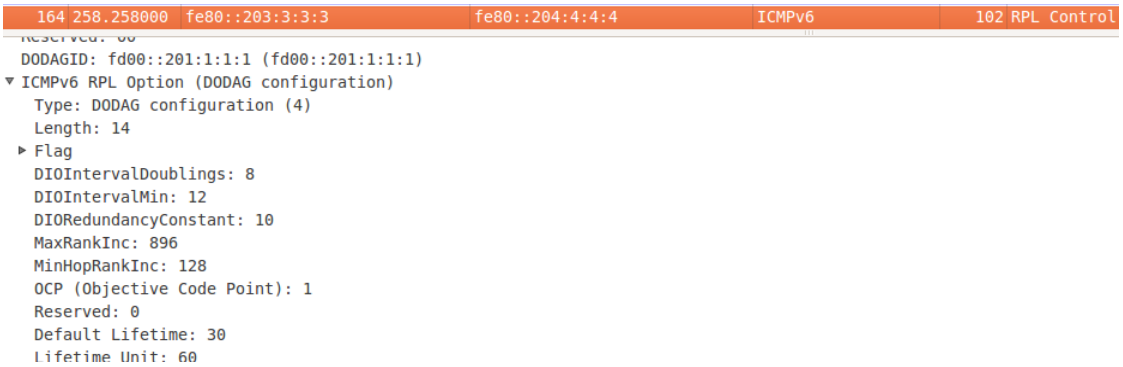
Εικόνα 60: Μηνύματα Πρωτόκολλων Δρομολόγησης (από Wireshark)

Όπως φαίνεται στην εικόνα 60 το λογισμικό Wireshark δείχνει ένα DIO μήνυμα από τον κόμβο 3 προς τον κόμβο 4. Το time είναι ο χρόνος προσομοίωσης που τρέχει, source είναι ο κόμβος που στέλνει το πακέτο και φαίνεται ότι ο κάθε κόμβος έχει την δική του μοναδική διεύθυνση όπως για παράδειγμα ο κόμβος 4 που προορίζεται το μήνυμα έχει μια IPv6

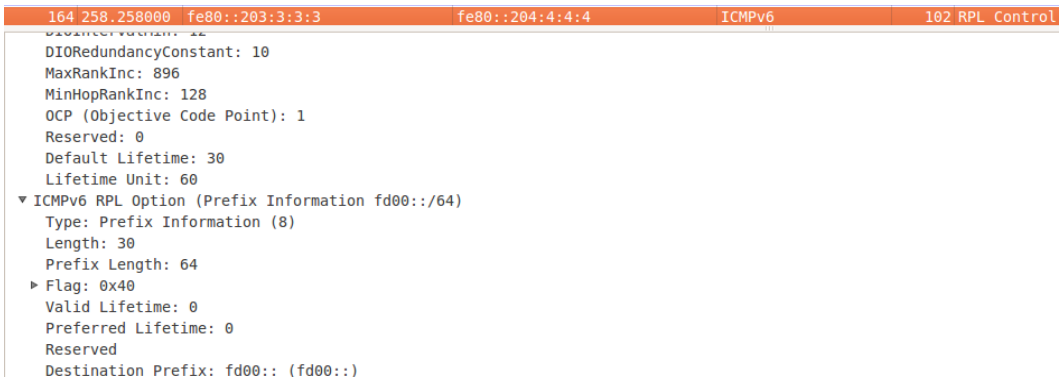
διεύθυνση fe80::204:4:4:4 καθώς και ο κόμβος 3 έχει μία IPv6 διεύθυνση fe80::203:3:3:3 αντίστοιχα. Σαν Info (Information) είναι η πληροφορία δηλαδή το DIO μήνυμα.

Εικόνα 61: Μηνύματα Πρωτόκολλων Δρομολόγησης (από Wireshark)

Στην εικόνα 61 παρατηρούμε ότι το Wireshark μας εμφανίζει ένα μήνυμα του πρωτοκόλλου δρομολόγησης (το οποίο μεταφέρεται ως μήνυμα Internet Control Message Protocol v6). Παραπάνω φαίνεται ο τύπος του μηνύματος ελέγχου του RPL (RPL Control). Στην συνέχεια το Code 1 προσδιορίζει το DIO μήνυμα δηλαδή το DODAG Information Object. Το RPL Instance ID προσδιορίζει την παρουσία (Instance) της τοπολογίας που συνδέεται με το DODAG. Επίσης παρατηρούμε ότι ο βαθμός της μεταξύ τους απόστασης των κόμβων είναι 384 (Rank=384). Τέλος φαίνεται ο αριθμός έκδοσης (Version) που ορίζεται από την ρίζα, κάποιες σημαίες, και το DODAG ID όπου είναι η διεύθυνση IPv6 της ρίζας όπου αυτή η διεύθυνση είναι μοναδική. Ο αριθμός DTSN (Destination Trigger Sequence Number) είναι ένας ακέραιος μη προσημασμένος αριθμός που ορίζεται από τον κόμβο που εκδίδει το μήνυμα DIO.



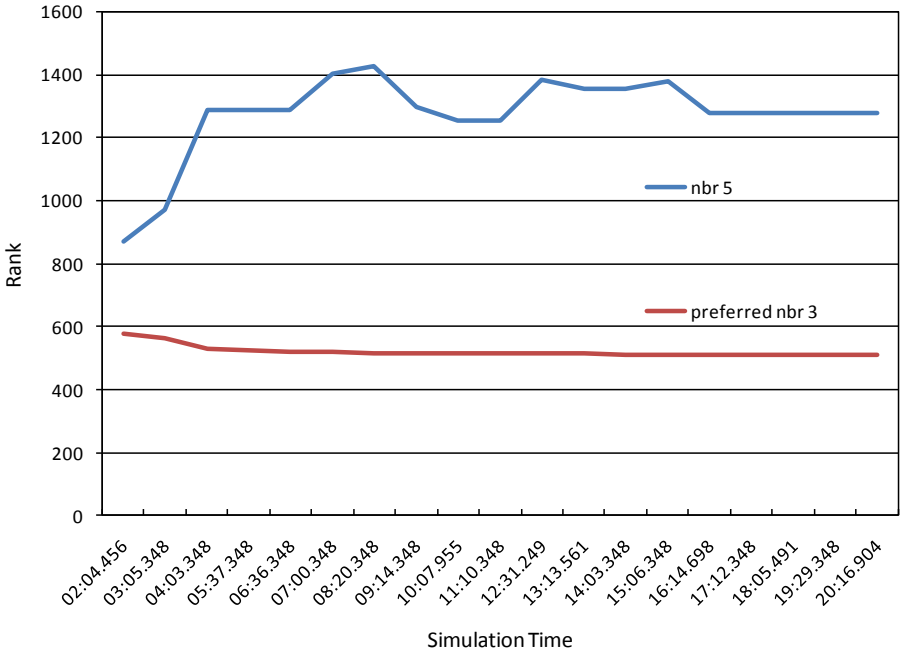
Εικόνα 62: Μηνύματα Πρωτόκολλων Δρομολόγησης (από Wireshark)



Εικόνα 63: Μηνύματα Πρωτόκολλων Δρομολόγησης (από Wireshark)

Στις εικόνες 62 και 63 παρατηρούμε κάποιες επιλογές (RPL Options) και κάποιες σημαίες flags. Το Max Rank Increase προσδιορίζει τον μέγιστο βαθμό της μεταξύ τους απόστασης και το Min Hop Rank Increase δείχνει το μικρότερο κόστος διαδρομής μεταξύ των κόμβων που είναι το 128. Το Objective Code Point προσδιορίζει το κωδικό σημείο που αναγνωρίζεται η αντικειμενική συνάρτηση μέσα στην MRHOF. Τέλος παρατηρούμε την επιλογή πληροφορίας διαδρομής (Route Information Option) που υπάρχει στο μήνυμα DIO. Βλέπουμε τον αριθμό του μήκους του προθέματος (prefix length), τον αριθμό της πληροφορίας του προθέματος καθώς και τις σημαίες. Η πληροφορία του προθέματος είναι μια IPv6 διεύθυνση.

Παρακάτω φαίνεται το διάγραμμα με τους προτιμώμενους γονείς (preferred parents) του κόμβου 4, δηλαδή της πηγής. Στο simulation του Cooja στο mote output στο φίλτρο πατήσαμε ID:4 RPL: nbr για να μας εμφανίσει τους προτιμώμενους γονείς με το rank τους. Επίσης για να μας εμφανίσει τα μηνύματα πήγαμε στο μονοπάτι contiki/core/net/rpl και ανοίξαμε τον φάκελο rpl-dag.c και στην εντολή #define DEBUG_NONE ορίσαμε το1 δηλαδή #define DEBUG 1 για να μας εκτυπώνει όλα τα μηνύματα από τον κώδικα στο mote output του Cooja.



Εικόνα 64: Διάγραμμα Προτιμώμενων Γονέων

Στην συνέχεια παρουσιάζονται συμπεράσματα και παρατηρήσεις από την εκτέλεση της προσομοίωσης.

Καθώς πραγματοποιήσαμε το πείραμα παρατηρήσαμε ότι η πλατφόρμα Z1 στο συγκεκριμένο σενάριο δεν δουλεύει σωστά δηλαδή τα αποτελέσματα με τις πιθανότητες επιτυχίας που ορίζαμε στους κόμβους δεν ήταν τα αναμενόμενα. Για αυτόν τον λόγο επιλέξαμε τα cooja motes. Επίσης από το παραπάνω διάγραμμα συμπεραίνουμε ότι ο κόμβος 4 δηλαδή η πηγή μας επιλέγει σαν προτιμώμενο γονέα τον 3 διότι έχει μικρότερο rank σε σύγκριση με τον κόμβο 5. Επομένως όπως φαίνεται και στο Wireshark το πακέτο UDP που στέλνει ο 4

μεταδίδεται στο 3 (προτιμώμενος γονέας), από τον 3 στον 2 και μετά στον 1 (ρίζα). Ο κόμβος 5 έχει πολύ μεγάλο rank διότι η ζεύξη με την πηγή είναι πολύ κακή και αυτό οφείλεται στην μικρή πιθανότητα επιτυχίας (40%) που έχουμε εμείς ορίσει. Ο κόμβος 3 αντίστοιχα έχει μικρό rank διότι η ζεύξη είναι πολύ καλύτερη και η πιθανότητα επιτυχίας που έχουμε ορίσει υψηλή (100%). Τέλος στο διάγραμμα παρατηρούμε κάποιες αυξομειώσεις του rank των κόμβων που αυτές οφείλονται στον τρόπο υπολογισμού του ETX στο contiki. Επομένως συμπεραίνουμε ότι το ETX αποσκοπεί στην μικρότερη κατανάλωση ενέργειας διότι αποφεύγει ζεύξεις με κακή ποιότητα.

5.3 Χρόνος Διάρκειας Ζωής Δικτύου

5.3.1 Σενάριο 2

Για την υλοποίηση του σεναρίου αυτού, δηλαδή για τον χρόνο διάρκειας ζωής του δικτύου, χρησιμοποιήθηκε το μοντέλο κατανάλωσης ενέργειας της μπαταρίας το οποίο υλοποιήσαμε στα πλαίσια της πειραματικής μελέτης. Χρησιμοποιήσαμε τα αρχεία του contiki καθώς και το cooja στο εξής μονοπάτι: contiki/tools/cooja. Επίσης χρησιμοποιήθηκαν τα μοτάκια της πλατφόρμας Z1 του contiki. Στην συνέχεια απενεργοποιήσαμε το Radio Duty Cycle μέσω χρήσης της εντολής #define NETSTACK_CONF_RDC nullrdc_driver στο αρχείο contiki/platform/Z1 contiki-conf.h . Απενεργοποιώντας το Radio Duty Cycle τα μοτάκια δεν μπαίνουν στη διαδικασία κατάστασης ύπνωσης (sleep mode) και είναι συνέχεια αναμμένα. Δηλαδή, το Radio on είναι 100% και ο ασύρματος πομποδέκτης θα σβήσει μόνο όταν τελειώσει η μπαταρία τους. Ουσιαστικά το Radio Duty Cycle μας δείχνει σε ένα ποσοστό χρόνου για πόση ώρα είναι ενεργός ο πομποδέκτης καθώς επίσης μας δείχνει τα ποσοστά του χρόνου που μεταδίδουν αλλά και που λαμβάνουν. Στην συνέχεια για να πάρουμε τις πληροφορίες των ποσοστών χρόνου μετάδοσης και λήψης, ανοίξαμε τον φάκελο του powertrace στο μονοπάτι contiki/apps/powertrace και στο αρχείο powertrace.c βρίσκεται ο κώδικας όπου τον μελετήσαμε βρήκαμε τα σημεία όπου υπολογίζονται τα ποσοστά χρόνου μετάδοσης και λήψης receive_perc transmit_perc και τα εκτυπώσαμε με την χρήση της εντολής printf.

```
140         receive_perc = (int)(100*((100L * listen) / time)) + (int)((10000L * listen) / time - (100L * listen / time) * 100);        //jvoug//
141         transmit_perc = (int)(100*((100L * transmit) / time)) + (int)((10000L * transmit) / time - (100L * transmit / time) * 100);     //jvoug//
142 printf("\nradio transmit perc = %d%% radio receive perc = %d%%\n", transmit_perc, receive_perc); //jvoug//
```

Εικόνα 65: Κώδικας των Ποσοστών Χρόνου Μετάδοσης και Λήψης

Στην συνέχεια όπως φαίνεται και από την εικόνα 65 πήραμε και εκτυπώσαμε τις πληροφορίες των ποσοστών χρόνου μετάδοσης και λήψης. Στην συνέχεια πήραμε τα αποτελέσματα από το mote output του cooja και τα χρησιμοποιήσαμε στο κώδικα κατανάλωσης ενέργειας της μπαταρίας. Τον κώδικα που υπολογίζει την ποσοστιαία κατανάλωση ενέργειας της μπαταρίας τον γράψαμε στο αρχείο unicast_sender.c που βρίσκεται στον φάκελο contiki/examples/ipv6/simple-udp-rpl.

```
106 unsigned long full_battery_mAh=2100;
107       unsigned long power_average_receive=300;
108       unsigned long power_average_transmit=600000;
109      extern int receive_perc;
110      extern int transmit_perc;
111        extern  uint16_t current_battery_level_perc;
112         unsigned long time_elapsed_in_seconds;
```

Εικόνα 66: Μεταβλητές για την Ποσοστιαία Κατανάλωση ενέργειας Μπαταρίας

Στην εικόνα 66 φαίνεται ότι έχουμε ορίσει κάποιες παραμέτρους του μοντέλου κατανάλωσης ενέργειας της μπαταρίας. Τις τιμές της ισχύος μετάδοσης (power average transmit) και λήψης (receive) αντίστοιχα τις ορίσαμε εμείς για τις ανάγκες του μοντέλου. Οι παρουσιαζόμενες τιμές, δεν αντιστοιχούν σε ρεαλιστικές τιμές – ενδεικτικά αναφέρεται ότι η ισχύς μετάδοσης (transmit power) είναι πολλές τάξεις μεγέθους μεγαλύτερη από αυτή που χαρακτηρίζει τα πραγματικά συστήματα. Η ισχύς αυτή ελήφθη εσκεμμένα πολύ μεγάλη προκειμένου να παρατηρήσουμε με γρήγορο τρόπο την επίδρασή της κατά την διάρκεια της προσομοίωσης. Οι μπαταρίες οι οποίες χρησιμοποιούνται στο μοντέλο μας είναι AA των 2100 mAh. Ωστόσο τις τιμές των ποσοστών του χρόνου μετάδοσης και λήψης τις πήραμε από τον κώδικα του powertrace. Στην παράμετρο time elapsed in seconds έχουμε ορίσει την συνάρτηση clock seconds όπου είναι του contiki και επιστρέφει τον χρόνο του συστήματος σε δευτερόλεπτα. Οι μεταβλητές που χρησιμοποιούμε στον κώδικα είναι unsigned long δηλαδή των 32 bits (4 bytes). Ο κώδικας του μοντέλου εκτελείται μέσα σε μια μακροεντολή PROCESS που δηλώνει μια νέα διαδικασία στο contiki.

```
142 time_elapsed_in_seconds = 2*clock_seconds();
143       printf("Clock system in seconds: %lu\n", time_elapsed_in_seconds);
144         printf("receive_perc is %d and transmit_perc is %d and time elapsed is %d\n", receive_perc, transmit_perc, time_elapsed_in_seconds);
145                 printf("int is %d and power_average_transmit is %d\n", sizeof(uint32_t), power_average_transmit);
146
147         transmit_perc = 94;
148         receive_perc = 9914;
149
150 current_battery_level_perc = 100*((full_battery_mAh - ((power_average_receive/3600.0)*(receive_perc/100.0) +  (power_average_transmit/3600.0)*
    (transmit_perc/100.0)))/100.0*time_elapsed_in_seconds)/full_battery_mAh);
151 printf("battery level is: %d\n",current_battery_level_perc);
```

Εικόνα 67: Κώδικας Ποσοστιαίας Κατανάλωσης ενέργειας Μπαταρίας

Όπως φαίνεται από την εικόνα 67 υπολογίζεται μέσα από μαθηματικές πράξεις και παραμέτρους που έχουμε ορίσει, η ποσοστιαία κατανάλωση ενέργειας της μπαταρίας. Τα αποτελέσματα των μεγεθών που προκύπτουν από τις πράξεις τα διαιρούμε με το 100 ώστε να έχουμε την ποσοστιαία (%) μορφή τους. Όπου 3600 τα δευτερόλεπτα της 1 ώρας διότι το επίπεδο κατανάλωσης ενέργειας της μπαταρίας που πέφτει εκφράζεται ανά ώρα. Στον κώδικα του μοντέλου υπολογίζεται η ποσοστιαία κατανάλωση ενέργειας όταν πραγματοποιείται λήψη (receive) και η ποσοστιαία κατανάλωση ενέργειας όταν πραγματοποιείται μετάδοση (transmission). Τέλος με την χρήση της εντολής printf εκτυπώνουμε στο mote output του Cooja τα αποτελέσματα της ποσοστιαίας κατανάλωσης ενέργειας μπαταρίας.

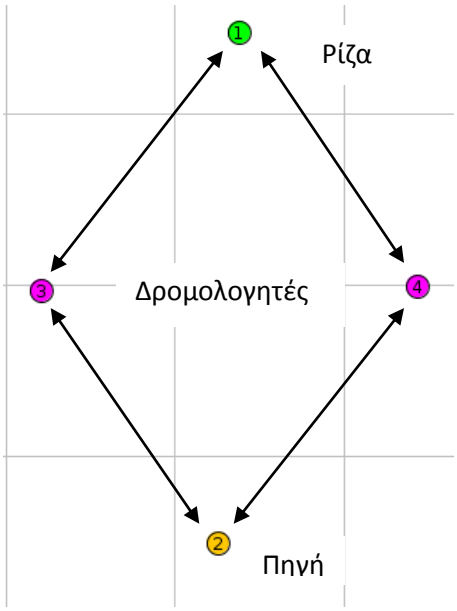
```
159       printf("Sending unicast to ");
160       uip_debug_ipaddr_print(addr);
161       printf("\n");
162       sprintf(buf, "Giannis %d", message_number);
163       message_number++;
164       simple_udp_sendto(&unicast_connection, buf, strlen(buf) + 1, addr);
```

Εικόνα 68: Δημιουργία και Αποστολή UDP πακέτου πληροφορίας

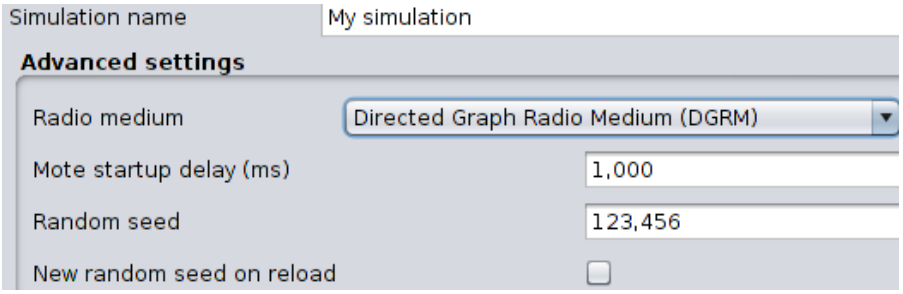
Στην εικόνα 68 φαίνεται ότι στο τμήμα της μνήμης (buffer) είναι αποθηκευμένη η πληροφορία που στέλνεται και είναι της μορφής “Giannis”.

Η πληροφορία αυτή στέλνεται σαν UDP πακέτο από την πηγή (sender) και είναι των 10-15 bytes. Επίσης τυπώνεται και ο αύξων αριθμός της πληροφορίας.

Έχουμε την παρακάτω τοπολογία ενός δικτύου.



Η τοπολογία του δικτύου μας χαρακτηρίζεται από τέσσερις κόμβους όπου ο 4 και ο 3 είναι δρομολογητές (relays), ο 2 είναι η πηγή που στέλνει τα πακέτα προς την ρίζα όπου η ρίζα είναι ο 1 δηλαδή ο δέκτης. Οι κόμβοι δρομολογητές μεταφέρουν τα πακέτα από τον κόμβο 2 προς την ρίζα. Κάνουμε μια εκτίμηση του χρόνου διάρκειας ζωής του δικτύου όπου όταν η ενέργεια της μπαταρίας του κόμβου 2 μηδενιστεί τότε όλο το δίκτυο θα βγει εκτός λειτουργίας. Θα κάνουμε δυο εκτιμήσεις χρόνου διάρκειας ζωής δικτύου. Η πρώτη εκτίμηση είναι όταν το power average transmit (ισχύς μετάδοσης) όπου συνδέεται ρητά με το μοντέλο κατανάλωσης ενέργειας της μπαταρίας που έχουμε δημιουργήσει, έχει power average transmit = 600000 mW και η δεύτερη όταν power average transmit = 300000 mW. Θα μετρήσουμε ξεχωριστά γι’ αυτές τις δύο περιπτώσεις, θα βγάλουμε ξεχωριστά πορίσματα, θα τα συγκρίνουμε και θα διατυπώσουμε τα συμπεράσματα μας.

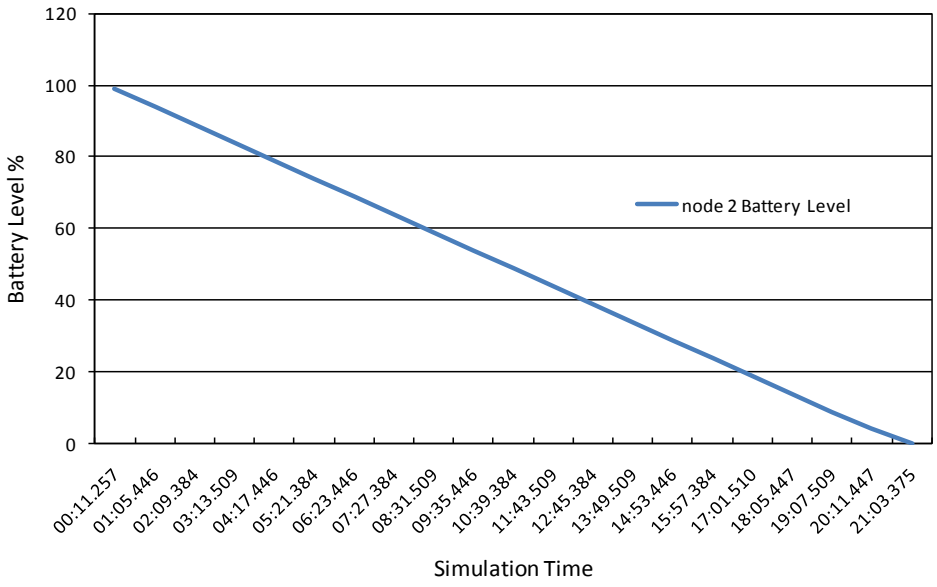


Εικόνα 69: Δημιουργία Προσομοίωσης Contiki-Cooja

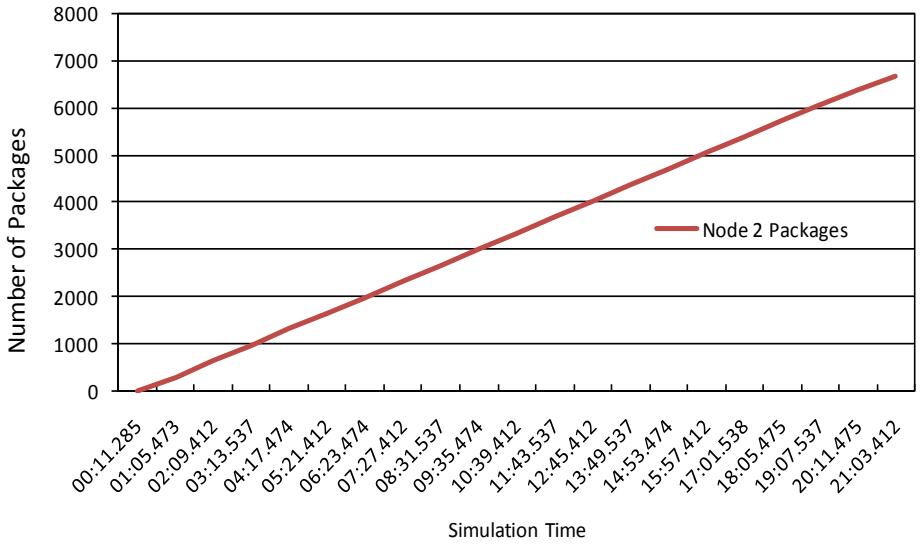
Source	Destination	RX Ratio	RSSI
Z1 2	Z1 3	100.0%	-10.0
Z1 3	Z1 2	100.0%	-10.0
Z1 3	Z1 1	100.0%	-10.0
Z1 1	Z1 3	100.0%	-10.0
Z1 2	Z1 4	100.0%	-10.0
Z1 4	Z1 2	100.0%	-10.0
Z1 4	Z1 1	100.0%	-10.0
Z1 1	Z1 4	100.0%	-10.0

Εικόνα 70: DGRM Configurator Contiki-Cooja

Για *power average transmit= 600000 mW* έχουμε τα αποτελέσματα που φαίνονται στα παρακάτω γραφήματα στις εικόνες 71 μέχρι 72:



Εικόνα 71: Διάγραμμα Χρόνου Διάρκειας Ζωής Δικτύου



Εικόνα 72: Διάγραμμα Συνολικού Αριθμού Πακέτων

Σύμφωνα από τις εικόνες 71 έως 73 παρατηρούμε ότι η ενέργεια της μπαταρίας του κόμβου 2 μηδενίζεται σε 21:03.375 που αντιστοιχεί σε 21 ώρες 3 λεπτά και 375 δευτερόλεπτα που σημαίνει και το τέλος διάρκειας ζωής του δικτύου. Μέσα σε αυτές τις ώρες ο κόμβος 2 έστειλε 6.678 πακέτα μέγεθος πληροφορίας UDP της μορφής “Giannis” των 13 bytes.

```
21:02.850  ID:1   Data received from aaaa::c30c:0:0:2 on port 1234 from port 1234 with length 13: 'Giannis 6675'
21:03.169  ID:1   Data received from aaaa::c30c:0:0:2 on port 1234 from port 1234 with length 13: 'Giannis 6676'
21:03.255  ID:1   Data received from aaaa::c30c:0:0:2 on port 1234 from port 1234 with length 13: 'Giannis 6677'
21:03.412  ID:1   Data received from aaaa::c30c:0:0:2 on port 1234 from port 1234 with length 13: 'Giannis 6678'
```

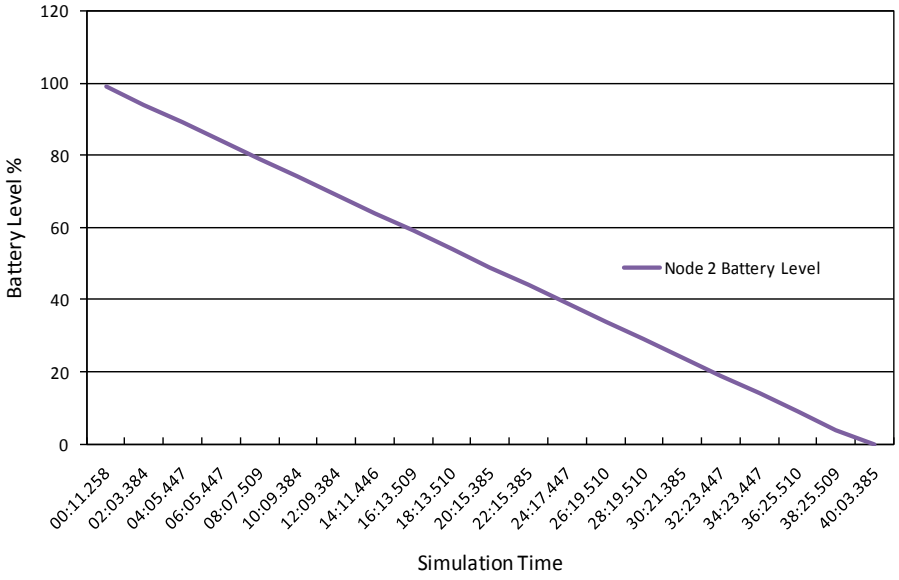
Εικόνα 73: Σύνολο Πακέτων που ελήφθησαν από τον προορισμό

```
7059 476.435000  2002:db8::c30c:0:0:2   2002:db8::c30c:0:0:1   UDP   64 Source port: search-agent
▸ IPHC Header
  Next header: IPv6 hop-by-hop option (0x00)
  Source: 2002:db8::c30c:0:0:2 (2002:db8::c30c:0:0:2)
  Destination: 2002:db8::c30c:0:0:1 (2002:db8::c30c:0:0:1)
▾ Internet Protocol Version 6, Src: 2002:db8::c30c:0:0:2 (2002:db8::c30c:0:0:2), Dst: 2002:db8::c30c:0:0:1 (2002:db8::c30c:0:0:1)
  0110 .... = Version: 6

0000  41 dc 1f cd ab 04 00 00  00 00 00 0c c1 02 00 00   A....... ........
0010  00 00 00 0c c1 7a f5 00  00 c3 0c 00 00 00 00 00   .....z.. ........
0020  01 11 00 63 04 00 1e 02  48 04 d2 04 d2 00 15 28   ...c.... H......(
0030  e6 47 69 61 6e 6e 69 73  20 35 31 32 36 00 ed 02   .Giannis  5126...
```

Εικόνα 74: Δεδομένα πακέτου UDP (από Wireshark)

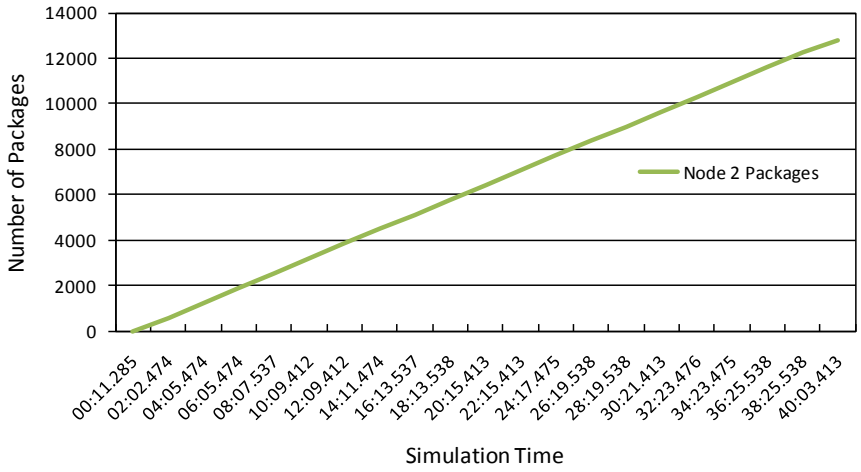
Για *power average transmit= 300000 mW* έχουμε τα αποτελέσματα που φαίνονται στα παρακάτω γραφήματα στις εικόνες 75 μέχρι 77.



Εικόνα 75: Διάγραμμα Χρόνου Διάρκειας Ζωής Δικτύου

```
40:02.822  ID:2   battery level is: 1
40:03.090  ID:2   battery level is: 1
40:03.229  ID:2   battery level is: 1
40:03.385  ID:2   battery level is: 0
```

Εικόνα 76: Χρόνος Ποσοστιαίας Κατανάλωσης Ενέργειας Μπαταρίας



Εικόνα 77: Διάγραμμα Συνολικού Αριθμού Πακέτων

Σύμφωνα από τις εικόνες 75 έως 77 παρατηρούμε ότι η ενέργεια της μπαταρίας του κόμβου 2 μηδενίζεται σε 40:03.413 που αντιστοιχεί σε 40 ώρες 3 λεπτά και 413 δευτερόλεπτα που σημαίνει και το τέλος διάρκειας ζωής του δικτύου. Μέσα σε αυτές τις ώρες ο κόμβος 2 έστειλε 12.758 πακέτα μέγεθος πληροφορίας UDP της μορφής “Giannis” των 14 bytes.

```
40:02.850  ID:1  Data received from aaaa::c30c:0:0:2 on port 1234 from port 1234 with length 14: 'Giannis 12755'
40:03.171  ID:1  Data received from aaaa::c30c:0:0:2 on port 1234 from port 1234 with length 14: 'Giannis 12756'
40:03.257  ID:1  Data received from aaaa::c30c:0:0:2 on port 1234 from port 1234 with length 14: 'Giannis 12757'
40:03.413  ID:1  Data received from aaaa::c30c:0:0:2 on port 1234 from port 1234 with length 14: 'Giannis 12758'
```

Εικόνα 78: Σύνολο Πακέτων που ελήφθησαν από τον προορισμό

```
8809 821.043000  2002:db8::c30c:0:0:2  2002:db8::c30c:0:0:1  UDP  57 Source port: search-agent
▸ Frame 8809: 57 bytes on wire (456 bits), 57 bytes captured (456 bits)
▸ IEEE 802.15.4 Data, Dst: c1:0c:0000:00:0000:01, Src: c1:0c:0000:00:0000:02
▸ 6LoWPAN
▸ Internet Protocol Version 6, Src: 2002:db8::c30c:0:0:2 (2002:db8::c30c:0:0:2), Dst: 2002:db8::c30c:0:0:1 (2002:db8::c30c:0:0:1)
▸ User Datagram Protocol, Src Port: search-agent (1234), Dst Port: search-agent (1234)
▸ Data (14 bytes)

0000  41 dc 05 cd ab 01 00 00  00 00 00 0c c1 02 00 00   A....... ........
0010  00 00 00 0c c1 7a f7 00  00 11 00 63 04 00 1e 01   .....z.. ...c....
0020  64 04 d2 04 d2 00 16 ef  e3 47 69 61 6e 6e 69 73   d....... .Giannis
0030  20 31 32 37 35 38 00 c0  93                        12758.. .
```

Εικόνα 79: Δεδομένα πακέτου UDP (από Wireshark)

Στους παρακάτω πίνακες φαίνονται αναλυτικά οι τιμές. Στον πίνακα 1 φαίνεται το επίπεδο της ποσοστιαίας κατανάλωσης ενέργειας της μπαταρίας συναρτήσει του χρόνου προσομοίωσης που αντιστοιχεί σε ώρες λεπτά και δευτερόλεπτα για δύο διαφορετικές περιπτώσεις ισχύος μετάδοσης. Στον πίνακα 2 φαίνεται ο αριθμός των πακέτων που έχουν σταλεί συναρτήσει του χρόνου προσομοίωσης για δύο διαφορετικές περιπτώσεις ισχύος.

Power Average Transmit = 600000 mW		*Power Average Transmit = 300000 mW*	
Simulation Time	*Battery level %*	*Simulation Time*	*Battery level %*
00:11.257	99	00:11.258	99
01:05.446	94	02:03.384	94
02:09.384	89	04:05.447	89
03:13.509	84	06:05.447	84
04:17.446	79	08:07.509	79
05:21.384	74	10:09.384	74
06:23.446	69	12:09.384	69
07:27.384	64	14:11.446	64
08:31.509	59	16:13.509	59
09:35.446	54	18:13.510	54
10:39.384	49	20:15.385	49
11:43.509	44	22:15.385	44
12:45.384	39	24:17.447	39
13:49.509	34	26:19.510	34
14:53.446	29	28:19.510	29
15:57.384	24	30:21.385	24
17:01.510	19	32:23.447	19
18:05.447	14	34:23.447	14
19:07.509	9	36:25.510	9
20:11.447	4	38:25.509	4
21:03.375	0	40:03.385	0

Πίνακας 1: Αποτελέσματα Προσομοιώσεων για το Σενάριο 2

Power Average Transmit = 600000 mW		*Power Average Transmit = 300000 mW*	
Simulation Time	*Number of Packages*	*Simulation Time*	*Number of Packages*
00:11.285	1	00:11.285	1
01:05.473	289	02:02.474	593
02:09.412	630	04:05.474	1249
03:13.537	972	06:05.474	1889
04:17.474	1313	08:07.537	2540
05:21.412	1654	10:09.412	3190
06:23.474	1985	12:09.412	3830
07:27.412	2326	14:11.474	4481
08:31.537	2668	16:13.537	5132
09:35.474	3009	18:13.538	5772
10:39.412	3350	20:15.413	6422
11:43.537	3692	22:15.413	7062
12:45.412	4022	24:17.475	7713
13:49.537	4364	26:19.538	8364
14:53.474	4705	28:19.538	9004
15:57.412	5046	30:21.413	9654
17:01.538	5388	32:23.476	10305
18:05.475	5729	34:23.475	10945
19:07.537	6060	36:25.538	11596
20:11.475	6401	38:25.538	12236
21:03.412	6678	40:03.413	12758

Πίνακας 2: Αποτελέσματα Προσομοιώσεων για το Σενάριο 2

Στην συνέχεια παρουσιάζονται συμπεράσματα και παρατηρήσεις από την εκτέλεση της προσομοίωσης.

Σύμφωνα με το μοντέλο της μπαταρίας που έχουμε υιοθετήσει, σημαντικό ρόλο έχει η ισχύς μετάδοσης (power average transmit) που συνδέεται με το μοντέλο ποσοστιαίας κατανάλωσης ενέργειας της μπαταρίας. Ως χρόνο ζωής του δικτύου θεωρούμε τον χρόνο από την αρχή της προσομοίωσης μέχρι την ώρα που η ποσοστιαία ενέργεια της μπαταρίας του κόμβου 2 (πηγή) μηδενιστεί. Η τοπολογία των κόμβων θεωρούμε ότι είναι στατική (δηλ. ότι αυτοί δεν μετακινούνται μέσα στο δίκτυο), καθώς επίσης ότι οι ζεύξεις είναι συμμετρικές μεταξύ τους. Από τα αποτελέσματα που προέκυψαν παρατηρούμε ότι όσο μεγαλώνει η ισχύς μετάδοσης τόσο πιο γρήγορα καταναλώνεται η ενέργεια της μπαταρίας με αποτέλεσμα τα μεγέθη όπως ο χρόνος διάρκειας ζωής του δικτύου αλλά και τα πακέτα να είναι μικρά (21 ώρες και 6,678 πακέτα) σε σύγκριση με την μικρότερη ισχύς μετάδοσης όπου εκεί ο χρόνος διάρκειας ζωής του δικτύου είναι διπλάσιος (40 ώρες) καθώς επίσης και τα πακέτα (12.758) τα οποία στάλθηκαν στην ρίζα. Επομένως σύμφωνα με την σύγκριση των αποτελεσμάτων και όπως φαίνεται και από τα διαγράμματα, καταλήγουμε ότι πρέπει να υπάρχει μια σωστά ισοσταθμισμένη ισχύς μετάδοσης τέτοια ώστε να έχουμε τον βέλτιστο χρόνο διάρκειας ζωής του δικτύου μας καθώς και την βέλτιστη λειτουργία του. Με τον όρο ισοσταθμισμένη ισχύς μετάδοσης εννοούμε ότι σε μια στατική τοπολογία όπου οι κόμβοι δεν κινούνται μεταξύ τους η ισχύς μετάδοσης μπορεί να ρυθμιστεί έτσι ώστε η πληροφορία να μπορεί να αποσταλεί στον γειτονικό κόμβο ανάλογα με την απόσταση την οποία βρίσκονται. Εάν η τοπολογία είναι

δυναμική και οι κόμβοι κινούνται μέσα στο δίκτυο τότε η ρύθμιση της ισχύος θα είναι πολύ πιο πολύπλοκη.

Τέλος, αναφέρεται ότι το πείραμα εκτελέστηκε στην πλατφόρμα Z1 mote (Zolertia platform) του Contiki όπου ο κώδικας της ποσοστιαίας κατανάλωσης ενέργειας της μπαταρίας μπορεί να "τρέξει" σε πραγματική συσκευή. Επίσης πρέπει να τονισθεί ότι τις τιμές της ισχύος μετάδοσης τις ορίσαμε εμείς για την επιβεβαίωση της ορθής συμπεριφοράς του μοντέλου κατανάλωσης ενέργειας μπαταρίας και δεν είναι πραγματικές.

5.4 Προτιμώμενος Γονέας Δρομολόγησης

5.4.1 Σενάριο 3

Για την υλοποίηση του σεναρίου αυτού, δηλαδή για την επιλογή του προτιμώμενου γονέα, χρησιμοποιήθηκε σαν μετρική το hop count και το κόστος της μπαταρίας (battery cost) από το μοντέλο της κατανάλωσης ενέργειας της μπαταρίας. Χρησιμοποιήσαμε το Cooja του contiki για την προσομοίωση του σεναρίου. Το πείραμα εκτελέστηκε στην πλατφόρμα Z1 mote (Zolertia Platform) του contiki. Πραγματοποιήσαμε κάποιες τροποποιήσεις στα αρχεία μέσα στον πυρήνα (core) του RPL στο μονοπάτι contiki/core/net/rpl. Στον φάκελο rpl-private.h ορίσαμε σαν minimum hop ranking δηλαδή το κόστος μονοπατιού να είναι 128 δηλαδή #define RPL_CONF_MIN_HOPRANKINC 128

```
119 #define RPL_CONF_MIN_HOPRANKINC      128
```

Εικόνα 80: Προσθήκη στο αρχείο rpl-private.h

Στην συνέχεια στον φάκελο rpl-conf.h ορίσαμε σαν αντικειμενική συνάρτηση το mrhof_ energy ως εξής #define RPL_OF rpl_mrhof_energy.

```
71 /* ETX is the default objective function
72 //#define RPL_OF rpl_mrhof
73 #define RPL_OF rpl_mrhof_energy
74 #endif /* RPL_CONF_OF */
```

Εικόνα 81: Τμήμα του αρχείου rpl-conf.h

Στο αρχείο dag.c ορίσαμε να εκτυπώνονται τα μηνύματα του προτιμώμενου γονέα στο Mote output του Cooja ως εξής #define DEBUG 1.

```
60 #define DEBUG 1          //jvoug - it was DEBUG_NONE
61 #include "net/ip/uip-debug.h"
```

Εικόνα 82: Τμήμα του αρχείου dag.c

Στο αρχείο rpl-mrhof_energy.c ορίσαμε να εκτυπώνονται όλα τα μηνύματα ως εξής #define DEBUG DEBUG_FULL. Στην συνέχεια δηλώνουμε την ποσοστιαία κατανάλωση ενέργειας της μπαταρίας όπου ο κώδικας της κατανάλωσης είναι γραμμένος στο αρχείο unicast-sender.c στο μονοπάτι contiki/examples/ipv6/simple-udp-rpl και επίσης ορίζουμε σαν μέγιστο επίπεδο ενέργειας το 100 με χρήση της #define MAX_ENERGY_LEVEL_100

```
88  uint16_t current_battery_level_perc;
89 #define MAX_ENERGY_LEVEL        100
```

Εικόνα 83: Τμήμα του αρχείου rpl-mrhof_energy.c

```
233  /* Maintain stability of the preferred parent in case of similar ranks. */
234  if(p1 == dag->preferred_parent || p2 == dag->preferred_parent) {
235    if(p1_metric < p2_metric + min_diff &&
236       p1_metric > p2_metric - min_diff) {
237      PRINTF("RPL - jvoug: MRHOF hysteresis: %u <= %u <= %u\n",
238             p2_metric - min_diff,
239             p1_metric,
240             p2_metric + min_diff);
241      return dag->preferred_parent;
242    }
243  }
244
245  return p1_metric < p2_metric ? p1 : p2;
246 }
```

Εικόνα 84: Τμήμα του αρχείου rpl-mrhof_energy.c

Ο κώδικας στην εικόνα 84 δείχνει το κατώφλι της υστέρησης. Δηλαδή το p1_metric που αντιστοιχεί στον προτιμώμενο γονέα 1 και το p2_metric που αντιστοιχεί στον προτιμώμενο γονέα 2 δείχνει ότι εάν ο πρώτος προτιμώμενος είναι εντός ορίων του δεύτερου προτιμώμενου και εντός (+ -) του περιθωρίου της υστέρησης να μην γίνει αλλαγή γονέα. Η αλλαγή θα γίνει μόνο όταν διαφημίσει αρκετά μικρότερο rank γονέα τόσο όσο το κατώφλι της υστέρησης που ορίζεται στον κώδικα (min difference).

```
//rank_increase = nbr->link_metric;          //deleted by jvoug
rank_increase = 128 + p->mc.obj.energy.energy_est;
if(base_rank == 0) {
  base_rank = p->rank;
```

Εικόνα 85: Τμήμα του αρχείου rpl-mrhof_energy.c

Στην εικόνα 85 φαίνεται ότι ορίζουμε το rank_increase δηλαδή την μεταξύ τους ζεύξη των κόμβων με το 128 (όπου είναι το κόστος) και προσθέτουμε την ενέργεια (energy estimation) όπου όπως θα δούμε παρακάτω την ενέργεια την ορίζουμε σαν battery cost.

```
PRINTF("jvoug - inside calculate_path_metric - returning %d + %d\n", p->rank, p->mc.obj.energy.energy_est);
return (p->rank + p->mc.obj.energy.energy_est);
```

Εικόνα 86: Τμήμα του αρχείου rpl-mrhof_energy.c

```
static void update_metric_container(rpl_instance_t *instance)
{
  rpl_path_metric_t path_metric;
  rpl_dag_t *dag;
#if RPL_DAG_MC == RPL_DAG_MC_ENERGY
  uint8_t type;
#endif

  uint16_t battery_cost;                //jvoug
  instance->mc.type = RPL_DAG_MC;
  instance->mc.flags = RPL_DAG_MC_FLAG_P;
  instance->mc.aggr = RPL_DAG_MC_AGGR_ADDITIVE;
  instance->mc.prec = 0;

  dag = instance->current_dag;
```

Εικόνα 87: Τμήμα του αρχείου rpl-mrhof_ energy.c

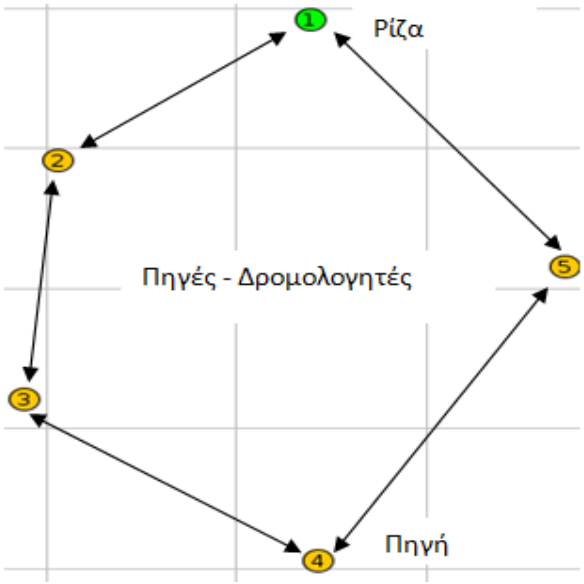
Στην εικόνα 86 φαίνεται ότι εκτυπώνουμε το rank δηλαδή το κόστος της μεταξύ τους ζεύξης, καθώς και την ενέργεια των κόμβων. Στην εικόνα 87 έχουμε ορίσει σαν metric container (δοχείο μετρικής) το κόστος της μπαταρίας.

```
instance->mc.obj.energy.flags = type << RPL_DAG_MC_ENERGY_TYPE;
//instance->mc.obj.energy.energy_est = path_metric;
PRINTF("jvoug - the current battery level perc is is %d\n", current_battery_level_perc);
battery_cost = MAX_ENERGY_LEVEL - current_battery_level_perc;
instance->mc.obj.energy.energy_est = battery_cost;    //jvoug - was 0xaa
PRINTF("jvoug - the energy value is %d\n", instance->mc.obj.energy.energy_est);
```

Εικόνα 88: Τμήμα του αρχείου rpl-mrhof_ energy.c

Στην εικόνα 88 φαίνεται ότι το κόστος της μπαταρίας (battery cost) το ορίζουμε σαν γινόμενο του επιπέδου μέγιστης ενέργειας (όπου το έχουμε ορίσει 100) μείον της ποσοστιαίας ενέργειας της μπαταρίας. Επίσης χρησιμοποιούμε έναν metric container (δοχείο μετρικής) όπου μέσα σε αυτό τοποθετείται το κόστος της μπαταρίας για κάθε κόμβο. Το επίπεδο μέγιστης ενέργειας το ορίσαμε 100. Με αυτή τη συνθήκη, όταν για παράδειγμα η ποσοστιαία ενέργεια της μπαταρίας βρίσκεται στο 98% τότε το κόστος θα είναι 2, όταν θα βρίσκεται στο 90% τότε το κόστος θα είναι 10 κ.ο.κ. Τέλος τυπώνουμε τις τιμές του κόστους της μπαταρίας και της ποσοστιαίας ενέργειας της μπαταρίας με την χρήση των εντολών PRINTF.

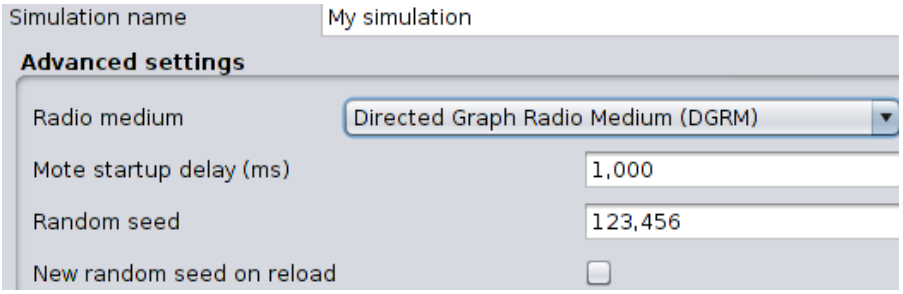
Έχουμε την παρακάτω τοπολογία δικτύου.



Η παραπάνω τοπολογία του δικτύου χαρακτηρίζεται από πέντε κόμβους όπου ο κόμβος 4 είναι η πηγή που στέλνει τα πακέτα προς τον κόμβο 1 όπου είναι η ρίζα. Οι κόμβοι 2,3,5 είναι πηγές-δρομολογητές διότι εκτός του ότι μεταφέρουν τα πακέτα πληροφορίας του κόμβου 4 στέλνουν επίσης και δικά τους πακέτα πληροφορίας προς την ρίζα. Επίσης θεωρούμε ότι οι ζεύξεις μεταξύ των κόμβων είναι συμμετρικές και το hop count δεν αλλάζει διότι το έχουμε ορίσει 128.

Αυτό όμως που αλλάζει είναι το κόστος της μπαταρίας καθώς πέφτει η ποσοστιαία κατανάλωση ενέργειας της μπαταρίας και επηρεάζει το rank των κόμβων. Θα παρατηρήσουμε το πώς η πηγή (κόμβος 4) θα επιλέξει προτιμώμενο γονέα για να στείλει τα πακέτα πληροφορίας προς στην ρίζα (κόμβος 1). Επίσης τα αρχεία με τους κώδικες που χρησιμοποιούνται στο σενάριο βρίσκονται στο μονοπάτι contiki/examples/ipv6/simple-udp-rpl και είναι το unicast-receiver.c (κόμβος 1) και το unicast-sender.c (κόμβοι 2,3,4,5) όπου μέσα εκεί βρίσκεται και το μοντέλο της κατανάλωσης ενέργειας της μπαταρίας.

Τα πακέτα πληροφορίας που στέλνονται προς την ρίζα από τους κόμβους είναι UDP πακέτα πληροφορίας της μορφής “Giannis” των 10-15 byte. Επίσης θεωρούμε ότι η ρίζα (κόμβος 1) έχει πάντα ενέργεια και το μέγιστο επίπεδο ενέργειας που διαφημίζει το έχουμε ορίσει 100 και το κόστος της μπαταρίας της ρίζας είναι μηδέν. Τέλος θα συγκρίνουμε τα αποτελέσματα και θα διατυπώσουμε τις παρατηρήσεις και τα συμπεράσματα μας.



Εικόνα 89: Δημιουργία Προσομοίωσης Contiki – Cooja

DGRM Configurator

Source	Destination	RX Ratio	RSSI	LQI
Z1 4	Z1 3	100.0%	-10.0	105
Z1 3	Z1 4	100.0%	-10.0	105
Z1 3	Z1 2	100.0%	-10.0	105
Z1 2	Z1 3	100.0%	-10.0	105
Z1 2	Z1 1	100.0%	-10.0	105
Z1 1	Z1 2	100.0%	-10.0	105
Z1 4	Z1 5	100.0%	-10.0	105
Z1 5	Z1 4	100.0%	-10.0	105
Z1 5	Z1 1	100.0%	-10.0	105
Z1 1	Z1 5	100.0%	-10.0	105

Εικόνα 90: DGRM Configurator Contiki – Cooja

Στην συνέχεια με την βοήθεια του Wireshark παρατηρούμε την δρομολόγηση του UDP πακέτου που στέλνει η πηγή (κόμβος 4) προς την ρίζα (κόμβος 1).

```
1187 67.208000   2002:db8::c30c:0:0:4          2002:db8::c30c:0:0:1          UDP
▸ Frame 1187: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
▾ IEEE 802.15.4 Data, Dst: c1:0c:0000:00:0000:05, Src: c1:0c:0000:00:0000:04
  ▸ Frame Control Field: Data (0xdc41)
    Sequence Number: 37
    Destination PAN: 0xabcd
    Destination: c1:0c:0000:00:0000:05 (c1:0c:00:00:00:00:00:05)
    Extended Source: c1:0c:0000:00:0000:04 (c1:0c:00:00:00:00:00:04)
    FCS: 0x34c8 (Correct)

0000  41 dc 25 cd ab 05 00 00  00 00 00 0c c1 04 00 00   A.%..... ........
0010  00 00 00 0c c1 7a f5 00  00 c3 0c 00 00 00 00 00   .....z.. ........
0020  01 11 00 63 04 00 1e 01  ed 04 d2 04 d2 00 13 5e   ...c.... .......^
```

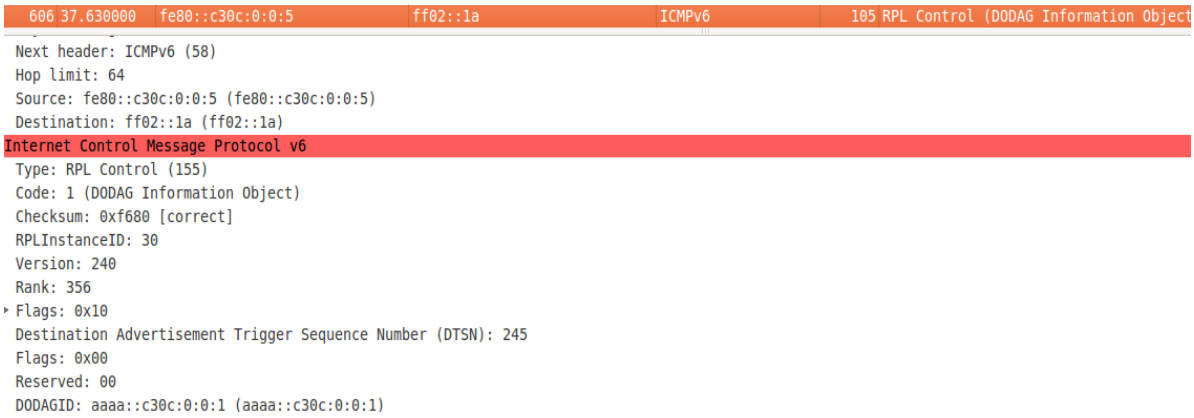
Εικόνα 91: Διαδρομή Πακέτου (από Wireshark)

```
1189 67.293000   2002:db8::c30c:0:0:4          2002:db8::c30c:0:0:1          UDP
▸ Frame 1189: 63 bytes on wire (504 bits), 63 bytes captured (504 bits)
▾ IEEE 802.15.4 Data, Dst: c1:0c:0000:00:0000:01, Src: c1:0c:0000:00:0000:05
  ▸ Frame Control Field: Data (0xdc41)
    Sequence Number: 14
    Destination PAN: 0xabcd
    Destination: c1:0c:0000:00:0000:01 (c1:0c:00:00:00:00:00:01)
    Extended Source: c1:0c:0000:00:0000:05 (c1:0c:00:00:00:00:00:05)
    FCS: 0x9f7b (Correct)

0000  41 dc 0e cd ab 01 00 00  00 00 00 0c c1 05 00 00   A....... ........
0010  00 00 00 0c c1 78 d7 00  00 3f c3 0c 00 00 00 00   .....x.. .?......
0020  00 04 11 00 63 04 00 1e  01 64 04 d2 04 d2 00 13   ....c... .d......
0030  5e 16 47 69 61 6e 6e 69  73 20 32 39 00 7b 9f      ^.Gianni s 29.{.
```

Εικόνα 92: Διαδρομή Πακέτου (από Wireshark)

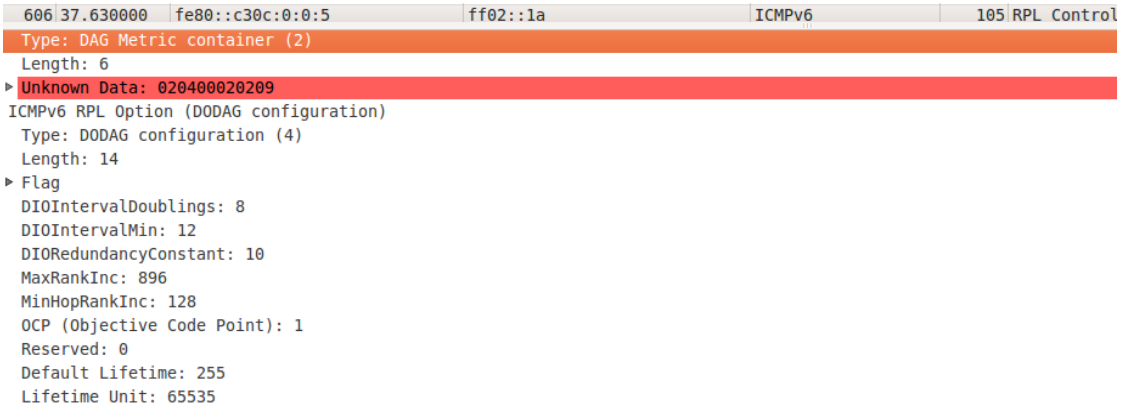
Από τις εικόνες 91 και 92 παρατηρούμε ότι ο κόμβος 4 που είναι η πηγή στέλνει πακέτο πληροφορίας τύπου UDP προς την ρίζα (κόμβος 1). Διαλέγει σαν προτιμώμενο γονέα (preferred parent) τον κόμβο 5 για να στείλει το πακέτο του στην ρίζα. Στην συνέχεια το πακέτο δρομολογείται από τον κόμβο 5 στον κόμβο 1 όπου είναι ο τελικός προορισμός. Επίσης φαίνονται και οι διευθύνσεις των κόμβων.



Εικόνα 93: Μηνύματα Πρωτόκολλων Δρομολόγησης (από Wireshark)

Από την εικόνα 93 παρατηρούμε ένα DIO μήνυμα από τον κόμβο 5 προς την ρίζα (κόμβος 1). Επίσης παρατηρούμε κάποιες πληροφορίες του πρωτοκόλλου ICMPv6 όπως τον τύπο του (RPL Control), τον κωδικό του μηνύματος (DODAG Information Object) τον βαθμό της ζεύξης (Rank=356), τον αριθμό έκδοσης (version) που ορίζεται από την ρίζα, κάποιες σημαίες, καθώς και το DODAG ID όπου είναι η διεύθυνση IPv6 της ρίζας όπου είναι μοναδική.

Ο αριθμός DTSN είναι ένας ακέραιος μη προσημασμένος αριθμός που ορίζεται από τον κόμβο που εκδίδει το μήνυμα DIO.



Εικόνα 94: Μηνύματα Πρωτόκολλων Δρομολόγησης (από Wireshark)

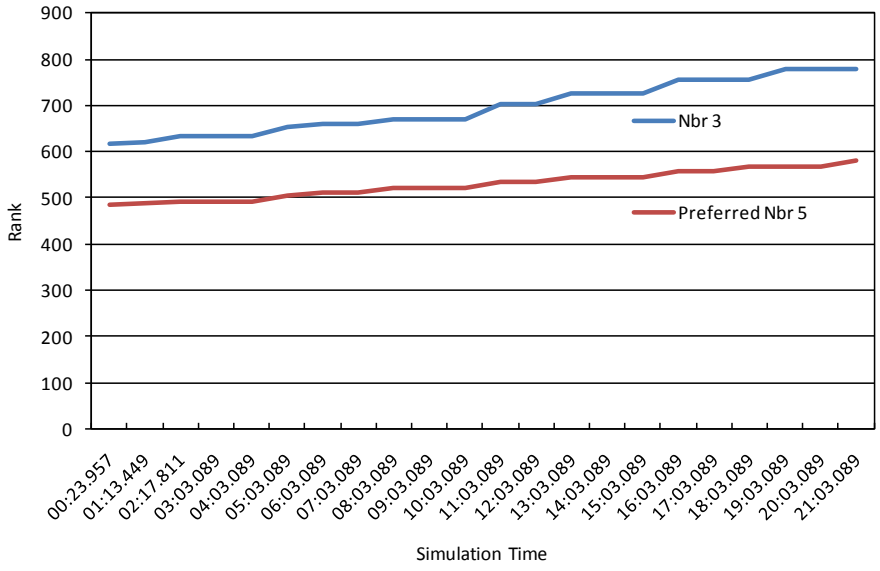
Στην εικόνα 94 του ίδιου μηνύματος DIO από τον κόμβο 5 προς την ρίζα παρατηρούμε κάποιες επιλογές του RPL. Το Max rank increase προσδιορίζει τον μέγιστο κόστος διαδρομής ενώ το Min hop rank increase προσδιορίζει το μικρότερο κόστος διαδρομής μέσα στον κόμβο όπου είναι το 128. Είναι σημαντικό να εξηγήσουμε γιατί το Rank (βλέπε εικόνα 93) είναι 356. Το Rank προκύπτει από το αρχείο του κώδικα mrhof_energy.c που είχαμε ορίσει το rank increase 128. Επομένως το rank της ζεύξης είναι: 128 (rank της ρίζας) + 128 (rank της μεταξύ τους ζεύξης) + 100 (μέγιστο επίπεδο ενέργειας της ρίζας) = 356. Επομένως ο κόμβος 5 σαν rank έχει 356 όπως φαίνεται και από το DIO μήνυμα στο Wireshark.

```
230 15.064000   fe80::c30c:0:0:4          ff02::1a                  ICMPv6
Checksum: 0xf601 [correct]
RPLInstanceID: 30
Version: 240
Rank: 488
Flags: 0x10
Destination Advertisement Trigger Sequence Number (DTSN): 244
Flags: 0x00
Reserved: 00
DODAGID: aaaa::c30c:0:0:1 (aaaa::c30c:0:0:1)
```

Εικόνα 95: Μηνύματα Πρωτόκολλων Δρομολόγησης (από Wireshark)

Από την εικόνα 95 παρατηρούμε ότι το rank της πηγής (κόμβου 4) είναι 488 το οποίο προκύπτει: από το rank (356) του κόμβου 5 + 128 (rank μεταξύ τους ζεύξης) + 4 (το κόστος της μπαταρίας)= 488. Το κόστος της μπαταρίας είναι 4 που σημαίνει ότι η ποσοστιαία κατανάλωση ενέργειας της μπαταρίας εκείνη την χρονική στιγμή του simulation ήταν 96% δηλαδή MAX ENERGY LEVEL 100 (που το ορίσαμε) – 96 = 4 (κόστος μπαταρίας).

Στο παρακάτω διάγραμμα παρατηρούμε τα rank των γειτονικών κόμβων της πηγής συναρτήσει του χρόνου προσομοίωσης.

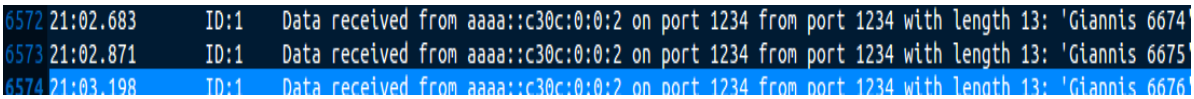


Εικόνα 96: Διάγραμμα Γονέων

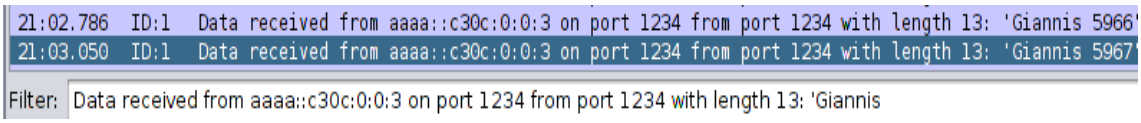
Από το διάγραμμα της εικόνας 96 παρατηρούμε ότι ο κόμβος 4 (πηγή) υπολογίζει τα rank ως προς τους δύο διαφορετικούς γονείς (κόμβος 5 , κόμβος 3) και διαλέγει σαν προτιμώμενο γονέα τον κόμβο 5 με το μικρότερο rank να στείλει τα πακέτα προς την ρίζα. Στο simulation του Cooja στο mote output στο φίλτρο πατήσαμε ID:4 RPL: nbr και μας τύπωσε τα αποτελέσματα των rank των διαφορετικών γονέων.

```
21:02.871  ID:1   Data received from aaaa::c30c:0:0:2 on port 1234 from port 1234 with length 13: 'Giannis 6675'
21:03.198  ID:1   Data received from aaaa::c30c:0:0:2 on port 1234 from port 1234 with length 13: 'Giannis 6676'
Filter:  Data received from aaaa::c30c:0:0:2 on port 1234 from port 1234 with length 13: 'Giannis
```

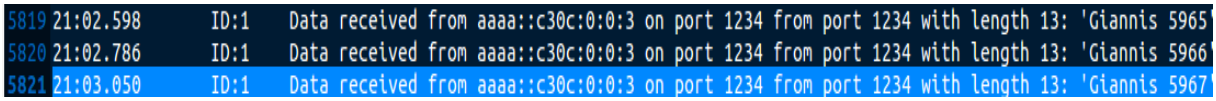
Εικόνα 97: Σύνολο Πακέτων που ελήφθησαν από τον προορισμό



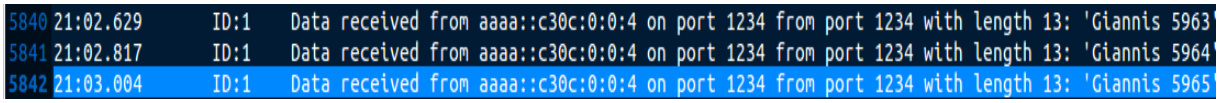
Εικόνα 98: Πακέτα Πληροφορίας UDP



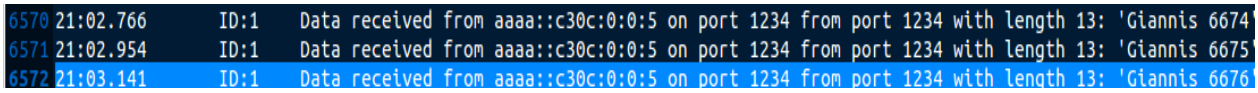
Εικόνα 99: Σύνολο Πακέτων που ελήφθησαν από τον προορισμό



Εικόνα 100: Πακέτα Πληροφορίας UDP



Εικόνα 101: Πακέτα Πληροφορίας UDP



Εικόνα 102: Πακέτα Πληροφορίας UDP

Από τις παραπάνω εικόνες (Εικόνα 97 έως Εικόνα 102) παρατηρούμε το συνολικό αριθμό των πακέτων UDP που στάλθηκαν στην ρίζα από τους κόμβους (2,3,4,5). Φαίνεται ότι στην ρίζα δεν φτάνουν όλα τα πακέτα από τους κόμβους και υπάρχει απώλεια. Παρακάτω φαίνεται αναλυτικά ο πίνακας με τον αριθμό αποστολής πακέτων και τα ποσοστά επιτυχίας και αποτυχίας αντίστοιχα.

Τύποι Κόμβων	*Αριθμός αποστολής Πακέτων*	*Αριθμός παραλαβής Πακέτων*	*Ποσοστό Επιτυχίας %*	*Ποσοστό Αποτυχίας %*
2	6676	6574	98	2
3	5967	5821	97	3
4	5965	5842	97	3
5	6676	6572	98	2

Πίνακας 3: Αποτελέσματα Προσομοιώσεων για το Σενάριο 3

Στην συνέχεια παρουσιάζονται συμπεράσματα και παρατηρήσεις από την εκτέλεση της προσομοίωσης:

Από το παραπάνω διάγραμμα (Εικόνα 95) παρατηρούμε ότι ο κόμβος 4 (πηγή) διαλέγει σαν προτιμώμενο γονέα (preferred parent) τον κόμβο 5 για να μεταφέρει τα πακέτα της πηγής στην ρίζα διότι έχει μικρό rank σε σύγκριση με τον κόμβο 3. Επίσης από το διάγραμμα φαίνεται ότι όσο περνάει ο χρόνος της προσομοίωσης τα rank των κόμβων αυξάνονται διότι η ενέργεια της μπαταρίας μειώνεται και το κόστος της αυξάνεται. Επομένως συμπεραίνουμε ότι η ενέργεια της μπαταρίας και το κόστος της επηρεάζει το rank των κόμβων διότι οι παράμετροι (της μπαταρίας) είναι δυναμικές και αλλάζουν κατά την διάρκεια της προσομοίωσης.

Η παράμετρος που δεν αλλάζει κατά την διάρκεια της προσομοίωσης και είναι σταθερή είναι το rank increase δηλαδή το κόστος της μεταξύ τους ζεύξης (hop count) που το έχουμε ορίσει στο mrhof_energy.c και είναι 128. Ωστόσο αξίζει να σημειωθεί ότι εάν η τοπολογία του δικτύου ήταν δυναμική και οι κόμβοι μετακινούνταν μέσα στο δίκτυο και οι παράμετροι όπως το hop count σε συνδυασμό με την ποιότητα ζεύξης των κόμβων (ETX) καθώς και το κόστος της ποσοστιαίας ενέργειας της μπαταρίας άλλαζε τότε η ανάλυση των αποτελεσμάτων θα ήταν πολύ πιο πολύπλοκη. Επίσης θα πρέπει να γίνει αναφορά και στον λόγο απώλειας πακέτων (βλέπε πίνακα 3). Παρατηρούμε κάποια απώλεια πακέτων που στέλνουν οι κόμβοι προς την ρίζα. Κάποιος προφανής λόγος είναι η υπερχείλιση του καταχωρητή (buffer) στην διεργασία εκπομπής, εφόσον ο καταχωρητής έχει συγκεκριμένο όριο μνήμης. Επομένως όταν γεμίζει με πακέτα πληροφορίας και η μνήμη ξεχειλίσει τα υπόλοιπα πακέτα που με την σειρά τους προσπαθούν να εισαχθούν στον καταχωρητή δεν αποστέλλονται.

Ένας άλλος λόγος που μπορεί να δικαιολογεί την απώλεια είναι ο πυκνός ρυθμός αποστολής των πακέτων που στέλνουν οι κόμβοι πηγές – δρομολογητές ανά τακτά μικρά χρονικά διαστήματα. Επίσης, ένας παράγοντας που μπορεί να δικαιολογεί την απώλεια είναι ο συγχρονισμός των μεταδόσεων που στέλνουν οι κόμβοι, δηλαδή την ίδια χρονική στιγμή μπορεί να στείλουν πακέτα όλοι οι κόμβοι με αποτέλεσμα την δημιουργία συμφόρησης στο δίκτυο και κάποια από τα πακέτα να συγκρούονται και να χάνονται.

Επιπλέον κατά την διεξαγωγή του πειράματος αντιμετωπίσαμε το εξής πρόβλημα. Κατά την προσομοίωση παρατηρήσαμε στην αρχή στα αποτελέσματα του mote output το μήνυμα Service 190 not found. Την υπηρεσία με αριθμό 190 την διαφημίζει η ρίζα (receiver) όπου είναι ο παραλήπτης των πακέτων της υπηρεσίας αυτής σαν αναγνωριστικό προς τους δρομολογητές – πηγές (senders) ώστε οι πηγές να στέλνουν τα πακέτα τους προς την ρίζα. Αφού διαφημιστεί το 190 στις πηγές – δρομολογητές τότε στέλνουν αυτές τα πακέτα προς την ρίζα (που είναι ο παραλήπτης για τα πακέτα της εφαρμογής 190). Κατά τη διάρκεια εμφάνισης του μηνύματος «Service 190 not found», παρατηρήσαμε ότι οι πηγές δεν έστελναν τα πακέτα τους στην ρίζα.

Για να λυθεί αυτό το πρόβλημα μπορεί να γίνουν κάποιες ενέργειες. Μια πρώτη ενέργεια είναι να πραγματοποιηθεί η προσομοίωση στην αρχή για κάποια δευτερόλεπτα ώστε να δημιουργηθούν τα μονοπάτια δρομολόγησης μεταξύ των κόμβων και να διαφημιστεί η υπηρεσία 190 προς τους senders και να αρχίζουν να στέλνουν τα πακέτα πληροφορίας στην ρίζα. Μια δεύτερη ενέργεια που μπορεί να γίνει είναι να τροποποιήσουμε τον κώδικα (receiver.c) στο contiki και εκεί που ορίζεται η υπηρεσία 190, τον χρόνο (timer) διαφήμισης να τον τροποποιήσουμε κατάλληλα ώστε να στέλνει σε πιο πυκνά χρονικά διαστήματα τον αναγνωριστικό αριθμό της υπηρεσίας. Μια τρίτη ενέργεια είναι στον κώδικα του sender.c να ορίσουμε εμείς την διεύθυνση της ρίζας ώστε να αποστέλλονται τα πακέτα κατευθείαν στην ρίζα. Τέλος τα πακέτα που στάλθηκαν ήταν πακέτα πληροφορίας UDP της μορφής “Giannis”. Το πείραμα εκτελέστηκε στην πλατφόρμα Z1 mote (Zolertia platform) του contiki.

ΚΕΦΑΛΑΙΟ 6

Συμπεράσματα

6.1 Διατύπωση Αποτελεσμάτων

Με βάση τα ειδικά συμπεράσματα ανά σενάριο καθώς και τις προσομοιώσεις που υλοποιήθηκαν καταλήγουμε ότι όσο μεγαλύτερο το κόστος της ποσοστιαίας κατανάλωσης ενέργειας της μπαταρίας τόσο αυξάνεται το rank των κόμβων και γι' αυτό τον λόγο χρήζει άμεσης προσοχής η κατάλληλη διαχείριση και βελτιστοποίηση της κατανάλωσης ενέργειας. Επίσης παρατηρήθηκε (από τις εικόνες των διαγραμμάτων) ότι οι πηγές για να στείλουν τα πακέτα πληροφορίας προς την ρίζα διαλέγουν σαν προτιμώμενους γονείς (preferred parents) τους κόμβους όπου διαθέτουν το μικρότερο rank σε σύγκριση με άλλους.

Οι μετρικές δρομολόγησης hop count καθώς και το ETX οι οποίες μελετώνται στην παρούσα εργασία αποσκοπούν στην μικρότερη κατανάλωση της ενέργειας. Η μετρική του ETX στοχεύει στην εξασφάλιση αξιοπιστίας των ζεύξεων των κόμβων, καθώς αποδίδει ένα κόστος ελάχιστου βάρους στις αξιόπιστες ζεύξεις με σκοπό την ελαχιστοποίηση κατανάλωσης ενέργειας και την βελτίωση απόδοσης του δικτύου. Επομένως καταλήγουμε στο συμπέρασμα ότι η ενέργεια σε συνδυασμό με τις μετρικές δρομολόγησης οι οποίες μελετώνται αφενός πρέπει να είναι απλές για να μπορούν να υλοποιηθούν στους κόμβους και αφετέρου να στοχεύουν στην σωστή εκτίμηση απόδοσης του πρωτοκόλλου δρομολόγησης RPL.

6.2 Πιθανά Πεδία Μελλοντικής Έρευνας

Στον τομέα της δρομολόγησης πιθανό πεδίο μελλοντικής έρευνας είναι η μελέτη της επίδοσης σύνθετων μετρικών που αποτελούνται από συνδυασμούς άλλων σύνθετων μετρικών όπως πολλαπλασιαστικές μετρικές. Επίσης μπορεί να μελετηθούν κάποια σενάρια επιθέσεων στο πρωτόκολλο δρομολόγησης RPL.

Τέτοια σενάρια επιθέσεων μπορεί να είναι η επίθεση πλημμύρας (flooding) όπου ο κακόβουλος κόμβος θα στέλνει μηνύματα DIO με σταθερό χρονικό διάστημα πλημμυρίζοντας το δίκτυο. Επίθεση μαύρης τρύπας (black hole attack) όπου ο κακόβουλος κόμβος θα δηλώνει ότι έχει ETX ίσο με ένα. Με αυτόν τον τρόπο, ο κακόβουλος κόμβος θα διαφημίζει ότι ο αναμενόμενος αριθμός μεταδόσεων για να φτάσει ένα πακέτο στον sink, αν περάσει από αυτόν, θα είναι ίσος με ένα. Δηλαδή θα δηλώνει ότι έχει τον sink γείτονά του. Επομένως με την ελκυστική αυτή διαφήμιση, υπάρχει πιθανότητα ο κακόβουλος κόμβος να προσελκύσει περισσότερα πακέτα που κινούνται στο δίκτυο.

Άλλος τύπος επίθεσης είναι η επίθεση sinkhole, η οποία μοιάζει με την επίθεση black hole με την διαφορά ότι η τιμή ETX που θα διαφημίσει ο κακόβουλος κόμβος θα είναι ίση με το μηδέν, έτσι ώστε τα μηνύματα DIO που θα στέλνονται να περιέχουν την εσφαλμένη

πληροφορία ότι ο κόμβος έχει rank ίσο με ένα. Με αυτόν τον τρόπο, ο κακόβουλος κόμβος θα διαφημίζει τιμές rank και ETX ίσες με αυτές που έχει η ρίζα (παραλήπτης των πακέτων). Στη συνέχεια, ο κόμβος που υλοποιεί την επίθεση sink hole δεν προωθεί τα πακέτα που λαμβάνει από τους γειτονικούς του κόμβους. Τέλος, ενδιαφέρον έχει και ο πειραματισμός με πραγματικές διατάξεις ασύρματα διασυνδεδεμένων αισθητήρων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1) 6Lowpan THE WIRELESS EMBEDDED INTERNET, ZACH SHELBY, CARSTEN BORMANN
2) Design of primary and composite routing metrics for RPL-compliant Wireless Sensor Networks, Panagiotis Karkazis, Helen C. Leligou, Lambros Sarakis, Theodore Zahariadis, Panagiotis Trakadas, Terpsihori H. Velivasaki, Christos Capsalis
3) IPv6 Low Power Wireless Personal Area Network (6LoWPAN) for Networking Internet of Things (IoT)-Analyzing its Suitability for IoT, C. Lakshmi Devasena, August 2016
4) IoT in 5 days Antonio Linan Colina, Alvaro Vives, Antoine Bagula, Marco Zennaro, Ermanno Pietrosemoli Revision 1.0 March 2015
5) Running and Testing Applications For Contiki OS Using Cooja Simulator, A. Velinov, A. Mileva, June, 2016
6) Wireless Sensor Networks From Theory to Applications Edited by Ibrahiem M. M. El Emary S. Ramakrishnan, February 2017
7) Average power consumption breakdown of Wireless Sensor Networks nodes using IPv6 over LLNs, Javier Schandy, Leonardo Steinfeld, Fernado Silveira June 2016
8) RPL-Routing over Low Power and Lossy Networks, Michael Richardson, Ires Robles IETF 94
9) Simulation of the RPL Routing Protocol for IPv6 Sensor Networks: two cases studies, Leila Ben Saad, Cedric Chauvenet, Bernard Tourancheau, Submitted on 2 December 2011
10) Evaluating routing metric composition approaches for QoS differentiation in low power and lossy networks, Panagiotis Karkazis, Panagiotis Trakadas, Helen C. Leligou, Lambros Sarakis, Ioannis Papaefstathiou, Theodore Zahariadis, Published online: 30 December 2012
11) Home Networking with IEEE 802.15.4: A Developing Standard for Low-Rate Wireless Personal Area Networks, Ed Callaway, Paul Gorday, and Lance Hester, Motorola Laboratories, Jose A. Gutierrez and Marco Naeve, Eaton Corporation, Bob Heile, Appairent Technologies, Venkat Bahl, Philips Semiconductors, IEEE Communications Magazine August 2002
12) Techniques to Enhance Lifetime of Wireless Sensor Networks: A Survey By Jyoti Saraswat, Neha Rathi & Partha Pratim Bhattacharya, Volume 12 Issue 14 Version 1.0 Year 2012
13) Ανάπτυξη Νέων Τεχνικών Διαχείρισης Πόρων σε Ασύρματα Δίκτυα, Διδακτορική Διατριβή, Τερψιχόρη - Ελένη Ν. Βελιβασάκη, Αθήνα, Ιανουάριος 2014
14) Μελέτη Συνύπαρξης Ασύρματων Δικτύων Αισθητήρων και Δικτύων Wi-Fi σε Πραγματικό Περιβάλλον, Διπλωματική Εργασία Χρηστίνα Α. Μακρή, Αθήνα, Ιούλιος 2011
15) https://sites.google.com/site/eisagogestadiktyaypologiston1/architektonike-diktyou/diastromatose
16) https://datatracker.ietf.org/doc/rfc7668/?include_text=1
17) https://tools.ietf.org/html/rfc768
18) http://www.contiki-os.org/
19) https://github.com/contiki-os/contiki
20) https://github.com/contiki-os/contiki/wiki/An-Introduction-to-Cooja
21) https://tools.ietf.org/html/rfc6551
22) https://tools.ietf.org/html/rfc6550
23) https://datatracker.ietf.org/doc/rfc4443/
24) https://tools.ietf.org/html/rfc4191
25) https://www.slideshare.net/ADunkels/building-day-2-upload-1
26) https://tools.ietf.org/html/rfc6719
27) http://anrg.usc.edu/contiki/index.php/Protocols_stack
28) https://commons.wikimedia.org/wiki/File:IPv6_header_rv1.svg