

Ατομική Διπλωματική Εργασία

**ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΗΤΙΚΟΤΗΤΑΣ ΣΕ 6LOWPAN ΔΙΚΤΥΑ
ΑΙΣΘΗΤΗΡΩΝ**

Χριστόδουλος Ηρακλέους

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ



ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάιος 2014

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Διαχείριση Κινητικότητας σε 6LoWPAN Δίκτυα Αισθητήρων

Χριστόδουλος Ηρακλέους

Επιβλέπων Καθηγητής
Βάσος Βασιλείου

Η Ατομική Διπλωματική Εργασία υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων απόκτησης του πτυχίου Πληροφορικής του Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου

Μάιος 2014

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Βάσο Βασιλείου, για την υποστήριξη που μου προσέφερε κατά την διάρκεια της έρευνας και υλοποίησης της παρούσας εργασίας, καθώς και την κατανόηση που επέδειξε σε όλα τα θέματα που προέκυψαν. Επίσης να ευχαριστήσω για την άμεση ανταπόκριση της Διδακτορικής φοιτήτριας του Ερευνητικού Εργαστηρίου Δικτύων Χριστιάνας Ιωάννου σχετικά με το πρόβλημα που αντιμετώπισα με το λειτουργικό σύστημα Contiki.

Ειδικές ευχαριστίες θα ήθελα να δώσω στον εργοδότη μου για τις ευκολίες που μου παρείχε σε θέματα ωραρίου για να ασχοληθώ με την διεκπεραίωση της διπλωματικής μου εργασίας.

Εν τέλει, θα ήθελα να ευχαριστήσω την οικογένεια μου για τη στήριξη που μου έδιναν κατά τη διάρκεια εκπόνησης της πτυχιακής μου εργασίας, αλλά και καθ' όλη τη διάρκεια των σπουδών μου στο Πανεπιστήμιο Κύπρου.

Περίληψη

Η εξέλιξη που παρατηρείται έντονα τις τελευταίες δεκαετίες στο τομέα της πληροφορικής δεν θα μπορούσε να μην επηρεάσει και τον τομέα των δικτύων, όπως επίσης και τον τομέα που αφορά τα δίκτυα αισθητήρων. Λόγω και των συνεχών αναγκών του ανθρώπου μέσω όλης αυτής της εξέλιξης τα δίκτυα αισθητήρων έχουν γίνει πλέον μέρος της καθημερινότητάς μας αν και πολλοί δεν το αντιλαμβάνονται τόσο. Έτσι είναι στο στόχαστρο πολλών ερευνών τα τελευταία χρόνια με σκοπό την όσο μεγαλύτερη βελτίωση και εξέλιξη τους. Μια περιοχή έρευνας αφορά το 6LoWPAN δίκτυο αισθητήρων. Η ακριβής ερμηνεία του είναι IPv6 Over Low Power Wireless Personal Area Network. Μέσα από το δίκτυο αυτό γίνεται προσπάθεια για να εφαρμοσθούν ή να υλοποιηθούν πρωτόκολλα για τη μεταφορά πακέτων με την ελάχιστη δυνατή απώλεια.

Έτσι λοιπόν και το θέμα την διπλωματικής εργασία όπου μεταξύ άλλων έχει τους εξής σκοπούς-στόχους. Την υλοποίηση πρωτοκόλλων 6LowPan σε Contiki και την δημιουργία συστήματος προσομοίωσης με τελικό σκοπό την αξιολόγηση τους μέσω σεναρίων και πειραμάτων. Η βάση για να υλοποιηθούν όλα αυτά είναι η κατανόηση βασικών πρωτοκόλλων και αρχιτεκτονικών, όπως IPv6, MIPv6, 6LowPan, Mobility in WSNs, καθώς και η μελέτη προϋπάρχουσας ερευνητικής εργασίας. Τέλος στόχος ήταν και η κατανόηση του λειτουργικού συστήματος Contiki και του συστήματος προσομοίωσης COOJA για την προσομοίωση των πρωτοκόλλων αλλά και τον πειραματισμό τους.

Επιπλέον έγινε υλοποίηση σεναρίων όπου μελετήθηκε το έγγραφο RPL και τον τρόπο λειτουργίας του πρωτοκόλλου Neighbor Discovery.

Περιεχόμενα

Κεφάλαιο 1	Εισαγωγή.....	7
	1.1 Γενική αναφορά και ο σκοπός της διπλωματικής εργασίας	7
	1.2 Δομή της διπλωματικής εργασίας	10
Κεφάλαιο 2	Αρχιτεκτονική και Πρωτόκολλα Δικτύου.....	11
	2.1 Αρχιτεκτονική και Πρωτόκολλα Δικτύου	11
	2.1.1 Internet Protocol Suite	12
	2.2 Internet Protocol	13
	2.2.1 Internet Protocol version 4	14
	2.2.2 Internet Protocol version 6	16
	2.2.2.1 ICMPv6	18
	2.2.2.2 IPv6 Neighbor Discovery	19
	2.2.3 Πρωτόκολλο UDP	23
	2.3 IEEE 802.11	24
	2.3.1 IEEE 802.15.4	25
	2.4 Αρχιτεκτονική Ασύρματου Αισθητήρα	26
	2.5 Ασύρματα Δίκτυα Αισθητήρων	28
Κεφάλαιο 3	Προηγούμενη Σχετική Εργασία	31
	3.1 6LoWPAN Δίκτυα	31
	3.2 6LoWPAN Neighbor Discovery	33
	3.3 Πρωτόκολλο Δρομολόγησης RPL	34
	3.4 Προηγούμενες Σχετικές Εργασίες - Υλοποιήσεις	36
Κεφάλαιο 4	Υλοποίηση.....	38
	4.1 Λειτουργικό Σύστημα Contiki	38
	4.2 COOJA	39
	4.3 Προσαρμογή Πρωτοκόλλων	40
	4.4 Προσαρμογή IPv6 Neighbor Discovery και RPL πρωτοκόλλου	40
	4.5 Προβλήματα	41

Κεφάλαιο 5	Σενάρια και Αποτελέσματα.....	42
5.1	Γενική Λειτουργία	42
5.2	Σενάριο Α	43
5.3	Σενάριο Β	44
5.4	Σενάριο Γ	46
 ΚΕΦΑΛΑΙΟ 6	 Αξιολόγηση και Μελλοντική Εργασία	 48
6.1	Γενικά Συμπεράσματα – Επισημάνσεις	48
6.2	Μελλοντική Εργασία	49
 Β ι β λ ι ο γ ρ α φ ί α		 50

Κεφάλαιο 1

Εισαγωγή

1.1 Γενική αναφορά και ο σκοπός της διπλωματικής εργασίας	7
1.2 Δομή της διπλωματικής Εργασίας	10

1.1 Γενική αναφορά και ο σκοπός της διπλωματικής εργασίας

Τα ασύρματα δίκτυα πλέον βρίσκονται για τα καλά στη ζωή μας αφού με την ραγδαία εξέλιξη της τεχνολογίας δεν μπορούσε να μείνει ανεπηρέαστος ο χώρος των δικτύων και ιδιαίτερα των ασύρματων δικτύων. Επίσης μέσα από την ανάπτυξη των αισθητήρων, στο γενικό περιβάλλον, ήταν μιας πρώτης τάξεως ευκαιρία για την εκμετάλλευσή τους στον τομέα των ασύρματων δικτύων. Έτσι τα ασύρματα δίκτυα αισθητήρων βρέθηκαν στο προσκήνιο με πολλά περιθώρια ανάπτυξης και πεδία έρευνας τα τελευταία πέντε χρόνια.

Τα ασύρματα δίκτυα αισθητήρων αποτελούνται συνήθως από μεγάλο αριθμό αισθητήρων χαμηλού κόστους και μικρού μεγέθους. Οι αισθητήρες είναι υπεύθυνοι για την μεταξύ τους επικοινωνία που γίνεται βάσει πρωτοκόλλων επικοινωνίας. Με αυτό τον τρόπο μπορεί ο άνθρωπος να παρατηρήσει εύκολα και χωρίς ιδιαίτερα μεγάλο κόστος φυσικά φαινόμενα (πλημμύρες, πυρκαγιές, ανεμοστρόβιλους) και να τα κατανοήσει πως εξελίσσονται κατά τη διάρκεια τους. Επιπλέον υπάρχει και η πιο εμπορική πλευρά, όπου μπορούν τα δίκτυα να χρησιμοποιηθούν στη βιομηχανία (εργοστάσια παραγωγής) αλλά και σε κτίρια-σπίτια και κοινόχρηστους χώρους.

Λόγω του ότι οι αισθητήρες που αποτελούν τα δίκτυα αυτά πέραν του χαμηλού κόστους έχουν δυστυχώς και μικρότερη διάρκεια ζωής, έγιναν προσπάθειες για

εξοικονόμηση ενέργειας του αισθητήρα. Η προσπάθεια αυτή είχε σαν στόχο τόσο την εξοικονόμηση κατά την λειτουργία (μέσω καινούριων ή τροποποιημένων πρωτοκόλλων) όσο και το πότε θα έπρεπε οι αισθητήρες να έμεναν σε λειτουργία (μέσω μακρών περιόδου σε κατάσταση ύπνου του αισθητήρα).

Αρχικά έγινε προσπάθεια για λειτουργία των δικτύων αυτών όπως και με τα υπόλοιπα δίκτυα που υπήρχαν. Όμως η μικρή διάρκεια ζωής των αισθητήρων λόγω μπαταρίας αλλά και μεγέθους που δεν μπορούσε να δώσει τον απαραίτητο χώρο για μεγαλύτερη πηγή ενέργειας έγινε η αφορμή για τη δημιουργία ενός νέου πρωτοκόλλου που θα ανταποκρινόταν στις ανάγκες των δικτύων αυτών σε μεγαλύτερο βαθμό από τα ήδη υπάρχοντα.

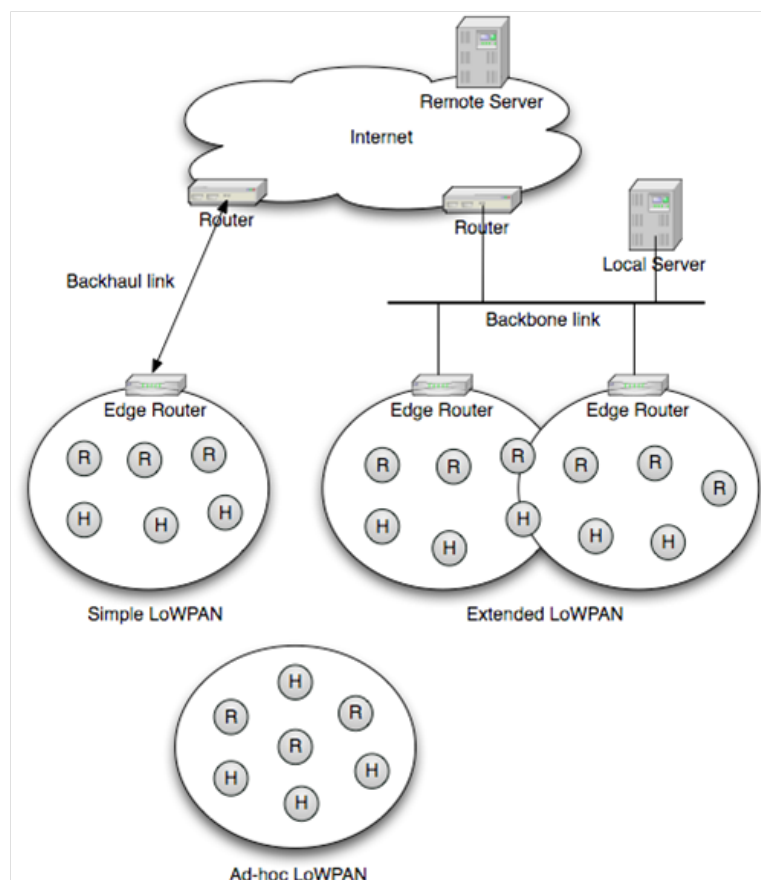
Έτσι δημιουργήθηκε το 6LoWPAN (IPv6 πάνω σε χαμηλής ισχύος ασύρματα δίκτυα) το οποίο στην ουσία προσφέρει ότι χρειάζεται το Network Layer χωρίς να είναι άμεσα απαραίτητο το Link Layer. Στην ουσία το 6LoWPAN πρωτόκολλο υποκαθιστούσε το Link Layer ως προς τις ανάγκες του προς το Network Layer.

Και ενώ με το 6LoWPAN μπορούσαν να διεκπεραιωθούν όλες οι λειτουργίες που θεωρούνται απαραίτητες έχουμε ένα σοβαρό θέμα με την κατανάλωση ενέργειας. Ο κύριος λόγος που παρατηρείται το πρόβλημα αυτό είναι από την εφαρμογή του Neighbor Discovery, αφού παρόλο που στα υπόλοιπα κομμάτια το 6LoWPAN υποκαθιστά Link Layer, εδώ δεν εφαρμόζει σωστά το Neighbor Discovery.

Συνεπακόλουθο αυτού ήταν οι προσπάθειες να κατευθυνθούν προς την επίλυση του προβλήματος αυτού και την εξεύρεση τροποποιήσεων όπου θα έκαναν το Neighbor Discovery πρωτόκολλο να υιοθετήσει τις απαιτήσεις των 6LoWPAN δικτύων. Επιπλέον οι ερευνητές έχουν ξεκινήσει να συνυπολογίζουν και τη μη σταθερότητα των κόμβων, έτσι ώστε να τροποποιήσουν το Neighbor Discovery πρωτόκολλο και να μην αντιμετωπίζουν εκ νέου άλλα προβλήματα. Να αναφέρω ότι σε μερικές περιπτώσεις όπου κάποιος κινητός κόμβος εισέλθει ή εξέλθει κάποιου τοπικού δικτύου προκαλούνται αντίστοιχα προβλήματα όπως θα δούμε από τα σενάρια που θα τρέξουμε στο κεφάλαιο 5.

Μέσα από τη διπλωματική εργασία είχαμε τους ακόλουθους στόχους. Αρχικά την μελέτη και κατανόηση βασικών πρωτοκόλλων και αρχιτεκτονικών που σχετίζονται άμεσα με τα ασύρματα δίκτυα, όπως Wireless Sensor Networks, IPv6, 6LowPAN, Mobility inWSNs και RPL. Μετέπειτα, και αφού εγκαταστήσαμε το λειτουργικό σύστημα Contiki και τον προσομοιωτή COOJA, θα έπρεπε να κατανοήσουμε τον τρόπο λειτουργίας τους μέσα από διάφορα παραδείγματα και σενάρια. Μέσα από το περιβάλλον προσομοίωσης στόχος ήταν η υλοποίηση σεναρίων με σταθερούς κόμβους την πρώτη φορά και μεταβλητούς κόμβους τη δεύτερη φορά έτσι ώστε να ληφθούν μετρήσεις με απώτερο σκοπό να εξαχθούν χρήσιμα συμπεράσματα. Έτσι μέσα από τον πειραματισμό των πιο πάνω σεναρίων με αλλαγές στις παραμέτρους είχαμε την ευκαιρία να μελετήσουμε τον τρόπο συμπεριφοράς των δικτύων με ασύρματους κόμβους.

Επιγραμματικά ο κύριος σκοπός της διπλωματικής εργασίας ήταν η εξαγωγή συμπερασμάτων μέσα από τις προσομοιώσεις ασύρματων δικτύων, εστιάζοντας στην διαχείριση της κινητικότητας στα δίκτυα αυτά.



Εικόνα 1.1

1.2 Δομή της διπλωματικής Εργασίας

Η Διπλωματική εργασία χωρίζεται σε έξι κεφάλαια ως ακολούθως.

Το κεφάλαιο ένα περιλαμβάνει την γενική εισαγωγή του θέματος καθώς και το παρόν κομμάτι όπου αναφέρεται η συγκεκριμένη δομή της Διπλωματικής εργασίας.

Το κεφάλαιο δύο περιλαμβάνει αναφορές και σύντομες περιγραφές αρχιτεκτονικών και πρωτοκόλλων που μελετήθηκαν κατά τη διάρκεια της Διπλωματικής εργασίας

Το κεφάλαιο τρία περιλαμβάνει σύντομη περίληψη προηγούμενων αντίστοιχων ερευνητικών εργασιών και των πληροφοριών που κράτησα από την κάθε περίπτωση.

Το κεφάλαιο τέσσερα αναφέρεται στην υλοποίηση των σεναρίων στον προσομοιωτή.

Στο κεφάλαιο πέντε παρουσιάζονται τα σενάρια με τα αποτελέσματα των σεναρίων.

Τέλος στο κεφάλαιο έξι αναφέρεται στην αξιολόγηση των σεναρίων που υλοποιήθηκαν.

Κεφάλαιο 2

Αρχιτεκτονική και πρωτόκολλα Δικτύου

2.1 Αρχιτεκτονική και Πρωτόκολλα Δικτύου	11
2.1.1 Internet Protocol Suite	12
2.2 Internet Protocol	13
2.2.1 Internet Protocol version 4	14
2.2.2 Internet Protocol version 6	16
2.2.2.1 ICMPv6	18
2.2.2.2 IPv6 Neighbor Discovery	19
2.2.3 Πρωτόκολλο UDP	23
2.3 IEEE 802.11	24
2.3.1 IEEE 802.15.4	25
2.4 Αρχιτεκτονική Ασύρματου Αισθητήρα	26
2.5 Ασύρματα Δίκτυα Αισθητήρων	28

2.1 Αρχιτεκτονική και Πρωτόκολλα Δικτύου

Για την ομαλή λειτουργία των δικτύων γενικά αλλά και κυρίως του διαδικτύου έπρεπε εξ αρχής να τεθούν κάποιοι “νόμοι”. Οι κανόνες αυτοί είναι τα πρωτόκολλα επικοινωνίας που χρησιμοποιούμε μέχρι και σήμερα. Έτσι είναι αναγκαίο όπως για κάθε προσπάθεια ανακάλυψης κάτι καινούριου στο χώρο των δικτύων να λαμβάνονται υπόψη και οι περιορισμοί από τα πρωτόκολλα αυτά. Στο κεφάλαιο αυτό γίνεται μια εκτενής αναφορά σε πρωτόκολλα και ορισμούς έτσι ώστε να γίνεται πιο εύκολα κατανοητός ο τρόπος λειτουργίας.

2.1.1 Internet Protocol Suite

Το internet protocol suite είναι γνωστό ως πρωτόκολλο TCP/IP. Το πρωτόκολλο αυτό πήρε την ονομασία του από δυο πρωτόκολλα, το TCP (Transmission Control Protocol = Πρωτόκολλο Ελέγχου Μετάδοσης) και το IP (Internet Protocol = Πρωτόκολλο Διαδικτύου). [1,2] Αυτά τα πρωτόκολλα αποτελούν μια συλλογή η οποία είναι οργανωμένη σε στρώματα. Για την παροχή γενικών πρωτοκόλλων και υπηρεσιών γίνεται χρήση της ενθυλάκωσης από το πρωτόκολλο IP. Τα κατώτερα στρώματα παρέχουν πρωτόκολλα τα οποία χρησιμοποιούνται από τα πρωτόκολλα του υψηλού στρώματος έτσι ώστε να μπορέσει να λειτουργήσει. Το Internet Protocol Suite αποτελείται από τέσσερα στρώματα. [24]

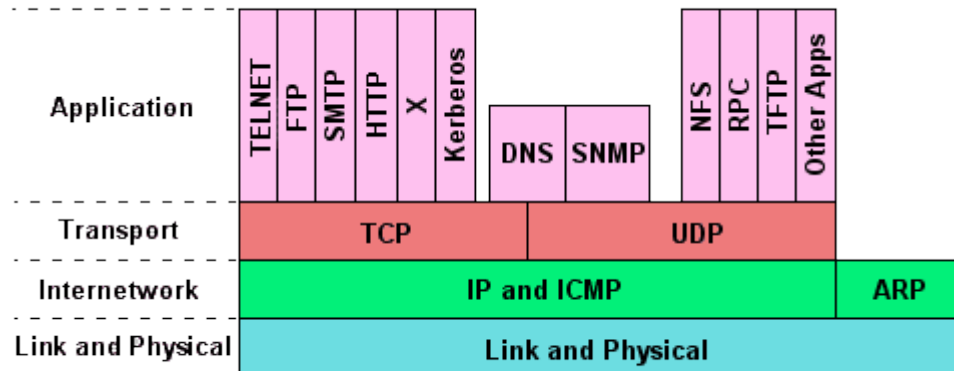
Τα στρώματα τα οποία αποτελούν αυτό το πρωτόκολλο είναι τα εξής[1,2]:

Link Layer (= Συνδέσμου): Το στρώμα αυτό είναι το χαμηλότερο στρώμα του Internet Protocol Suite και περιέχει όλα τα πρωτόκολλα επικοινωνίας. Βρίσκονται εν λειτουργία εφόσον είναι φυσικά συνδεδεμένος ο host με το δίκτυο (Ethernet). Στο Link Layer συχνά θεωρείται μέρος και το Physical Layer (Φυσικό Επίπεδο), το οποίο αποτελείται από τα φυσικά στοιχεία του δικτύου.

Internet Layer (= Δικτύου): Το στρώμα αυτό περιέχει σύνολο μεθόδων, πρωτοκόλλων και ανήκει στο πρωτόκολλο Internet protocol suite. Αυτό το στρώμα διαχειρίζεται την κίνηση των πακέτων στο δίκτυο. Τα πακέτα δρομολογούνται από αυτό το στρώμα. Το κύριο χαρακτηριστικό του στρώματος αυτού είναι η δημιουργία του Διαδικτύου, και αυτό επιτυγχάνεται με την ένωση των τοπικών δικτύων.

Transport Layer (= Μεταφοράς): Το στρώμα αυτό παρέχει τη ροή των δεδομένων μεταξύ δύο υπολογιστών αλλά παρέχει και end-to-end επικοινωνία. Επίσης περιλαμβάνει πολλά σημαντικά χαρακτηριστικά, όπως connection – oriented communication, αξιοπιστία, έλεγχο ροής (flow control), έλεγχο της συμφόρησης (Congestion avoidance), πολυπλεξία (Multiplexing) και τέλος τα πακέτα όταν σταλούν με κάποια συγκεκριμένη σειρά τότε φτάνουν με την ίδια σειρά στον προορισμό τους (same order delivery).

Application Layer (=Εφαρμογής): Το στρώμα αυτό χρησιμοποιεί το underlying transport layer πρωτόκολλο για την εγκατάσταση επικοινωνίας process – to –process. Παράδειγμα ενός πρωτοκόλλου που προσφέρει για την επικοινωνία είναι το HTTP.



Εικόνα 2.1

2.2 Internet Protocol

[3]Οι Vint Cerf και Bob Kahn ήταν οι πρώτοι που όρισαν το πρωτόκολλο διαδικτύου (IP) το 1974. Η τέταρτη έκδοση (IPv4) ήταν η πρώτη στην οποία εμφανίστηκε το πρωτόκολλο IP, η έκδοση αυτή υπάρχει μέχρι σήμερα. Λόγω ανεπάρκειας διευθύνσεων έχει αναπτυχθεί η έκδοση του πρωτοκόλλου από τη τέταρτη έκδοση στην έκτη έκδοση (IPv6).

Το πρωτόκολλο διαδικτύου ή αλλιώς IP αποτελεί το βασικό πρωτόκολλο του επιπέδου δικτύου. Κατά τη διάρκεια μετάδοσης ενός πακέτου λόγω αναξιοπιστίας μπορεί να φτάσει σε λάθος προορισμό, να διπλασιαστεί μέσα στο δίκτυο αλλά και να χαθεί στο δρόμο προς τον προορισμό του. Για τη δρομολόγηση πακέτων εκτός ορίων υπεύθυνο είναι το πρωτόκολλο αυτό.[4] Το IP στέλνει το πακέτο στο φυσικό δίκτυο για να παραδοθεί στον προορισμό του.

2.2.1 Internet Protocol version 4

Το Internet Protocol version 4 είναι το πιο διαδεδομένο πρωτόκολλο στο Link Layer που σχεδιάστηκε στα τέλη του 1980. [5] Το πρωτόκολλο αυτό χρησιμοποιεί διευθύνσεις των 32bits. Παρόλα αυτά πολλές από τις διευθύνσεις που προσφέρονται είναι δεσμευμένες σε ιδιωτικά δίκτυα. Με αυτό τον τρόπο ο αριθμός διευθύνσεων που μπορούν να προσφερθούν σε δημόσιες υπηρεσίες μειώνονται. Αποτέλεσμα αυτής της μείωσης είναι η μη ικανοποίηση πολλών υπηρεσιών και έτσι γίνεται αναφορά σε ένα πρωτόκολλο ανώτερου στρώματος το internet protocol version 6.

Με τη μεταφορά ενός πακέτου αυτό το πρωτόκολλο δεν εγγυάται την παράδοση του πακέτου, επίσης δεν σου εγγυάται την αποστολή του ίδιου πακέτου και για δεύτερη φορά, αλλά επίσης δε σου εγγυάται την αποστολή των πακέτων με τη σωστή σειρά.

Ένα πακέτο IPv4 έχει κεφαλίδα με τα πιο κάτω πεδία:

Έκδοση (Version): Αυτό το πεδίο έχει μέγεθος 4bit, είναι το σημείο στο οποίο αναφέρεται η έκδοση του πρωτοκόλλου, άρα αφού μιλάμε για το πρωτόκολλο IP σε έκδοση 4, θα έχει τη τιμή 4.

Μήκος Κεφαλίδας (IP Header Length – IHL): Περιγράφει το μήκος της κεφαλίδας σε λέξεις των 32bytes. Η τιμή του πεδίου είναι 5 για το λόγο ότι οι λέξεις αυτές είναι συνήθως 5. Το μέγεθος του πεδίου αυτού είναι 4 bits.

Τύπος Υπηρεσίας (Type of Service – T.o.S): Γίνεται περιγραφή του τρόπου με τον οποίο γίνεται η δρομολόγηση του πακέτου. Το πεδίο αυτό έχει μέγεθος 8 bits.

Συνολικό Μήκος πακέτου (Total Length): Το πεδίο αυτό καθορίζει το συνολικό μήκος του πακέτου, το οποίο περιέχει το μήκος των δεδομένων μαζί με το μήκος της κεφαλίδας. Το πεδίο αυτό περιέχει ένα ακέραιο αριθμό μεγέθους 16bit.

Ταυτότητα (Identification): Ένας αριθμός ταυτότητας που βοηθά στην αναγνώριση του πακέτου. Όταν ένα πακέτο αποτελείται από πολλά κομμάτια, δηλαδή έχει κατακερματιστεί, τότε το κάθε κομμάτι του πακέτου θα έχει τον ίδιο αριθμό ταυτότητας έτσι ώστε να φαίνεται ότι αποτελούν μέρος του ίδιου πακέτου. Το πεδίο αυτό έχει μέγεθος 16 bit.

Σημαίες (Flags): Κάθε bit του πεδίου αυτού αποτελεί μια σημαία. Ανάλογα με τη τιμή της σημαίας τότε εκτελούνται οι ανάλογες διαδικασίες κατακερματισμού. Οι τιμές που μπορεί να πάρει μια σημαία είναι 0 ή 1. Επίσης με βάση τη σημαία φαίνεται αν κάποιο μέρος του πακέτου είναι το τελευταίο ή όχι.

Χρόνος Ζωής (Time to Live – TTL): Για την αποφυγή ύπαρξης ενός πακέτου επ'αόριστον στο δίκτυο, υπάρχει αυτό το πεδίο έτσι ώστε να ορίζεται η διάρκεια ζωής του πακέτου. Ο αριθμός αυτός μειώνεται κάθε φορά που εισέρχεται σε κάποιο δρομολογητή. Όταν φτάσει στο μηδέν τότε αυτό το πακέτο απορρίπτεται. Το πεδίο αυτό έχει μέγεθος 8bit.

Τύπος Πρωτοκόλλου (Protocol): Στο Transport Layer χρησιμοποιούνται πρωτόκολλα, για το καθορισμό του πρωτοκόλλου που χρησιμοποιείται σημαντικό είναι αυτό το πεδίο με μέγεθος 8bit.

Άθροισμα Ελέγχου Κεφαλίδας (Header Checksum): Αυτό το πεδίο είναι χρήσιμο όχι στον έλεγχο όλου του πακέτου αλλά στον έλεγχο της ορθής μετάδοσης της κεφαλίδας. Δηλαδή γίνεται έλεγχος για σφάλματα στη κεφαλίδα. Το μέγεθος αυτού του πεδίου είναι 16 bit.

IP Διεύθυνση Αφετηρίας (Source IP Address): Το πεδίο αυτό περιέχει τη διεύθυνση του αποστολέα του πακέτου και έχει μέγεθος 32 bit.

IP Διεύθυνση Προορισμού (Destination IP Address): Το πεδίο αυτό περιέχει τη διεύθυνση του παραλήπτη του πακέτου και έχει μέγεθος 32 bit.

Επιλογές IP (IP Options): Τις περισσότερες φορές δεν χρησιμοποιείται. Συμπληρώνεται με μηδενικά στη περίπτωση που δε θα χρησιμοποιηθεί ολόκληρο, αλλιώς το πεδίο Μήκος της Κεφαλίδας (LHL) θα είναι μεγαλύτερο από 5 ώστε να δείχνει το μέγεθος του.

version	H. length	TOS	total length	
identification			flags	fragment offset
Time to Live		protocol	header checksum	
32-bit source address				
32-bit destination address				
options				

Εικόνα 2.2

2.2.2 Internet Protocol version 6

Το διαδίκτυο έχει αναπτυχθεί στο βασικό πρωτόκολλο επικοινωνίας IP με τελευταία αναθεώρηση το IPv6 που ορίστηκε το 1988. [6] Το πρωτόκολλο IPv6 αναπτύχθηκε έτσι ώστε να λυθεί το πρόβλημα που αντιμετωπίζεται από το πρωτόκολλο IPv4. Το πρόβλημα που παρουσίασε το πρωτόκολλο IPv4 ήταν η μη εξυπηρέτηση των μεγάλων αναγκών σε συνδέσεις που χρειαζόταν το διαδίκτυο. Ο λόγος ήταν ότι το IPv4 μπορούσε να διαθέσει μόνο 2^{32} διευθύνσεις, έτσι έπρεπε να βρεθεί μια λύση για περισσότερες διευθύνσεις, και έτσι αναπτύχθηκε το IPv6 το οποίο μπορούσε να διαθέσει 2^{128} . Με την αλλαγή του πρωτοκόλλου IP από τη τέταρτη έκδοση στην έκτη είχε και ως αποτέλεσμα την αλλαγή της μορφής της κεφαλίδας, διαφέρει σχεδόν σε όλα τα πεδία η κεφαλίδα τη έκδοσης 6 από την κεφαλίδα της έκδοσης 4.

Ένα πακέτο IPv6 έχει κεφαλίδα με τα πιο κάτω πεδία:

Έκδοση (Version): Αυτό το πεδίο έχει μέγεθος 4bit, είναι το σημείο στο οποίο αναφέρεται η έκδοση του πρωτοκόλλου, άρα αφού μιλούμε για το πρωτόκολλο IP με έκδοση 6, θα έχει τη τιμή 6.

Κατηγορία Κυκλοφορίας (Traffic Class): Αυτό το πεδίο έχει μέγεθος 8bit. Για την επιλογή κάποιου δρομολογίου χρησιμοποιείται αυτό το πεδίο.

Ετικέτα Ροής (Flow Label): Το πεδίο αυτό έχει μέγεθος 20bit. Καθορίζει συγκεκριμένη διαδρομή μέσω του δικτύου.

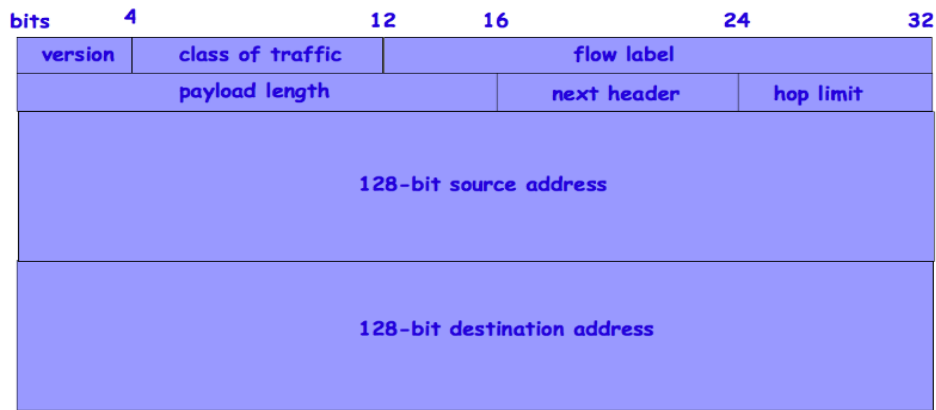
Μήκος Ωφέλιμου Φορτίου (Payload Length): Προσδιορίζει το μέγεθος των δεδομένων που μεταφέρει το πακέτο και δε συμπεριλαμβάνει το μέγεθος της κεφαλίδας. Το πεδίο αυτό έχει μέγεθος 16bit.

Επόμενη κεφαλίδα (Next Header): Καθορίζει τον τύπο των πληροφοριών της επόμενης κεφαλίδας. Έχει μέγεθος 8bit.

Όριο Αλμάτων (Hop Limit): Για να μην μπορεί να υπάρξει κάποιο πακέτο στο δίκτυο συνεχώς, καθορίζεται κάποιος χρόνος, ως ο χρόνος ζωής των πακέτων στο δίκτυο. Αυτό το πεδίο έχει μέγεθος 8bit.

IP Διεύθυνση Αφετηρίας (Source IP Address): Περιέχει την IP διεύθυνση του αποστολέα του πακέτου. Έχει μέγεθος 128bit.

IP Διεύθυνση Προορισμού (Destination IP Address): Περιέχει την IP διεύθυνση του τελικού παραλήπτη του πακέτου. Το πεδίο αυτό έχει μέγεθος 128 bit .



Εικόνα 2.3

2.2.2.1 ICMPv6

Το ICMPv6 (Internet Control Message Protocol version 6) είναι η εφαρμογή του ICMP για το IPv6 πρωτόκολλο. [7] Αποτελεί αδιάσπαστο κομμάτι του IPv6 και εκτελεί αναφορά σφαλμάτων αλλά και λειτουργίες διάγνωσης. Επίσης έχει και κάποιο πλαίσιο για τις επεκτάσεις που μπορεί να εφαρμοστούν από μελλοντικές αλλαγές.

Πολλές επεκτάσεις έχουν δημοσιευθεί, καθορίζοντας νέους τύπους μηνυμάτων ICMPV6 καθώς και νέες επιλογές για τους υφιστάμενους τύπους μηνυμάτων ICMPv6. Το πρωτόκολλο Neighbor Discovery είναι ένα πρωτόκολλο που μπορεί να ανακαλύψει κόμβους στο IPv6, το οποίο αντικαθιστά αλλά και ενισχύει τις λειτουργίες του ARP (Address Resolution Protocol). Το πρωτόκολλο Secure Neighbor Discovery αποτελεί προέκταση του πρωτοκόλλου Neighbor Discovery αλλά προσφέρει επιπλέον ασφάλεια. Το πρωτόκολλο Multicast Router Discovery επιτρέπει την ανακάλυψη των multicast δρομολογητών.

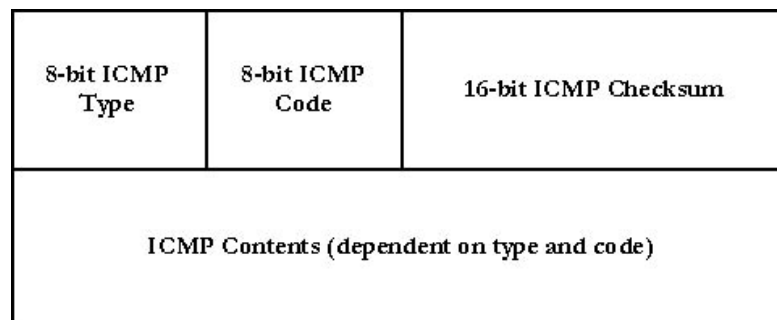
Τα ICMPv6 μηνύματα μπορούν να χωριστούν σε δύο κατηγορίες, στην κατηγορία Μηνύματα Λάθους (Error Messages), και στη κατηγορία Ενημερωτικά Μηνύματα (Informational Messages).

Το πακέτο ICMPv6 αποτελείται από μια κεφαλίδα και το ωφέλιμο φορτίο του πρωτοκόλλου. Η κεφαλίδα περιέχει μόνο τρεις τομείς: *type* (8 bits), *code* (8 bits), και *checksum*(16 bits).

Type: καθορίζει τον τύπο του μηνύματος. Οι τιμές έχουν εύρος 0 - 127 εμφανίζει ένα μήνυμα λάθους, ενώ οι τιμές στο εύρος 128-255 εμφανίζει ένα μήνυμα πληροφοριών.

Code: Η τιμή του πεδίου εξαρτάται από τον τύπο του μηνύματος.

Checksum: Το πεδίο αυτό παρέχει ένα ελάχιστο επίπεδο για την επαλήθευση της ακεραιότητας του μηνύματος ICMP.



Εικόνα 2.4

2.2.2.2 IPv6 Neighbor Discovery

Το Neighbor Discovery πρωτόκολλο, είναι πρωτόκολλο το οποίο υπάρχει στο Internet Protocol Suite που χρησιμοποιείται μέσω του IPv6. [8] Λειτουργεί στο Link Layer και είναι υπεύθυνο για την ανίχνευση άλλων κόμβων στο σύνδεσμο, αλλά επίσης και στο καθορισμό των διευθύνσεων άλλων κόμβων στο Link Layer, ανιχνεύει επαναλαμβανόμενες διευθύνσεις, βρίσκει διαθέσιμους routers και servers, είναι υπεύθυνο για την διατήρηση των πληροφοριών σχετικά με την προσβασιμότητα στους ενεργούς γειτονικούς κόμβους.

Το πρωτόκολλο ορίζει πέντε διαφορετικούς ICMPv6 τύπους πακέτων για την εκτέλεση λειτουργιών του IPv6, που αντίστοιχες λειτουργίες στο IPv4 γίνονταν μέσω των Address Resolution Protocol, Internet Control Message Protocol, Router Discovery Protocol και Router Redirect Protocol. Ωστόσο παρέχει πάρα πολλές βελτιώσεις σε σχέση με τις λειτουργίες που πρόσφεραν τα πρωτόκολλα στο IPv4.

Οι hosts χρησιμοποιούν το πρωτόκολλο αυτό έτσι ώστε να ανακαλύψουν γειτονικούς δρομολογητές, αλλά και για διευθύνσεις και άλλες παραμέτρους διαμόρφωσης. Παρόμοια μπορούν να χρησιμοποιήσουν το πρωτόκολλο αυτό και οι δρομολογητές αλλά και οι κόμβοι.

Οι δρομολογητές θα το χρησιμοποιήσουν έτσι ώστε να διαφημίσουν την ύπαρξη τους αλλά επίσης για να διαφημίσουν και την ύπαρξη του δικτύου. Αυτό επιτυγχάνεται με την αποστολή από κάθε δρομολογητή multicast Router Advertisement μηνύματα. Κάθε κόμβος που λαμβάνει αυτά τα μηνύματα από τους δρομολογητές ενημερώνει τη λίστα με τους ήδη υπάρχοντες δρομολογητές έτσι ώστε να δημιουργήσει τη δική του παγκόσμια διεύθυνση.

Τέλος οι κόμβοι το χρησιμοποιούν έτσι ώστε να προσδιορίσουν αν κάποιος γείτονας είναι ακόμη προσβάσιμος, για να καθορίσει πότε μια διεύθυνση του link layer έχει αλλάξει αλλά επίσης και για την επιδιόρθωση κάποιας διεύθυνσης του link-layer ενός γειτονικού κόμβου στον οποίο έγινε προώθηση πακέτου.

Οι πέντε διαφορετικοί ICMPv6 τύποι πακέτων που ορίζει το πρωτόκολλο:

Router Solicitation - Ενεργοποίησης

Τα μηνύματα αυτά στέλνονται αρχικά μόλις ενεργοποιηθεί ο οποιοσδήποτε κόμβος για να εντοπίσει κάποιο γειτονικό διακομιστή (router) και να ζητήσει Router Advertisement Message. Έτσι εξοικονομεί χρόνο και δεν περιμένει μέχρι την επόμενη κανονική ενημέρωση ρουτίνας.

Router Advertisement – Διαφήμισης Διακομιστή

Οι διακομιστές στέλνουν ανά τακτά διαστήματα τα μηνύματα αυτά για να ενημερώσουν τους γειτονικούς κόμβους ότι βρίσκονται εντός της εμβέλειας τους και μπορούν να τους παρέχουν το prefix και τα υπόλοιπα αναγκαία. Επιπλέον τα μηνύματα στέλνονται σε περίπτωση που δεχθούν μήνυμα ενεργοποίησης(Router Solicitation Message) από κάποιο κόμβο προς απάντηση του αρχικού μηνύματος.

Neighbor Solicitation- Εντοπισμός γειτονικών κόμβων – Διαφήμιση του κόμβου στους γείτονες τους

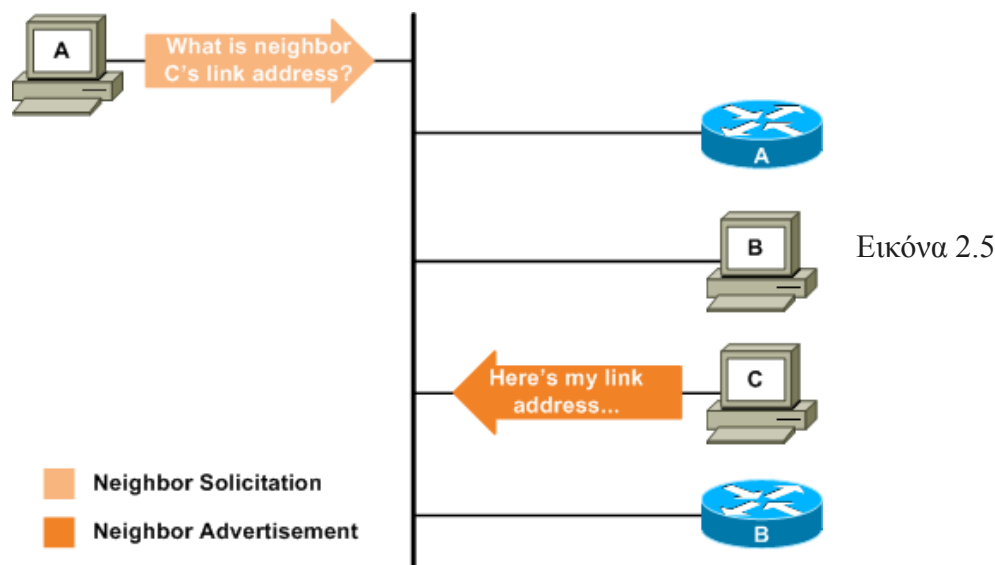
Οι κόμβοι θέλοντας να εντοπίζουν τους γειτονικούς τους κόμβους αλλά και να στέλνουν αυτά τα μηνύματα, για να ανακαλύψει άλλους κόμβους (determine link-layer address of a neighbor) ή να επαληθεύσουν την ύπαρξη άλλων κόμβων (μέσω της cached link-layer address) ζητώντας να μεταδώσουν Neighbor Advertisement Message. Επίσης, χρησιμοποιούνται για τον έλεγχο Duplicate Address Detection.

Neighbor Advertisement – Ενημέρωση από κόμβους

Οι κόμβοι για να απαντήσουν σε μηνύματα Neighbor Solicitation Message στέλνουν τα μηνύματα αυτά. Έτσι προβάλλουν την ύπαρξη τους δίνοντας περισσότερες πληροφορίες. Επιπλέον στέλνουν τα πιο πάνω μηνύματα σε περίπτωση όπου έγινε κάποια αλλαγή στο link-layer address.

Redirect

Οι διακομιστές μετά από κάποια αλλαγή στο δίκτυο(ένταξη καινούριου διακομιστή ή κόμβου) ενημερώνουν τους ήδη υπάρχοντες κόμβους ότι πλέον υπάρχει η δυνατότητα χρήσης καινούριων μονοπατιών για την αποστολή πακέτων σε συγκεκριμένο/ους προορισμό/ους



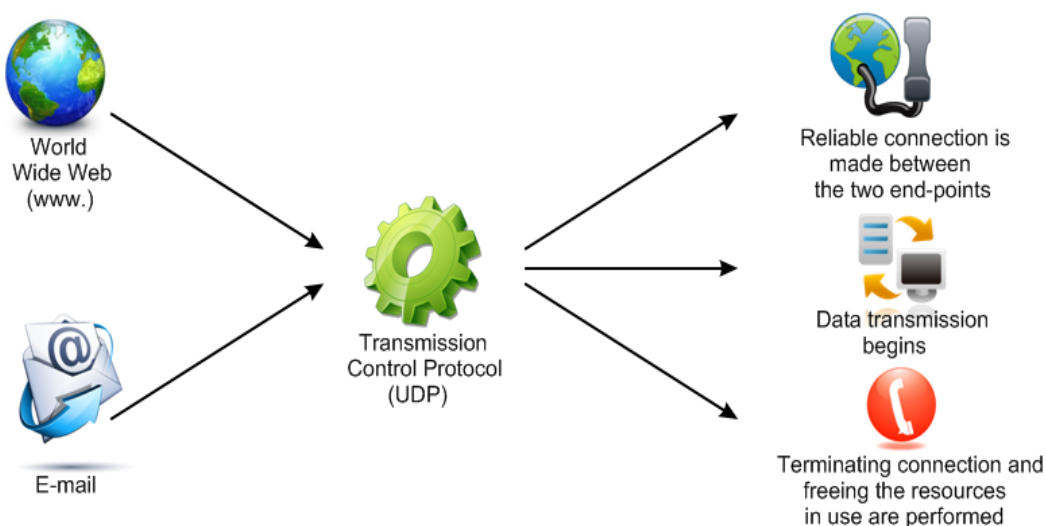
0	Reserved	
1	Destination Unreachable	[RFC4443]
2	Packet Too Big	[RFC4443]
3	Time Exceeded	[RFC4443]
4	Parameter Problem	[RFC4443]
100	Private experimentation	[RFC4443]
101	Private experimentation	[RFC4443]
102- 126	Unassigned	
127	Reserved for expansion of ICMPv6 error messages	[RFC4443]
128	Echo Request	[RFC4443]
129	Echo Reply	[RFC4443]
130	Multicast Listener Query	[RFC2710]
131	Multicast Listener Report	[RFC2710]
132	Multicast Listener Done	[RFC2710]
133	Router Solicitation	[RFC4861]
134	Router Advertisement	[RFC4861]
135	Neighbor Solicitation	[RFC4861]
136	Neighbor Advertisement	[RFC4861]
137	Redirect Message	[RFC4861]
138	Router Renumbering	[Matt_Crawfor]
139	ICMP Node Information Query	[RFC4620]
140	ICMP Node Information Response	[RFC4620]
141	Inverse Neighbor Discovery Solicitation Message	[RFC3122]
142	Inverse Neighbor Discovery Advertisement Message	[RFC3122]
143	Version 2 Multicast Listener Report	[RFC3810]
144	Home Agent Address Discovery Request Message	[RFC6275]
145	Home Agent Address Discovery Reply Message	[RFC6275]
146	Mobile Prefix Solicitation	[RFC6275]
147	Mobile Prefix Advertisement	

2.2.3 Πρωτόκολλο UDP

Βασικό πρωτόκολλο το οποίο χρησιμοποιείται στο Διαδίκτυο. Η ονομασία του UDP προέρχεται από το User Datagram Protocol Universal αλλά επίσης και από το Datagram Protocol. Είναι χρήσιμο για την αποστολή σύντομων μηνυμάτων μέσα σε ένα δίκτυο υπολογιστών και γι' αυτό χρησιμοποιείται από πολλά προγράμματα. Κάποια από τα κύρια χαρακτηριστικά του πρωτοκόλλου αυτού είναι η αναξιόπιστη επικοινωνία, η λανθασμένη σειρά παραλαβής κάποιων πακέτων, η διπλή παραλαβή του ίδιου πακέτου όπως επίσης η μη παραλαβή του πακέτου λόγω εξαφάνισης μέσα στο δίκτυο. Για το λόγο ότι δε γίνεται κάποιος έλεγχος για την παραλαβή των πακέτων αποτελεί ένα γρήγορο και αποτελεσματικό πρωτόκολλο για εφαρμογές οι οποίες δεν χρειάζονται αξιόπιστη επικοινωνία.

Το πρωτόκολλο UDP προτιμάται για εφαρμογές ήχου και εικόνας, διότι είναι αρκετά γρήγορο και είναι σημαντικό να παραδοθούν στον παραλήπτη χωρίς κάποια διακοπή στη ροή του ήχου ή της εικόνας. Αν τυχόν κάποιο πακέτο χαθεί τότε παρεμβένουν οι μηχανισμοί διόρθωσης έτσι ώστε να μην γίνει αντιληπτό στο παραλήπτη η αλλοίωση ή διακοπή του ήχου. Με τη χρήση του πρωτοκόλλου αυτού οι εφαρμογές έχουν τη δυνατότητα να κάνουν broadcasting, δηλαδή να γίνεται αποστολή ενός πακέτου σε όλους τους υπολογιστές του δικτύου αλλά επίσης μπορεί να κάνει και multicasting δηλαδή την αποστολή ενός πακέτου σε συγκεκριμένους υπολογιστές ενός δικτύου.

Με τα χαρακτηριστικά αυτά ταιριάζει στην περίπτωση των ασύρματων δικτύων αισθητήρων αφού σημαντικό είναι η άμεση αποστολή των πακέτων χωρίς ιδιαίτερο έλεγχο παραλαβής. Έτσι αποφεύγεται σπατάλη ενέργειας με το ρίσκο όμως ότι μερικά πακέτα δεν θα φτάσουν στον προορισμό τους.



Εικόνα 2.6

2.3 IEEE 802.11

Το πιο γνωστό πρωτόκολλο για ενσύρματη δικτύωση είναι το 802.3 (Ethernet) για την επέκταση αυτού του πρωτοκόλλου, έτσι ώστε να αναπτυχθεί και κάποιο πρωτόκολλο για τα ασύρματα δίκτυα (WLAN), κατέληξαν στην ανάπτυξη ενός συνόλου προτύπων που ανήκουν στην IEEE, αυτό το σύνολο ονομάστηκε IEEE 802.11. [9] Αποτελεί το σημαντικότερο σύνολο προτύπων στο χώρο των ασύρματων δικτύων. Τα πρότυπα αυτά είναι γνωστά ως «WiFi». Το WiFi στα ελληνικά σημαίνει «ασύρματη πιστότητα» και γενικά με την αναφορά σε αυτό τον όρο, γίνεται αυτόματα αναφορά στα ασύρματα δίκτυα.

Το WiFi παρέχει κάποιες εφαρμογές, οι οποίες είναι γνωστές σε κάθε γειτονιά και χωριό. Αρχικά μπορούμε να αναφέρουμε τη δυνατότητα πρόσβασης στο Internet, επικοινωνία από το τηλέφωνο μέσω του διαδικτύου αλλά επίσης και δυνατότητα που προσφέρεται σε ηλεκτρονικές συσκευές για να συνδεθούν μεταξύ τους. Στις ηλεκτρονικές συσκευές υπάρχουν πολλές εφαρμογές που μπορούν βοηθήσουν στη μεταφορά δεδομένων από κάποια ψηφιακή συσκευή σε κάποιο υπολογιστή, για την εκτύπωση αυτών των δεδομένων χρησιμοποιείται κάποιο άλλο είδος ασύρματης δικτύωσης το Bluetooth.

Το γνωστό πρωτόκολλο 802.2 είναι το σημαντικότερο πρωτόκολλο στα ενσύρματα δίκτυα αλλά και στο Ethernet, ταυτόχρονα υπάρχει και το επίπεδο LLC που βασικές του ευθύνες είναι ο έλεγχος ροής, ο έλεγχος σφαλμάτων αλλά και το επίπεδο δικτύου. Αυτά τα δύο ταυτίζονται.

Η απόσταση που υπάρχει μεταξύ των κόμβων παίζει βασικό ρόλο στο ρυθμό μετάδοσης των δεδομένων. Η ταχύτητα μετάδοσης είναι χαμηλότερη αν η ασύρματη συσκευή βρίσκεται πολύ μακριά από το σημείο πρόσβασης, Όσο μεγαλώνει η απόσταση τόσο πιο πολύ χαμηλώνει η ταχύτητα.

Το πρωτόκολλο IEEE 802.11s είναι τροποποίηση του IEEE 802.11 για mesh networking, ορίζοντας τον τρόπο με τον οποίο ασύρματες συσκευές μπορούν να διασυνδεθούν για να δημιουργούν WLAN mesh network, οι οποίες μπορούν να

χρησιμοποιηθούν για στατικές τοπολογίες και ad hoc δίκτυα. Το 802.11 είναι ένα σύνολο από πρότυπα IEEE που χαρακτηρίζουν τις μεθόδους ασύρματης μετάδοσης.

2.3.1 IEEE 802.15.4

Το IEEE 802.15.4 υλοποιεί μια απλή μέθοδο ώστε να επιτρέψει σε πολλαπλές συσκευές να χρησιμοποιήσουν το ίδιο κανάλι συχνότητας ως το τηλεπικοινωνιακό τους μέσο. [10] Ο μηχανισμός πρόσβασης στο κανάλι που χρησιμοποιείται είναι το CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance). Στο CSMA-CA, κάθε φορά που μια συσκευή θέλει να μεταδώσει το μήνυμα που θέλει, πρώτα ελέγχει κατά πόσο ένα κανάλι είναι ελεύθερο (clear channel assessment, CCA), έτσι ώστε να σιγουρευτεί ότι το κανάλι δεν χρησιμοποιείται από κάποια άλλη συσκευή. Τότε η συσκευή ξεκινάει τη μετάδοση του μηνύματός της.

Τα στρώματα Physical control και το media access control είναι για χαμηλού ρυθμού ασύρματων δικτύων (low-rate wireless personal area networks) καθορίζονται από αυτό το πρωτόκολλο. [11] Το πρωτόκολλο IEEE 802.15.4 καθορίζει διαφορετικούς τύπους συσκευών, τις συσκευές μειωμένης λειτουργίας αλλά επίσης και τις συσκευές πλήρους λειτουργίας.

Τα δίκτυα LR-WPANs μπορούν να λειτουργούν είτε σε peer- to – peer τοπολογία, είτε σε star τοπολογία. Εάν δυο κόμβοι βρίσκονται εντός εμβέλειας τότε μπορεί να χρησιμοποιηθεί η τοπολογία peer - to – peer. Η τοπολογία αυτή προσφέρει ευελιξία, αφού επιτρέπει όλων των ειδών πλέγματα αλλά με αυτό αυξάνεται και η κατανάλωση των κόμβων, επίσης χρειάζεται ένας PAN για αυτή τη τοπολογία.

Στην δεύτερη περίπτωση, της star τοπολογίας, η επικοινωνία όλων των συσκευών γίνεται μέσω του κεντρικού κόμβου, ο οποίος είναι ένας PAN συντονιστής. Έτσι, ο PAN συντονιστής είναι ο καθόλα υπεύθυνος για την έναρξη, τη δρομολόγηση και τον τερματισμό κάθε επικοινωνίας στο δίκτυο.

Το MAC (medium access control) στρώμα έχει τα πιο κάτω καθήκοντα, διαχείριση Beacon, σύνδεση και αποσύνδεση PAN δικτύου, χρήση του CSMA-CA μηχανισμού για πρόσβαση σε κάποιο κανάλι, διαχείριση και διατήρηση του Guaranteed Time Slot (GTS) μηχανισμού, επικύρωση πλαισίου, αναγνωρισμένη παράδοση πλαισίου, και τέλος υποστήριξη της ασφάλειας της συσκευής.

Επίσης το MAC στρώμα καθορίζει τέσσερις διαφορετικούς τύπους πλαισίων:

Beacon πλαίσια: Αυτά τα πλαίσια χρησιμοποιούνται στο μηχανισμό συγχρονισμού.

-Πλαίσια αναγνώρισης: αυτά τα πλαίσια είναι χρήσιμα για την αναγνώριση εκπομπών, αλλά η τους δεν είναι υποχρεωτική.

-Πλαίσια MAC: Εκτελούν εντολές του πρωτοκόλλου IEEE 802.15.4. Κάποιες εντολές που μπορούν να δοθούν από το πρωτόκολλο είναι αίτηση δεδομένων αλλά επίσης και αίτηση σύνδεσης.

-Πλαίσια Δεδομένων: Αυτά τα πλαίσια χρησιμοποιούνται για τις μεταφορές των δεδομένων.

2.4 Αρχιτεκτονική Ασύρματου Αισθητήρα

Κάθε ασύρματο δίκτυο αισθητήρων καλείται να υλοποιήσει κάποια εφαρμογή, ανάλογα με την εφαρμογή που ανατίθεται τότε αναλόγως και η αρχιτεκτονική που θα έχουν ασύρματοι κόμβοι θα διαφέρει. Όμως ο κάθε κόμβος έχει κάποια σταθερά βασικά δομικά στοιχεία που θα αναλυθούν πιο κάτω.

Κάθε κόμβος χρειάζεται Μικροελεγκτή, Μνήμη, Πομπός – Δέκτη – Κεραία, Πηγή Ενέργειας, Αναλογικές / Ψηφιακές Είσοδοι – Αισθητήρες.

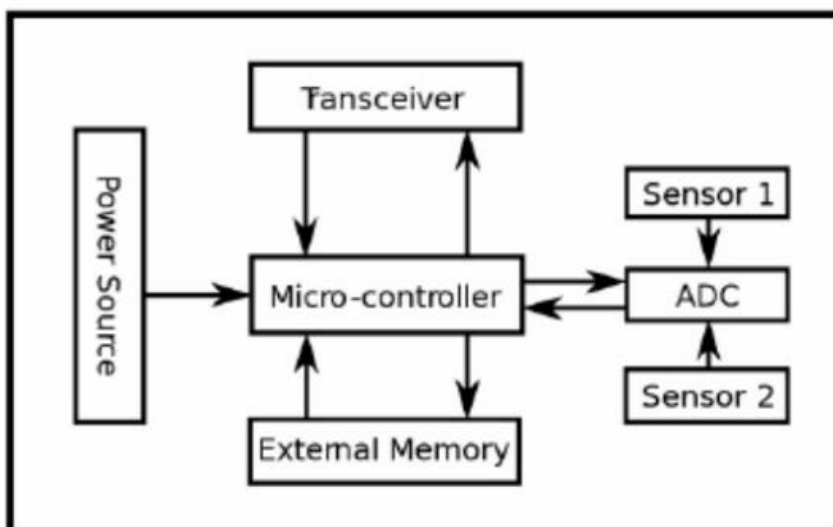
Μικροελεγκτής: Αποτελεί το κεντρικό δομικό στοιχείο και είναι υπεύθυνος για την εκτέλεση και το συγχρονισμό όλων των λειτουργιών. Η αποστολή, η επεξεργασία και η επεξεργασία των πληροφοριών γίνεται μέσω αυτού.

Μνήμη: Μαζί με τη μνήμη που είναι το chip χρησιμοποιείται Flash memory. Επίσης σε αρκετά nodes παρατηρούμε να γίνεται διαχωρισμός της περιοχής της μνήμης σε περιοχή όπου αποθηκεύονται δεδομένα και εφαρμογές του χρήστη και στην άλλη δεδομένα για την ομαλή λειτουργία του κόμβου.

Πομπός – Δέκτης – Κεραία: Η ικανότητα των κόμβων να επικοινωνούν ασύρματα μεταξύ τους ή με άλλες, παρόμοιες συσκευές, οφείλεται σε αυτό το δομικό στοιχείο. Η επικοινωνία μπορεί να επιτευχθεί με Radio Frequency, Optical Communication αλλά και infrared. Η συνηθέστερη επιλογή είναι η χρήση Radio Frequency διότι οι δύο άλλες λύσεις έχουν σοβαρά μειονέκτηματα που δεν μπορούν να ξεπεραστούν σε τέτοιου είδους δίκτυα.

Πηγή Ενέργειας: Το απολύτως απαραίτητο στοιχείο σε όλες τις ηλεκτρονικές συσκευές είναι η πηγή ενέργειας. Το κάθε δομικό στοιχείο του κόμβου χρειάζεται ενέργεια η οποία παρέχεται από μπαταρίες και πυκνωτές. Σε κάποιες εφαρμογές είναι δυνατό να παρέχουμε ενέργεια στην συσκευή με διαφορετικές μεθόδους από τις συμβατικές όπως με εκμετάλλευση της ηλιακής ενέργειας, την διαφορά θερμοκρασίας και γενικά με οποιοδήποτε τρόπο μπορούμε να μετατρέψουμε ενέργεια από το περιβάλλον σε ηλεκτρική μορφή.

Αναλογικές /Ψηφιακές είσοδοι – Αισθητήρες: Η ικανότητα των κόμβων να μπορούν να συλλέγουν πληροφορίες από το περιβάλλον οφείλεται στο τελευταίο δομικό τους στοιχείο. Αρκετές συσκευές έχουν ενσωματωμένους συγκεκριμένους αισθητήρες. Άλλες συσκευές, πιο γενικού σκοπού, έχουν αναλογικές στις οποίες ο σχεδιαστής μπορεί να εφαρμόσει αναλογικούς αισθητήρες και με κατάλληλες τροποποιήσεις στο software να μπορεί να συλλέξει πληροφορίες από το περιβάλλον.

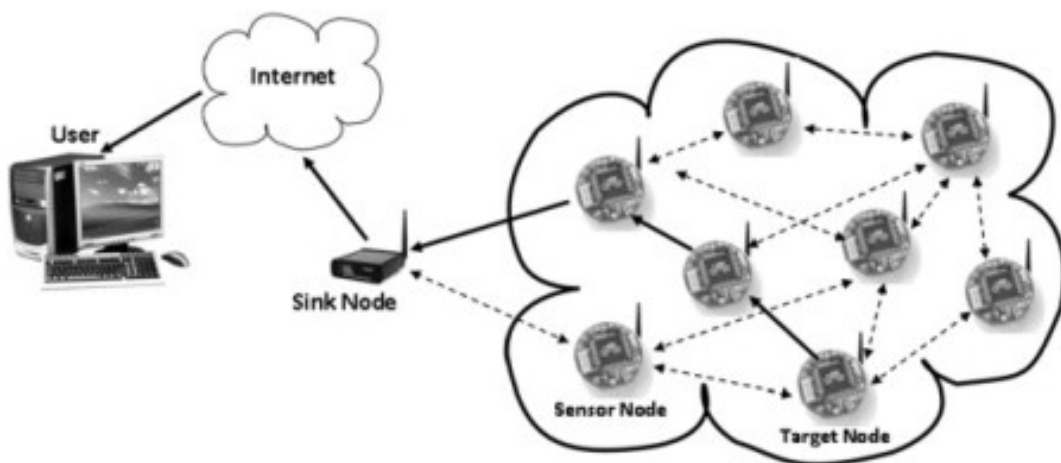


Εικόνα 2.7

2.5 Ασύρματα Δίκτυα Αισθητήρων

Πάρα πολλοί από τους ερευνητές πιστεύουν ότι οι αισθητήρες θα μπουν στην καθημερινότητα μας, δηλαδή θα είναι στα σπίτια μας στα αυτοκίνητα μας ακόμη και στο ανθρώπινο σώμα. [12] Επίσης, τα δίκτυα αισθητήρων αποκτούν ολοένα και μεγαλύτερη σημασία σε διάφορες εφαρμογές, όπως η απογραφή για διαχείριση καταστροφών, η παρακολούθηση της υγείας διαφόρων υποδομών, η στρατιωτική επιτήρηση και αναγνώριση, ακόμη και η παρακολούθηση ασθενών.[13]

Ένα ασύρματο δίκτυο αισθητήρων αποτελείται από αυτόνομους αισθητήρες καταναμημένος στο χώρο οι οποίοι μέσω συνεργασίας παρακολουθούν παραμέτρους όπως θερμοκρασία, ήχο κ.λ.π. Οι κόμβοι του δικτύου αποτελούνται από τρία στοιχεία. Αυτά τα στοιχεία είναι ένας πομποδέκτης, ένας μικροελεγκτής και μια μπαταρία ή οποία θεωρείται πηγή ενέργειας. Στη τελική κάποιο δίκτυο που περιέχει ένα αριθμό κόμβων αποτελεί ένα ασύρματο ad-hoc δίκτυο, με βάση αυτό το δίκτυο η μεταφορά της πληροφορίας, γίνεται από κόμβο σε κόμβο μέχρι να φτάσει στο τελικό προορισμό.



Εικόνα 2.8

Τα ασύρματα δίκτυα αισθητήρων έχουν κάποια χαρακτηριστικά τα οποία θα αναλυθούν πιο κάτω.

Χαμηλή κατανάλωση: Όπως αναφέρθηκε και πιο πάνω ένα από τα στοιχεία που αποτελούν τους κόμβους είναι η μπαταρία, έτσι ώστε να στέλνει ενέργεια. Οι μπαταρίες αυτές μετά από κάποιο χρονικό διάστημα εργασίας θα αδειάσει άρα μετά το άδειασμα της μπαταρίας αυτής το δίκτυο πλέον δε θα θεωρείται χρήσιμο. Μειώνετε το κόστος συντήρησης αν κάθε κόμβος έχει χαμηλή κατανάλωση.

Αυτόνομη και προγραμματιζόμενη λειτουργία: Κάθε κόμβος θα πρέπει να λειτουργεί αυτόνομα, να έχει πρωτοβουλία για το τι θα κάνει, πότε θα το κάνει και που θα στείλει. Επίσης θα έχει τη δυνατότητα να προγραμματίζεται δυναμικά.

Χαμηλό Κόστος: Για μεγάλων διαστάσεων δίκτυα τη δεδομένη στιγμή θα χρειαστούμε εκατομμύρια κόμβους, που θα έχουν κάλυψη από αισθητήρες με εμβέλεια γύρω στα 100 μέτρα. Για να μπορέσουμε να καλύψουμε το δίκτυο αυτό θα χρειαστούν πολλά εκατομμύρια χρήματα.

Γρήγορη δημιουργία δικτύου: Μέσα σε λίγα λεπτά κάποιο δίκτυο μπορεί να χαρτογραφηθεί και να ξεκινήσει σε σύντομο διάστημα τη λειτουργία τους. Εξαρτάται σίγουρα και από το μέγεθος του δικτύου.

Προσαρμοστικότητα: Με τα νέα δεδομένα που μπορεί να προκύψουν από απώλειες κόμβων ή άλλων προβλημάτων, το είδος αυτού του δικτύου μπορεί να ανταπεξέλθει και να προσαρμοστεί με τη δημιουργία νέων μονοπατιών έτσι ώστε να μην καταστραφεί ολόκληρο το δίκτυο.

Απλότητα: Οι πόροι του κάθε κόμβου απαίτησαν το σχεδιασμό απλών και αποδοτικών αλγορίθμων για να πραγματοποιηθούν οι λειτουργίες που προγραμματίστηκαν.

Απόδοση: Θυσιάζοντας τη ταχύτητα αποστολής δεδομένων, οι κόμβοι μειώνουν τις επαναλαμβανόμενες εκπομπές πακέτων λόγω σφαλμάτων, αυξάνοντας την αξιοπιστία στην μετάδοση του κάθε πακέτου.

Κεφάλαιο 3

Προηγούμενη Σχετικές Εργασίες - Υλοποιήσεις

3.1 6LoWPAN Δίκτυα	31
3.2 6LoWPAN Neighbor Discovery	33
3.3 Πρωτόκολλο Δρομολόγησης RPL	34
3.4 Προηγούμενες Σχετικές Εργασίες -Υλοποιήσεις	36

3.1 6LoWPAN Δίκτυα

Το 6LoWPAN ουσιαστικά είναι προέκταση του IPv6 και αναλύεται σε Low Power Personal Area Network. [14] Μεγάλη προσπάθεια έγινε έτσι ώστε το IP να ενσωματωθεί στα ασύρματα δίκτυα, αυτό πραγματοποιήθηκε με μια πολύ σημαντική προσπάθεια που έγινε από την IETF(Internet Engineering Task Force), με αποτέλεσμα την επιτυχή δημιουργία του 6LowPAN. [15] Η ομάδα IETF στόχο είχε τη χρήση του IPv6 πάνω στο πρωτόκολλο IEEE 802.15.4.

Μεταξύ του Network Layer και του Link Layer υπάρχει ένα στρώμα προσαρμογής, αυτό το στρώμα είναι το πρωτόκολλο 6LowPAN. Επίσης μέσω του στρώματος αυτού παρέχονται κάποιες υπηρεσίες οι οποίες δε προσφέρονται από το Link Layer αλλά τις χρειάζεται το Network Layer.

Οι υπηρεσίες που παρέχονται από το 6LowPAN μεταξύ των δυο στρωμάτων είναι η διαδικασία κατακερματισμού έτσι ώστε να ικανοποιεί το ελάχιστο maximum transmission unit του IPv6 αλλά επίσης και για να ικανοποιείται το layer two forwarding για τη μετάδοση του IPv6 πακέτου, τέλος για τη μείωση του overhead γίνεται συμπίεση της κεφαλίδας. Στην περίπτωση των ασύρματων δικτύων ο

κατακερματισμός δεν είναι επιθυμητός λόγω του ότι αν χαθεί κάποιο τμήμα, θα πρέπει να γίνει μετάδοση ολόκληρου του πακέτου.

Το 6LowPAN πρωτόκολλο διαθέτει τρεις μορφές κεφαλίδας, την κεφαλίδα αποστολής, την κεφαλίδα πλέγματος (mesh) και τέλος την κεφαλίδα κατακερματισμού. Οι 6LowPAN δρομολογητές και κόμβοι αλλά και οι edge δρομολογητές, αποτελούν ένα δίκτυο 6LowPAN. Για τις δρομολογήσεις μεταξύ δικτύων 6LowPAN και άλλων IP δικτύων ευθύνονται οι edge δρομολογητές. Για τις δρομολογήσεις εντός του δικτύου ευθύνη έχουν οι 6LowPAN δρομολογητές και τέλος ευθύνη των 6LowPAN κόμβων είναι η αποστολή και η παραλαβή πακέτων.

Μέσα σε ένα δίκτυο 6LowPAN IPv6 συμμετέχουν όλοι οι κόμβοι που έχουν το ίδιο IPv6 prefix που βρίσκονται υπό το σύνολο LowPAN δικτύων. Το δίκτυο αυτό έχει τη δυνατότητα να συνδέετε είτε με άλλα δίκτυα ή και με το διαδίκτυο. Σε ένα LowPAN δίκτυο υπάρχει μόνο ένας edge δρομολογητής αλλιώς εάν αποτελείται από περισσότερους είναι extended LowPAN δίκτυο. Για τη λειτουργία του extended LowPAN δικτύου και τη διαχείριση των πληροφοριών χρησιμοποιείται ένα καλώδιο Ethernet.

Application	Application	
Transport	UDP	ICMP
Network	IPv6 with LoWPAN	
Data Link	IEEE 802.15.4 MAC	
Physical	IEEE 802.15.4 PHY	

Εικόνα 3.1

3.2 6LoWPAN Neighbor Discovery

Για την ανάπτυξη του 6LoWPAN Neighbor Discovery [20], χρησιμοποιήθηκε ένα σύνολο από τροποποιήσεις που πάρθηκαν από το IPv6 Neighbor Discovery έτσι ώστε να μην αναπτυχθεί κάποιο καινούριο πρωτόκολλο. [16] Ο βασικός στόχος για τον οποίο έγιναν τροποποιήσεις είναι για να βελτιστοποιηθεί το Neighbor Discovery έτσι ώστε να περιοριστεί η ισχύς των συσκευών που μπορούν να χρησιμοποιηθούν από μη μεταβατικούς συνδέσμους. Για τη στήριξη της κινητικότητας, της ανοχής σφαλμάτων, του bootstrapping αλλά και πολλών άλλων προστέθηκαν κάποια νέα μηνύματα.

Για το σχεδιασμό του νέου αυτού πρωτοκόλλου λήφθηκαν υπόψιν κάποιες παράμετροι. Αρχικά λαμβάνεται υπόψιν η συνεχώς μεταβαλλόμενη ασύρματη σύνδεση, το ότι γίνεται ανάθεση διευθύνσεων για σύντομο χρονικό διάστημα. Επίσης λήφθηκε υπόψη το επίπεδο μοντέλο που έχει το 6LoWPAN δίκτυο, το ότι γίνεται χρήση δύο επιπέδων γραμμών αλλά και οι τεχνικές δρομολόγησης που χρησιμοποιούνται.

Επιπλέον η έλλειψη της μητρικής multicast, η κινητή φύση μερικών εκ των ασύρματων κόμβων έπαιξαν σημαντικό ρόλο για το σχεδιασμό του πρωτοκόλλου. Πέραν όμως των πιο πάνω, ακόμη σημαντικότερο ρόλο είχε η περιορισμένη ενέργεια και η υπολογιστική ικανότητα των κόμβων, κυρίως λόγω του μεγέθους των κόμβων. Τέλος εξίσου σημαντικό ρόλο έπαιξαν και οι μεγάλοι χρονικοί κύκλοι αδράνειας των κόμβων που έπρεπε να συνυπολογιστούν και να ληφθούν υπόψιν από το πρωτόκολλο.

Η χρήση της πολλαπλής εκπομπής αποφεύγεται, καθώς και η λειτουργία των hosts διατηρείται όσο το δυνατόν πιο απλή. Οι IPv6 διευθύνσεις έχουν άμεση χαρτογράφηση, έτσι ώστε να γίνει η σύνδεση στρώματος MAC διευθύνσεων και ταυτόχρονα κάποιο δευτερεύον δίκτυο επεκτείνεται σε ολόκληρο το 6LoWPAN.

Μόλις ο κόμβος ενεργοποιηθεί για πρώτη φορά, τότε αποκτά και μια MAC διεύθυνση. Με την ενεργοποίησή του κύριος σκοπός του είναι η δημιουργία μιας καινούργιας σύνδεσης με ένα 6LoWPAN δίκτυο. Αρχικά στέλνει ένα μήνυμα Router Solicitation και λαμβάνει απάντηση από τους τοπικούς δρομολογητές Router Advertisement. Τα μηνύματα που λάμβανε τα αναζητά έτσι ώστε να βρεθεί ένα έγκυρο prefix network.

Ανακαλύπτοντας αυτού του prefix network, δημιουργούνται αυτόματα παγκόσμιες διευθύνσεις. Προχωρώντας γίνεται κάποια προσπάθεια από τον κόμβο για εγγραφή του στο δρομολογητή.

Εάν ο edge δρομολογητής βρίσκεται σε μακρινή απόσταση όπου δε μπορεί να σταλεί το μήνυμα κατευθείαν από τον κόμβο τότε γίνεται προσπάθεια το μήνυμα να σταλεί μέσω τοπικού δρομολογητή. Στην ουσία ο τοπικός δρομολογητής θα μεσολαβήσει έτσι ώστε να επικοινωνήσουν έμμεσα ο κόμβος με τον edge δρομολογητή. Επίσης ο edge δρομολογητής κάνει επιβεβαίωση εάν η διεύθυνση του κόμβου είναι μοναδική και δε χρησιμοποιείται από κάποιο άλλο κόμβο του δικτύου. Εάν τερματιστεί επιτυχώς ο έλεγχος τότε ο δρομολογητής στέλνει μήνυμα στον κόμβο για να επιλέξει από τις διαθέσιμες διευθύνσεις, και έτσι να ξεκινήσει επιτυχώς η επικοινωνία μεταξύ τους.

3.3 Πρωτόκολλο Δρομολόγησης RPL

Το πρωτόκολλο Δρομολόγησης RPL (Routing Protocol for Low power and Lossy Networks), είναι μια κατηγορία δικτύου, αλλά σε αυτή την κατηγορία δικτύου περιορίζεται ο αριθμός δρομολογητών και συνδέσεων.[17]

Στη λειτουργία των δρομολογητών υπάρχει περιορισμός στη μνήμη, στην ενέργεια και στην υπολογιστική δύναμη. Ο χαρακτηρισμοί που μπορούν να δοθούν στις συνδέσεις αυτές υψηλά ποσοστά απώλειας, αστάθεια αλλά και χαμηλά ποσοστά δεδομένων.[18]

Οι μορφές ροών κυκλοφορίας που παρέχει το πρωτόκολλο RPL αναφέρονται πιο κάτω. Αρχικά εμφανίζεται η μορφή point – to – point, δηλαδή είναι η ροή κυκλοφορίας που γίνεται μεταξύ κόμβων εντός του δικτύου. Μια άλλη μορφή είναι η point – to – multipoint, η ροή γίνεται από ένα κεντρικό σημείο ελέγχου σε υποσύνολο κόμβων εντός του δικτύου. Μια τελευταία μορφή είναι η multipoint – to – point, και η ροή κυκλοφορίας γίνεται από τους κόμβους που βρίσκονται εντός του δικτύου σε κεντρικό σημείο ελέγχου.

Το πρωτόκολλο RPL διατίθεται για κάποιους κόμβους. Αυτοί οι κόμβοι που έχουν στη διάθεση τους το πρωτόκολλο έχουν την δυνατότητα να αναπτύξουν μια τοπολογία δικτύου ανεξάρτητα και αυτόνομα, αλλά επίσης έχουν τη δυνατότητα να εγκαταστήσουν και να υπολογίσουν διαδρομές.

Βασικός στόχος αυτού του πρωτοκόλλου είναι η κατασκευή των γραφημάτων DODAG, δηλαδή των προσανατολισμένων κατευθυνόμενων μη κυκλικών γραφημάτων. Τα γραφήματα αυτά θα έχουν σαν ρίζα ένα sink κόμβο. Η κατασκευή του γραφήματος γίνεται αναλόγως της ροής κυκλοφορίας που θα ζητηθεί. Αν η ροή κυκλοφορίας είναι multipoint – to – point τότε πραγματοποιείται κίνηση από κάτω προς τα πάνω. Αλλά αν η ροή κυκλοφορίας είναι point – to – multipoint τότε πραγματοποιείται κίνηση από πάνω προς τα κάτω. Επιπρόσθετα, υποστηρίζεται και η point-to-point ροή κυκλοφορίας μέσω της διαδικασίας από τον sink κόμβο προς τα κάτω.

Οι μετρητές δρομολόγησης χρησιμοποιούνται από το πρωτόκολλο RPL έτσι ώστε να υπολογιστεί το συντομότερο μονοπάτι. Οι κύριες μετρήσεις που χρησιμοποιούνται για τον υπολογισμό αυτού του μονοπατιού είναι η σύνδεση έναντι των μετρήσεων του κόμβου, η μέτρηση της ποιότητας έναντι της ποσότητας, και η μέτρηση δυναμικού έναντι του στατικού.

Χρησιμοποιώντας τις κύριες μετρήσεις δημιουργείται το γράφημα, με πλεονέκτημα την επιλογή της πιο σύντομης διαδρομής. Υπολογίζεται και εγκαθίσταται μια νέα διαδρομή εάν οποιοσδήποτε κόμβος δεν θα είναι προσβάσιμος στο δίκτυο, ή οποιαδήποτε σύνδεση μεταξύ δυο κόμβων δεν είναι πλέον εφικτή.

3.4. Προηγούμενες Σχετικές Εργασίες -Υλοποιήσεις

Για την κατανόηση του θέματος αλλά και για να έχω τη δυνατότητα να προχωρήσω με τη Διπλωματική μου εργασία, θεωρήθηκε χρήσιμο και απόλυτα αναγκαίο όπως μελετήσω προηγούμενες ερευνητικές εργασίες. Κυρίως μελέτησα την Διπλωματική εργασία του φοιτητή Νικόλα Τσεκούρα με θέμα Διαχείριση Κινητικότητας σε 6LoWPAN Δίκτυα Αισθητήρων. [19] Επίσης είχα την ευκαιρία να μελετήσω την Διπλωματική εργασία του φοιτητή Μαρίνου Στυλιανού «Υλοποίηση Και Αξιολόγηση του Αλγορίθμου Htar για Έλεγχο Συμφόρησης σε Ασύρματα Δίκτυα Αισθητήρων», έτσι ώστε να κατανοήσω ακόμη καλύτερα το αντικείμενο των ασύρματων δικτύων αισθητήρων. [20]

Επίσης μέσα από τις διπλωματικές καταγράφηκαν οι ανάγκες που χρειάζονται έτσι ώστε να λειτουργούν σωστά τα πρωτόκολλα μέσα από τον Network Layer.

Μέσα από την διπλωματική εργασία Διαχείριση Κινητικότητας σε 6LoWPAN Δίκτυα Αισθητήρων, μελετήθηκε η συμπεριφορά των αισθητήρων μέσα στα 6LoWPAN δίκτυα, τα προβλήματα που παρουσιάστηκαν. Επίσης δόθηκε ιδιαίτερη έμφαση στην συμπεριφορά των αισθητήρων όταν αυτοί ήταν εν κινήσει. Για το λόγο αυτό μελετήθηκαν ιδιαίτερα τα σενάρια όπου κινητοί κόμβοι εισέρχονται και εξέρχονται από τοπικά δίκτυα αισθητήρων.

Από την ερευνητική ομάδα του Contiki έγιναν διάφορες υλοποιήσεις (και αξιολόγηση τους στη συνέχεια) του πρωτοκόλλου 6LoWPAN με παραλλαγές έτσι ώστε να καταλήξουν στο βέλτιστο. Ιδιαίτερο βάρος δόθηκε στο πρωτόκολλο ανίχνευσης κόμβων αφού προκαλεί αυξημένη χρήση ενέργειας. [21,22] Σκοπός των παραλλαγών που υλοποιήθηκαν ήταν να εντοπιστεί σε ποια περίπτωση ο αισθητήρας χρησιμοποιεί λιγότερη ενέργεια.

Ακόμη ένα πρόβλημα που προσπάθησαν να λύσουν μέσα από την υλοποίηση μερικών αλλαγών στο 6LoWPAN ήταν και η μη συμπερίληψη μερικών βελτιώσεων που έγιναν στο 6LoWPAN και δεν υποστήριζε το Contiki.

Σε μια άλλη εργασία, έγινε υλοποίηση του 6LoWPAN για σύστημα TinyOS. Σκοπός ήταν η σύνδεση των ασύρματων δικτύων αισθητήρων με το διαδίκτυο. Τροποποιήθηκαν ανάλογα οι κεφαλίδες που μπορούσαν να τροποποιηθούν. Το σημαντικότερο θετικό σημείο της υλοποίησης είναι ότι υλοποιήθηκε ο κατακερματισμός πακέτων και η επιτυχής συγκόλλησης τους από τον παραλήπτη. Πέραν από τα θετικά που προέκυψαν παρατηρήθηκε και μια σημαντική αρνητική παράμετρος. Δεν ήταν δυνατή η υλοποίηση του Neighbor Discovery πρωτοκόλλου, το οποίο υποκαταστάθηκε με τις διευθύνσεις εκπομπής από το Link Layer.

Κεφάλαιο 4

Υλοποίηση

4.1 Λειτουργικό Σύστημα Contiki

4.2 COOJA

4.3 Προσαρμογή Πρωτοκόλλων

4.4 Προσαρμογή IPv6 Neighbor Discovery & RPL πρωτοκόλλου

4.5 Προβλήματα

4.1 Λειτουργικό Σύστημα Contiki

Το λειτουργικό σύστημα Contiki είναι ανοικτού κώδικα λειτουργικό σύστημα. Κύριος σκοπός του συστήματος είναι η προσαρμογή πρωτοκόλλων και η προσομοίωση δικτύων ασύρματων αισθητήρων αλλά και ενσωματωμένων συστημάτων. Μερικά παραδείγματα όπου το Contiki χρησιμοποιείται είναι τα συστήματα συναγερμού, το σύστημα φωτισμού δρόμων, συστήματα εντοπισμού υγρασίας, συστήματα ανίχνευσης ακτινοβολίας κλπ. [21,22]

Το λειτουργικό σύστημα δημιουργήθηκε από τον Adam Dunkels το 2002 και πήρε το όνομα του από τη διάσημη σχεδία του Thor Heyerdahl. Μετά την δημιουργία του λειτουργικού συστήματος ομάδα από προγραμματιστές, μερικοί εκ των οποίων είναι μέλη της Cisco του SAP, είτε από διάφορες εταιρείες και πανεπιστήμια ανέλαβαν να αναπτύξουν το σύστημα.

Ένα άλλο σημαντικό στοιχείο για το λειτουργικό σύστημα Contiki είναι ότι παρά το ότι είναι κατασκευασμένο σε TCP / IP στοίβα δεν χρειάζεται μεγάλες μονάδες μνήμης για να τρέξει.. Έτσι έγινε εύκολο εργαλείο χρήσης σε πολλά κέντρα έρευνας. Ακόμη ένα αξιοσημείωτο γεγονός είναι η εισχώρηση στην εμπορική και παραγωγική βιομηχανία εφαρμογές που αναπτύχθηκαν στο λειτουργικό σύστημα του Contiki.

Μέσα από το λειτουργικό σύστημα Contiki παρέχονται τρία περιβάλλοντα προσομοίωσης. Στην παρούσα διπλωματική καταπιαστήκαμε μόνο με την προσομοιωτή περιβάλλοντος COOJA. [23] Σύμφωνα με την διαδικασία ανάπτυξης οποιασδήποτε εφαρμογής που αναπτύσσεται εντός του λειτουργικού συστήματος Contiki, θα πρέπει να περάσει και από τους τρεις προσομοιωτές που παρέχει ο Contiki με επιτυχία. Εάν και εφόσον η εφαρμογή περάσει με επιτυχία τις 3 προσομοιώσεις τότε και μόνο προχωρά η υλοποίηση της σε hardware.

4.2 COOJA

Ο Cooja είναι ένας προσομοιωτής δικτύου που χρησιμοποιείται για τη λειτουργία ασύρματων δικτύων. Το λειτουργικό σύστημα Contiki χρησιμοποιεί τον Cooja για να τρέξει τις λειτουργίες του χωρίς να υπάρχουν οι πόροι(hardware). Έτσι με τον Cooja υπάρχει η δυνατότητα να αναπτυχθούν εικονικά δίκτυα, αξιόπιστα για μετρήσεις και αξιολογήσεις.

Μια προσομοίωση στο COOJA παρουσιάζει τρία κύρια χαρακτηριστικά, τα δεδομένα μνήμης του, τον τύπο των κόμβων/ου, και τέλος τις περιφερειακές συσκευές. Ο τύπος του κόμβου μπορεί να είναι ο ίδιος για πολλούς κόμβους και καθορίζει τις κοινές ιδιότητες τους. Θα εκτελέσουν ακριβώς τον ίδιο κώδικα κατά την εκτέλεση της προσομοίωσης και θα έχουν τα ίδια κοινά χαρακτηριστικά. Ωστόσο δεδομένα μερικών κόμβων θα είναι διαφορετικά λόγω διαφορετικών εισόδων που θα δεχτούν.

Ο COOJA είναι σε θέση να εκτελέσει προγράμματα Contiki με δύο διαφορετικούς τρόπους . Είτε με την εκτέλεση του κώδικα του προγράμματος απευθείας στο CPU υποδοχής, ή εκτελώντας μεταγλωττισμένο κώδικα του προγράμματος σε TI MSP430 εξομοιωτή .

4.3 Μελέτη - Προσαρμογή Πρωτοκόλλων

Η μορφή των πρωτοκόλλων δεν μπορούσε να υποστηρίξει τον τρόπο λειτουργίας των κόμβων στο δίκτυο αλλά τη σωστή λειτουργία του δικτύου. Έτσι σύμφωνα και με προηγούμενη διπλωματική εργασία έπρεπε να γίνουν αρκετές αλλαγές τόσο στα αρχεία ρυθμίσεων όσο και στις υλοποιήσεις των πρωτοκόλλων(όπου υπήρχε η δυνατότητα)έτσι ώστε να έχουμε τα επιθυμητά αποτελέσματα.

Στην παρούσα διπλωματική εργασία έγινε προσπάθεια για βελτίωση των αλλαγών αυτών για καλύτερη απόδοση σε συγκεκριμένα σενάρια που προσομοιώθηκαν.

4.4 Προσαρμογή IPv6 Neighbor Discovery & RPL πρωτοκόλλου

Σε προηγούμενα στάδια έγιναν αρκετές αλλαγές στον τρόπο λειτουργίας τόσο του πρωτοκόλλου IPv6 Neighbor Discovery όσο και το RPL πρωτοκόλλου. Όσο αφορά το πρώτο προστέθηκε flag για αποφυγή συνύπαρξης περισσοτέρων από ένα δρομολογητή αλλά και το ότι θα υπάρχει δρομολογητής. Μεταξύ άλλων επιβεβαιώνεται η σωστή ενεργοποίηση του N.Solicitation και N.Advertisement και η δημιουργία παγκόσμιας διεύθυνσης πάντα βασισμένος στο prefix του δικτύου.

Σύμφωνα και με την τελευταία έκδοση του εγγράφου λόγω του ότι δεν συμπεριλάμβαναν πρωτόκολλο δρομολόγησης έπρεπε με κάποιο τρόπο να “κατευθυνθούν” βάσει κάποιον κανόνων έτσι ώστε να φτάνουν στον προορισμό τους έστω και αν ο παραλήπτης δεν ήταν γνώριμος γείτονας. Έτσι έγινε προσπάθεια για αλλαγή στο αρχείο λειτουργιών του εξυπηρετητή. Σε γενικές γραμμές αφού αυτό-δημιουργήσει τη μοναδική του διεύθυνση, αποθηκεύει τα “συντομότερα” μονοπάτια μέσω ενός γράφου εάν δεν βρίσκεται μέσα σε κάποιο δίκτυο. Στην περίπτωση τώρα που βρίσκεται ήδη σε κάποιο δίκτυο δεν επηρεάζεται.

4.5 Προβλήματα

Τα προβλήματα που παρουσιάστηκαν δεν ήταν τόσο στην υλοποίηση των τροποποιήσεων όσο στην προσπάθεια για κατανόηση των προηγούμενων αλλαγών. Έπρεπε αρχικά να εντοπίσω τις αλλαγές που έγιναν ήδη, να επισημάνω τις βελτιστοποιήσεις και να προσπαθήσω να προσθέσω και άλλες. Αν και αφιέρωσα πολλές ώρες στο κομμάτι αυτό δεν σημείωσα ιδιαίτερη βελτίωση σε κάποιο συγκεκριμένο κομμάτι. Όσο αφορά τον κώδικα στον οποίο καταπιάστηκα κατάφερα να διορθώσω όλα τα warning messages τα οποία εμφάνιζε ο κώδικας και σε μια περίπτωση αλλοίωνε το τελικό αποτέλεσμα.

Κεφάλαιο 5

Σενάρια και αποτελέσματα

5.1 Γενική Λειτουργία

5.2 Σενάριο Α

5.3 Σενάριο Β

5.4 Σενάριο Γ

5.1 Γενική Λειτουργία

Σκοπός μέσα από τα σενάρια που τρέξαμε ήταν κατά κύριο λόγο να μελετήσουμε το κατά πόσο το πρωτόκολλο Neighbor Discovery λειτουργεί ορθά στα κινητά δίκτυα αισθητήρων. Το πώς επικοινωνούν οι κόμβοι με τον router του δικτύου αλλά και εάν αντιλαμβάνονται πως μπορούν να στείλουν τα πακέτα τους μέσα από ενδιάμεσο γειτονικό τους κόμβο.

Πιο κάτω θα αναφερθούν αναλυτικά τα σενάρια τα οποία τρέξαμε με τα αποτελέσματα τους. Επίσης θα γίνει αναλυτική περιγραφή της προσομοίωσης, τα μηνύματα που ανταλλάχθηκαν μεταξύ κινητού κόμβου, σταθερών κόμβων και του εξυπηρετητή.

Στο πρώτο σενάριο θα μελετήσουμε την απλούστερη περίπτωση λειτουργία του Neighbor Discovery, όπου ένας σταθερός κόμβος προσπαθεί να επικοινωνήσει με τον εξυπηρετητή που βρίσκεται εντός της εμβέλειας του.

Στο δεύτερο σενάριο θα μελετήσουμε το πώς επηρεάζει την λειτουργία ενός κινητού κόμβου η έξοδος του από την εμβέλεια του εξυπηρετητή και στη συνέχεια επανέρχεται εντός της εμβέλειας του εξυπηρετητή.

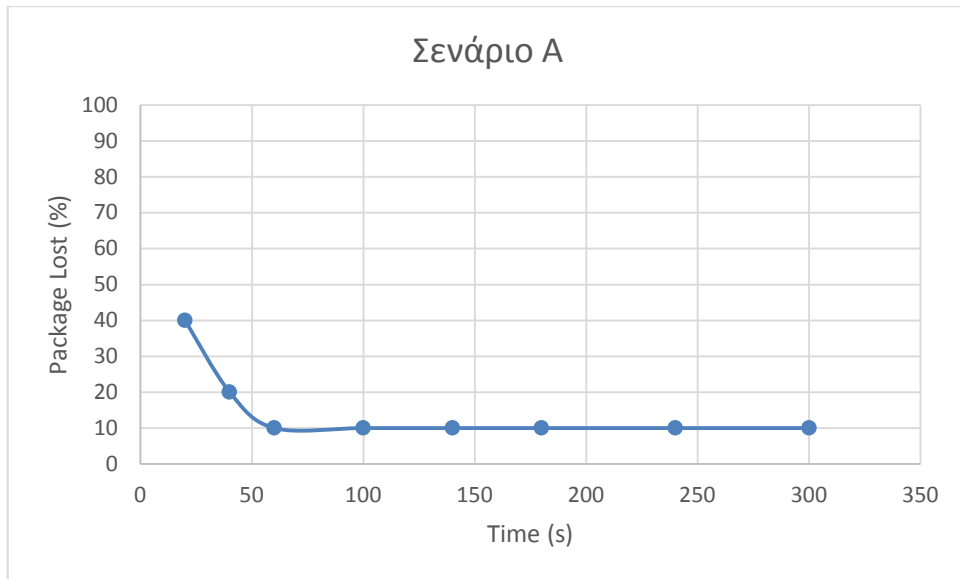
Τέλος στο τρίτο σενάριο θα μελετήσουμε την περίπτωση όπου ο κινητός κόμβος ξεκινά την πορεία του εκτός εμβέλειας του εξυπηρετητή και στην συνέχεια εισέρχεται εντός τη εμβέλειας του εξυπηρετητή.

5.2 Σενάριο Α

Όπως αναφέραμε και πιο πάνω στη προσομοίωση του σεναρίου αυτού χρησιμοποιήσαμε ένα εξυπηρετητή και ένα σταθερό κόμβος. Στην περίπτωση μας ο εξυπηρετητής βρίσκεται εντός της εμβέλειας το κόμβου. Ο εξυπηρετητής αφού δημιουργήσει την δική του, μοναδική, διεύθυνση, ξεκινά να διαφημίζει, ανά τακτά διαστήματα την ύπαρξη του στέλνοντας «διαφημιστικά πακέτα»(Router Advertisement Packages).

Εφόσον ο σταθερός κόμβος βρίσκεται εντός εμβέλειας του εξυπηρετητή θα λάβει κάποιο από τα πακέτα αυτά. Αφού παραλάβει το πακέτο προσπαθεί με τη σειρά του να δημιουργήσει τη δική του μοναδική διεύθυνση. Για να το επιτύχει αυτό στέλνει αρχικά Neighbor Solicitation μήνυμα στον εξυπηρετητή με μια υπονήφια διεύθυνση. Εάν ο εξυπηρετητής του απαντήσει με Neighbor Advertisement Message τότε επαναλαμβάνει την διαδικασία με καινούρια παγκόσμια διεύθυνση μέχρι να μην πάρει απάντηση ένα Advertisement Message. Εάν συμβεί αυτό τότε ο κόμβος υιοθετεί την διεύθυνση αυτή και ορίζεται η δική του μοναδική παγκόσμια διεύθυνση. Επίσης αποθηκεύει τον εξυπηρετητή σας γειτονικό του κόμβο. Από την στιγμή που συμβούν αυτά η επικοινωνία μεταξύ τους είναι πλέον εφικτή.

Όπως φάνηκε και από τις μετρήσεις που πάρθηκαν επειδή τόσο ο εξυπηρετητής όσο και ο κόμβος είναι σταθεροί, υπάρχει ένας αριθμός χαμένων πακέτων στην αρχή μέχρι να εγκαταστήσουν την σύνδεσή τους. Από το σημείο όμως που θα εγκατασταθεί η σύνδεση τους το ποσοστό χαμένων πακέτων περιορίζεται σε μηδαμινά ποσοστά.



Σχήμα 5.1

5.3 Σενάριο B

Στο δεύτερο σενάριο έχουμε σε ένα τοπικό δίκτυο ένα εξυπηρετητή και εντός της εμβέλειας του αριθμό σταθερών κόμβων και ένα κινητό. Ο κινητός κόμβος βρίσκεται εξ αρχής εντός της εμβέλειας του εξυπηρετητή, ενώ στη συνέχεια απομακρύνεται μέχρι να βγει εκτός εμβέλειας. Αφού εξέλθει της εμβέλειας, θα μελετήσουμε τι βήματα κάνει, τι επιπτώσεις θα έχει και πως θα επανέλθει η σύνδεση του.

Αρχικά όλοι οι κόμβοι(σταθεροί και ο κινητός) δημιουργούν την δική τους παγκόσμια διεύθυνση μέσω του τοπικού δρομολογητή. Οι κόμβοι λόγω ότι αναγνωρίζουν τον εξυπηρετητή ως “γείτονα” αποθηκεύουν μόνο την τοπική διεύθυνση του εξυπηρετητή αφού δεν είναι αναγκαίο να αναγνωρίζουν την μοναδική παγκόσμια διεύθυνση του. Ακριβώς το ίδιο συμβαίνει και με τους κόμβους μεταξύ τους αφού βρίσκονται μέσα στο ίδιο τοπικό δίκτυο.

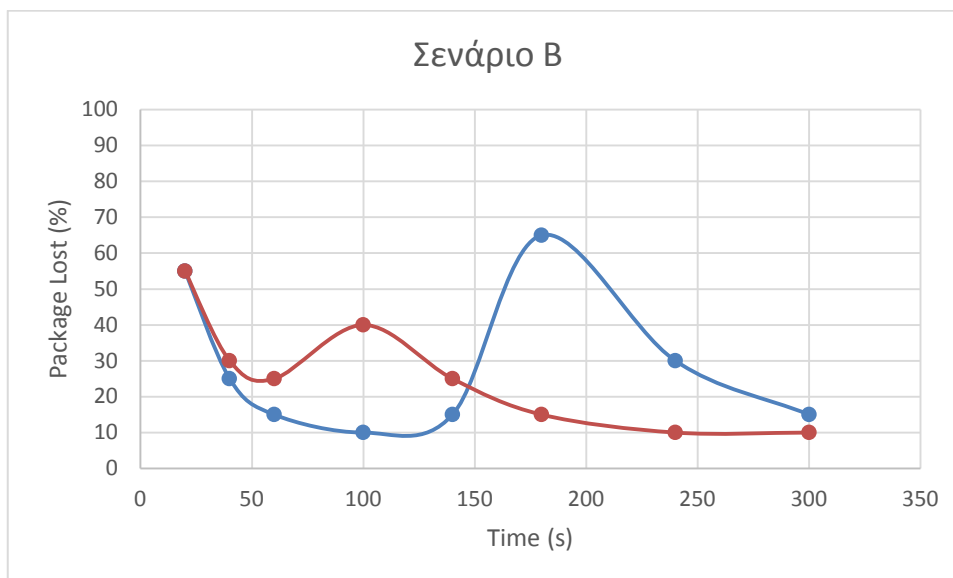
Όταν ο κινητός κόμβος βγει εκτός εμβέλειας του εξυπηρετητή τότε για ορισμένο χρονικό διάστημα αδυνατεί να επικοινωνήσει με τον εξυπηρετητή. Ο λόγος που συμβαίνει αυτό είναι γιατί ο κινητός κόμβος γνώριζε μόνο την τοπική διεύθυνση του εξυπηρετητή. Έτσι εξερχόμενος του δικτύου συνέχισε να στέλνει τα πακέτα του στην

τοπική διεύθυνση που γνώριζε με αποτέλεσμα να αποτύχουν όλα να φτάσουν στον προορισμό τους.

Στην συνέχεια ο κινητός κόμβος ορίστηκε να εισέλθει ξανά στο αρχικό δίκτυο. Έτσι τώρα ξανακάνοντας την διαδικασία αναγνώρισης θα αποθηκεύσει την μοναδική παγκόσμια διεύθυνση του εξυπηρετητή. Με αυτό τον τρόπο διασφαλίζει ότι εάν ξαναβγεί εκτός δικτύου θα μπορεί να στέλνει πακέτα στον εξυπηρετητή μέσω γειτονικών του κόμβων.

Η πιο πάνω προσομοίωση έτρεξε αρκετές φορές και με διαφορετικές παραμέτρους έτσι ώστε να έχουμε μια πιο σφαιρική εικόνα. Οι παράμετροι που λήφθηκαν υπόψη στην προσομοίωση ήταν η ταχύτητα του κινητού κόμβου αλλά και η συχνότητα αποστολής του κινητού κόμβου. Έγινε προσπάθεια επίσης για να δούμε πως οι σταθεροί κόμβοι βοηθούσαν τα πακέτα που αντάλλασσαν εξυπηρετητής και κινητός κόμβος να φθάσουν στον τελικό τους προορισμό. Οι ενδείξεις δεν ήταν οι αναμενόμενες μάλλον λάθος υπολογισμών που έγιναν κατά την υλοποίηση. Οι ενδείξεις μερικές φορές έδειξαν ότι το μήνυμα μεταφερόταν μέσω σταθερών κόμβων ενώ άλλες πως είχαμε απώλεια πακέτων μόλις έχανε την άμεση σύνδεση με τον εξυπηρετητή.

Ενδεικτικά παραθέτουμε στην πιο κάτω γραφική παράσταση τις μετρήσεις για 2 από τις προσομοιώσεις του σεναρίου που έτρεξαν.



Σχήμα 5.2

Εύκολα μπορεί κάποιος να εντοπίσει ότι σε κάποιο χρονικό σημείο(ανάλογα με την ταχύτητα του κόμβου) το ποσοστό χαμένων πακέτων αυξάνεται κατακόρυφα. Ο λόγος είναι φανερός αφού το συγκεκριμένο χρονικό σημείο είναι η στιγμή που ο κόμβος εξέρχεται από το δίκτυο και συνεχίζει να στέλνει τα πακέτα του στην τοπική διεύθυνση του εξυπηρετητή. Για το χρονικό διάστημα το οποίο ο κινητός κόμβος βρίσκεται εκτός δικτύου το ποσοστό χαμένων πακέτων ανέρχεται σε ψηλά ποσοστά. Το ποσοστό μειώνεται ξανά εφόσον ο κινητός κόμβος εισέρχεται εντός της εμβέλειας είτε του εξυπηρετητή, είτε εντός της εμβέλειας κάποιου από των κόμβων του δικτύου.

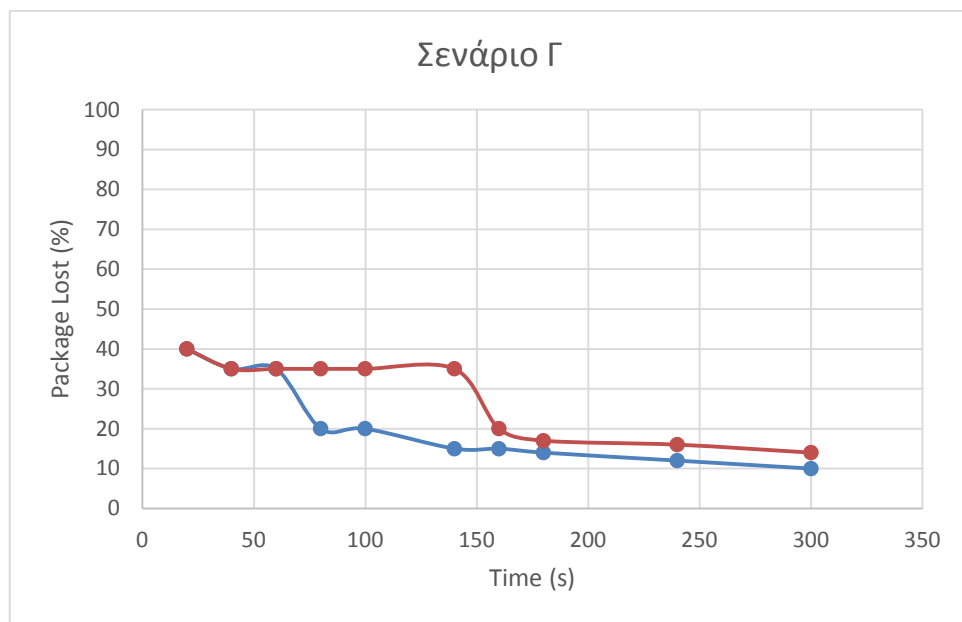
5.4 Σενάριο Γ

Στο τρίτο μας σενάριο αντιστρέψαμε τη σειρά των γεγονότων και ορίσαμε τον κινητό κόμβο εκτός τοπικού δικτύου και στη συνέχεια να εισέρχεται στο δίκτυο. Αρχικά όλοι οι κόμβοι που βρίσκονται εντός του δικτύου δημιουργούν την δική τους παγκόσμια διεύθυνση μέσω του τοπικού δρομολογητή. Οι κόμβοι λόγω ότι αναγνωρίζουν τον εξυπηρετητή ως “γείτονα” αποθηκεύουν μόνο την τοπική διεύθυνση του εξυπηρετητή αφού δεν είναι αναγκαίο να αναγνωρίζουν την μοναδική παγκόσμια διεύθυνση του. Ακριβώς το ίδιο συμβαίνει και με τους κόμβους μεταξύ τους αφού βρίσκονται μέσα στο ίδιο τοπικό δίκτυο. Ο κινητός κόμβος επειδή βρίσκεται εκτός εμβέλειας του δικτύου δημιουργεί την δική του τοπική διεύθυνση.

Στην συνέχεια και αφού ο κινητός κόμβος εισέλθει στην εμβέλεια, είτε του εξυπηρετητή είτε κάποιου άλλου κόμβου του τοπικού δικτύου, δέχεται Neighbor Advertisement μήνυμα. Έτσι ο κινητός κόμβος δημιουργεί τη δική του παγκόσμια μοναδική διεύθυνση αφού πλέον μέσω του εξυπηρετητή έχει τη δυνατότητα αυτή. Έτσι πλέον ο κινητός κόμβος γνωρίζει την παγκόσμια διεύθυνση του εξυπηρετητή και μπορεί να επικοινωνήσει μαζί είτε κατευθείαν είτε μέσω άλλων γειτονικών τους κόμβων.

Όπως και στο δεύτερο μας σενάριο, έτσι και εδώ σημαντικές απώλειες πακέτων έχουμε όταν ο κινητός κόμβος βρίσκεται εκτός εμβέλειας του δικτύου. Μέχρι να μπει στο δίκτυο τα ποσοστά παραμένουν ψηλά. Αλλά αφότου εισέλθει στο δίκτυο μειώνονται

συνεχώς λόγω του ότι πλέον γνωρίζει την παγκόσμια διεύθυνση του εξυπηρετητή. Οπότε αν οποτεδήποτε θέλει να στείλει πακέτο μπορεί να το κάνει.



Σχήμα 5.3

Κεφάλαιο 6

Αξιολόγηση και Μελλοντική Εργασία

6.1 Γενικά Συμπεράσματα - Επισημάνσεις

6.2 Μελλοντική Εργασία

6.1 Γενικά Συμπεράσματα - Επισημάνσεις

Μέσα από την ολοκλήρωση της διπλωματικής εργασίας, μπορούμε να εξάγουμε κάποια συμπεράσματα και κάποιες επισημάνσεις σχετικά με τα ασύρματα δίκτυα αισθητήρων. Κυρίως όμως μπορούμε να επικεντρωθούμε στο πως ανταποκρίνεται το Neighbor Discovery Protocol στα δίκτυα αυτά.

Καταρχάς επιβεβαιώθηκε ότι αν ο κόμβος είναι σταθερός και εντός της εμβέλειας του εξυπηρετητή το πρωτόκολλο λειτουργεί χωρίς οποιαδήποτε προβλήματα. Τα ποσοστά χαμένων πακέτων βρίσκονται εντός ικανοποιητικών πλαισίων.

Εντοπίζεται και πάλι σοβαρό πρόβλημα όταν κάποιος κόμβος ενεργοποιηθεί εντός κάποιου δικτύου και στην πορεία βγει εκτός εμβέλειας του δικτύου. Χάνεται αμέσως η σύνδεση με τον εξυπηρετητή με αποτέλεσμα τις πλείστες των περιπτώσεων η απώλεια πακέτων να αυξάνονταν κατακόρυφα αμέσως. Σε ελάχιστες περιπτώσεις η προσομοίωση έδειξε ότι τα πακέτα συνέχιζαν να στέλνονται κανονικά- ίσως αυτό να αποτελεί την εξαίρεση και όχι τον κανόνα.

Σε αντίθεση με το σενάριο Β στο σενάριο Γ το Neighbor Discovery πρωτόκολλο ανταποκρίνεται πλήρως, αφού με το που θα εισέλθει ο κινητός κόμβος εντός της εμβέλειας του εξυπηρετητή ή εντός της εμβέλειας άλλου κόμβου του δικτύου τότε

υπάρχει η δυνατότητα δημιουργίας παγκόσμιας διεύθυνσης. Έτσι η επικοινωνία από τον κινητό κόμβο μπορεί να ξεκινήσει σχεδόν αμέσως.

6.2 Μελλοντική Εργασία

Μια μελλοντική εργασία η οποία θα μπορούσε να υλοποιηθεί θα ήταν η δοκιμή των πιο πάνω σεναρίων με πραγματικούς αισθητήρες. Εάν και εφόσον αυτό είναι δυνατόν ίσως να επιβεβαιωθούν οι μετρήσεις που έγιναν μέσω του προσομοιωτή.

Επίσης ένα άλλο σενάριο που θα μπορούσε να μελετηθεί είναι αυτό όπου κάποιος κινητός κόμβος ενεργοποιείται αρχικά εντός ενός τοπικού δικτύου, μεταφέρεται σε κάποιο δεύτερο τοπικό δίκτυο και στην συνέχεια επανέρχεται στο αρχικό δίκτυο. Να μελετηθεί κατά πόσο θα υπάρχει άμεση σύνδεση στα δίκτυα και πόσα από τα πακέτα ου θα στείλει θα φτάσουν στον προορισμό τους

Μέσα από την εξαγωγή ρεαλιστικών αποτελεσμάτων θα είναι εφικτή η χρησιμοποίηση των ασύρματων δικτύων αισθητήρων στη αγορά μέσω έξυπνων εφαρμογών.

Βιβλιογραφία

- [1] http://en.wikipedia.org/wiki/Internet_Protocol_Suite
- [2] <http://docs.oracle.com/cd/E19455-01/806-0916/6ja85398k/index.html>
- [3] <http://www.webopedia.com/TERM/I/IP.html>
- [4] http://en.wikipedia.org/wiki/Internet_Protocol
- [5] <http://en.wikipedia.org/wiki/IPv4>
- [6] <http://en.wikipedia.org/wiki/IPv6>
- [7] <http://en.wikipedia.org/wiki/ICMPv6>
- [8] <http://packetlife.net/blog/2008/aug/28/ipv6-neighbor-discovery/>
- [9] http://el.wikipedia.org/wiki/IEEE_802.11
- [10] <http://el.wingwit.com/Networking/wireless-networking/83304.html#.U3U78fmSxUU>
- [11] http://en.wikipedia.org/wiki/IEEE_802.15.4
- [12] http://en.wikipedia.org/wiki/Wireless_sensor_network
- [13] <http://210.32.200.159/download/20100130212654891.pdf>
- [14] <http://en.wikipedia.org/wiki/6LoWPAN>
- [15] <http://6lowpan.net/>

- [16] http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/111221-Luis_Maqueda-with-cover.pdf
- [17] <http://cnds.eecs.jacobs-university.de/courses/nds-2010/kuryla-rpl.pdf>
- [18] http://www.net.in.tum.de/fileadmin/TUM/NET/NET-2011-07-1/NET-2011-07-1_09.pdf
- [19] https://ktree.cs.ucy.ac.cy:443/action.php?kt_path_info=ktcore.actions.document.view&fDocumentId=11374
- [20] https://ktree.cs.ucy.ac.cy:443/action.php?kt_path_info=ktcore.actions.document.view&fDocumentId=6808
- [21] <http://www.contiki-os.org/start.html>
- [22] <http://en.wikipedia.org/wiki/Contiki>
- [23] <https://github.com/contiki-os/contiki/wiki/An-Introduction-to-Cooja>
- [24] <http://www.sixsape.com/joomla/sixsape/index.php/technical-backgrounders/tcp-ip/ip-the-internet-protocol/ipv6-internet-protocol-version-6/icmpv6-internet-control-message-protocol-for-ipv6>