# Ενσωμάτωση Μηχανισμών Διαχείρισης Εμπιστοσύνης, Πρόβλεψης Απώλειας Ζεύξης και Αντιμετώπισης Εγωισμού στο πρωτόκολλο Dynamic Source Routing Κινητών Αδόμητων Δικτύων

Ευάγγελος Αγγελάκης

ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Πανεπιστήμιο Κρήτης
Σχολή Θετικών & Τεχνολογικών Επιστημών
Τμήμα Επιστήμης Υπολογιστών

Ηράκλειο Μάρτιος 2004

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ & ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

# Ενσωμάτωση Μηχανισμών Διαχείρισης Εμπιστοσύνης, Πρόβλεψης Απώλειας Ζεύξης και Αντιμετώπισης Εγωισμού στο πρωτόκολλο Dynamic Source Routing Κινητών Αδόμητων Δικτύων

Εργασία που υποβλήθηκε από τον
Ευάγγελο Αγγελάκη
ως μερική εκπλήρωση των απαιτήσεων για την απόκτηση
Μεταπτυχιακού Διπλώματος Ειδίκευσης
στην Επιστήμη Υπολογιστών

ΣΥΓΓΡΑΦΕΑΣ: _____

Ευάγγελος Αγγελάκης

ΕΙΣΗΓΗΤΙΚΗ
ΕΠΙΤΡΟΠΗ:

Επόπτης: _____

Απόστολος Τραγανίτης, Καθηγητής

Μέλος: _____

Βασίλειος Σύρης, Επίκουρος Καθηγητής

Μέλος: _____

Παναγιώτης Τσακαλίδης, Αναπληρωτής Καθηγητής

ΔΕΚΤΗ: _____

Δημήτρης Πλεξουσάκης, Αναπληρωτής Καθηγητής
Πρόεδρος Επιτροπής Μεταπτυχιακών Σπουδών

Ηράκλειο, Μάρτιος 2004

*στο Γιώργο & τη Ναυσικά*

# Ενσωμάτωση Μηχανισμών Διαχείρισης Εμπιστοσύνης, Πρόβλεψης Απώλειας Ζεύξης και Αντιμετώπισης Εγωισμού στο πρωτόκολλο Dynamic Source Routing Κινητών Αδόμητων Δικτύων

Ευάγγελος Αγγελάκης
Μεταπτυχιακή Εργασία

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

## ΠΕΡΙΛΗΨΗ

Με την ευρεία διάδοση του συνόλου προδιαγραφών ασύρματων δικτύων IEEE 802.11, τα κινητά αδόμητα δίκτυα (mobile ad hoc networks: MANETs) αναδείχθηκαν σε ένα ταχέως αναπτυσσόμενο πεδίο έρευνας. Έχοντας μεγάλο εύρος εφαρμογών, από στρατιωτικές επιχειρήσεις, αποστολές διάσωσης και επέμβασης εκτάκτου ανάγκης ως απροσχεδίαστα δίκτυα οικιακής χρήσης, τα MANET προσφέρουν ένα περιβάλλον με πολλές προκλήσεις.

Η επικοινωνία στα MANET στηρίζεται στο ασύρματο μέσο μετάδοσης και στην συνεργασία των κόμβων που συμμετέχουν σε αυτά. Έτσι, η επικοινωνία σε αυτά επηρεάζεται όχι μόνο από την κακή ποιότητα ζεύξεων, αλλά και από κόμβους που δεν συμμετέχουν ορθά στις διαδικασίες δρομολόγησης.

Ορίζουμε ένα γενικό, συνεργατικό σχήμα διαχείρισης εμπιστοσύνης, στο οποίο κάθε κόμβος κατασκευάζει μία μετρική εμπιστοσύνης, για καθέναν από τους υπόλοιπους που συμμετέχουν στο δίκτυο, βασιζόμενος στις άμεσες αλληλεπιδράσεις που είχε μαζί τους, αλλά και στις φήμες που διαδίδονται από τρίτους κόμβους. Επίσης, στην εργασία αυτή προτείνουμε ένα μηχανισμό πρόβλεψης απώλειας ζεύξης και έναν

μηχανισμό ανακάλυψης και αντιμετώπισης κόμβων που επιδεικνύουν εγωιστική συμπεριφορά.

Και οι τρεις μηχανισμοί που προτείνονται, έχουν σχεδιαστεί και υλοποιηθεί ώστε να ενσωματώνονται στο Πρωτόκολλο Dynamic Source Routing (DSR). Η υλοποίηση, ο πειραματισμός και η αποτίμηση του κάθε μηχανισμού έγινε στην πλατφόρμα τηλεπικοινωνιακών προσομοιώσεων OPNET.

Τα πειράματα μας έδειξαν ότι η απώλεια ζεύξης μπορεί να προβλεφθεί και η εγωιστική συμπεριφορά κόμβου να εντοπιστεί επιτυχώς και εγκαίρως. Τα αποτελέσματά μας κατέδειξαν ότι για να αντιμετωπιστούν οι επιδράσεις των παραπάνω, χρειάζεται μία υλοποίηση του DSR με καλά σχεδιασμένες Caches Διαδρομών.

Επόπτης: Απόστολος Τραγανίτης, Καθηγητής

# Integrating Mechanisms for Trust Management, Link Failure Prediction and Selfishness Countermeasures into the Dynamic Source Routing Protocol for Mobile Ad Hoc Networks

Evangelos Angelakis
Master of Science Thesis

UNIVERSITY OF CRETE
COMPUTER SCIENCE DEPARTMENT

## ABSTRACT

With the wide spread of the IEEE 802.11 Specifications for Wireless LAN, mobile ad hoc networks (MANETs) have become a fast-growing field of research. With a range of applications that spans from military or emergency / rescue operations to unplanned or home networks, MANETs present a challenging environment.

Communication in MANETs relies on the wireless medium and the cooperation of their participants. Thus, their communication is susceptible both to poor link quality, as well as nodes that do not cooperate in the routing functions.

We defined a generic, contributory trust management scheme, in which a node builds a Trust Metric of each of the rest of the participants on the network, based on immediate interactions with them, as well as through rumors spread from others. We also propose a link failure prediction mechanism and a mechanism to detect and deal with selfish nodes.

All three mechanisms proposed have been designed and implemented as integrations into the Dynamic Source Routing (DSR) Protocol.Our implementation, testing and final evaluation for

each of the proposed mechanisms was performed, in the OPNET modelling platform.

Our tests have shown that link failure can be predicted and selfish behaviour can be successfully identified. Results have also indicated that in order to deal with their effects, a DSR implementation with well-designed route caches is required.

Supervisor: Apostolos Traganitis, Professor

# ΕΥΧΑΡΙΣΤΙΕΣ

Έχοντας ολοκληρώσει την Μεταπτυχιακή μου Εργασία, νιώθω την ανάγκη να ευχαριστήσω το Ινστιτούτο Πληροφορικής του ΙΤΕ καθώς και το Τμήμα Επιστήμης Υπολογιστών του για την υλικοτεχνική και οικονομική υποστήριξη τους, τους καθηγητές, τους συνεργάτες και τους φίλους, που με το δικό του τρόπο ο καθένας με βοήθησαν.

Ας είναι λοιπόν πρώτος ο επόπτης μου, Καθηγητής Απόστολος Τραγανίτης που μου έδωσε την ευκαιρία να ασχοληθώ με το θέμα που παρουσιάζεται εδώ, αλλά και με παρότρυνε να ασχολούμαι με πληθώρα άλλων θεμάτων κατά τη διάρκεια των σπουδών μου ως μεταπτυχιακός φοιτητής στο Τμήμα Επιστήμης Υπολογιστών. Οι εύστοχες παρατηρήσεις του και οι «πατρικές» συμβουλές του έπαιξαν το βασικότερο, ίσως, ρόλο στην ερεύνα μου. Ευχαριστώ τον Καθηγητή Βασίλειο Σύρη, για τις εκτενείς και καθοριστικές συζητήσεις που είχαμε κατά τη διάρκεια των πιο κρίσιμων περιόδων της εργασίας αυτής. Ευχαριστώ τον Καθηγητη Παναγιώτη Τσακαλίδη, για τις καίριες συμβουλές του για καλή έρευνα, αλλά και για την εμπιστοσύνη του σ' εμένα. Τέλος, οφείλω να ευχαριστήσω τους Καθηγητές Γιάννη Στυλιανού και Ευάγγελο Μαρκάτο για τη συμβολή τους στην εργασία αυτή.

Από τους συνεργάτες ευχαριστώ πρώτο το Στέφανο Παπαδάκη για την άψογη συνεργασία αλλά περισσότερο για τη φιλία του, το Γιώργο Τζαγκαράκη και τη Φένια Παπαγάλου που περάσαμε μαζί τις τελευταίες δύσκολες μέρες, το Γιάννη Αγιομυργιαννάκη για τις έμπειρες συμβουλές του, το Γιάννη Ασκοξυλάκη για την προθυμία και τη φροντίδα του, τον Δήμο Παναγόπουλο, τον Μιχάλη Λυγεράκη, το Βαγγέλη Καραγιάννη, τον Παναγιώτη Συκά και τους Στέλιο Κουτσάκη, Χρήστο Οικονομάκη και Φώτη Κίτσο για την όμορφη συνεργασία, την υπομονή και την βοήθεια τους και ύστατο αλλά μη ελάσσων το Γιώργο Παγώνη για την βοήθεια του για την παρουσίαση της εργασίας.

Ευχαριστώ το Σπύρο, τον Ανδρέα, τον Οδυσσέα, το Βαγγέλη, τη Ειρήνη, τη Λένα, την Εύα, το Θάνο, το Βασίλη, τη Σοφία, την Πέλα, και την Μαρία. Ο καθένας τους ξέρει το γιατί…

Κλείνοντας, θέλω να πω το μεγαλύτερο ευχαριστώ στον πατέρα και την μητέρα μου, που με αμέτρητη αγάπη και καμία φειδώ παρείχαν όλα αυτά που ήταν απαραίτητα για να φτάσω εδώ.

# ΠΕΡΙΕΧΟΜΕΝΑ

# Α΄ ΜΕΡΟΣ: ΕΙΣΑΓΩΓΗ

## 1. Σύνολο Προδιαγραφών Ασύρματων Δικτύων IEEE 802.11

Το 1997 η IEEE[1] επικύρωσε το σύνολο προδιαγραφών: IEEE Std. 802.11-1997 [1], που ήταν το πρώτο πρότυπο Ασύρματων Τοπικών Δικτύων (Wireless Local Area Networks: WLANs). Αυτό το σύνολο προδιαγραφών καθορίζει το επίπεδο ελέγχου πρόσβασης μέσου (Medium Access Control: MAC) και το φυσικό επίπεδο (Physical: PHY) ενός LAN με ασύρματες ζεύξεις. Στην παράγραφο αυτή γίνεται μία σύντομη παρουσίαση των θεμελιωδών στοιχείων των προδιαγραφών IEEE 802.11.

Το IEEE 802.11 είναι από πολλές απόψεις παρόμοιο με το πρότυπο του Ethernet IEEE 802.3, συγκεκριμένα το IEEE 802.11 καθορίζει:

- Τις λειτουργίες που πρέπει να υποστηρίζονται από μία συμμορφούμενη προς το πρότυπο συσκευή ασύρματης επικοινωνίας, ώστε να λειτουργεί είτε κατά το μοντέλο ομοτιμίας (peer-to-peer model) μαζί με αντίστοιχες συσκευές, ή να ενσωματώνεται σε ένα προϋπάρχον ενσύρματο LAN.
- Τη λειτουργία μίας συμμορφούμενης προς το πρότυπο συσκευή ασύρματης επικοινωνίας μέσα σε πιθανόν αλληλοεπικαλυπτώμενα ασύρματα LAN και τις δυνατότητες κινητικότητας αυτής της συσκευής ανάμεσα σε διάφορα ασύρματα LAN
- Τις τεχνικές σηματοδοσίας και διεπαφής φυσικού επιπέδου
- Την ιδιωτικότητα (privacy) και την ασφάλεια (security) των δεδομένων που μεταφέρουν οι χρήστες πάνω από το ασύρματο μέσο.

Τα χαρακτηριστικά που κάνουν ένα ασύρματο LAN διαφορετικό από ένα ενσύρματο και λαμβάνονται υπόψη στο 802.11 είναι ποικίλα. Τα φυσικά χαρακτηριστικά του ασύρματου LAN περιλαμβάνουν ισχυρό περιορισμό εμβέλειας, αναξιόπιστο μέσο, δυναμικές τοπο-λογίες, κινητικότητα κόμβων, παρεμβολές, θόρυβο *κλπ.*

(1) *IEEE: Institute of Electrical and Electronics Engineers*

Αυτοί οι περιορισμοί οδήγησαν στην δημιουργία βασικών ορισμών για μικρής εμβέλειας ασύρματα LAN που αποτελούνται από δικτυακά στοιχεία τα οποία βρίσκονται σε σχετικά μικρές αποστάσεις μεταξύ τους.

## 1.1 Η αρχιτεκτονική του IEEE 802.11

Οι αρχιτεκτονική του 802.11 αποτελείται από διάφορα στοιχεία και υπηρεσίες που αλληλεπιδρούν, ώστε να προσφέρουν διάφανη κινητικότητα των σταθμών στα ανώτερα επίπεδα της στοίβας πρωτοκόλλων.

### 1.1.α *Σταθμοί Ασύρματου LAN*

Ο σταθμός (station: STA) είναι το βασικότερο στοιχείο ενός ασύρματου δικτύου. Είναι οποιαδήποτε συσκευή υποστηρίζει την λειτουργικότητα του προτύπου 802.11, ως προς τα επίπεδα MAC και PHY. Στη συντριπτική πλειοψηφία οι λειτουργίες του 802.11 υλοποιούνται με υλικό και λογισμικό πάνω σε μία κάρτα διεπαφής δικτύου (network interface card: NIC). Ο σταθμός μπορεί να είναι ένας φορητός υπολογιστής, μία συσκευή χειρός ή ένα Access Point και να είναι κινούμενος, ή στατικός.

### 1.1.β *Βασικό Σύνολο Εξυπηρέτησης (Basic Service Set: BSS)*

Το 802.11 ορίζει το Βασικό Σύνολο Εξυπηρέτησης ως το βασικό δομικό στοιχείο ενός ασύρματου LAN. Το BSS αποτελείται από ένα αυθαίρετο πλήθος από σταθμούς. Σαν οντότητα το BSS δεν αποκτά ενδιαφέρον παρά μόνο όταν οριστούν οι τοπολογίες του 802.11

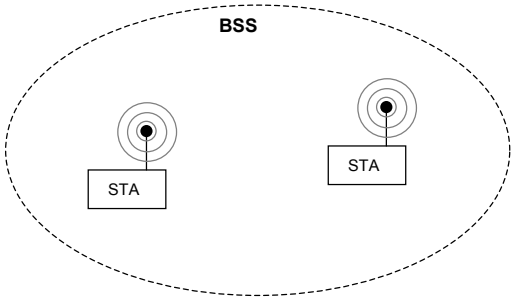
## 1.2 Τοπολογίες του IEEE 802.11

### 1.2.α *Ανεξάρτητο βασικό σύνολο εξυπηρέτησης*

Η πιο βασική τοπολογία ενός WLAN είναι αυτή ενός συνόλου σταθμών που έχουν αλληλο-αναγνωριστεί και έχουν συνδεθεί μέσω του ασύρματου μέσου, σε μία βάση ομοτιμίας (peer-to-peer fashion). Αυτή η δικτυακή τοπολογία, αναφέρεται ως *Ανεξάρτητο BSS* (Independent BSS: IBSS) ή *αδόμητο ασύρματο δίκτυο*.

### 1.2.β *Εκτεταμένο σύνολο υπηρεσίας*

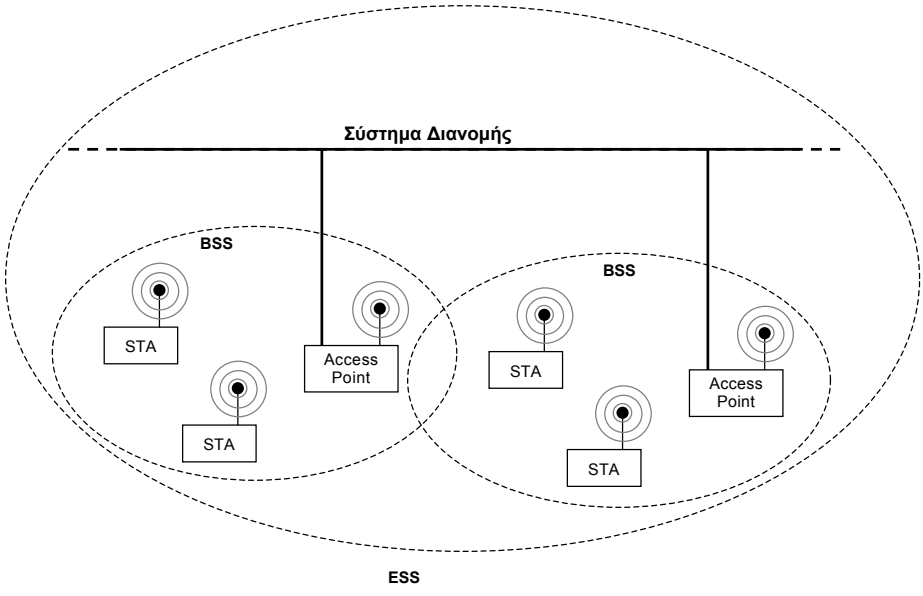
Ένα Δομημένο Βασικό Σύνολο εξυπηρέτησης (Infrastructured BSS) είναι ένα BSS με ένα Access Point. Το Access Point παρέχει υπηρεσίες τοπικής αναμετάδοσης για το BSS, καθώς και τη δυνατότητα σύνδεσης σε ένα σύστημα διανομής. Το σύστημα διανομής μπορεί να είναι ένα ενσύρματο δίκτυο ή ένα άλλο ασύρματο δίκτυο, το οποίο διασυνδέει πολλαπλά Access Points διάφορων BSS, σχηματίζοντας έτσι ένα *Εκτεταμένο Σύνολο Υπηρεσίας* (extended




service set: ESS).

(α)

(β)




Σχήμα Α.1.1 (α): *Το βασικότερο ασύρματο δίκτυο: δύο σταθμοί σε τοπολογία IBSS.* (β): *Ένα ESS σχηματίζεται με τη διασύνδεσης πολλαπλών BSS μέσω ενός συστήματος διανομής.*

## 1.3 Υπηρεσίες

Το πρότυπο 802.11 ορίζει διάφορες υπηρεσίες, μέσω των οποίων παρέχονται διάφορες λειτουργίες στους σταθμούς. Οι υπηρεσίες των σταθμών του 802.11 WLAN, υλοποιούνται σε όλους τους σταθμούς (και στα Access Points). Ο ρόλος των υπηρεσιών είναι να προσφέρουν ασφαλή και αξιόπιστη μεταφορά δεδομένων στο ασύρματο δίκτυο.

### 1.3.α *Ταυτοποίηση Σταθμού (station Authentication)*

Καθώς τα ασύρματα LAN έχουν περιορισμένη φυσική ασφάλεια λόγω του απροστάτευτου μέσου μετάδοσης, οποιοσδήποτε θα μπορούσε να αποκτήσει πρόσβαση σε αυτά. Έτσι, το IEEE 802.11 ορίζει υπηρεσίες ταυτοποίησης σταθμών για τον έλεγχο πρόσβασης στο WLAN. Ο στόχος αυτής της υπηρεσίας είναι να παρέχει έλεγχο πρόσβασης ισοδύναμο ενός ενσύρματου LAN.

Η υπηρεσία ταυτοποίησης, παρέχει ένα μηχανισμό με τον οποίο ένας σταθμός μπορεί να πιστοποιήσει έναν άλλο σταθμό. Χωρίς την πιστοποίηση της ταυτότητας του, ένας σταθμός δεν μπορεί να χρησιμοποιήσει το WLAN για μεταφορά δεδομένων. Έτσι στο 802.11 όλοι οι σταθμοί, ανεξάρτητα από το αν ανήκουν σε ένα IBSS ή σε ένα ESS, πρέπει να χρησιμοποιήσουν, επιτυχώς, την υπηρεσία ταυτοποίησης, προτού μπορέσουν να επικοινωνήσουν με έναν άλλο κόμβο. Στο IEEE 802.11 ορίζονται δύο τύποι υπηρεσίας ταυτοποίησης:

#### 1.3.α.1 Ταυτοποίηση Ανοιχτού Συστήματος

Η ταυτοποίηση ανοιχτού συστήματος είναι μία κενή (null) ταυτοποίηση σταθμού. Ένας σταθμός που θέλει να ταυτοποιηθεί σε έναν άλλο σταθμό στέλνει απλά ένα πλαίσιο διαχείρισης ταυτοποίησης (authentication management frame) που περιέχει την ταυτότητα του αποστολέα που στην ουσία ανακοινώνει την πρόθεση του να επικοινωνήσει με τον παραλήπτη.

### 1.3.α.2 Ταυτοποίηση Διαμοιρασμένου Κλειδιού (shared key)

Σε αυτόν τον τύπο της ταυτοποίησης, υπάρχει η προϋπόθεση ότι ο κάθε σταθμός έχει εφοδιαστεί με ένα κρυφό κλειδί, μέσω ενός ασφαλούς καναλιού το οποίο είναι ανεξάρτητο από το δίκτυο του 802.11. Οι σταθμοί ταυτοποιούνται αμφίδρομα, με απόδειξη της γνώσης του κλειδιού. Η χρήση αυτής της μορφής ταυτοποίησης απαιτεί την κρυπτογράφηση των πλαισίων μέσω του αλγόριθμου *Ισοδύναμης Ενσύρματης Ασφάλειας* (Wired Equivalent Privacy: WEP).

## 1.4 Το επίπεδο MAC του IEEE 802.11

Το επίπεδο MAC του 802.11 παρέχει τη λειτουργικότητα που επιτρέπει την αξιόπιστη μεταφορά δεδομένων στα ανώτερα επίπεδα δικτύου πάνω από το ασύρματο φυσικό μέσο. Η μεταφορά στηρίζεται στην ασύγχρονη, ασύνδετη παράδοση «βέλτιστης προσπάθειας» (best effort) πλαισίων δεδομένων του επιπέδου MAC και δεν υπάρχει εγγύηση ότι τα πλαίσια θα παραδοθούν επιτυχώς.

Σε αυτό το επίπεδο παρέχεται μία μέθοδος για ελεγχόμενη πρόσβαση στο διαμοιραζόμενο μέσο, με το πρωτόκολλο CSMA/CA (Carrier-Sense Multiple Access with Collision Avoidance). Σύμφωνα με το πρωτόκολλο αυτό, ένας σταθμός που έχει να μεταδώσει ένα πλαίσιο ελέγχει πρώτα το μέσο για να διαπιστώσει αν μπορεί να μεταδώσει σε αυτό. Η αποφυγή των συγκρούσεων (Collision Avoidance) επιτυγχάνεται με την υλοποίηση ενός τυχαίου χρόνου οπισθοχώρησης στην περίπτωση που ο σταθμός διαπιστώσει ότι το μέσο είναι απασχολημένο.

Τέλος στο επίπεδο αυτό παρέχονται υπηρεσίες ιδιωτικότητας (privacy) και ασφάλειας (security). Αυτές παρέχονται από τις υπηρεσίας ταυτοποίησης χρήστη καθώς και μέσω του αλγόριθμου Ισοδύναμης Ενσύρματης Ασφάλειας.

## 1.5 Το φυσικό επίπεδο IEEE 802.11

Το φυσικό επίπεδο του 802.11 είναι η διεπαφή ανάμεσα στο επίπεδο έλεγχου πρόσβασης μέσου και στο πραγματικό φυσικό μέσο όπου μεταδίδονται τα πλαίσια. Το επίπεδο αυτό χρησιμοποιεί

διαμορφώσεις ή διασκορπισμένου φάσματος (DSSS), ή OFDM για να μεταδώσει πλαίσια δεδομένων πάνω από το μέσο. Τέλος παρέχει στο επίπεδο MAC την ένδειξη που δηλώνει ότι το κανάλι είναι απασχολημένο, κατά τη χρήση του μηχανισμού ακρόασης του μέσου.

Στο 802.11 παρέχονται τρεις ορισμοί του επιπέδου PHY: Τόσο η Διασκόρπιση Φάσματος με Μεταπήδηση Συχνότητας (Frequency Hopping Spread Spectrum: FHSS) όσο και η Διασκόρπιση Φάσματος με Ευθεία Ακολουθία (Direct Sequence Spread Spectrum :DSSS) υποστηρίζουν ρυθμούς 1 και 2 Mbps, λειτουργώντας στην ISM[2] ζώνη συχνοτήτων των 2,4GHz. Η επέκταση 802.11a του πρωτοκόλλου χρησιμοποιεί διαφορετικές τεχνικές διαμόρφωσης (OFDM) και μπορεί να υποστηρίξει ρυθμούς έως τα 54Mbps, λειτουργώντας στην ζώνη των 5GHz. Η πιο διαδεδομένη εμπορικά επέκταση 802.11b με χρήση Υψηλού DSSS (High Rate DSSS: HR/DSSS), υποστηρίζει ρυθμούς των 11 και 5.5Mbps, αλλά επίσης ορίζει και τεχνικές αυτόματης αλλαγής ρυθμού όπου κόμβοι των 11Mbps μπορούν να πέσουν στα 5.5, 2 ή 1 Mbps, λόγο θορύβου στο κανάλι ή για να υποστηρίξουν την διαλειτουργικότητα με συσκευές που χρησιμοποιούν το 802.11, καθώς και το 802.11b λειτουργεί στα 2.4GHz. Τέλος, πρόσφατα προτυποποιήθηκε η επέκταση 802.11g, που χρησιμοποιεί παρόμοιες τεχνικές πολυπλεξίας και διαμόρφωσης με αυτές του 802.11a, λειτουργεί στη ζώνη των 2,4 και είναι συμβατό με το 802.11b.

### 1.6 Κατακλείδα

Η ευρεία εμπορική ανάπτυξη συσκευών βασισμένων στο πρότυπο IEEE 802.11 και τις προεκτάσεις του έχει δώσει μία μεγάλη ώθηση στην ερευνητική δραστηριότητα του τομέα ασύρματων LAN, καθώς προσφέρει ένα περιβάλλον με πληθώρα εφαρμογών, ευρεία χρήση και φτηνό εξοπλισμό αλλά και πολλές προκλήσεις.

## 2. Ασύρματα αδόμητα δίκτυα

Μία συλλογή από αυτόνομες τερματικές συσκευές –κόμβους πού επικοινωνούν μεταξύ τους σχηματίζοντας ένα ραδιοδίκτυο πολλαπλών βημάτων (hops) το οποίο διατηρεί την διασύνδεση του με αποκεντρικοποιημένο τρόπο ονομάζεται *ασύρματο αδόμητο δίκτυο*

(2) *ISM: Industrial, Scientific, Medical.*

(wireless ad hoc network). Δεδομένου ότι οι κόμβοι επικοινωνούν μέσω ασύρματων ζεύξεων, πρέπει να αντιπαρέρχονται τις διάφορες επιβλαβείς επιδράσεις της ραδιοεπικοινωνίας όπως ο θόρυβος, οι διαλείψεις και οι παρεμβολές. Επιπλέον, οι ασύρματες ζεύξεις συνήθως υποστηρίζουν μικρότερο εύρος φάσματος (bandwidth) από ότι οι ενσύρματες.

Ο έλεγχος ενός ασύρματου αδόμητου δικτύου κατανέμεται στους κόμβους, καθώς κάθε ένας από αυτούς μπορεί και οφείλει να λειτουργεί ως τερματική συσκευή και ως δρομολογητής. Η τοπολογία ενός τέτοιου δικτύου είναι δυναμική, διότι η αλληλοσύνδεση των κόμβων μπορεί να ποικίλει στο χρόνο λόγω αποχώρησης ή εισαγωγής κόμβων στο δίκτυο, αλλά και γιατί μπορεί να υπάρχουν κινούμενοι χρήστες. Συνεπώς, σε τέτοια δίκτυα υπάρχει ανάγκη για χρήση αποδοτικών πρωτοκόλλων δρομολόγησης που να επιτρέπουν στους κόμβους να επικοινωνούν χρησιμοποιώντας μονοπάτια πολλαπλών βημάτων (multi-hop paths) που καταναλώνουν κατά το δυνατό ελάχιστους πόρους.

Μερικοί από τους παραπάνω περιορισμούς χαρακτήριζαν ραδιοδίκτυα πακέτων που μελετήθηκαν εκτενώς κατά τις δεκαετίες του 1970 και 1980 [2,3,4]. Με την εμφάνιση του πρωτοκόλλου IEEE 802.11 το ενδιαφέρον της ακαδημαϊκής, βιομηχανικής και στρατιωτικής ερευνητικής κοινότητας αναζωπυρώθηκε χάρη στην ευρεία διάδοση φτηνών ράδιοσυσκευών δικτύου που λειτουργούν στην ISM ζώνη συχνοτήτων. Καθώς τα δίκτυα αυτά θέτουν πολλά και περίπλοκα ζητήματα, υπάρχουν αρκετά ανοιχτά προβλήματα για έρευνα επάνω σε αυτόν τον τομέα.

Υπάρχουν δύο κύριες κατηγορίες ασύρματων αδόμητων δικτύων: τα *κινητά αδόμητα δίκτυα* (mobile ad hoc networks: MANETs) και τα *δίκτυα ευφυών αισθητήρων* (smart sensor networks). Η εργασία αυτή αφορά στην πρώτη κατηγορία.

## 2.1 Κινητά αδόμητα δίκτυα (*Mobile Ad Hoc Networks: MANETs*)

Στην παρούσα γενιά συστημάτων ασύρματων επικοινωνιών υπάρχει πολλές φορές ανάγκη για ταχεία ανάπτυξη αυτόνομων δικτύων κινούμενων χρηστών. Από τα πιο ενδεικτικά παραδείγματα που μπορούν να αναφερθούν είναι η εγκατάσταση βιώσιμης, ασφαλούς,

αποδοτικής και δυναμικής επικοινωνίας για επιχειρήσεις εκτάκτου ανάγκης ή διάσωσης, αντιμετώπισης καταστροφών και στρατιωτικές επιχειρήσεις. Λόγω της φύσης των παραπάνω σεναρίων, στα οποία μπορούν να αναπτυχθούν κάποια MANET, τα δίκτυα αυτά δεν πρέπει να βασίζονται σε κεντρικές υποδομές οι οποίες εξασφαλίζουν την διασύνδεση των τερματικών κόμβων. Ένα MANET είναι ένα αυτόνομο σύνολο από κινούμενους χρήστες που επικοινωνούν μέσω ασύρματων ζεύξεων σχετικά περιορισμένου εύρους φάσματος. Λόγω της δυνατότητας κίνησης των χρηστών, δηλαδή των κόμβων του δικτύου, η τοπολογία μπορεί να αλλάζει γρήγορα και χωρίς κάποιο προβλέψιμο τρόπο στο χρόνο. Ένα τέτοιο δίκτυο είναι αποκεντρικοποιημένο, καθώς όλες οι δικτυακές δραστηριότητες, όπως η ανακάλυψη της τοπολογίας και η παράδοση των μηνυμάτων, πρέπει να εκτελούνται από τους ίδιους τους κόμβους, συνεπώς και οι λειτουργίες της δρομολόγησης πρέπει να εκτελούνται από τους ίδιους τους κινούμενους κόμβους.

Ο σχεδιασμός και η ανάπτυξη τέτοιων δικτύων είναι ιδιαίτερα περίπλοκα ζητήματα, καθώς το εύρος των εφαρμογών για τα MANET είναι μεγάλο και εκτείνεται από μικρά, στατικά, οικιακά δίκτυα, μέχρι μεγάλης κλίμακας, έντονα δυναμικά στρατιωτικά δίκτυα. Ανεξάρτητα από την χρήση του, ένα MANET χρειάζεται αποδοτικούς κατανεμημένους αλγορίθμους για να καθορίσει την οργάνωση του, τον προγραμματισμό των ζεύξεων (link scheduling) και την δρομολόγηση. Όμως, ο εντοπισμός εφικτών μονοπατιών (viable routing paths) και η παράδοση μηνυμάτων σε ένα αποκεντρικοποιημένο δικτυακό περιβάλλον, όπου η τοπολογία μεταβάλλεται δεν είναι ένα «καλά ορισμένο πρόβλημα». Ενώ στα στατικά ενσύρματα δίκτυα το συντομότερο (κατά μία συνάρτηση κόστους) μονοπάτι από μία πηγή (source) ως έναν προορισμό (destination) συνήθως είναι η βέλτιστη διαδρομή, η ιδέα αυτή δεν επεκτείνεται κατ’ ανάγκη εύκολα για να καλύψει τα MANET. Παράγοντες όπως η μεταβαλλόμενη ποιότητα ζεύξης, οι απώλειες διάδοσης, οι διαλείψεις, οι παρεμβολές άλλων χρηστών, η ανάγκη εξοικονόμησης ενέργειας και οι τοπολογικές μεταβολές παίζουν πλέον κάποιο ρόλο. Το δίκτυο πρέπει να προσαρμόζεται και να προσπαθεί να απαλείψει την επιρροή τους, αλλάζοντας τα μονοπάτια του προσαρμοζόμενο στις εκάστοτε επιδράσεις των παραπάνω παραγόντων. Για παράδειγμα σε ένα στρατιωτικό περιβάλλον, η ασφάλεια, οι καθυστερήσεις, η

αξιοπιστία και η ανοχή σε ηθελημένες παρεμβολές είναι πρώτιστες ευθύνες του σχεδιαστή.

Ζητήματα που αφορούν στην διερεύνηση βασικών εννοιών, λειτουργικές απαιτήσεις καθώς και στην ανάπτυξη προτύπων για τα MANET, αντιμετωπίζονται από την ομάδα εργασίας *manet* της IETF [3].

## 3. Δρομολόγηση σε Ασύρματα αδόμητα δίκτυα

Πολλά πρωτόκολλα έχουν προταθεί για την επίλυση του προβλήματος της δρομολόγησης πολλαπλών βημάτων σε αδόμητα δίκτυα. Παρόλο πού καθένα βασίζεται σε διαφορετικές αντιλήψεις και υποθέσεις, κοινό χαρακτηριστικό όλων των πρωτοκόλλων είναι η προϋπόθεση πλήρους συμμετοχής των κόμβων στους μηχανισμούς τους.

Τα υπάρχοντα πρωτοκόλλα μπορούν να χωριστούν σε δύο κατηγορίες: *δρομολόγηση κατ' απαίτηση* ή *αντιδραστική* (on-demand ή reactive αντίστοιχα) και *προνοητική δρομολόγηση* ή *οδηγούμενη από πίνακα* (proactive/table-driven αντίστοιχα). Στην πρώτη κατηγορία εντάσσονται πρωτόκολλα τα οποία δημιουργούν διαδρομές μόνο όταν αυτό χρειάζεται να γίνει για την μεταφορά ενός πακέτου από μία πηγή προς έναν προορισμό. Σε αυτά μια *διαδικασία ανακάλυψης διαδρομής* (route discovery process) ξεκινάει στο δίκτυο όταν ένας κόμβος ζητήσει να πληροφορηθεί μία διαδρομή για έναν προορισμό. Αντίθετα τα πρωτόκολλα της δεύτερης κατηγορίας προσπαθούν να διατηρούν συνεπή και ενημερωμένη πληροφορία για τη δρομολόγηση μέσα στο δίκτυο. Συνήθως αυτό επιτυγχάνεται με την περιοδική ενημέρωση πινάκων δρομολόγησης σε κάθε κόμβο.

Τα πιο διαδεδομένα και εκτενώς μελετημένα πρωτόκολλα δρομολόγησης είναι: το DSDV[5], το TORA [6] το AODV[7] και το DSR[8]. Μια αρκετά ενημερωμένη λίστα που περιλαμβάνει σχεδόν όλα τα πρωτόκολλα δρομολόγησης που έχουν προταθεί βρίσκεται στο [9].

### 3.1 DSVD: Destination-Sequenced Distance Vector

Το πρωτόκολλο διανύσματος απόστασης ακολουθίας προορισμού DSVD είναι ένα πρωτόκολλο διανύσματος απόστασης βήμα-προς-βήμα

(3) *IETF: International Engineering Task Force*

(hop-by-hop) που απαιτεί από κάθε κόμβο να ενημερώνει περιοδικά όλους τους γείτονες του για τις πληροφορίες δρομολόγησης που έχει. Ανήκει στην κατηγορία των προνοητικών πρωτοκόλλων και το ουσιαστικό πλεονέκτημα του είναι η εγγύηση που παρέχει για αποφυγή βρόγχων.

Ο κάθε κόμβος διαθέτει και ενημερώνει έναν πίνακα δρομολόγησης ο οποίος έχει το «*επόμενο βήμα*» για κάθε προορισμό στο δίκτυο. Ο DSVD χαρακτηρίζει κάθε διαδρομή με έναν αριθμό σειράς και θεωρεί ότι η διαδρομή R είναι προτιμότερη της R' αν η R έχει μεγαλύτερο αριθμό σειράς. Σε περίπτωση ίσων αριθμών σειράς προτιμάται η διαδρομή με χαμηλότερη τιμή μιας άλλης μετρικής που ορίζεται από το πρωτόκολλο. Κάθε κόμβος περιοδικά διαφημίζει έναν άρτιο, γνησίως αύξοντα αριθμό σειράς για τον εαυτό του. Όταν ένας κόμβος Β αποφασίσει ότι η διαδρομή του για τον D έχει κοπεί διαφημίζει την διαδρομή προς τον D με άπειρη τιμή της μετρικής και αριθμό σειράς μεγαλύτερο κατά ένα (περιττό) από αυτόν που είχε. Με τον τρόπο αυτό κάθε κόμβος Α που δρομολογεί πακέτα μέσω του Β κρατάει την άπειρη μετρική για αυτήν τη διαδρομή ως ότου ακούσει μια νέα διαδρομή προς τον D με μεγαλύτερο αριθμό σειράς.

## 3.2 TORA: Temporally-Ordered Routing Algorithm

Ο αλγόριθμος χρονικά διατεταγμένης δρομολόγησης TORA, είναι ένα κατανεμημένο πρωτόκολλο που βασίζεται στον αλγόριθμο αναστροφής ζεύξης. Έχει σχεδιαστεί για να ανακαλύπτει γρήγορα διαδρομές κατ' απαίτηση, να παρέχει πολλαπλές διαδρομές προς έναν προορισμό, να ανακαλύπτει διχοτόμηση του δικτύου και να ελαχιστοποιεί την *πλεονάζουσα πληροφορία* (overhead) περιορίζοντας τοπικά τις αντιδράσεις σε τοπολογικές αλλαγές όταν αυτό είναι εφικτό. Η δημιουργία βέλτιστων διαδρομών θεωρείται δευτερεύουσας σημασίας και αρκετές φορές θέτει σε χρήση μεγαλύτερες από το βέλτιστο διαδρομές για να αποφύγει τον επιπλέον φόρτο που θα απαιτούσε η ανακάλυψη των βέλτιστων διαδρομών.

## 3.3 DSR Dynamic Source Routing

Το πρωτόκολλο δυναμικής δρομολόγησης πηγής DSR χρησιμοποιεί την τεχνική της δρομολόγησης πηγής, όπου κάθε πακέτο που δρομολογείται μεταφέρει στην επικεφαλίδα (header) του μια πλήρη, διατεταγμένη λίστα από τους κόμβους μέσω των οποίων το πακέτο πρέπει να περάσει για να φτάσει στον προορισμό του. Με την τεχνική αυτή δεν είναι απαραίτητο οι ενδιάμεσοι κόμβοι να διατηρούν πλήρως ενημερωμένη πληροφορία δρομολόγησης για να συμμετέχουν στην διαδικασία προώθησης πακέτων στον προορισμό. Η λειτουργία του χωρίζεται σαφώς σε δύο μηχανισμούς: *Ανακάλυψης Διαδρομής* και *Συντήρησης Διαδρομών*, στα πρότυπα του [10]. Είναι ένα πρωτόκολλο που προσφέρεται ιδιαίτερα για μελέτη μηχανισμών συμπεριφοράς χρηστών σε αδόμητα ασύρματα δίκτυα και για το λόγο αυτό έχει χρησιμοποιηθεί εκτενώς όπως θα δούμε και παρακάτω. Καθώς το DSR ήταν το πρωτόκολλο που επιλέξαμε για την μελέτη μας στην επόμενη παράγραφο του κεφαλαίου γίνεται μία λεπτομερής περιγραφή των βασικών του μηχανισμών.

### 3.4 AODV Ad hoc On Demand Distance Vector Routing

Το πρωτόκολλο AODV είναι στην ουσία ένας συνδυασμός των DSR και DSDV. Δανείζεται τους βασικούς μηχανισμούς Ανακάλυψης Διαδρομής και Συντήρησης Διαδρομής από το DSR και χρησιμοποιεί την τεχνική της βήμα-προς-βήμα δρομολόγησης, τους αριθμούς σειράς και ορισμένα από τα περιοδικά πακέτα σηματοδοσίας του DSDV. Παρόλα αυτά εντάσσεται στην πρώτη κατηγορία των «κατ' απαίτηση» πρωτοκόλλων δρομολόγησης.

## 4. Το πρωτόκολλο Δυναμικής Δρομολόγησης Πηγής DSR

Το πρωτόκολλο δυναμικής δρομολόγησης πηγής DSR, είναι ένα απλό και αποδοτικό πρωτόκολλο δρομολόγησης που σχεδιάστηκε ειδικά για χρήση σε ασύρματα αδόμητα δίκτυα πολλαπλών βημάτων. Ένα δίκτυο που χρησιμοποιεί το DSR επιτυγχάνει την αυτοοργάνωση και αυτορύθμιση του, χωρίς να απαιτεί την ύπαρξη δομημένης δικτυακής υποδομής ή κεντρικής διαχείρισης. Οι κόμβοι συνεργάζονται για να προωθήσουν, μέσω πολλαπλών βημάτων, πακέτα ο ένας στον άλλο, επιτρέποντας έτσι την επικοινωνία απομακρυσμένων κόμβων, οι οποίοι βρίσκονται σε αποστάσεις μεγαλύτερες από την ακτίνα ασύρματης μετάδοσης. Καθώς διάφοροι κόμβοι στο δίκτυο

μετακινούνται, αποσυνδέονται, ή συνδέονται σε αυτό, και καθώς οι συνθήκες της ασύρματης μετάδοσης αλλάζουν, η δρομολόγηση καθορίζεται και συντηρείται αυτόματα από το DSR.

Το πρωτόκολλο DSR επιτρέπει στους κόμβους να ανακαλύπτουν δυναμικά μία διαδρομή πηγής η οποία οδηγεί, ενδεχομένως και κατά μήκος πολλαπλών βημάτων, σε οποιονδήποτε δυνατό προορισμό στο αδόμητο δίκτυο. Κάθε πακέτο που στέλνεται έχει στην επικεφαλίδα του μια πλήρη, διατεταγμένη λίστα των κόμβων μέσω των οποίων πρέπει να περάσει επιτρέποντας έτσι στην δρομολόγηση να είναι άκυκλη και παράλληλα αποφεύγοντας την ανάγκη για χρονικά ευαίσθητη πληροφόρηση δρομολόγησης στους κόμβους μέσω των οποίων θα δρομολογηθεί.

Το πρωτόκολλο DSR αποτελείται από δύο μηχανισμούς που συνεργάζονται για να πραγματοποιήσουν την ανακάλυψη και την συντήρηση των διαδρομών πηγής σε ένα αδόμητο δίκτυο:

- Ο μηχανισμός *Ανακάλυψης Διαδρομής* (Route Discovery mechanism) είναι αυτός χάρη στον οποίο ένας κόμβος-πηγή S, που θέλει να στείλει ένα πακέτο σε ένα κόμβο-προορισμό D, αποκτά μια *διαδρομή πηγής* (source route) προς τον προορισμό. Ο μηχανισμός αυτός χρησιμοποιείται μονάχα όταν μία πηγή έχει να στείλει ένα πακέτο σε κάποιο προορισμό και δεν γνωρίζει ήδη μια διαδρομή για αυτόν.
- Ο μηχανισμός *Συντήρησης Διαδρομής* (Route Maintenance mechanism) είναι αυτός χάρη στον οποίο ένας κόμβος-πηγή S κατά την χρήση μίας διαδρομής πηγής προς τον προορισμό D μπορεί να διαπιστώσει εάν η τοπολογία του δικτύου άλλαξε, κατά τρόπο πού δεν του επιτρέπει να χρησιμοποιεί πλέον την γνωστή αυτή διαδρομή, διότι κάποια ζεύξη της έχει κοπεί. Όταν ο μηχανισμός Συντήρησης Διαδρομής διαπιστώσει ότι μία υπάρχουσα διαδρομή πηγής δεν ισχύει πια, ο S μπορεί είτε να προσπαθήσει στο μέλλον να χρησιμοποιήσει μία εναλλακτική γνωστή διαδρομή προς τον D, ή να ενεργοποιήσει το μηχανισμό Ανακάλυψης Διαδρομής ξανά, ώστε να βρει μία νέα διαδρομή για τα ακόλουθα πακέτα που προορίζει για τον D. Ο μηχανισμός αυτός πάντως ενεργοποιείται μόνο όταν ο S μπαίνει στη διαδικασία να στείλει ένα πακέτο στον D.

Όπως έγινε φανερό, στο πρωτόκολλο DSR τόσο ο μηχανισμός Ανακάλυψης Διαδρομής όσο και ο μηχανισμός Συντήρησης Διαδρομής λειτουργούν εξ' ολοκλήρου «κατ' απαίτηση». Σε αντίθεση με άλλα πρωτόκολλα δρομολόγησης, το DRS δεν απαιτεί περιοδικές αποστολές πακέτων κάποιου τύπου μέσα στο δίκτυο. Για παράδειγμα, δεν υπάρχει ανάγκη για περιοδικές διαφημίσεις διαδρομών, πακέτα ανίχνευσης κατάστασης ζεύξεων ή ανακάλυψης γειτόνων και δεν αφήνεται καμία από αυτές τις λειτουργίες σε πρωτόκολλα χαμηλότερων επιπέδων. Η εξ' ολοκλήρου «κατ' απαίτηση» λειτουργία του DSR και η παντελής έλλειψη περιοδικών λειτουργιών επιτρέπουν σε ακίνητα αδόμητα δίκτυα να μηδενίζουν τα πλεονάζοντα (overhead) πακέτα ελέγχου μετά από μικρό χρόνο λειτουργίας που θα επιτρέψει την ανακάλυψη των διαδρομών που απαιτούνται για την επικοινωνία των κόμβων. Αντίθετα, σε κινούμενα δίκτυα, η πλεονάζουσα πληροφορία που εισάγουν οι μηχανισμοί του DSR ανέρχεται στο ελάχιστο δυνατό ποσό που θα επιτρέψει την σωστή διαχείριση των χρησιμοποιούμενων διαδρομών. Αυτό συμβαίνει διότι αλλαγές στην τοπολογία οι οποίες δεν επηρεάζουν τις διαδρομές που χρησιμοποιούνται δεν προκαλούν την αντίδραση του πρωτοκόλλου.

Ως αποτέλεσμα του μηχανισμού Ανακάλυψης Διαδρομής, ένας κόμβος μπορεί να μάθει και να αποθηκεύσει πολλαπλές διαδρομές προς κάποιον προορισμό. (Το ίδιο μπορεί να συμβεί αν ο κόμβος «υποκλέψει» πληροφορίες δρομολόγησης που προορίζονται για τρίτους.). Αυτό επιτρέπει μια μεγαλύτερη ταχύτητα αντίδρασης σε αλλαγές δρομολόγησης, καθώς ένας κόμβος με πολλαπλές επιλογές διαδρομών προς έναν προορισμό μπορεί να χρησιμοποιήσει μία εναλλακτική αποθηκευμένη διαδρομή στην περίπτωση που αποτύχει η χρησιμοποιούμενη. Η αποθήκευση (caching) πολλαπλών διαδρομών επίσης αποφεύγει τον πλεονασμό που απαιτείται για να εκτελέσει μια ανακάλυψη διαδρομής στην περίπτωση που μία διαδρομή διακοπεί.

Η λειτουργία των μηχανισμών Ανακάλυψης και Συντήρησης Διαδρομών του DSR είναι σχεδιασμένη ώστε να επιτρέπει μονόδρομες (unidirectional) ζεύξεις και να υποστηρίζει εύκολα ασύμμετρες διαδρομές ανάμεσα σε δύο κόμβους. Το σκεπτικό είναι ότι σε ασύρματα δίκτυα ενδέχεται μια ζεύξη δύο κόμβων να μην λειτουργεί εξίσου καλά και προς τις δύο κατευθύνσεις, λόγω διαφορετικών κεραιών, πομποδεκτών ή ακόμα και λόγω διαγραμμάτων διάδοσης ή

παρεμβολών. Το DSR επιτρέπει να χρησιμοποιούνται τέτοιες μονόδρομες ζεύξεις όταν κρίνεται απαραίτητο για να βελτιωθεί η ολική απόδοση και συνδεσιμότητα του δικτύου.

## 4.1 Υποθέσεις του πρωτοκόλλου

Η πρώτη υπόθεση του πρωτοκόλλου είναι ότι όλοι οι κόμβοι που επιθυμούν να επικοινωνούν με άλλους κόμβους μέσα στο αδόμητο δίκτυο είναι διατεθειμένοι να συμμετέχουν πλήρως στα πρωτόκολλα του δικτύου. Συγκεκριμένα, κάθε κόμβος του θα πρέπει να είναι διατεθειμένος να προωθεί πακέτα άλλων στο δίκτυο.

Ως *διάμετρος του δικτύου* ορίζεται ο ελάχιστος απαιτούμενος αριθμός βημάτων ώστε το πακέτο ενός κόμβου που βρίσκεται στο ένα άκρο του δικτύου να φτάσει στον κόμβο στο πιο απομακρυσμένο άκρο του δικτύου. Η υπόθεση του DSR εδώ είναι ότι η διάμετρος αυτή θα είναι συχνά μικρή (π.χ. συνήθως 5 με 10 βήματα), αλλά σχεδόν πάντα θα είναι μεγαλύτερη από 1 βήμα.

Είναι γνωστό ότι τα πακέτα ενδέχεται να χάνονται ή να αλλοιώνονται κατά τη μετάδοση τους σε ασύρματα δίκτυα. Η σχετική υπόθεση του DSR είναι ότι ένα αλλοιωμένο πακέτο ανιχνεύεται και απορρίπτεται από το δέκτη από τα πρωτόκολλα χαμηλότερων επιπέδων.

Οι κόμβοι ενός αδόμητου δικτύου μπορούν να μετακινηθούν ανά πάσα στιγμή, χωρίς προειδοποίηση και ενδέχεται η κίνηση τους να είναι συνεχής. Το DSR υποθέτει ότι η ταχύτητα με την οποία θα κινηθούν οι κόμβοι είναι χαμηλή σε σχέση με τις μέγιστες ταχύτητες που ανέχονται οι δικτυακές συσκευές που χρησιμοποιούνται στο αδόμητο δίκτυο. Συγκεκριμένα το DSR μπορεί να υποστηρίξει πολύ ταχείς ρυθμούς κινητικότητας, αλλά υποθέτει ότι οι κόμβοι δεν κινούνται συνεχώς και τόσο γρήγορα ώστε το μόνο δυνατό πρωτόκολλο δρομολόγησης να είναι το flooding κάθε πακέτου στο δίκτυο.

Ένα κοινό χαρακτηριστικό αρκετών καρτών διεπαφής δικτύου, συμπεριλαμβανομένων και των σύγχρονων συσκευών WLAN, είναι η ικανότητα λειτουργίας με το *μηχανισμό αδιάκριτης λήψης* (promiscuous reception mode). Ο μηχανισμός αυτός επιτρέπει στο υλικό να παραδίδει κάθε πακέτο που λαμβάνεται στο λογισμικό του οδηγού της συσκευής δικτύου χωρίς να φιλτράρει τα πακέτα με βάση

την διεύθυνση επιπέδου ζεύξης (link layer address). Συγκεκριμένα στο πρωτόκολλο IEEE 802.11, όπου υπάρχει πρόβλεψη για διαχείριση ενέργειας των συσκευών, η χρήση του μηχανισμού αδιάκριτης λήψης συνεπάγεται ότι οι συσκευές δεν πέφτουν στην κατάσταση ύπνωσης (doze state), καταναλώνοντας έτσι περισσότερη ενέργεια. Παρόλο που δεν απαιτείται η δυνατότητα υποστήριξης αδιάκριτης λήψης, αρκετές από τις βελτιστοποιήσεις του DSR εκμεταλλεύονται τις δυνατότητες που προσφέρει ο μηχανισμός αυτός.

Η ασύρματη επικοινωνία ανάμεσα σε δύο κόμβους μπορεί κάποιες φορές να μην δουλεύει το ίδιο καλά και προς τις δύο κατευθύνσεις. Αυτό μπορεί να οφείλεται για παράδειγμα σε διαφορετικές κεραίες, διαγράμματα διάδοσης, πηγές παρεμβολών κλπ. Η ασύρματη επικοινωνία ανάμεσα σε δύο κόμβους στην γενική της περίπτωση είναι αμφίδρομη, ενδέχεται όμως μία ζεύξη ανάμεσα σε δύο κόμβους να είναι μονόδρομη, επιτρέποντας μόνο στον ένα κόμβο να μπορεί να στείλει πακέτα στον άλλο. Παρόλο που πολλά πρωτόκολλα δρομολόγησης λειτουργούν με την προϋπόθεση αμφίδρομων ζεύξεων, το DSR μπορεί να ανακαλύψει διαδρομές που περιέχουν μονόδρομες ζεύξεις και να προωθήσει πακέτα μέσω σε αυτών. Βελτιστοποιήσεις του DSR μπορούν να υλοποιηθούν στην περίπτωση που η ύπαρξη αμφίδρομων ζεύξεων είναι εγγυημένη, όπως στο IEEE 802.11, στο οποίο η εκπομπή unicast πακέτων περιορίζεται σε αμφίδρομες ζεύξεις.

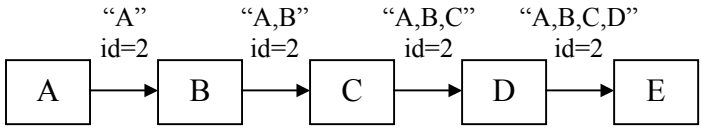
Η μέθοδοι που θα χρησιμοποιούνται για τον σχηματισμό του αδόμητου δικτύου και για τη διευθυνσιοδότηση των κόμβων δεν περιγράφονται από το DSR. Έτσι οι διευθύνσεις IP κόμβων που χρησιμοποιούν το DSR μπορούν να ανατεθούν με οποιονδήποτε μηχανισμό (π.χ. με στατική ανάθεση, ή με χρήση DHCP για δυναμική ανάθεση).

## 4.2 Η βασική Ανακάλυψη Διαδρομής του DSR

Όταν κάποιος κόμβος S παράγει ένα πακέτο που προορίζεται για κάποιον άλλο κόμβο D, τοποθετεί στην επικεφαλίδα του πακέτου τη διαδρομή πηγής η οποία δίνει την ακολουθία των κόμβων που

πρέπει να το προωθήσουν ώστε το πακέτο να φτάσει στον προορισμό D. Αναμενόμενο είναι ο κόμβος S να βρει την κατάλληλη ακολουθία, με μία αναζήτηση στην cache διαδρομών (Route Cache) πού έχει γεμίσει με πληροφορία που απέκτησε κατά το πρόσφατο παρελθόν. Εάν μία διαδρομή για τον προορισμό D δεν βρεθεί αποθηκευμένη στην cache, τότε ενεργοποιείται ο μηχανισμός Ανακάλυψης Διαδρομής για να βρει δυναμικά μια καινούρια διαδρομή προς τον D. Σε μία τέτοια περίπτωση ο κόμβος S θα ονομάζεται *αφετηρία* (initiator) και ο κόμβος D *στόχος* (target) της Ανακάλυψης Διαδρομής.
Για παράδειγμα, ας υποθέσουμε ότι ο κόμβος A στο σχήμα A.4.1 προσπαθεί να ανακαλύψει μία διαδρομή προς τον κόμβο E. Η Ανακάλυψη Διαδρομής που ξεκινά από τον A θα είχε ως εξής:

Ο κόμβος A εκπέμπει ένα μήνυμα Αίτησης Διαδρομής (Route Request) μέσω ενός πακέτου τοπικής ευρυπομπής (broadcast), το οποίο λαμβάνεται από όλους τους κόμβους στην ακτίνα ασύρματης επικοινωνίας του A, συμπεριλαμβανομένου και του κόμβου B στο παράδειγμα του σχήματος A.4.1. Κάθε μήνυμα Αίτησης Διαδρομής προσδιορίζει ρητά την αφετηρία και τον στόχο της Ανακάλυψης Διαδρομής και φέρει ένα μοναδικό προσδιοριστικό αίτησης (request identification) –στο παράδειγμα μας τον αριθμό 2, το οποίο προσδιορίζεται από την αφετηρία της Αίτησης. Επίσης, κάθε μήνυμα Αίτησης Διαδρομής, περιλαμβάνει ένα κατάλογο με τη λίστα των ενδιάμεσων κόμβων από τους οποίους έχει ήδη προωθηθεί το συγκεκριμένο αντίγραφο της Αίτησης. Η λίστα αυτή αρχικοποιείται από τον κόμβο της αφετηρίας. Στο παράδειγμα μας αρχικά η λίστα περιλαμβάνει μόνο τον κόμβο A.




Σχήμα A.4.1: *Βασική Ανακάλυψη διαδρομής από τον κόμβο A στον κόμβο E.*

Όταν ένας κόμβος λάβει μία τέτοια Αίτηση Διαδρομής (για παράδειγμα στο σχήμα A.4.1 πρώτος ο κόμβος B), εάν είναι ο στόχος της Αίτησης τότε επιστρέφει στην αφετηρία ένα μήνυμα Απάντησης Διαδρομής (Route Reply). Η Απάντηση Διαδρομής περιλαμβάνει την συσσωρευμένη πληροφορία διαδρομής που δημιουργήθηκε από την

Αίτηση Διαδρομής της αφετηρίας. Όταν η αφετηρία πάρει την Απάντηση, αποθηκεύει την διαδρομή που περιέχει στην cache Διαδρομών του κόμβου της, ώστε να στείλει μέσω αυτής της τα επόμενα πακέτα που έχουν τον ίδιο προορισμό. Εάν ο κόμβος που πάρει μια Αίτηση έχει δει πρόσφατα ένα αντίγραφο της με ίδιο προσδιοριστικό αίτησης, ίδια αφετηρία και ίδιο στόχο, ή βρει τη δική του διεύθυνση στην λίστα των ενδιάμεσων κόμβων της Αίτησης, τότε την απορρίπτει. Σε κάθε άλλη περίπτωση ο κόμβος αυτός επισυνάπτει την διεύθυνση του στην λίστα των ενδιάμεσων κόμβων της Αίτησης και την προωθεί, μεταδίδοντας την ως τοπικό πακέτο ευρυπομπής διατηρώντας το ίδιο προσδιοριστικό αίτησης. Στο παράδειγμα μας, ο κόμβος Β εκπέμπει την Αίτηση Διαδρομής, η οποία λαμβάνεται από τον C. Οι κόμβοι C και D διαδοχικά εκπέμπουν την Αίτηση με αποτέλεσμα τη λήψη της από τον Ε.

Λαμβάνοντας ο κόμβος Ε μία Αίτηση που τον φέρει ως στόχο, οφείλει να απαντήσει στην αφετηρία στέλνοντας ένα πακέτο Απάντησης Διαδρομής (Route Reply). Τυπικά η διαδικασία που ακολουθείται είναι ότι ο κόμβος Ε εξετάζει την cache διαδρομών του για να βρει μια αποθηκευμένη διαδρομή για τον Α, την οποία θα χρησιμοποιήσει ως διαδρομή πηγής για το πακέτο της Απάντησης, εάν δεν βρει μια τέτοια διαδρομή, ξεκινάει μία δική του Ανακάλυψη Διαδρομής για τον Α. Στην περίπτωση αυτή, για να αποφευκτεί πιθανή ατέρμονη σειρά Ανακαλύψεων Διαδρομής ανάμεσα στους Α και Ε, ο Ε πρέπει να προσαρτήσει την Απάντηση Διαδρομής του για τον Α στην νέα Αίτηση που ξεκίνησε.

Απλούστερα ο Ε θα μπορούσε να χρησιμοποιήσει την ανεστραμμένη ακολουθία των βημάτων που περιγράφει στην απάντηση του ως διαδρομή πηγής για το πακέτο της Απάντησης Διαδρομής. Για πρωτόκολλα 1$^{ου}$ και 2$^{ου}$ επιπέδου OSI, όπως το IEEE 802.11, που απαιτούν την ύπαρξη αμφίδρομων ζεύξεων, αυτή η αναστροφή διαδρομής είναι προφανώς προτιμητέα, καθώς αποφεύγει το overhead μιας πιθανής δεύτερης Ανακάλυψης Διαδρομής.

Όταν ξεκινάει μία διαδικασία Ανακάλυψης Διαδρομής, ο κόμβος πού την ξεκίνησε αποθηκεύει ένα αντίγραφο του αρχικού πακέτου σε έναν τοπικό ενταμιευτή (buffer) που αποκαλείται ενταμιευτής αποστολής (send buffer). Ο ενταμιευτής αποστολής περιέχει ένα αντίγραφο από

κάθε πακέτο που δεν μπόρεσε να αποσταλεί από τον κόμβο διότι δεν υπήρχε διαθέσιμη ακόμα μία διαδρομή πηγής για τον προορισμό του. Μαζί με κάθε πακέτο πού αποθηκεύεται στον ενταμιευτή αποστολής κρατείται και ο χρόνος της αποθήκευσης, ώστε να αποβάλλεται μετά από μία προκαθορισμένη χρονική περίοδο λήξης (timeout). Για να αποφεύγεται η υπερχείλιση του συνήθως χρησιμοποιείται κάποια στρατηγική οργάνωσης του π.χ. τύπου FIFO.

Όσο ένα πακέτο παραμένει στον ενταμιευτή αποστολής, ο κόμβος οφείλει σε συγκε-κριμένες χρονικές στιγμές να εκκινεί την Αναζήτηση Διαδρομής για τον προορισμό του. Ο κόμβος όμως πρέπει να εξασφαλίσει ότι ο ρυθμός με τον οποίο ξεκινούν οι Αναζητήσεις Διαδρομής για τον ίδιο προορισμό είναι περιορισμένος, καθώς είναι πιθανό ο προορισμός αυτός να μην είναι προσβάσιμος και συνεπώς οι συχνές αναζητήσεις να μην φέρουν αποτέλεσμα, παρά μόνο επιβάρυνση στο δίκτυο. Συγκεκριμένα λόγω της περιορισμένης ακτίνας κάλυψης μίας ασύρματης μετάδοσης και της ελευθερίας κίνησης των κόμβων του δικτύου, είναι πιθανό το δίκτυο να διαμεριστεί. Σε μία τέτοια περίπτωση θα υπάρχουν κόμβοι για τους οποίους δεν θα είναι δυνατό να βρεθεί ακολουθία βημάτων για την προώθηση ενός πακέτου ώστε να φτάσει σε κάποιον προορισμό. Η συχνότητα εμφάνισης και το πλήθος τέτοιων διαμερίσεων εξαρτώνται από τον τύπο της κίνησης και την πυκνότητα των κόμβων στο δίκτυο.

Για να ελαττωθεί ο πλεονασμός που θα εισήγαγαν τέτοιες μη καρποφόρες Αναζητήσεις Διαδρομής οι κόμβοι πρέπει να χρησιμοποιούν έναν αλγόριθμο εκθετικής οπισθοχώρησης (exponential back-off), ώστε να περιορίζεται ο ρυθμός με τον οποίο ξεκινούν Αναζητήσεις Διαδρομής για τον ίδιο στόχο. Στην περίπτωση που ένας κόμβος παράγει πακέτα για τον ίδιο στόχο πιο γρήγορα από όσο ο παραπάνω αλγόριθμος έχει θέσει ως όριο, τα ακόλουθα πακέτα μπορούν να ενταμιεύονται στον Send Buffer μέχρι να φτάσει ένα πακέτο από το μηχανισμό Απάντησης Διαδρομής που θα δίνει στον κόμβο μία διαδρομή προς το στόχο· αυτό που δεν πρέπει να γίνει είναι να ξεκινήσει μια νέα Αναζήτηση Διαδρομής προτού παρέλθει το ελάχιστο επιτρεπόμενο διάστημα μεταξύ Αναζητήσεων Διαδρομής.

## 4.3 Συντήρηση Διαδρομών του DSR

Κάθε κόμβος που ξεκινάει την αποστολή ή προωθεί ένα πακέτο κατά μία διαδρομή πηγής είναι υπεύθυνος για να επιβεβαιώσει ότι το πακέτο παραλήφθηκε σωστά από τον επόμενο κόμβο, όπως αυτός περιγράφεται στην διαδρομή πηγής. Το πακέτο μπορεί να αναμεταδοθεί (για έναν περιορισμένο αριθμό επαναλήψεων), ωσότου να ληφθεί επιβεβαίωση παραλαβής του. Για παράδειγμα στο σχήμα Α.4.2 παρακάτω, ο κόμβος Α ξεκινάει την αποστολή ενός πακέτου για τον Ε, χρησιμοποιώντας μία διαδρομή πηγής μέσω των κόμβων Β, C και D.


Σχήμα Α.4.2: *Συντήρηση διαδρομής.*

Εδώ, ο κόμβος Α είναι υπεύθυνος για την παραλαβή του πακέτου από τον κόμβο Β, ο Β για την παραλαβή του πακέτου από τον κόμβο C *κ.ο.κ.*.

Μία επιβεβαίωση παραλαβής σε πολλές περιπτώσεις μπορεί να παρέχεται στο DSR χωρίς κόστος: μία δυνατότητα είναι να εξαχθεί από ρητή επιβεβαίωση του πρωτοκόλλου MAC που χρησιμοποιείται, (για παράδειγμα τα πλαίσια επιβεβαίωσης (acknowledgement frames) επιπέδου ζεύξης όπως ορίζονται στο IEEE 802.11). Μία άλλη δυνατότητα είναι η *παθητική επιβεβαίωση* (passive acknowledgement). Στο παράδειγμα, ο Β θα μπορούσε να επιβεβαιώσει παθητικά τη λήψη του πακέτου από τον C όταν θα τον άκουγε (μέσω του αδιάκριτου μηχανισμού λήψης) να το εκπέμπει για να το προωθήσει στον D. Στην περίπτωση που κανένας από τους παραπάνω μηχανισμούς δεν είναι διαθέσιμος, ο κόμβος που μεταδίδει ένα πακέτο μπορεί να απαιτήσει ρητά από τον επόμενο κόμβο μια επιβεβαίωση πρωτοκόλλου DSR, η οποία στη συνήθη περίπτωση θα μεταδοθεί άμεσα προς τον αρχικό αποστολέα, αλλά στην περίπτωση μονόδρομης ζεύξης επιτρέπεται να περάσει πάνω από διαφορετική διαδρομή που μπορεί να αποτελείται και από περισσότερα βήματα.

Εάν δεν ληφθεί επιβεβαίωση μετά από την τελευταία επιτρεπόμενη αναμετάδοση ενός πακέτου, ο κόμβος που προσπάθησε να προωθήσει το

πακέτο αυτό οφείλει να επιστρέψει στον αρχικό αποστολέα του πακέτου, ένα μήνυμα Σφάλματος Διαδρομής (Route Error) με το οποίο προσδιορίζεται η ζεύξη πάνω από την οποία δεν μπόρεσε να προωθήσει το πακέτο του. Στο παράδειγμα του σχήματος Α.4.2, εάν ο C δεν μπορεί να παραδώσει στον D το πακέτο του A, τότε ο C επιστρέφει στον A ένα Σφάλμα Διαδρομής που δηλώνει ότι η ζεύξη από τον C στον D είναι κομμένη. Ο κόμβος A λαμβάνοντας το Σφάλμα Διαδρομής, αφαιρεί από την cache διαδρομών του την κομμένη ζεύξη C-D. Αναμεταδόσεις του χαμένου αρχικού πακέτου πραγματοποιούνται, εάν απαιτούνται, από πρωτόκολλα υψηλότερων επιπέδων όπως για παράδειγμα το TCP. Για την αποστολή αναμεταδιδόμενων ή νέων πακέτων στον ίδιο προορισμό Ε εάν ο A έχει στην cache διαδρομών του μία άλλη διαδρομή για τον Ε μπορεί να την χρησιμοποιήσει για να ξεκινήσει την αποστολή άμεσα. Διαφορετικά θα πρέπει να ξεκινήσει μια νέα Ανακάλυψη Διαδρομής για τον στόχο Ε όπως περιγράφηκε στο προηγούμενο τμήμα αυτής της παραγράφου.

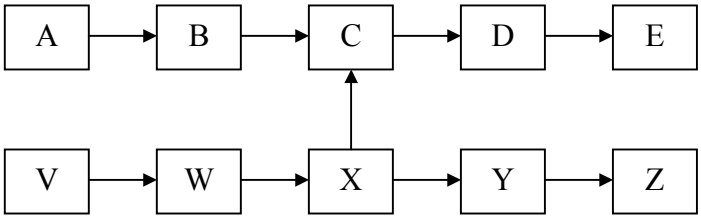
## 4.4 Πρόσθετα χαρακτηριστικά Ανακάλυψης Διαδρομής

### 4.4.α. *Αποθήκευση έμμεσης πληροφορίας δρομολόγησης*

Ένας κόμβος που προωθεί ή κρυφακούει ένα πακέτο μπορεί να προσθέσει την πληροφορία δρομολόγησης του πακέτου αυτού στην cache διαδρομών του. Συγκεκριμένα, η διαδρομή πηγής που περιέχεται στην επικεφαλίδα ενός πακέτου δεδομένων, η συσσωρευμένη λίστα ενδιάμεσων κόμβων διαδρομής μίας Αίτησης Διαδρομής, ή η διαδρομή που επιστρέφεται με μία Απάντηση Διαδρομής, μπορούν να αποθηκευτούν από οποιονδήποτε κόμβο. Γενικά, οποιαδήποτε πληροφορία δρομολόγησης που περιέχεται σε ένα πακέτο από τα παραπάνω μπορεί να αποθηκευτεί ανεξάρτητα από το αν το πακέτο δεν προοριζόταν για τον κόμβο που το χειρίζεται, αν το πακέτο είχε σταλεί σε μία διεύθυνση ευρυπομπής ή εάν η κάρτα δικτύου του κόμβου είναι ρυθμισμένη για αδιάκριτη λήψη.

Ένας περιορισμός για την αποθήκευση τέτοιας έμμεσης πληροφορίας δρομολόγησης είναι η πιθανή ύπαρξη μονόδρομων ζεύξεων. Για παράδειγμα στο σχήμα Α.4.3 ο κόμβος A στέλνει ένα πακέτο με την διαδρομή πηγής A→B→C→D→E για να επικοινωνήσει με τον κόμβο Ε. Καθώς το προωθεί, ο C μπορεί να προσθέσει στην cache του την ύπαρξη των επόμενων ζεύξεων: από τον εαυτό του στον D καθώς και

από τον D στον E. Όμως, η ανάστροφη διαδρομή προηγούμενων ζεύξεων που εμφανίζονται στο πακέτο (από τον C στον B, και από τον B στον A), ενδέχεται να μην λειτουργεί καθώς οι ζεύξεις αυτές μπορεί να είναι μονόδρομες. Εάν ο C γνωρίζει ότι οι ζεύξεις είναι πράγματι αμφίδρομες, για παράδειγμα στηριζόμενος σε γνώση του πρωτοκόλλου επιπέδου ζεύξης που χρησιμοποιείται, τότε μπορεί να τις αποθηκεύσει, σε άλλη περίπτωση δεν θα πρέπει να το κάνει.




Σχήμα Α.4.3: *Ο Α στέλνει ένα πακέτο στον Ε με την διαδρομή πηγής A→B→C→D→E. Με αυτό ο C μπορεί να μάθει την ύπαρξη των ζεύξεων C→D και D→E.*

Όμοια ο κόμβος V του σχήματος Α.4.3 στέλνει δεδομένα με τη διαδρομή V→W→X→Y→Z στον Z. Εάν ο C κρυφακούσει τον X να προωθεί ένα τέτοιο πακέτο στον Y τότε, προτού προσπαθήσει να αποθηκεύσει οποιαδήποτε πληροφορία δρομολόγησης, ο κόμβος C πρέπει να λάβει υπόψη του εάν οι σχετικές ζεύξεις είναι αμφίδρομες ή όχι. Στην περίπτωση για παράδειγμα που ο C γνωρίζει (ή μπορεί έμμεσα να συνάγει) ότι η ζεύξη με τον X που ανακάλυψε είναι αμφίδρομη, τότε από ένα τέτοιο πακέτο μπορεί να αποθηκεύσει αυτή τη ζεύξη του με τον X, την ζεύξη του X με τον Y και την ζεύξη του Y με τον Z. Εάν επίσης γνώριζε ότι όλες οι ζεύξεις είναι αμφίδρομες, τότε θα μπορούσε να αποθηκεύσει και τις ζεύξεις C→X, X→W, W→V. Όμοιο σκεπτικό εφαρμόζεται σε πληροφορία δρομολόγησης που μπορεί να γίνει γνωστή από πακέτα των άλλων τύπων που περιγράψαμε πιο πάνω.

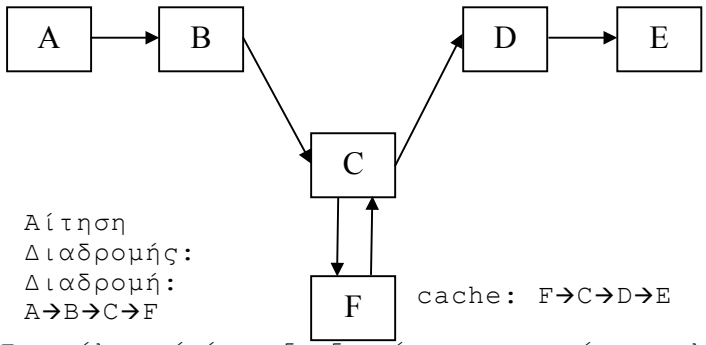
### 4.4.β. *Απάντηση σε Αιτήσεις Διαδρομών με χρήση αποθηκευμένων διαδρομών*

Όταν ένας κόμβος πάρει μία Αίτηση Διαδρομής για την οποία δεν είναι ο αυτός ο στόχος, ψάχνει στην cache του για μία διαδρομή στον στόχο της Αίτησης, εάν βρει μία τέτοια διαδρομή αποθηκευμένη, ο κόμβος αυτός στη γενική περίπτωση επιστρέφει μία Απάντηση Διαδρομής στην αφετηρία αντί να προωθήσει την Αίτηση παραπέρα. Στην Απάντηση Διαδρομής, θέτει ως διαδρομή την μέχρις

αυτόν διαδρομή της Αίτησης, ακολουθούμενη από την διαδρομή προς τον στόχο που βρήκε στην cache του. Προτού όμως ο κόμβος στείλει αυτό το πακέτο Απάντησης Διαδρομής, πρέπει να βεβαιωθεί ότι η συνολική διαδρομή όπως περιγράφηκε πιο πριν δεν έχει κάποιο κόμβο δύο φορές.

Για παράδειγμα στο σχήμα Α.4.4 παρακάτω βλέπουμε μία περίπτωση στην οποία μία Αίτηση Διαδρομής για τον στόχο Ε, παραλήφθηκε από τον κόμβο F ο οποίος ήδη είχε στην cache του μία διαδρομή προς τον Ε αλλά τελικά δεν θα μπορέσει να απαντήσει.

Η διαδρομή που προκύπτει με την επισύναψη της αποθηκευμένης διαδρομής της cache του F στην διαδρομή από την Αίτηση Διαδρομής θα περιλάμβανε για δεύτερη φορά τον κόμβο C. Έτσι ο F θα μπορούσε στην περίπτωση αυτή να τροποποιήσει την διαδρομή για να εξαλείψει τον βρόγχο C→F→C που εμφανίζεται, επιστρέφοντας τελικά ως διαδρομή το A→B→C→D→E. Όμως τότε ο F δεν θα παρουσιαζόταν στην διαδρομή που επέστρεψε με δική του Απάντηση Διαδρομής. Ο μηχανισμός Ανακάλυψης Διαδρομής του DSR *απαγορεύει* στον κόμβο να επιστρέψει μια τέτοιου τύπου Απάντηση Διαδρομής από την cache του για λόγους που αφορούν στην συνέπεια των διαδρομών που δημιουργούνται κατ' αυτό τον τρόπο.




Σχήμα Α.4.4: *Ο F παρόλο πού έχει διαδρομή για τον στόχο, τελικά δεν θα μπορέσει να απαντήσει, διότι ή θα δημιουργούσε βρόγχο στη διαδρομή ή θα έδινε διαδρομή χωρίς να είναι σε αυτήν .*

### 4.4.γ. *Αποφυγή καταιγισμού Απαντήσεων Διαδρομών:*

Η δυνατότητα των κόμβων να παρέχουν σε Αιτήσεις Διαδρομών απαντήσεις από την cache διαδρομών τους, όπως περιγράφηκε στην προηγούμενη παράγραφο, μπορεί να έχει ως αποτέλεσμα ένα καταιγισμό απαντήσεων (route reply storm) σε ορισμένες

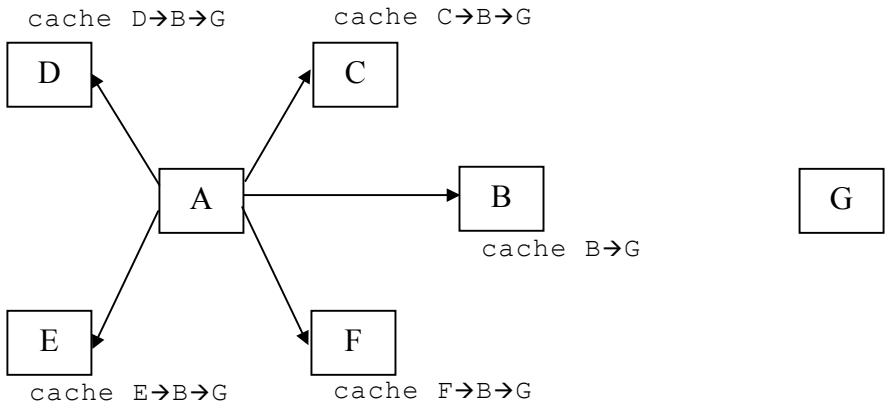
περιπτώσεις. Συγκεκριμένα, εάν ένας κόμβος εκπέμψει μία Αίτηση Διαδρομής για έναν στόχο, για τον οποίο οι γείτονες του κόμβου αυτού έχουν διαδρομές στις cache διαδρομών τους, τότε ακόμη και όλοι οι γείτονες μπορεί να προσπαθήσουν να απαντήσουν, κατασπαταλώντας πόρους και πιθανώς αυξάνοντας τις συγκρούσεις τοπικά.

Για παράδειγμα στο παρακάτω σχήμα βλέπουμε μία περίπτωση στην οποία οι κόμβοι B, C, D, E και F λαμβάνουν την Αίτηση Διαδρομής του A για το στόχο G και ο καθένας από αυτούς έχει αποθηκευμένη μια διαδρομή για τον στόχο αυτό.

Θα μπορούσαν όλοι τους να προσπαθήσουν να απαντήσουν από την δική τους cache διαδρομών ο καθένας και συνεπώς θα έστελναν τις απαντήσεις τους την ίδια περίπου στιγμή, καθώς όλοι τους έλαβαν την Αίτηση Διαδρομής που εξέπεμψε ο A περίπου την ίδια χρονική στιγμή. Τέτοιες ταυτόχρονες απαντήσεις από διαφορετικούς κόμβους πού έλαβαν την Αίτηση Διαδρομής μπορεί στην χείριστη περίπτωση να προκαλέσει συγκρούσεις πακέτων μεταξύ όλων των απαντήσεων, ή σε μία πιο ευνοϊκή περίπτωση τοπική συμφόρηση στο δίκτυο. Επίσης διαφορετικές απαντήσεις θα περιέχουν πιθανότατα διαδρομές με διάφορα μήκη, όπως στο παράδειγμα εδώ.

Εάν ένας κόμβος που μπορεί να θέσει την κάρτα δικτύου του σε αδιάκριτο μηχανισμό λήψης, θα μπορούσε να καθυστερήσει την αποστολή της δικής του απάντησης για μία σύντομη περίοδο, περιμένοντας και ακούγοντας το κανάλι για να δει εάν ο κόμβος στον οποίο θα απαντήσει άρχισε εντωμεταξύ να χρησιμοποιεί κάποια μικρότερη διαδρομή πρώτα. Ο κόμβος θα μπορούσε να καθυστερήσει την δική του Απάντηση Διαδρομής για μία τυχαία χρονική διάρκεια $d = H \cdot (h - 1 + r)$ , όπου $h$ είναι το μήκος της διαδρομής που σκοπεύει να επιστρέψει -σε αριθμό βημάτων, $H$ μια μικρή σταθερή καθυστέρηση – κατ' ελάχιστο διπλάσια της καθυστέρησης διάδοσης ζεύξης και $r$ ένας τυχαίος αριθμός μεταξύ 0 και 1. Αυτή η καθυστέρηση με επιτυχία δημιουργεί συνθήκες τυχαιότητας για τον χρόνο κατά τον οποίο ο κάθε κόμβος στέλνει την δική του Απάντηση Διαδρομής και μάλιστα όλοι οι κόμβοι που στέλνουν διαδρομές με μήκος μικρότερο του $h$ στέλνουν την απάντηση τους πριν από τον κόμβο αυτό, ενώ κόμβοι με

διαδρομές με μήκος μεγαλύτερο του $h$ στέλνουν την απάντηση τους μετά τον κόμβο αυτό. Στην διάρκεια αυτής της καθυστέρησης $d$ ο κόμβος παρακολουθεί με τον αδιάκριτο μηχανισμό να δει αν θα λάβει πακέτα δεδομένων από την αφετηρία της Αίτησης με προορισμό το στόχο της Αίτησης. Εάν όντως ο κόμβος λάβει ένα τέτοιο πακέτο κατά τη διάρκεια του χρόνου $d$, το οποίο χρησιμοποιεί μία διαδρομή πηγής με μήκος μικρότερο ή ίσο του $h$ τότε συμπεραίνει ότι η αφετηρία έλαβε ήδη μία Απάντηση Διαδρομής, η οποία παρείχε μία τουλάχιστον εξίσου σύντομη διαδρομή. Σε αυτήν την περίπτωση ο κόμβος αυτός θα πρέπει να ακυρώσει την αποστολή της Απάντησης




Διαδρομής πού ετοίμασε για αυτή την Ανακάλυψη Διαδρομής.

Σχήμα Α.4.5: *Ο Α στέλνει μία αίτηση διαδρομής για τον G. Οι γείτονές του έχουν αποθηκευμένη ο καθένας μια διαδρομή για τον G, πράγμα που μπορεί να προκαλέσει καταιγισμό απαντήσεων*

### 4.4.δ. *Όριο βημάτων (hop limit) Αίτησης Διαδρομής*

Κάθε μήνυμα Αίτησης Διαδρομής περιέχει ένα όριο βημάτων που μπορεί να χρησιμοποιηθεί για να περιορίσει τον αριθμό των ενδιάμεσων κόμβων που επιτρέπεται να προωθήσουν ένα αντίγραφο του μηνύματος. Η υλοποίηση του πεδίου αυτού σύμφωνα με το πρωτόκολλο, πραγματοποιείται χρησιμοποιώντας το πεδίο TTL (Time-To-Live) της IP επικεφαλίδας του πακέτου που μεταφέρει την Αίτηση Διαδρομής. Καθώς προωθείται η Αίτηση, αυτό το όριο ελαττώνεται και το πακέτο της Αίτησης απορρίπτεται όταν το όριο φτάσει στο μηδέν προτού βρεθεί ο στόχος.

Αυτό το όριο βημάτων μπορεί να χρησιμοποιηθεί για να υλοποιήσει μια πληθώρα από αλγορίθμους για έλεγχο της εξάπλωσης της Αίτησης Διαδρομής σε μια Ανακάλυψη Διαδρομής. Για παράδειγμα ένας κόμβος μπορεί να στείλει το πρώτο πακέτο Αίτησης Διαδρομής για έναν στόχο θέτοντας όριο βημάτων ίσο με 1 ώστε όποιος κόμβος λάβει την αρχική μετάδοση της αφετηρίας να μην το προωθήσει. Αυτού του τύπου η Αίτηση Διαδρομής χαρακτηρίζεται ως *μη διαδοτική* (non-propagating) και παρέχει μια ανέξοδη μέθοδο για να προσδιοριστεί εάν ο στόχος είναι γειτονικός κόμβος της αφετηρίας ή έστω εάν ένας γειτονικός κόμβος της αφετηρίας έχει αποθηκευμένη μία διαδρομή για το στόχο. Εάν μια Απάντηση Διαδρομής δεν ληφθεί μετά από μια προκαθορισμένη χρονική περίοδο λήξης, τότε μία *διαδοτική* Αίτηση Διαδρομής (χωρίς όριο βημάτων) στέλνεται.

Μία άλλη δυνατή χρήση του ορίου βημάτων είναι στην υλοποίηση μίας αναζήτησης «διαστελλώμενου δακτυλίου» για το στόχο. Για παράδειγμα, η αφετηρία μπορεί στην αρχή να στείλει μία μη διαδοτική αίτηση όπως περιγράφηκε παραπάνω, εάν δεν ληφθεί καμία Απάντηση Διαδρομής, τότε θα στείλει μία νέα Αίτηση Διαδρομής με όριο βημάτων ίσο με 2. Για κάθε Αίτηση Διαδρομής που ξεκινά, εάν δεν ληφθεί απάντηση, η αφετηρία διπλασιάζει το όριο βημάτων που χρησιμοποιήθηκε στην προηγούμενη απόπειρα, ώστε προοδευτικά να αναζητά όλο και πιο μακριά τον στόχο, χωρίς όμως να αφήνεται η Αίτηση Διαδρομής να διαδίδεται σε ολόκληρο το δίκτυο. Ωστόσο, αυτή η μέθοδος αναζήτησης διαστελλώμενου δακτυλίου μπορεί να έχει ως αποτέλεσμα την αύξηση της μέσης καθυστέρησης της Ανακάλυψης Διαδρομής, καθώς πολλαπλές απόπειρες Ανακάλυψης Διαδρομής με τους αντίστοιχους χρόνους αναμονής ενδέχεται να χρειαστούν προτού να βρεθεί διαδρομή για το στόχο.

## 4.5 Πρόσθετα χαρακτηριστικά Συντήρησης Διαδρομής

### 4.5.α *Διάσωση πακέτων*

Αφού στείλει ένα μήνυμα Σφάλματος Διαδρομής κατά τη λειτουργία του μηχανισμού Συντήρησης Διαδρομής, όπως περιγράφηκε στην παράγραφο 4.3, ο κόμβος μπορεί να προσπαθήσει να διασώσει αντί απλά να απορρίψει το πακέτο δεδομένων που προξένησε το Σφάλμα Διαδρομής. Για να το κάνει αυτό αναζητά στην cache του μία διαφορετική διαδρομή από τον ίδιο προς τον προορισμό του πακέτου δεδομένων. Εάν βρεθεί μια τέτοια διαδρομή, ο

κόμβος μπορεί, αφότου στείλει το Σφάλμα Διαδρομής, να προσπαθήσει να διασώσει το πακέτο αντικαθιστώντας το κατάλληλο τμήμα της αρχικής διαδρομής πηγής του, με τη διαδρομή που αυτός έχει βρήκε στην cache του. Στη συνέχεια προωθεί το πακέτο κατά τη νέα διαδρομή πηγής. Για παράδειγμα στο σχήμα Α.4.2 εάν ο κόμβος C έχει αποθηκευμένη μία διαφορετική διαδρομή για τον κόμβο E, μπορεί να διασώσει το πακέτο, χρησιμοποιώντας αυτήν αντί να το απορρίψει.

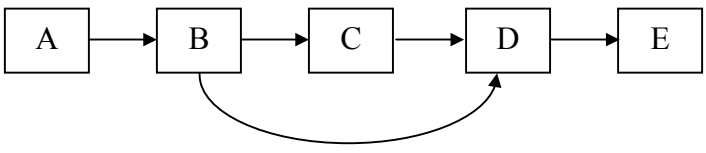
Διασώζοντας ένα πακέτο κατ' αυτόν τον τρόπο, πρέπει να κρατείται ένας μετρητής στο πακέτο που θα γνωρίζει τον αριθμό των διασώσεων του πακέτου, ώστε να αποφεύγεται η συνεχής διάσωση του ίδιου πακέτου. Διαφορετικά θα ήταν δυνατό να έμπαινε το πακέτο σε ένα βρόγχο διαδρομών, όπου διάφοροι κόμβοι θα έσωζαν το πακέτο αλλάζοντας τις διαδρομές πηγής με διαδρομές δικές τους.

### 4.5.β *Αυτόματη συντόμευση διαδρομών*

Οι χρησιμοποιούμενες διαδρομές μπορούν να συντομευτούν αυτόματα εάν ένα ή και περισσότερα βήματα δεν έχουν λόγο ύπαρξης πλέον. Αυτός ο μηχανισμός αυτόματης συντόμευσης διαδρομών είναι παρόμοιος με την χρήση των παθητικών επιβεβαιώσεων που αναφέραμε πιο πάνω. Συγκεκριμένα, εάν ένας κόμβος κρυφακούσει ένα πακέτο που έχει κάποια διαδρομή πηγής, τότε ελέγχει το μη χρησιμοποιημένο τμήμα της. Εάν βρει τον εαυτό του σε θέση μακρινότερη από αυτή του επόμενου βήματος, τότε συνάγει ότι οι κόμβοι που καταγράφονται μεταξύ του αποστολέα του πακέτου και του ίδιου στην διαδρομή πηγής του πακέτου δεν είναι πλέον αναγκαίοι.

Για παράδειγμα έστω ότι στο σχήμα Α.4.6 ο κόμβος D κρυφακούει ένα πακέτο δεδομένων (data packet) που μεταδίδεται από τον B προς τον C, για να προωθηθεί αργότερα στον D και τέλος στον E.

Σε αυτήν την περίπτωση ο κόμβος D στέλνει μια *χαριστική απάντηση διαδρομής* (gratuitous route reply) στην πηγή του πακέτου -τον κόμβο A. Αυτή η απάντηση διαδρομής φέρει την συντομευμένη διαδρομή A→B→D→E.



Σχήμα Α.4.6: *Ο Β προωθεί στον C ένα πακέτο δεδομένων για τον Ε με διαδρομή πηγής Α→Β→C→D→Ε. Ο D το κρυφακούει πριν από τον C, άρα ο C δεν χρειάζεται πια στην διαδρομή*

### 4.5.γ. *Αυξημένη διάδοση μηνυμάτων Σφάλματος Διαδρομής*

Όταν μία πηγή λάβει ένα Σφάλμα Διαδρομής για ένα πακέτο δεδομένων που είχε στείλει, μπορεί να επισυνάψει το μήνυμα του σφάλματος στο επόμενο μήνυμα Αίτησης Διαδρομής ενημερώνοντας έτσι τους γείτονες της. Έτσι παλαιωμένη πληροφορία που μπορεί να υπάρχει στις caches των γειτόνων της πηγής δεν θα προκαλέσει Απαντήσεις Διαδρομής με την κομμένη ζεύξη από την οποία προξενήθηκε το αρχικό Σφάλμα Διαδρομής.

Για παράδειγμα στο σενάριο του σχήματος Α.4.2 ο κόμβος Α μαθαίνει μέσω του μηνύματος Σφάλματος Διαδρομής από τον C ότι η ζεύξη C→D έχει κοπεί. Συνεπώς αφαιρεί αυτή τη ζεύξη από την δική του cache διαδρομών και ξεκινάει μία νέα Ανακάλυψη Διαδρομής –στην περίπτωση που δεν έχει εναλλακτική διαδρομή για τον Ε αποθηκευμένη. Στο πακέτο Αίτησης Διαδρομής ο Α επισυνάπτει ένα αντίγραφο αυτού του μηνύματος Σφάλματος Διαδρομής, εξασφαλίζοντας έτσι ότι (α) το μήνυμα αυτό φτάνει έμμεσα σε αρκετούς παραπάνω κόμβους και (β) ότι καμία απάντηση διαδρομής από αυτές που θα πάρει δεν θα έχει την κομμένη ζεύξη.

## 5. Ανάρμοστη συμπεριφορά κόμβων σε Αδόμητα δίκτυα

Τα αδόμητα ασύρματα δίκτυα μεγιστοποιούν το ολικό throughput χρησιμο-ποιώντας όλους τους διαθέσιμους κόμβους για τις υπηρεσίες της ανακάλυψης διαδρομών και της προώθησης πακέτων. Συνεπώς όσο περισσότεροι κόμβοι συμμετέχουν στην δρομολόγηση των πακέτων, τόσο μεγαλύτερο θα είναι το συνολικό εύρος φάσματος, τόσο μικρότερα θα είναι τα δυνατά μονοπάτια δρομολόγησης, τόσο μικρότερη θα είναι η πιθανότητα διαμέρισης του δικτύου. Παρόλα αυτά ένας κόμβος ενδέχεται να *επιδείξει ανάρμοστη συμπεριφορά* (misbehave), υποσχόμενος να προωθήσει πακέτα, χωρίς πράγματι στη συνέχεια να το κάνει. Διάφοροι λόγοι μπορεί να τον οδηγήσουν σε μία τέτοια συμπεριφορά:

- *Κακία* (maliciousness): ο κόμβος προσπαθεί ενεργά να μειώσει τις επιδώσεις του δικτύου, εκτελώντας *επιθέσεις άρνησης υπηρεσίας* (denial of service attacks)
- *Εγωισμός* (selfishness): ο κόμβος προσπαθεί να διασώσει τους πόρους του (ενέργεια, κύκλους CPU, bandwidth) για δική του χρήση, έτσι δεν θεωρεί σκόπιμο να προωθήσει πακέτα που δεν του ανήκουν.
- Εγγενή προβλήματα: ο κόμβος μπορεί να έχει χαλάσει, να είναι υπερφορτωμένος κοκ.

Οι ίδιοι λόγοι μπορούν να οδηγήσουν έναν κόμβο στο να μη συμμετέχει στις διαδικασίες ανακάλυψης διαδρομής.

Όπως μελέτησαν οι R. Molva και S. Marti στα [14] και [11] αντίστοιχα, οι κόμβοι που δεν συνεργάζονται αποτελούν σημαντικό πρόβλημα στο δίκτυο, ελαττώνοντας το μέσο ρυθμό μετάδοσης, αυξάνοντας παράλληλα την πλεονάζουσα πληροφορία.

## 5.1 Συγκεκριμένα προβλήματα από ανάρμοστες συμπεριφορές κόμβων στο DSR.

Κόμβοι οι οποίοι επιθυμούν να επιδείξουν κακή συμπεριφορά (maliciousness) στον DSR έχουν πολλές και ιδιαίτερα εύκολες επιλογές για να το κάνουν, εκτελώντας επιθέσεις στο επίπεδο της δρομολόγησης. Σημειώνεται ότι τέτοιοι κόμβοι δεν πρέπει να ενδιαφέρονται για τίποτα άλλο εκτός από το να υποβαθμίσουν το δίκτυο, καθώς οι ενεργές επιθέσεις είναι αρκετά απαιτητικές σε πόρους.

### 5.1.α. *Διαφήμιση ψευδών διαδρομών*

Ένας κόμβος μπορεί σε μία Αίτηση Διαδρομής να απαντήσει με μία ψευδή διαδρομή. Ο αρχικός κόμβος και όλοι οι ενδιάμεσοι ενημερώνονται με το πακέτο Απάντησης και ως αποτέλεσμα το επόμενο πακέτο δεδομένων που θα αποσταλεί σε αυτήν τη διαδρομή, θα προκαλέσει σφάλμα, στον «κακό» κόμβο. Ο «κακός» κόμβος τότε μπορεί να ενημερώσει για αυτό προκαλώντας μια νέα Αίτηση Διαδρομής από Σφάλμα. Την αίτηση αυτή με μεγάλη πιθανότητα θα

απαντήσει ο ίδιος (εκτός προλάβει εάν κάποιος ορθά συνεργαζόμενος κόμβος χάρη σε δυναμική τοπολογία) δίνοντας την ίδια διαδρομή και ξεκινώντας έτσι έναν ατέρμονο βρόγχο.

Η παραπάνω μορφή αυτής της επίθεσης μπορεί να πραγματοποιηθεί ακόμα πιο καταστροφικά με χρήση των χαριστικών απαντήσεων που δεν τις προκαλούν Αιτήσεις διαδρομής.

### 5.1.β. *Μετάδοση ψευδών πακέτων Σφάλματος Διαδρομής*

Ένας κόμβος μπορεί, ακόμα και σε κάθε πακέτο δεδομένων που του φτάνει για το προωθήσει να απαντάει στην πηγή με ένα πακέτο Σφάλματος Διαδρομής. Με τον τρόπο αυτό μπορεί να αποκόψει όσες διαδρομές συμμετέχει προκαλώντας πιθανών διαμέριση του δικτύου.

Το εγγενές πρόβλημα με επιθέσεις στον DSR όπως οι δύο που αναφέρθηκαν παραπάνω είναι ότι είναι πρακτικά αδύνατο να εντοπιστεί ως αίτιο τους η επιλογή της κακής συμπεριφοράς του κόμβου, λόγω των υποθέσεων καλής συμμετοχής και κινητικότητας των κόμβων.

### 5.1.γ. *Αλλοίωση προωθούμενων μηνυμάτων*

Ένας κόμβος μπορεί να αλλοιώσει την διαδρομή πηγής που μεταφέρεται σε οποιοδήποτε πακέτο καλείται να προωθήσει. Αυτή η στρατηγική μπορεί να προκαλέσει σοβαρά προβλήματα, όταν η αλλοίωση γίνει σε τελευταία βήματα μεγάλων διαδρομών πηγής, από έναν κόμβο κοντά στην πηγή.

Αυτής της μορφής η επίθεση μπορεί να αποφευχθεί με την χρήση κρυπτογράφησης της πληροφορίας δρομολόγησης που προσθέτει ο κάθε κόμβος σε ένα πακέτο, εισάγοντας όμως τεράστια επιπρόσθετη πληροφορία.

Οι παραπάνω επιθέσεις προϋπόθεταν την ενεργή συμμετοχή του κόμβου σε αυτές. Αντίθετα ένας κόμβος που δεν επιθυμεί να καταναλώσει ενέργεια πάλι μπορεί να βλάψει το δίκτυο φερόμενος εγωιστικά.

### 5.1.δ. *Αποχή από την Ανακάλυψη Διαδρομής*

Ένας κόμβος μπορεί παρόλο που έχει την απαιτούμενη πληροφορία δρομολόγησης στην cache διαδρομών του να μην την

χρησιμοποιήσει για να απαντήσει σε μία αίτηση διαδρομής. Με τον τρόπο αυτό ο κόμβος αυτός εξασφαλίζει ότι (α) δεν θα «σπαταλήσει» πόρους για αυτό το πακέτο αλλά κυριότερα ότι (β) γλιτώνει την προώθηση του πακέτου δεδομένων που προκάλεσε την Αίτηση Διαδρομής αλλά και των πακέτων που θα του ζητούσαν όσοι κόμβοι μάθαιναν στο μέλλον αυτήν τη διαδρομή.

Η συμπεριφορά αυτή γίνεται ιδιαίτερα σοβαρή εάν η υλοποίηση του DSR δεν χρησιμοποιεί το μηχανισμό αποθήκευσης έμμεσης πληροφορίας δρομολόγησης. Σε μία τέτοια περίπτωση, ένας κόμβος, όπως περιγράφηκε παραπάνω, που δεν συμμετέχει στην ανακάλυψη διαδρομής μπορεί να μείνει για πάντα στα άκρα διαδρομών, και ποτέ να μην του ζητηθεί να προωθήσει πακέτα, ενώ τοπολογικά θα είχε την δυνατότητα να το κάνει. Μία τέτοια συμπεριφορά σε μία τέτοια υλοποίηση του DSR δεν είναι δυνατό να ανιχνευθεί, εκτός εάν οι cache διαδρομών οργανωθεί με την μορφή γράφων και χρησιμοποιηθούν τεχνικές αυτόματης συμπλήρωσης συνδέσμων, πράγμα το οποίο θα είχε μεγάλο υπολογιστικό κόστος για κόμβους ενός ασύρματου αδόμητου δικτύου.

### 5.1.ε. *Άρνηση Προώθησης Πακέτων*

Ένας κόμβος μπορεί να απορρίψει, ένα πακέτο στου οποίου τη διαδρομή πηγής φέρεται ως ο επόμενος παραλήπτης και έχει την υποχρέωση να το προωθήσει. Έτσι, ο κόμβος αυτός και εδώ εξοικονομεί την ενέργεια που θα απαιτούσε η προώθηση του πακέτου, αλλά και το εύρος ζώνης που θα μπορέσει να χρησιμοποιήσει για δική του κίνηση δεδομένων.

Η συμπεριφορά αυτή δημιουργεί το πρόβλημα διότι δεν γίνεται άμεσα αντιληπτή στο επίπεδο του DSR, καθώς ο αποστολέας του πακέτου λαμβάνοντας την επιβεβαίωση λήψης από τον εγωιστή κόμβο υποθέτει ότι το πακέτο προωθήθηκε κανονικά. Ιδιαίτερα όταν πάνω από μια τέτοια διαδρομή προσπαθήσει ένας κόμβος να στείλει κίνηση TCP τα προβλήματα θα ήταν ιδιαίτερα ενδιαφέροντα λόγω των μηχανισμών αξιόπιστης παράδοσης και του έλέγχου ροής [11].

Η ανίχνευση μίας τέτοιας συμπεριφοράς είναι σχετικά εύκολη υπό την προϋπόθεση αδιάκριτης λήψης: ένας κόμβος που ζητάει από έναν γείτονα του να προωθήσει ένα πακέτο προς έναν απομακρυσμένο

προορισμό, δεν έχει παρά να παρατηρήσει εάν ο γείτονας πράγματι προώθησε το πακέτο σε ένα εύλογο χρονικό διάστημα.

## 5.2 Σχετικές Εργασίες

Αρκετές εργασίες έχουν παρουσιαστεί τα τελευταία χρόνια, όπου αντιμετωπίζουν την ανάρμοστη συμπεριφορά κόμβων σε αδόμητα ασύρματα δίκτυα. Δεδομένης της ομοιότητας των δικτύων αυτών με peer-to-peer δίκτυα, Αναζητήσαμε παρόμοιες εργασίες και σε αυτόν τον τομέα. Εδώ παρουσιάζουμε δύο εργασίες σχετικές με μηχανισμούς αντιμετώπισης ανάρμοστων συμπεριφορών κόμβων, από την οπτική των αδόμητων δικτύων, αλλά και μία ακόμη από την οπτική των δικτύων peer-to-peer.

### 5.2.α *CONFIDANT*

Το πρωτόκολλο CONFIDANT [12] (**C**ooperation **O**f **N**odes: **F**airness **I**n **D**ynamic **A**d Hoc **N**e**T**works), βασίζεται στον επιλεκτικό αλτρουισμό και τον ωφελιμισμό. Ο στόχος του πρωτοκόλλου είναι να εντοπίσει και να απομονώσει τους κόμβους ενός δικτύου με δρομολόγηση DSR που συμπεριφέρονται κακά, ώστε στερώντας τους από τα οφέλη κακών συμπεριφορών, να κάνει την συνεργασία των κόμβων σε ένα τέτοιο δίκτυο ελκυστική.

Οι Buchegger και Boudec αντλώντας εμπειρία από οικολογικά παραδείγματα στηρίζονται στο ότι ο ανταποδοτικός αλτρουισμός είναι ωφέλιμος σε συστήματα όπου μία εξυπηρέτηση ανταποδίδεται άμεσα, άρα υπάρχει εγγενώς το κίνητρο συνεργασίας λόγω της άμεσης ικανοποίησης. Αντίθετα τα οφέλη της καλής συνεργασίας δεν είναι τόσο προφανή όταν υπάρχει καθυστέρηση ανάμεσα στην παροχή μίας εξυπηρέτησης και στην ανταπόδοση της. Ο ισχυρισμός τους είναι ότι κάτι ανάλογο συμβαίνει και στα MANET, όπου οι κόμβοι προωθούν πακέτα για λογαριασμό άλλων.

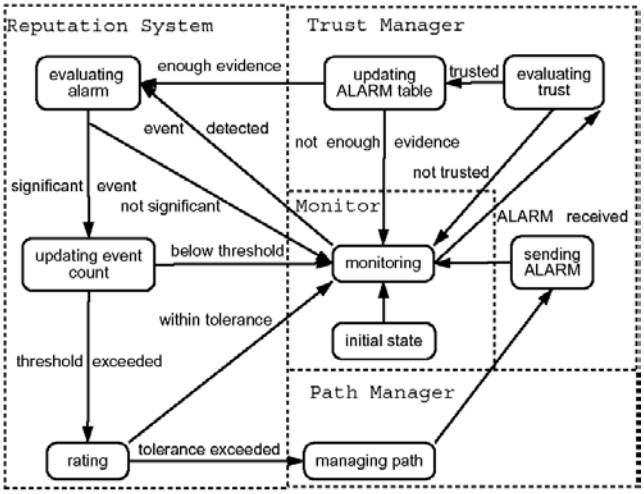
Έτσι, για χάρη οικονομίας πόρων, προτείνουν δύο βασικές ιδέες πάνω στις οποίες στηρίζουν το πρωτόκολλο CONFIDANT:

1. Ένας κόμβος πρέπει να παρατηρεί και να μαθαίνει από την συμπεριφορά των γειτόνων του, ώστε, αναλύοντας το πώς

συμπεριφέρονται οι γύρω του μπορεί να γλιτώσει ο ίδιος μία ίδια κακή συναλλαγή.

2. Ένας κόμβος πρέπει να μαθαίνει για τη συμπεριφορά κόμβων μέσω αναφορών τρίτων. Συγκεκριμένα κάθε κόμβος πρέπει αν μοιράζεται την πληροφορία κακών εμπειριών με συγκεκριμένους φίλους κόμβους.

Το CONFIDANT αποτελείται από τα εξής στοιχεία: Τον Ελεγκτή (monitor), το Σύστημα Φήμης (Reputation System), τον Διαχειριστή Μονοπατιών (Path Manager) και τον Διαχειριστή Εμπιστοσύνης (Trust Manager), τα οποία είναι ενεργά σε κάθε κόμβο του δικτύου.




Σχήμα Α.5.1: *Το σχηματικό διάγραμμα της μηχανής καταστάσεων του CONFIDANT*

**Ο ελεγκτής**

Ο κάθε κόμβος ελέγχει τους γείτονες του, αναζητώντας ενδείξεις για τη μη ορθή συμπεριφορά τους. Συγκεκριμένα ακούει τόσο τις εκπομπές τους αλλά παρατηρεί και τη συμπεριφορά του πρωτοκόλλου δρομολόγησης. Στην υλοποίηση των συγγραφέων με χρήση της βιβλιοθήκης GloMoSim [13] έχει υλοποιηθεί ο ελεγκτής για την μη συμμετοχή σε προώθηση πακέτων.

**Ο διαχειριστής της Εμπιστοσύνης**

Οι συγγραφείς υλοποιούν την εμπιστοσύνη στους κόμβους διαχειριζόμενοι μηνύματα συναγερμού (alarm), τα οποία μεταδίδονται ανάμεσα σε φίλους κόμβους, τους οποίους δεν έχουν ορίσει σαφώς. Ένα μήνυμα συναγερμού παράγεται όταν παρατηρηθεί ή

αναφερθεί μία κακή συμπεριφορά ενός κόμβου. Λαμβανόμενο ένα μήνυμα συναγερμού φιλτράρεται με έναν μηχανισμό παρόμοιο του μηχανισμού εμπιστοσύνης του PGP [??], για να ελεγχθεί η αξιοπιστία του.

**Το σύστημα Φήμης**

Ο κάθε κόμβος τοπικά διατηρεί μία λίστα με βαθμολογίες από τη συμπεριφορά των υπόλοιπων κόμβων, καθώς και μία μαύρη λίστα, στην οποία περιλαμβάνονται τα «μαύρα πρόβατα» του δικτύου.

Στις Αιτήσεις Διαδρομής ένας κόμβος μπορεί να περιλαμβάνει τα μαύρα πρόβατα που πρέπει να αποφευχθούν κατά την διαδρομή πηγής που επιθυμεί, διαδίδοντας παράλληλα αυτήν την πληροφορία και στους υπόλοιπους κόμβους. Επίσης ένας κόμβος ελέγχει τη μαύρη λίστα του προτού εξυπηρετήσει έναν άλλο κόμβο για να δει εάν πρέπει να τον εξυπηρετήσει.

Η πρώτη λίστα με τις βαθμολογίες συμπεριφοράς των κόμβων ανανεώνεται με βάση τις παρατηρήσεις του ελεγκτή, αλλά και των μηνυμάτων συναγερμών, με κατάλληλα βάρη στην κάθε πληροφορία. Όταν η βαθμολογία πέσει κάτω από ένα κατώφλι τότε καλείται να δράσει ο διαχειριστής διαδρομών.

**Ο διαχειριστής διαδρομών**

Ο μηχανισμός αυτός είναι επιφορτισμένος με:

- Την βαθμολόγηση των μονοπατιών, ανάλογα με την φήμη των κόμβων που περιλαμβάνονται σε αυτά.
- Τη διαγραφή μονοπατιών που περιέχουν κακούς κόμβους
- Την λήψη της απόφασης για την τακτική που θα ακολουθήσει ο κόμβος σε μία Αίτηση Διαδρομής ενός κακού κόμβου
- Την λήψη της απόφασης για την τακτική που θα ακολουθήσει ο κόμβος σε μία Αίτηση Διαδρομής η οποία στην μέχρι τότε συσσωρευμένη διαδρομή πηγής περιέχει έναν κακό κόμβο.

### 5.2.β *CORE*

Οι P. Michiardi και R. Molva, μετά από την ανάλυση βασισμένη σε προσομοιωμένα πειράματα, [14], όπου ποσοτικοποιήσαν τις επιδράσεις που έχουν σε αδόμητα DSR δίκτυα κόμβοι με εγωιστική συμπεριφορά, πρότειναν το CORE (**Co**llaborative **Re**putation)[15], το οποίο για να παρέχει ένα μηχανισμό επιβολής της συνεργασίας των κόμβων ενός δικτύου βασίζεται όπως και το CONFIDANT στην τεχνική της *συνεργατικής παρακολούθησης* (collaborative monitoring).

Το CORE είναι ένας μηχανισμός γενικός και επεκτάσιμος στον οποίο, με τον τρόπο που έχει οριστεί, μπορεί να ενσωματώσει κάθε λειτουργία ενός δικτύου, όπως η προώθηση πακέτων, η ανακάλυψη διαδρομών η διαχείριση του δικτύου και η διαχείριση θέσης. Κάθε κόμβος στο CORE ελέγχει την συνεργασιμότητα των υπόλοιπων με την τεχνική της Φήμης [16]. Η μετρική της Φήμης για έναν κόμβο υπολογίζεται τοπικά σε κάθε κόμβο με βάση τα στοιχεία που έχει συλλέξει για τον πρώτο, τόσο από άμεσες παρακολουθήσεις, αλλά και από πληροφορίες που του έχουν συνεισφέρει τρίτοι κόμβοι.

Συγκεκριμένα, η μετρική της φήμης σε έναν κόμβο $s_i$ για έναν κόμβο $s_j$ κατά τη χρονική στιγμή $t$ υπολογίζεται από την εξίσωση:

$$r_{s_i}^t\left(s_j\right)=\sum_k w_k\cdot\left\{r_{s_i}^t\left(s_j\mid f_k\right)+ir_{s_i}^t\left(s_j\mid f_k\right)\right\}$$

Όπου $k$ είναι οι διάφορες λειτουργίες που αξιολογούνται, τα βάρη $w_k$ σταθμίζουν τη σημασία της καθεμιάς, $ir_{s_i}^t\left(s_j\mid f_k\right)$ είναι η *έμμεση φήμη* (indirect reputation) που αποκτά ο κόμβος $s_i$ για τον κόμβο $s_j$ για τη λειτουργία $f_k$ τη στιγμή $t$. Τέλος, ο όρος $r_{s_i}^t\left(s_j\mid f_k\right)$ είναι η *υποκειμενική φήμη* (subjective reputation) που έχει σχηματίσει ο κόμβος $s_i$ για τον κόμβο $s_j$ για τη λειτουργία $f_k$ τη στιγμή $t$. Υπολογίζεται ως:

$$r_{s_i}^t\left(s_j\mid f\right)=\sum_k\rho\left(t,t_k\right)\cdot\sigma_k$$

Όπου $\sigma_k$ είναι η βαθμολογία για την $k$-οστή συναλλαγή του κόμβου $s_i$ με τον κόμβο $s_j$ για τη λειτουργία $f$. Η $\rho\left(t,t_k\right)$ είναι μία συνάρτηση

βάρους εξαρτώμενη από το χρόνο που δίνει περισσότερη βαρύτητα στις παλαιότερες βαθμολογίες $\sigma_k$. Η τιμή της $\sigma_k$ κυμαίνεται στο [-1,1] και η $\rho(t,t_k)$ είναι κανονικοποιημένη, ώστε τελικά η τιμή της *υποκειμενικής φήμης* να είναι και αυτή στο [-1,1].

Το CORE χωρίζει τους κόμβους του δικτύου, κατά την τέλεση μίας λειτουργίας σε δύο κατηγορίες: τον *αιτώντα* (requestor) και τους *παροχείς* (providers). Ο αιτών ζητάει από τους γείτονές του την εκπλήρωση μίας υπηρεσίας, αποθηκεύει προσωρινά τα «αναμενόμενα αποτελέσματα» από την αίτηση του και παρακολουθεί την εξέλιξη. Εάν κάποιος από τους γείτονες-παροχείς αρνηθεί να συνεργαστεί, τότε ο μηχανισμός παρακολούθησης αντιδρά δίνοντας του μία αρνητική βαθμολογία $\sigma_k$ για τη συγκεκριμένη υπηρεσία. Η βαθμολογία αυτή ανανεώνει τον τοπικό *Πίνακα Φημών* (Reputation Table) του κόμβου.

Η επιβολή της συνεργασίας επιτυγχάνεται σύμφωνα με του συγγραφείς κατά τη φάση της αίτησης παροχής μίας υπηρεσίας: Όταν σε έναν παροχέα φτάσει μία τέτοια αίτηση, ο παροχέας ελέγχει την τιμή της Φήμης του αιτούντα. Εάν είναι αρνητική, που δηλώνει, ότι ο αιτών έχει κατά το παρελθόν παρουσιάσει επανειλημμένα ανάρμοστη συμπεριφορά, τότε ο παροχέας αρνείται να τον εξυπηρετήσει.

Τέλος οι συγγραφείς περιγράφουν πως υλοποίησαν το CORE ως ένα μηχανισμό σε ένα επίπεδο πάνω από το DSR, όπου ελέγχει και βαθμολογεί τις λειτουργίες της Ανακάλυψης Διαδρομής και Προώθησης Πακέτων, αλλά δεν παρουσιάζουν αποτελέσματα της δουλειάς αυτής.

### 5.2.γ *Peer-Trust*

Οι L. Xiong και L. Liu, στο [17], παρατηρούν αρχικά ότι συστήματα *Εμπιστοσύνης* (Trust) που βασίζονται σε φήμες, συχνά χρησιμοποιούν κάποια απλή μέθοδο άθροισης θετικών και αρνητικών εντυπώσεων η οποία δεν αντανακλά εύστοχα την *αξιοπιστία* (Trustwrothyness) των κόμβων. Έπειτα, τονίζουν ότι σε τέτοια συστήματα κακοί κόμβοι μπορούν εύκολα να επιδεικνύουν ανάρμοστες συμπεριφορές, όπως την παροχή ψευδών φημών για άλλους. Με βάση τα παραπάνω, εντοπίζουν ως βασική πρόκληση στο σχεδιασμό ενός

τέτοιου συστήματος την ικανότητα του να λειτουργεί εύρωστα σε ένα περιβάλλον όπου οι κόμβοι θα συμπεριφέρονται με κακία.

Στην εργασία τους παρουσιάζουν ένα μοντέλο Εμπιστοσύνης για peer-to-peer δίκτυα: το PeerTrust, που εκτιμά και ποσοτικοποιεί την αξιοπιστία ενός κόμβου. Εξέχων χαρακτηριστικό του μοντέλου τους θεωρείται η αναγνώριση πέντε σημαντικών παραγόντων για την εκτίμηση της αξιοπιστίας των συμμέτοχων σε μία δυναμική p2p (peer-to-peer) κοινότητα. Επίσης στην εργασία τους ορίζεται μία γενική μετρική για την εμπιστοσύνη που συνδυάζει τους παράγοντες αυτούς.

Συγκεκριμένα στο PeerTrust η αξιοπιστία ενός κόμβου ορίζεται με την αποτίμηση του με βάση την φήμη που έχει σχετικά με τις υπηρεσίες που παρείχε σε άλλους κόμβους στο παρελθόν. Αυτή η φήμη εκφράζει τον βαθμό εμπιστοσύνης που οι άλλοι κόμβοι της κοινότητας έχουν στον δεδομένο κόμβο, με βάση τις παρελθούσες εμπειρίες τους. Ορίζονται οι παρακάτω πέντε παράγοντες για μία τέτοια αποτίμηση:

- *Η φήμη* ως ανάδραση (feedback) που μετρά την ικανοποίηση που απολαμβάνει ένας κόμβος συναλλασσόμενος με άλλους.
- *Ο αριθμός των συναλλαγών* που είχε ένας κόμβος με άλλους, ώστε να αποτελεί ένα μέτρο σύγκρισης της αξίας των φημών που παρέχονται.
- *Η αξιοπιστία* (credibility) *των κόμβων που παρέχουν φήμες*, με σκοπό την αντιμετώπιση κόμβων που κακόβουλα παρέχουν ψευδείς φήμες.
- *Ο παράγοντας πλαισίου συναλλαγής* (transaction context factor), που έχει να κάνει με τα εγγενή χαρακτηριστικά μίας συναλλαγής, όπως πχ. ο τύπος της συναλλαγής ή το μέγεθος της συναλλαγής.
- *Ο παράγοντας περιβάλλοντος κοινότητας* (community context factor), που έχει να κάνει τις χαρακτηριστικές ιδιότητες της συγκεκριμένης κοινότητας κόμβων.

Με βάση αυτούς τους παράγόντες ορίζεται η τιμή της εμπιστοσύνης στον κόμβο u, T(u) ως:

$$T(u) = \alpha \cdot \frac{\sum_{i=1}^{I(u)} S(u,i) \cdot Cr\left(p(u,i)\right) \cdot TF(u,i)}{I(u)} + \beta \cdot CF(u)$$

όπου το $I(u)$ είναι το πλήθος των συναλλαγών του $u$, $S(u,i)$ η κανονικοποιημένη τιμή της ικανοποίησης (satisfaction) που είχε ο κόμβος $u$ από έναν άλλο κόμβο $p(u,i)$ κατά την $i$-οστη συναλλαγή, $Cr\left(p(u,i)\right)$ είναι η αξιοπιστία του κόμβου $p(u,i)$ που παρείχε την φήμη για τον κόμβο $u$. Το $TF(u,i)$ είναι ο παράγοντας συναλλαγής και το

# Β΄ ΜΕΡΟΣ: ΕΝΣΩΜΑΤΩΣΗ ΕΜΠΙΣΤΟΣΥΝΗΣ ΚΟΜΒΩΝ ΣΤΟ DSR

## 1. Εισαγωγή

Αρχικός στόχος της εργασίας μας ήταν να ορίσουμε ένα επεκτάσιμο, γενικό, συνεργατικό σχήμα διαχείρισης εμπιστοσύνης των κόμβων του δικτύου στο πλαίσιο του DSR το οποίο θα εξασφάλιζε την επιβολή της συνεργασίας. Στο σχήμα που ορίσαμε και παρουσιάζεται σε αυτό το κεφάλαιο, κάθε κόμβος κατασκευάζει μία μετρική για την εμπιστοσύνη που έχει στους υπόλοιπους κόμβους του δικτύου, στηριζόμενος στις άμεσες αλληλεπιδράσεις που είχε μαζί τους και στην πληροφορία που κυκλοφορεί στο δίκτυο για αυτούς με τη μορφή διαδόσεων (rumor). Με στόχο να διαφοροποιηθούμε από τους [12] και [15], ενσωματώσαμε ως νέα πεδία επικεφαλίδας στα ήδη ορισμένα από το DSR πακέτα εξ' ολοκλήρου και κατά αρκετά αποδοτικό τρόπο τις πληροφορίες διαδόσεων. Τέλος περιγράψαμε έναν τρόπο χρήσης του μηχανισμού αυτού, για την επιβολή της συνεργασίας των κόμβων. Στην πειραματική μελέτη της υλοποίησης ανέκυψαν ορισμένα ζητήματα λογικής και σχεδίασης που οδήγησαν στο δεύτερο μέρος αυτής της εργασίας.

Η ενότητα αυτή ξεκινάει παρουσιάζοντας το θεωρητικό τμήμα του μηχανισμού: Στο κεφάλαιο 2 γίνεται μία καταγραφή των υποθέσεων που κάνουμε για να ορίσουμε το την μετρική της Εμπιστοσύνης Κόμβου. Στο κεφάλαιο 3 παρουσιάζουμε τον ορισμό της Εμπιστοσύνης και στο κεφάλαιο 4 περιγράφεται ο μηχανισμός Εξάπλωσης Διαδόσεων. Έπειτα παρουσιάζεται η στρατηγική που προτείναμε για τη χρήση αυτού του μηχανισμού σχηματισμού εμπιστοσύνης, ώστε να επιβάλλεται η συνεργασία των κόμβων. Στο κεφάλαιο 6 περιγράφεται

η υλοποίηση του μηχανισμού: στην πρώτη παράγραφο κάνουμε μια σύντομη περιγραφή στο OPNET, το εργαλείο που χρησιμοποιήσαμε για τις προσομοιώσεις μας και παρουσιάζουμε το μοντέλο του DSR για OPNET που χρησιμοποιήσαμε. Στην παράγραφο 6.2 παρουσιάζουμε τις υπηρεσίες που χρησιμο-ποιήθηκαν για τον σχηματισμό της Εμπιστοσύνης ενός κόμβου. Στην παράγραφο 6.3 παρουσιάζουμε τις τροποποιήσεις που έπρεπε να του γίνουν για να ενσωματωθούν οι μηχανισμοί για τον σχηματισμό της μετρικής της Εμπιστοσύνης και για τη διάδοση των φημών. Στο κεφάλαιο 7 παρουσιάζουμε αποτελέσματα του μηχανισμού υπολογισμού της εμπιστοσύνης και ολοκληρώνουμε στο κεφάλαιο 8 παρουσιάζοντας μια σειρά από συμπεράσματα στα οποία καταλήξαμε με βάση τα πειράματα που κάναμε.

## 2. Υποθέσεις

Α. Σχετικά με την υποδομή του δικτύου κάναμε τις ακόλουθες υποθέσεις:

1. Όλοι οι κόμβοι που μετέχουν ή επιθυμούν να μετάσχουν στο δίκτυο χρησιμοποιούν το πρωτόκολλο IEEE 802.11. Έτσι απαλείφουμε την περίπτωση για μονόδρομες ζεύξεις που είδαμε ότι δημιουργεί περιπλοκές στον DSR.
2. Υπάρχει μία «ένα-προς-ένα» αντιστοίχηση κάθε κόμβου με μία μοναδική IP διεύθυνση. Όλες οι IP διευθύνσεις και οι φυσικές τους αντιστοιχήσεις είναι γνωστές σε κάθε κόμβο πριν ακόμη αυτός αποκτήσει πρόσβαση στο δίκτυο.
3. Θεωρούμε ότι όλοι οι κόμβοι είναι εφοδιασμένοι με τα απαραίτητα κοινά μυστικά: το ssid του δικτύου, τα κλειδιά του wep, ή οτιδήποτε άλλο μπορεί να απαιτηθεί κατά τη φάση σχηματισμού του δικτύου ή κατά τη φάση που ένας κόμβος προσπαθεί να αποκτήσει πρόσβαση στο δίκτυο.
4. Όλοι οι κόμβοι λειτουργούν τις κάρτες δικτύου με τον μηχανισμό αδιάκριτης λήψης.
5. Για χάρη ομοιομορφίας, θεωρούμε ότι όλοι οι κόμβοι έχουν πανκατευθυντικές κεραίες.

Β. Σχετικά με την συμπεριφορά των κόμβων:

1. Οι κόμβοι μπορούν να κινούνται ελεύθερα, υπό τις προϋποθέσεις που θέτει το DSR.
2. Η πυκνότητα του δικτύου στη διάρκεια του χρόνου παραμένει αρκετά χαμηλή, ώστε να είναι πράγματι ένα δίκτυο πολλαπλών βημάτων.
3. Δεν υπάρχουν κόμβοι που εμπλέκονται σε ενεργές επιθέσεις στο δίκτυο. Οι κόμβοι ενδέχεται να απορρίψουν πακέτα, αλλά δεν πρόκειται να αλλοιώσουν πληροφορία σε πακέτα που προωθούν, ή να μεταδώσουν αυθαίρετα πακέτα.

Με το παραπάνω σύνολο υποθέσεων δύο είναι τα κύρια προβλήματα που έχει αντι-μετωπίζει το DSR: Η αυξημένη πλεονάζουσα πληροφορία λόγω της κινητικότητας και τα προβλήματα που δημιουργεί η εγωιστική συμπεριφορά των χρηστών. Στην επόμενη παράγραφο ορίζουμε τον υπολογισμό της εμπιστοσύνης κόμβων.

## 3. Ορισμοί για την Εμπιστοσύνη

Σε κάθε συναλλαγή ανάμεσα σε δύο κόμβους μία πληθώρα από παρατηρήσεις και μετρήσεις μπορούν να πραγματοποιηθούν από τους συναλλασσόμενους. Για παράδειγμα, εάν η εν λόγω συναλλαγή είναι η προώθηση ενός πακέτου δεδομένων του κόμβου-πηγή Α από τον Β, τότε ο Β μπορεί να μετρήσει την ισχύ του λαμβανόμενου σήματος (Received Signal Strength: RSS) από τον κόμβο Α καθώς και την καθυστέρηση του πακέτου· ο Α αντίστοιχα μπορεί εάν χρησιμοποιεί το μηχανισμό αδιάκριτης λήψης, μπορεί να παρατηρήσει αν ο Β πράγματι προώθησε το πακέτο καθώς και να κάνει μετρήσεις για το RSS και καθυστέρηση. Μία τέτοιου τύπου παρατήρηση ή μέτρηση την ονομάζουμε *υπηρεσία* (service). Κάθε υπηρεσία βαθμολογείται με μία πραγματική τιμή από το διάστημα [0,1], όπου το 0 σημαίνει απόλυτη δυσαρέσκεια (*π.χ.* «ο γείτονας μου επιβεβαίωσε τη λήψη ενός πακέτου δεδομένων το οποίο έπρεπε να προωθήσει, αλλά δεν τον άκουσα να το προωθεί μέσα στο επιθυμητό χρονικό παράθυρο») και το 1 σημαίνει απόλυτη ικανοποίηση. Έτσι κάθε κόμβος σχηματίζει έναν *πίνακα βαθμών* (grade table) που περιέχει τους βαθμούς των πρόσφατων συναλλαγών, με κάθε άλλο κόμβο και για κάθε υπηρεσία ενδιαφέροντος.

Ορίζουμε την *εκτίμηση υπηρεσίας* (Service Appreciation) που έχει ο κόμβος A, μέχρι την χρονική στιγμή $t$, για την υπηρεσία $F$ η οποία προσφέρεται από τον B, ως το σταθμισμένο μέσο όρο των δεδομένων βαθμών, κατ' αναλογία προς τον ορισμό της υποκειμενικής φήμης (subjective reputation) στο CORE [15],

$$S_{F_A}^t(B) = \sum_{T_F^t} \left( h(t) \cdot g_A(B;t) \right)$$

όπου το $T_F^t$ υποδηλώνει το σύνολο των παρατηρήσεων του A για τον B για την υπηρε-σία $F$ ως τη στιγμή t, $gA(B|t)$ είναι ο βαθμός της παρατήρησης της χρονικής στιγμής $t$ και η $h(t)$ είναι μία συνάρτηση απόδοσης βάρους στο βαθμό της χρονικής στιγμής $t$.

Η συνάρτηση απόδοσης βάρους $h(t)$ μπορεί είτε να δίνει ίσα βάρη σε όλες τις παρατηρήσεις της F ή ενδεχομένως να ακολουθεί την πρόταση από το [15], κατά την οποία οι παλαιότερες παρατηρήσεις αξίζουν περισσότερο βάρος. Σε κάθε περίπτωση πρέπει να ισχύει ότι $\sum_{T_F^t} h(t) = 1$, ώστε να εξασφαλίζεται ότι $S_{F_A}^t(B) \in [0,1]$

Η *Εκτίμηση* (Appreciation) του κόμβου A για τον κόμβο B μέχρι τη χρονική στιγμή t είναι ένας σταθμισμένος μέσος των υπολογισμένων εκτιμήσεων υπηρεσιών:

$$S_A^t(B) = \sum_F \left( w_F \cdot S_{F_A}^t(B) \right)$$

Τα $w_F$ είναι παράγοντες βάρους που σχετίζονται με κάθε υπηρεσία και εξαρτώνται από το πλήθος των ολοκληρωμένων συναλλαγών καθεμίας υπηρεσίας. Διαφορετικοί παράγοντες βάρους μπορούν να αποδοθούν σε διαφορετικές υπηρεσίες ανάλογα με τα χαρακτηριστικά του δικτύου. Για παράδειγμα, σε ένα περιβάλλον με υψηλή κινητικότητα οι εκτίμηση της υπηρεσίας του RSS μπορεί να θεωρηθεί ως η πιο σημαντική.

Τέλος, ορίζουμε ως Εμπιστοσύνη του κόμβου A στον κόμβο B κατά τη χρονική στιγμή $t$ το επόμενο σταθμισμένο άθροισμα:

$$T_A^t(B) = w_1 \cdot S_A^t(B) + w_2 \sum_X \frac{\mathsf{F}\left(f\left(S_A^t(X)\right), S_X^t(B)\right)}{\|X\|}$$

όπου $X$ είναι το σύνολο των κόμβων που συνεισέφεραν στον Α τις τιμές της εκτίμησης τους για τον κόμβο Β και το ||$X$|| δηλώνει το πλήθος των κόμβων του $X$. Τα $w_1$ και $w_2$ είναι βάρη που έχουν να κάνουν με το ολικό πλήθος των συναλλαγών του Α με τον Β και των κόμβων του Χ με τον Β αντίστοιχα: εάν το πλήθος των συναλλαγών που είχε ο Α με τον Β ήταν $m_A$ και $m_X$ ήταν τότε τα $w_1$ και $w_2$ μπορούν να οριστούν να είναι: $w_1$=$m_A$/($m_A$+$m_X$) και $w_2$=$m_X$/($m_A$+$m_X$) Τέλος, η $\mathsf{F}$ είναι μία συνάρτηση που χρησιμοποιείται για να φιλτράρει τις συνεισφερόμενες τιμές της εκτίμησης, χρησιμοποιώντας μία απεικόνιση $f$ της τιμής εκτίμησης του κόμβου προς τον συνεισφέροντα στο [0,1]. Για απλότητα, μπορούμε να χρησιμοποιήσουμε την $\mathsf{F}(x,y) = x \cdot y$, οπότε θα είναι:

$$\mathsf{F}\left(f\left(S_A^t(X)\right), S_X^t(B)\right) = \mathsf{F}\left(f\left(S_A^t(X)\right) \cdot S_X^t(B)\right)$$

Θα χρησιμοποιήσουμε τον όρο *Φήμη* (reputation) του κόμβου Β που φτάνει στον κόμβο Α, για να περιγράψουμε τον δεύτερο όρο στην εξίσωση ορισμού της Εμπιστοσύνης.

## 4. Ο μηχανισμός Εξάπλωσης Διαδόσεων

Η τιμή της Φήμης του κόμβου Β που φτάνει στον κόμβο Α, όπως είδαμε στον ορισμό της μετρικής της Εμπιστοσύνης, κατασκευάζεται από τις συνισφερόμενες τιμές της εκτίμησης που έχουν διάφοροι κόμβοι για τον κόμβο Β τις οποίες ονομάζουμε *διαδόσεις* (rumors). Σχεδιαστική επιλογή μας ήταν να μην κατασκευάσουμε ένα μηχανισμό, σε υψηλότερο επίπεδο από αυτό του DSR, ο οποίος θα αναλάμβανε σε τακτά χρονικά διαστήματα να εξαπλώνει αυτές τις διαδόσεις, αλλά να προσπαθήσουμε να τον ενσω-ματώσουμε μέσα στο ίδιο το πρωτόκολλο του DSR. Κύριος μοχλός αυτής της επιλογής ήταν να κρατήσουμε σε χαμηλά επίπεδα την πλεονάζουσα πληροφορία που θα

εισήγαγε και θα διακινούσε ένας τέτοιος μηχανισμός, επίσης θέλαμε να διατηρήσουμε τον αμιγώς «κατ' απαίτηση» χαρακτήρα του DSR.

Δύο ήταν τα σημαντικότερα ερωτήματα που έπρεπε να απαντηθούν: ποια πακέτα του DSR θα μετέφεραν τις διαδόσεις και για ποιους κόμβους θα παρείχαν πληροφορίες μέσω των διαδόσεων.

Μετά από θεωρητική και πειραματική μελέτη του πρωτοκόλλου DSR, καταλήξαμε ότι ο πιο συμφέρον τρόπος να μεταφέρονται οι διαδόσεις είναι τα πακέτα δεδομένων (data packets) του DSR. Ο κυριότερος λόγος είναι ότι σε ένα ακίνητο, μη δυναμικό, αδόμητο δίκτυο ο DSR μετά από λίγο χρόνο που θα χρειαστεί για να ανακαλύψει όλες τις δυνατές διαδρομές που χρειάζονται στους κόμβους θα πάψει να μεταφέρει πακέτα ελέγχου (πακέτα Αίτησης Διαδρομής, Απάντησης Διαδρομής *κ.ο.κ.*), συνεπώς τα μόνα πακέτα που θα υπάρχουν διαθέσιμα για να μεταφέρουν τις διαδόσεις είναι τα πακέτα δεδομένων. Εκτός αυτού, με τον μηχανισμό αποφυγής καταιγισμού απαντήσεων διαδρομής, πολλά πακέτα Απάντησης Διαδρομής καταστρέφονται νωρίς, οπότε ακόμη και σε ένα δίκτυο που καθ' όλη τη διάρκεια της ζωής του υπάρχουν τέτοια πακέτα ελέγχου δεν διανύουν μεγάλες αποστάσεις ικανές να εξαπλώσουν πολύ τις διαδόσεις που θα μπορούσαν να μεταφέρουν.

Από τον ορισμό της Εμπιστοσύνης είναι φανερό, ότι η πληροφορία που πρέπει να συνεισφέρει ως διάδοση ένας κόμβος σχετικά με έναν άλλο κόμβο είναι (α) η τιμή της εκτίμησης του για αυτόν και (β) το πλήθος των συναλλαγών βάσει τον οποίων έχει υπολογίσει την τιμή αυτή. Για να περιορίσουμε την μεταφερόμενη πληροφορία κρίναμε ότι αρκεί σε κάθε πακέτο δεδομένων η πηγή του να επισυνάπτει τις πληροφορίες αυτές για τους κόμβους της διαδρομής πηγής.

Συνοψίζοντας, κάθε φορά που ένας κόμβος στέλνει ένα πακέτο δεδομένων DSR μέσω μίας διαδρομής πηγής, για κάθε κόμβο της διαδρομής αυτής επισυνάπτει: (α) την αντίστοιχη τιμή της εκτίμησης που έχει σχηματίσει για τον κόμβο αυτό μέσω άμεσων αλληλεπιδράσεων μαζί του κατά το παρελθόν και (β) το πλήθος των συναλλαγών με τον εν λόγω κόμβο βάσει του οποίου υπολόγισε την εκτίμηση αυτή.

Εδώ γίνεται φανερή η ανάγκη που υπάρχει για την υπόθεση που κάναμε ότι πρέπει να μην υπάρχουν κόμβοι που αλλοιώνουν τα δεδομένα των πακέτων που προωθούν. Αντιμετωπίζουμε δηλαδή ένα μοντέλο εγωισμού το οποίο προκύπτει όχι από ενεργητική *κακία* (maliciousness), αλλά από προσπάθεια «παρασιτικής επιβίωσης» μέσα στο δίκτυο.

## 5. Χρήση της Εμπιστοσύνης για επιβολή της συνεργασίας

Οποτεδήποτε ένας κόμβος λαμβάνει ένα πακέτο δεδομένων DSR που φέρει τις διαδόσεις της πηγής του για τους κόμβους της διαδρομής, μία τιμή φήμης μπορεί να εξαχθεί για καθέναν από αυτούς τους κόμβους, άρα οι τιμές για την Εμπιστοσύνη που τους έχει ο παραλήπτης μπορούν να ανανεωθούν. Εάν η ανανεωμένη τιμή της Εμπιστοσύνης σε έναν κόμβο πέσει κάτω από ένα ορισμένο κατώφλι, θεωρείται ως ένδειξη ότι ο κόμβος αυτός δεν πληροί τις προϋποθέσεις καλής συνεργασίας για συμμετοχή στο δίκτυο. Συνεπώς, η cache διαδρομών του παραλήπτη πρέπει να εξεταστεί και όσες διαδρομές περιέχουν τον κόμβο αυτόν να διαγραφούν. Επίσης ο παραλήπτης θα πρέπει να πάψει να εξυπηρετεί τον αναξιόπιστο κόμβο.

Εάν η cache διαδρομών στην υλοποίηση του DSR περιλαμβάνει περισσότερες από μία διαδρομές ανά κόμβο, τότε η συνδεσιμότητα του δικτύου δεν βλάπτεται άμεσα. Αλλιώς, όταν προκύψει η ανάγκη για να σταλεί ή να προωθηθεί ένα πακέτο σε έναν προορισμό για τον οποίο δεν είναι γνωστή καμία διαδρομή, τότε ο μηχανισμός Ανακάλυψης Διαδρομής του DSR πρέπει να προσαρμοστεί ως εξής: Τα πακέτα Αίτησης Διαδρομής πρέπει να περιέχουν μία λίστα των κόμβων τους οποίους η πηγή της αίτησης θεωρεί ως αναξιόπιστους. Ένας κόμβος που λαμβάνει μία τέτοια αίτηση, στέλνει μία Απάντηση Διαδρομής, μόνο εάν μπορεί να παρέχει μία διαδρομή, που δεν περιλαμβάνει κανέναν αναξιόπιστο κόμβο. Αυτό σημαίνει ότι ο κόμβος πού θα στείλει την απάντηση αυτή είτε την είχε αποθηκευμένη, ή προωθώντας την Αίτηση, πήρε μία Απάντηση Διαδρομής που περιείχε μία τέτοια διαδρομή.

Με τον τρόπο αυτό, σύντομα, κόμβοι που χαρακτηρίζονται αναξιόπιστοι λόγω της συμπεριφοράς τους θα εξάγονται από τις

caches και συνεπώς δεν θα χρησιμοποιούνται ως ενδιάμεσοι για προώθηση πακέτων, επίσης δικά τους πακέτα δεν θα εξυπηρετούνται, οπότε ουσιαστικά θα απομονώνονται από το δίκτυο. Αυτοί οι κόμβοι μπορούν να ξαναμπούν στο δίκτυο, μετά από ένα προκαθορισμένο *διάστημα τιμωρίας* (penalty time), μετά τη λήξη του οποίου πρέπει οι κόμβοι που τους θεωρούσαν αναξιόπιστους να τους δώσουν μία «δεύτερη ευκαιρία» επανένταξης, θέτοντας την τιμή της εμπιστοσύνης τους στο ελάχιστο αποδεκτό όριο (συγκεκριμένα την τιμή ½). Προϋπόθεση για να γίνει αυτό είναι ότι κατά το χρονικό αυτό διάστημα, ο κόμβος που θεωρείτο αναξιόπιστος θα πρέπει να μην προσπαθήσει «παράνομα» να λειτουργήσει μέσα στο δίκτυο. Δηλαδή, εάν ένας κόμβος λάβει ένα πακέτο Αίτησης Διαδρομής και βρει τον εαυτό του μέσα στη λίστα των αναξιόπιστων κόμβων, τότε πρέπει να μην προχωρήσει το μηχανισμό ανακάλυψης διαδρομής, καθώς οποιαδήποτε περαιτέρω συμμετοχή του σε αυτόν, θα οδηγούσε σε μία *Παράνομη Απάντηση* (Illegal Reply) για την Αίτηση που την προκάλεσε.

Έτσι, όλοι οι κόμβοι για να εξασφαλίσουν τη συνεχή παραμονή τους στο δίκτυο θα πρέπει να φροντίσουν ώστε να παρέχουν τις μετρούμενες υπηρεσίες κατά τρόπο ικανοποιητικό προς τους κόμβους που τις παρατηρούν.

## 6. Υλοποίηση

Για να δούμε στην πράξη το πρωτόκολλο του DSR κατά τη διάρκεια της αρχικής μας μελέτης, αλλά και για να υλοποιήσουμε το σχήμα που παρουσιάστηκε στο προηγούμενο κεφάλαιο, χρησιμοποιήσαμε το μοντέλο του DSR για το OPNET από το Wireless Communications Technologies Group του NIST (National Institute of Standards and Technology) των ΗΠΑ. Πρόκειται για ένα ευρέως διαδεδομένο μοντέλο στην ερευνητική κοινότητα. Η επιλογή αυτού του για χρήση στην εργασία μας έγινε σε πολύ πρώιμο στάδιο και έτσι αντιμετωπίσαμε αρκετά προβλήματα με ασυμβατότητες και σφάλ-ματα που υπήρχαν στο αρχικό μοντέλο, τα οποία δυσκόλεψαν τόσο την μελέτη του DSR, όσο και την τροποποίηση του μοντέλου για την ενσωμάτωση του σχήματος της Εμπιστοσύνης που περιγράψαμε στο προηγούμενο κεφάλαιο.

Για να κάνουμε μία σύντομη εισαγωγή πριν παρουσιάσουμε το συγκεκριμένο μοντέλο, η μοντελοποίηση στο OPNET διαιρείται σε 3 επίπεδα. Το ανώτατο είναι το *επίπεδο δικτύου* (network level), στο οποίο περιγράφονται τα συστατικά και η τοπολογία του δικτύου. Το μεσαίο επίπεδο είναι το *επίπεδο κόμβου* (node level), όπου, με την μορφή μίας στοίβας από διαδικασίες, περιγράφεται κάθε στοιχείο που χρησιμοποιήθηκε στο παραπάνω επίπεδο. Το τρίτο και τελικό επίπεδο είναι το *επίπεδο διαδικασίας* (process level), όπου με τη δομή μιας πεπερασμένης μηχανής καταστάσεων γράφεται κώδικας σε ένα υπερσύνολο της C, την Proto-C για την περιγραφή κάθε διαδικασίας ενός κόμβου. Για μία γενικότερη περιγραφή του OPNET παραπέμπουμε στα: [18, 19, 20].

## 6.1 Το μοντέλο του DSR από το WCTG του NIST

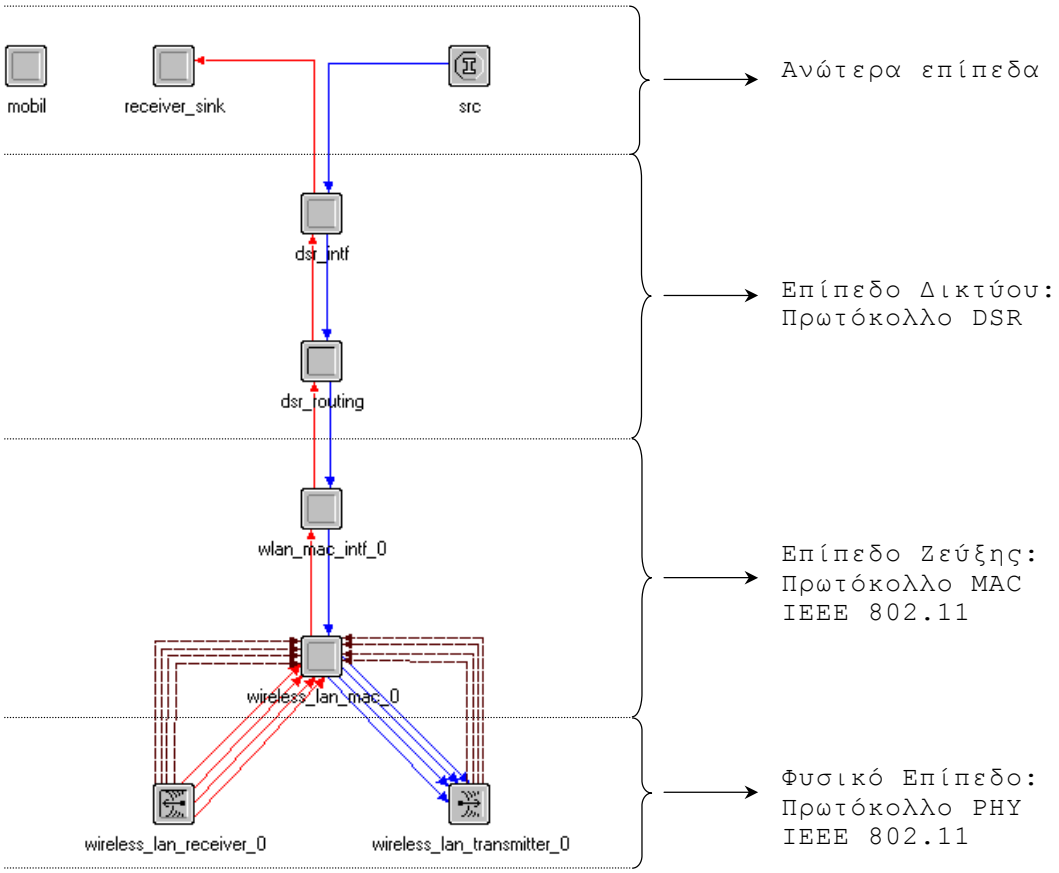
Η περιγραφή του μοντέλου του DSR από το WCTG του NIST, που θα κάνουμε εδώ, αφορά στα επίπεδα μοντέλων κόμβου και διαδικασίας, καθώς αυτά είναι που ορίζουν το καθ' αυτό πρωτόκολλο. Στο επίπεδο δικτύου για αυτό το μοντέλο, απλώς, πριν από την εκτέλεση μίας προσομοίωσης τοποθετούμε τους ασύρματους κόμβους του δικτύου που θέλουμε να μελετήσουμε σε κάποιες αρχικές θέσεις και θέτουμε διάφορες παραμέτρους για την προσομοίωση, όπως η εμβέλεια της μετάδοσης, οι παράμετροι της κινητικότητας των κόμβων.

### 6.1.α *Το μοντέλο κόμβου*

Το μοντέλο κόμβου (*βλ.* Σχήμα Β.6.1) είναι κατ΄ ουσία μία στοίβα από διαδικασίες, όπου κάθε διαδικασία ή ομάδα από διαδικασίες αντιστοιχούν με τη σειρά τους σε ένα επίπεδο στο μοντέλο διαστρωμάτωσης OSI.

Το φυσικό επίπεδο αποτελείται από έναν πομπό και έναν δέκτη: στο σχήμα Β.6.1 τα μπλοκ wireless_lan_transmitter_0 και wireless_lan_reciver_0. Καθένα από αυτά τα δύο μπλοκ *δεν* είναι μια διαδικασία OPNET, αλλά ορίζει τον κώδικα C που απαιτείται για χρήση στο μηχανισμό της ασύρματης επικοινωνίας (*βλ.* [20] για περισσότερες λεπτομέρειες). Ο εν λόγω κώδικας έχει αναπτυχθεί από τους δημιουργούς του OPNET. Συγκεκριμένα, το φυσικό επίπεδο και το επίπεδο ζεύξης του

μοντέλου είναι παρμένα από το μοντέλο Wireless_Lan πού έχει αναπτυχθεί από τους δημιουργούς του OPNET.




Σχήμα Β.6.1: *Το μοντέλο κόμβου του μοντέλου DSR του WCTG του NIST.*

Η βάση του επίπεδου ζεύξης του μοντέλου είναι το μοντέλο του IEEE 802.11 του OPNET. Οι δημιουργοί του μοντέλου του DSR έχουν κάνει ορισμένες τροποποιήσεις, όπως π.χ. την προσθήκη του μηχανισμού αδιάκριτης λήψης, την αποστολή συγκεκριμένων μηνυμάτων επιβεβαίωσης επιπέδου MAC και σφαλμάτων επιπέδου MAC. Η επιλογή αυτού του πρωτοκόλλου για το επίπεδο ζεύξης έγινε ακολουθώντας τον συρμό της ερευνητικής κοινότητας των MANET. Το επίπεδο ζεύξης αποτελείται από δύο διαδικασίες-μπλοκ: το wireless_lan_mac_0 είναι το καθ' αυτό πρωτόκολλο 802.11, ενώ το wireless_lan_intf_0 είναι μια απαιτούμενη διεπαφή με το παραπάνω επίπεδο. Ένα σοβαρό πρόβλημα που αντιμετω-πίσαμε είναι ότι το μοντέλο δεν λειτουργεί σωστά σε ρυθμούς μεγαλύτερους από 2 Mbps. Το πρόβλημα αυτό είναι γνωστό στην υπόλοιπη ερευνητική κοινότητα, χωρίς κάποιος να έχει δώσει

λύση, όπως διαπιστώσαμε μέσα από λίστες ηλεκτρονικής αλληλογραφίας με θέμα τα MANET.

Το επίπεδο δικτύου είναι ο πυρήνας του μοντέλου κόμβου του DSR, καθώς περιέχει τη διαδικασίας δρομολόγησης του DSR που θα παρουσιάσουμε παρακάτω. Όπως και το προηγούμενο επίπεδο, έτσι και αυτό είναι χωρισμένο σε δύο διαδικασίες: η dsr_routing είναι η διαδικασίας δρομολόγησης του DSR και η dsr_inft είναι η διεπαφή με τα ανώτερα επίπεδα, όπου και επιλέγεται η διεύθυνση προορισμού ενός πακέτου που πρέπει να μεταδοθεί στο δίκτυο.

Τα ανώτερα επίπεδα έχουν προσομοιωθεί με δύο διαδικασίες. Η src είναι μία διαδικασία του OPNET, όπως ο πομπός και ο δέκτης παραπάνω, η οποία παράγει την πακέτα δεδομένων για να δημιουργηθεί η κίνηση πληροφορίας στο δίκτυο. Η διαδικασία receiver είναι αυτή που παραλαμβάνει τα πακέτα δεδομένων που καταφτάνουν σε έναν κόμβο και τα καταστρέφει, μετά την όποια επεξεργασία τους.

Τέλος η διαδικασία mobil. είναι επιφορτισμένη με την κινητικότητα των κόμβων του δικτύου. Περιλαμβάνει το μοντέλο κίνησης μπιλιάρδου, στο οποίο ο κάθε κόμβος επιλέγει μία κατεύθυνση και την ακολουθεί με σταθερή ταχύτητα, μέχρι τα όρια του χώρου προσομοίωσης οπότε και «ανακλάται» επιλέγοντας μια νέα τυχαία κατεύθυνση.

### 6.1.β *Το μοντέλο της διαδικασίας δρομολόγησης DSR*

Σε αυτήν την παράγραφο περιγράφουμε την υλοποίηση του μοντέλου της διαδικασίας dsr_routing: ξεκινάμε παρουσιάζοντας τις λεπτομέρειες που αφορούν στον μηχανισμό Ανακάλυψης Διαδρομής, στη συνέχεια εστιάζουμε στον μηχανισμό Συντήρησης Διαδρομής, έπειτα βλέπουμε τον τρόπο που είναι οργανωμένες οι cache των διαδρομών και τέλος κάνουμε μία περιγραφή της μηχανής καταστάσεων όπου υλοποιούνται τα παραπάνω.

#### 6.1.β.1 Ο Μηχανισμός Ανακάλυψης Διαδρομής

Αιτήσεις Διαδρομής:

Υλοποιείται ο βασικός μηχανισμός ανακάλυψης διαδρομής στον οποίο χρησιμο-ποιείται ο μηχανισμός μη προωθητικών αιτήσεων, όπως ακριβώς περιγράφεται στο πρωτόκολλο του DSR. Μία βασική λεπτομέρεια που διέπει το μοντέλο είναι ότι το όριο των βημάτων εισάγεται σαν πεδίο της επικεφαλίδας των πακέτων του DSR και δεν υλοποιείται με το πεδίο TTL του IP, καθώς δεν υπάρχει υλοποίηση του IP, επίσης η υλοποίηση υποθέτει ότι η διάμετρος του δικτύου (άρα και ο μέγιστος αριθμός βημάτων) που απαιτούνται είναι 7. Επιπλέον, χρησιμοποιείται η τεχνική της απάντησης με χρήση αποθηκευμένων διαδρομών. Υπάρχει η τεχνική αποφυγής καταιγισμού απαντήσεων, που υλοποιείται με χρήση της καθυστέρησης των Απαντήσεων, όπως περιγράφεται στο πρωτόκολλο, αλλά και με χρήση του μηχανισμού αδιάκριτης λήψης. Δεν υλοποιείται η αναζήτηση δακτυλίου και δεν υλοποιείται η αποθήκευση έμμεσης πληροφορίας δρομο-λόγησης –με εξαίρεση στα πακέτα σφάλματος (*βλ.* παρακάτω).

Αίτηση Διαδρομής από Σφάλμα:

Σε περίπτωση αποστολής πακέτου Αίτησης Διαδρομής μετά από τη λήψη ενός Σφάλματος Διαδρομής, δεν χρησιμοποιείται ο μηχανισμός μη προωθητικής αίτησης με το σκεπτικό ότι οι γειτονικοί κόμβοι δεν μπορεί να έχουν έγκυρη διαδρομή για τον προορισμό στην cache τους. Δεν υλοποιείται ο μηχανισμός αυξημένης διάδοσης μηνυμάτων Σφάλματος με την επισύναψη του πακέτου Σφάλματος Διαδρομής στο πακέτο της νέας Αίτησης, οδηγώντας έτσι όπως διαπιστώσαμε από πειράματα σε απαντήσεις από τις caches γειτονικών κόμβων που δεν άκουσαν ποτέ το τελευταίο πακέτο Σφάλματος Διαδρομής.

### 6.1.β.2 Ο Μηχανισμός Συντήρησης Διαδρομής

Μηχανισμός επιβεβαίωσης λήψης πακέτου:

Στο μοντέλο του DSR όπως είδαμε χρησιμοποιείται το MAC επίπεδο του IEEE 802.11 ως επίπεδο ζεύξης. Έτσι, αυτό το επίπεδο παρέχει τα μηνύματα επιβεβαίωσης και σφαλμάτων που απαιτούνται από το επίπεδο δρομολόγησης. Συγκεκριμένα, το μοντέλο δεν έχει ενταμιευτή επαναμετάδοσης, αλλά μέσω ενός χρονομετρητή μπορεί να παρα-τηρήσει ότι δεν έχει ληφθεί η απαραίτητη επιβεβαίωση για ένα πακέτο δεδομένων που μεταδόθηκε στο παρελθόν. Με αυτόν το μηχανισμό παράλληλα ελέγχεται και η ορθή λειτουργία του επιπέδου

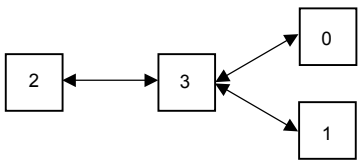
ζεύξης, καθώς στον προκαθορισμένο χρόνο πρέπει να ληφθεί είτε ένα πακέτο επιβεβαίωσης ή ένα πακέτο σφάλματος, για κάθε πακέτο που έχει σταλεί.

Χρήση του μηχανισμού αδιάκριτης λήψης για τη συντήρηση διαδρομών:

Το μόνο κομμάτι από το μηχανισμό αποθήκευσης έμμεσης πληροφορίας δρομο-λόγησης που υλοποιείται στο μοντέλο είναι η χρήση οποιουδήποτε πακέτου Σφάλματος Διαδρομής που θα ακούσει ένας κόμβος. Όταν ένας κόμβος, μέσω του μηχανισμού αδιάκριτης λήψης, ακούσει ένα πακέτο Σφάλματος Διαδρομής, αμέσως ελέγχει την cache διαδρομών του για να διαγράψει τη ζεύξη που το πακέτο φέρει ως κομμένη, ανεξάρτητα από το εάν περιλαμβάνεται στην διαδρομή πηγής του πακέτου ή όχι. Η δεύτερη εφαρμογή του μηχανισμού αδιάκριτης λήψης στη συντήρηση διαδρομών είναι η υλοποίηση της αυτόματης συντόμευσης διαδρομών, όπως την περιγράψαμε στο μέρος Α, στην παρά-γραφο 4.5.β.

### 6.1.β.3 Οργάνωση των caches διαδρομών

Στην υλοποίηση αυτή του DSR, η Cache Διαδρομών κάθε κόμβου είναι ένας δυναμικός δι-διάστατος πίνακας. Οι γραμμές του δεικτοδοτούνται (indexed) με τις διευθύνσεις επιπέδου δικτύου των κόμβων (*βλ.* σχήμα Β.6.2). Κάθε γραμμή του περιέχει μία λίστα από τις διευθύνσεις των κόμβων οι οποίοι αποτελούν τη διαδρομή πηγής από τον παρόντα κόμβο προς τον προορισμό. Προφανές είναι ότι, με αυτήν την οργάνωση, για κάθε δυνατό προορισμό στο δίκτυο μπορεί να αποθηκευτεί μία το πολύ διαδρομή. Οι δημιουργοί του μοντέλου ισχυρίζονται ότι «προφανώς» αυτή είναι και η συντομότερη, πράγμα το οποίο επιβεβαιώσαμε πειραματικά. Δυστυχώς, όπως θα δούμε και στο παρακάτω, αυτή η οργάνωση των caches διαδρομών αποδείχτηκε το μεγαλύτερο μειονέ-κτημα του μοντέλου για τη μελέτη μας.




| | | | |
|---|---|---|---|
| 0 | 2 | 3 | 0 |
| 1 | 2 | 3 | 1 |
| 2 | -1 | | |
| 3 | 2 | 3 | |

Σχήμα Β.6.2: *Ένα αδόμητο δίκτυο και η cache διαδρομών του κόμβου 2 σε κάποια συγκεκριμένη χρονική στιγμή.*

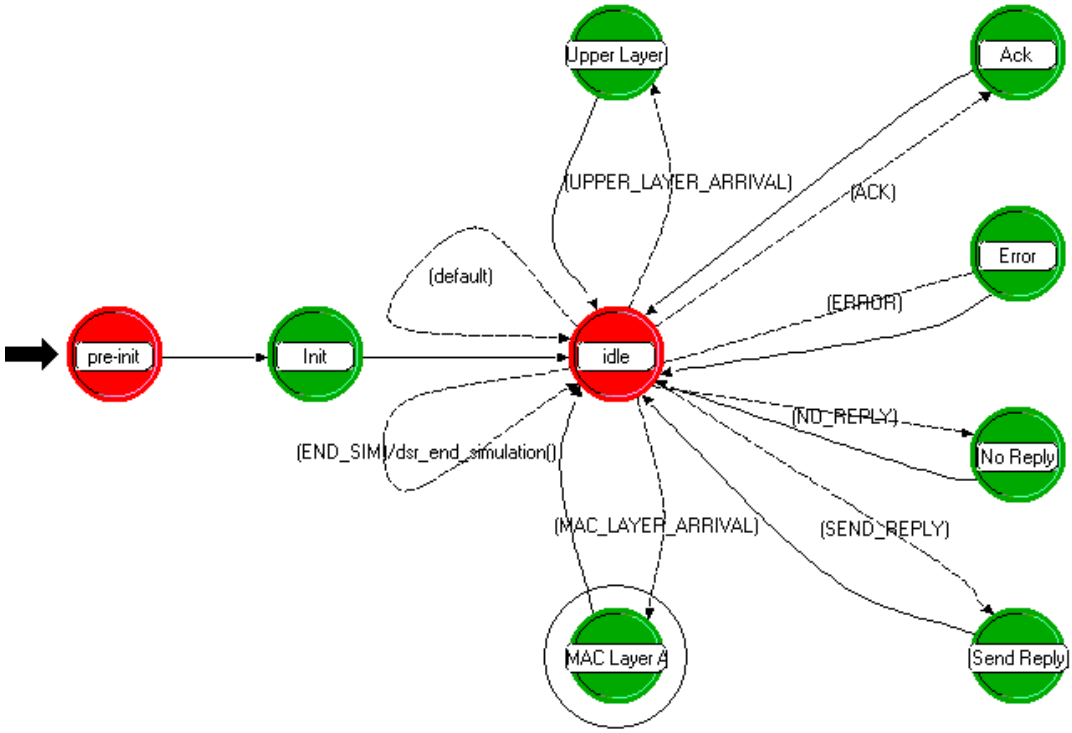
## 6.1.γ *Η μηχανή καταστάσεων του μοντέλου διαδικασίας του DSR*

Στο σχήμα Β.6.3 βλέπουμε πως είναι η μηχανή καταστάσεων, δηλαδή το μοντέλο της διαδικασίας, δρομολόγησης **dsr_routing** του DSR. Ακολουθεί η περιγραφή του ρόλου της καθεμιάς από τις καταστάσεις που φαίνονται σε αυτό.

pre-init: Γίνεται πρώτη αρχικοποίηση του κόμβου, όπου του αποδίδεται διεύθυνση επιπέδου δικτύου (στην υλοποίηση χρησιμοποιείται ως διεύθυνση επιπέδου δικτύου του κόμβου η διεύθυνση MAC) και ελέγχεται η εγκυρότητα της στο υπόλοιπο δίκτυο.

Init: Αρχικοποιούνται όλες οι μεταβλητές, στατιστικές προσομοίωσης. πίνακες και παράμετροι προσομοίωσης του χρήστη που χρησιμοποιούνται στο μοντέλο διαδικασίας

Upper Layer Arrival: Χειρίζεται κάθε πακέτο δεδομένων που δημιουργήθηκε από την διαδικασία **src** του κόμβου και έφτασε στη διαδικασία δρομολόγησης έχοντας ένα συγκεκριμένο κόμβο-προορισμό μέσω της διαδικασίας **dsr-intf**.




Σχήμα Β.6.3: *Η μηχανή καταστάσεων (μοντέλο διαδικασίας) του μοντέλου DSR του WCTG του NIST.*

MAC Layer Arrival: Χειρίζεται κάθε πακέτο που παρέλαβε το επίπεδο ζεύξης. Αναλόγως τον τύπο του πακέτου (δεδομένων, Αίτησης, Απάντηση, ή Σφάλματός) καλείται ο μηχανισμός του DSR που χρειάζεται για να το χειριστεί.

Send Reply: Καλείται όταν παρέλθεί το χρονικό διάστημα αναμονής (timeout) που αφορά σε ένα πακέτο Αίτησης που έστειλε ο κόμβος. Αυτό σηματοδοτεί ότι το προηγούμενο βήμα της Αίτησης Διαδρομής απέτυχε, συνεπώς ένα νέο πακέτο Αίτησης παράγεται και να στέλνεται από τον κόμβο.

Idle: Είναι η κατάσταση στην οποία η διαδικασία αναμένει να συμβεί ένα γεγονός (event).

Ack: Χειρίζεται κάθε επιβεβαίωση που φτάνει από το επίπεδο ζεύξης 802.11. Έτσι βεβαιώνεται ότι η ζεύξη που χρησιμοποιήθηκε για την αποστολή του τελευταίου πακέτου δεδομένων είναι όντως ενεργή και συνεπώς ο κόμβος μπορεί να την χρησιμοποιήσει ξανά σύντομα για να στείλει πακέτα δεδομένων μέσω αυτής. Επίσης ακυρώνει την αντίστροφη μέτρηση που είχε τεθεί από το μηχανισμό ελέγχου σφάλματος ο οποίος περίμενε αυτήν την επιβεβαίωση.

Error: Καλείται όταν ένα σφάλμα ληφθεί από το επίπεδο του 802.11. Η ζεύξη που χρησιμοποιήθηκε για να σταλεί το μη επιβεβαιωμένο (unacknowledged) πακέτο δεδομένων χαρακτηρίζεται κομμένη (broken), διαγράφεται από την cache διαδρομών και στέλνεται ένα πακέτο σφάλματος στην πηγή του πακέτου.

## 6.2 Περιγραφή των εκτιμήσεων υπηρεσιών στην υλοποίηση

Στην υλοποίηση μας, οι τιμές της εκτίμησης κόμβου υπολογίζονται με βάση τις τιμές εκτίμησης υπηρεσίας από τέσσερις υπηρεσίες που υπολογίζουμε: τη συμμετοχή στην διαδικασία της Ανακάλυψης Διαδρομής, την προώθηση πακέτων την μέτρηση του RSS και την καθυστέρηση. Οι κανόνες με τους οποίους κάναμε τη βαθμοδότηση σε καθεμιά από τις παραπάνω υπηρεσίες περιγράφονται παρακάτω:

Προώθηση: Οποτεδήποτε ένας κόμβος επιτυχώς στείλει ένα πακέτο δεδομένων σε έναν άλλο κόμβο, ο οποίος σύμφωνα με την διαδρομή

πηγής του πακέτου πρέπει να το προωθήσει στον τελικό του προορισμό, τότε ο ενδιάμεσος (relaying node) που το παρέλαβε θα στείλει στον αποστολέα μία επιβεβαίωση ορθής παραλαβής (στο μοντέλο η επιβεβαίωση έρχεται από το επίπεδο ζεύξης 802.11). Βασισμένοι στην υπόθεση των πανκατευθυντικών κεραιών, εάν ο παραλήπτης πράγματι το προωθήσει, τότε ο αποστολέας χάρη στον μηχανισμό αδιάκριτης λήψης θα ακούσει την αποστολή αυτή. Ανάλογα με τον χρόνο που παρήλθε μεταξύ της λήψης της επιβεβαίωσης και της αδιάκριτης λήψης της προώθησης του πακέτου, ο πρώτος αποστολέας αποδίδει μία τιμή «θετικής» εκτίμησης υπηρεσίας (που πλησιάζει το 1). Εάν παρέλθει ένα προκαθορισμένο χρονικό διάστημα και δεν παρατηρηθεί προώθηση του πακέτου, τότε αποδίδεται μηδενική τιμή ικανοποίησης για την υπηρεσία της προώθησης για τον ενδιάμεσο κόμβο.

Ανακάλυψης Διαδρομής: Στο πνεύμα του CORE [15], κρίναμε σκόπιμο να βαθμολογήσουμε την συμμετοχή ενός κόμβου στην ανακάλυψη διαδρομής. Η χρήση όμως του μηχανισμού αδιάκριτης λήψης στον μηχανισμό Ανακάλυψης Διαδρομής του μοντέλου, για να υλοποιείται η αποφυγή του καταιγισμού απαντήσεων, έχει ως αποτέλεσμα να μην μπορεί με απλή παρατήρηση της συμπεριφοράς ενός κόμβου να αποφανθεί ένας τρίτος εάν το γεγονός ότι ο κόμβος αυτός δεν απάντησε σε μία Αίτηση οφείλεται (α) στο ότι δεν συμμετείχε στην Ανακάλυψη Διαδρομής, ή (β) στο ότι σταμάτησε την Ανακάλυψη Διαδρομής του λόγω του μηχανισμού αποφυγής καταιγισμού απαντήσεων όπως υλοποιείται στο μοντέλο. Προφανώς, εξετάσαμε την επιλογή της αφαίρεσης του μηχα-νισμού αποφυγής καταιγισμού απαντήσεων από το μοντέλο, αλλά τόσο η δυσκολία αφαίρεσης ενός ήδη υπάρχοντος μηχανισμού, όσο και τα οφέλη του συγκεκριμένου μηχανισμού μας απέτρεψαν ισχυρά.

Έτσι κατασκευάσαμε την ακόλουθη βαθμολόγηση για την εκτίμηση στην υπηρεσία της Ανακάλυψης Διαδρομής: Οποτεδήποτε ένα πακέτο Απάντησης Διαδρομής φτάνει σε έναν κόμβο, αποδίδεται στον αποστολέα της Απάντησης μία τιμή εκτίμησης υπηρεσίας που εξαρτάται από την απόσταση του μήκους της διαδρομής πηγής που φέρει το πακέτο από την μέση απόσταση όλων των διαδρομών που υπάρχουν αποθηκευμένες στην cache διαδρομών του παραλήπτη. Με το σκεπτικό αυτό κόμβοι που διαφημίζουν κοντινές διαδρομές

θεωρούνται πιο ικανοποιητικοί από κόμβους που δίνουν μακρύτερες διαδρομές.

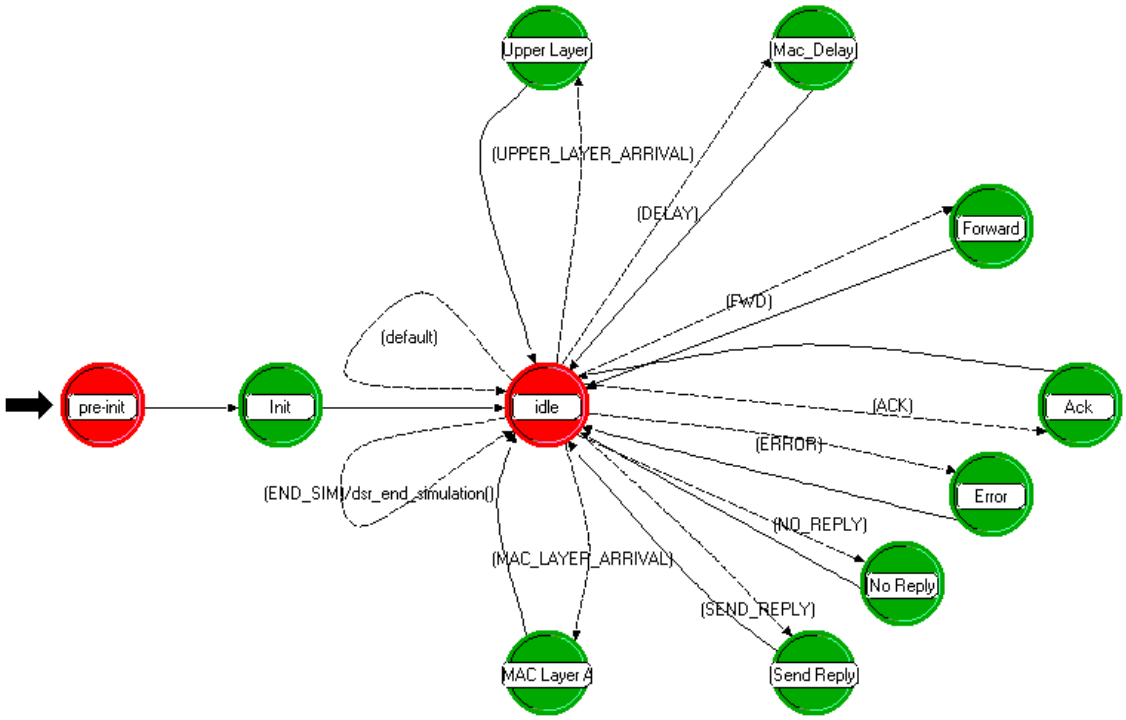
RSS: Λαμβάνοντας υπόψη ότι κόμβοι που επικοινωνούν με χαμηλό σήμα είναι πιθανό σύντομα να προκαλέσουν απώλεια ζεύξης (link failure), κάθε κόμβος που λαμβάνει ένα πακέτο δεδομένων βαθμολογεί τον αποστολέα για την «υπηρεσία του RSS», ανάλογα με την μετρούμενη τιμή ισχύος του λαμβανόμενου σήματος.

Καθυστερήσεις: Θεωρώντας ότι η καθυστέρηση ενός βήματος (hop delay) αποτελεί ένδειξη της πιθανότητας απώλειας ζεύξης σύντομα, όσο μεγαλύτερη η παρατηρούμενη καθυστέρηση ενός πακέτου τόσο χαμηλότερη είναι τιμή εκτίμησης για την υπηρεσία αυτή που προσφέρεται από τον κόμβο που έστειλε το πακέτο.

## 6.3 Τροποποιήσεις στο μοντέλο του DSR για την ενσωμάτωση της Εμπιστοσύνης

1. Απαιτήθηκε η δημιουργία δύο νέων καταστάσεων στο μοντέλο (*βλ.* σχήμα Β.6.4):

   - Η MAC_Delay χρησιμοποιείται για να ελέγξει τα πλαίσια που καταφτάνουν από το επίπεδο MAC, να κάνει τους υπολογισμούς για την καθυστέρηση ενός λαμβανόμενου πακέτου και τέλος να υπολογίσει την εκτίμηση της υπηρεσίας καθυστέρησης του αποστολέα.
   - Η Forward καλείται μετά την πάροδο ενός προκαθορισμένου χρονικού διαστήματος από την αποστολή ενός πακέτου προς έναν κόμβο, ο οποίος έπρεπε να το προωθήσει. Αυτό που γίνεται στη Forward είναι ότι ελέγχεται ο πίνακας Προωθήσεων που κατασκευάσαμε (βλ. πλαίσιο 6.1) για να διαπιστωθεί εάν ο κόμβος στον οποίο στάλθηκε το πακέτο όντως το προώθησε και να δοθεί η κατάλληλη τιμή για την εκτίμηση της υπηρεσίας προώθησης του ενδιάμεσου κόμβου.



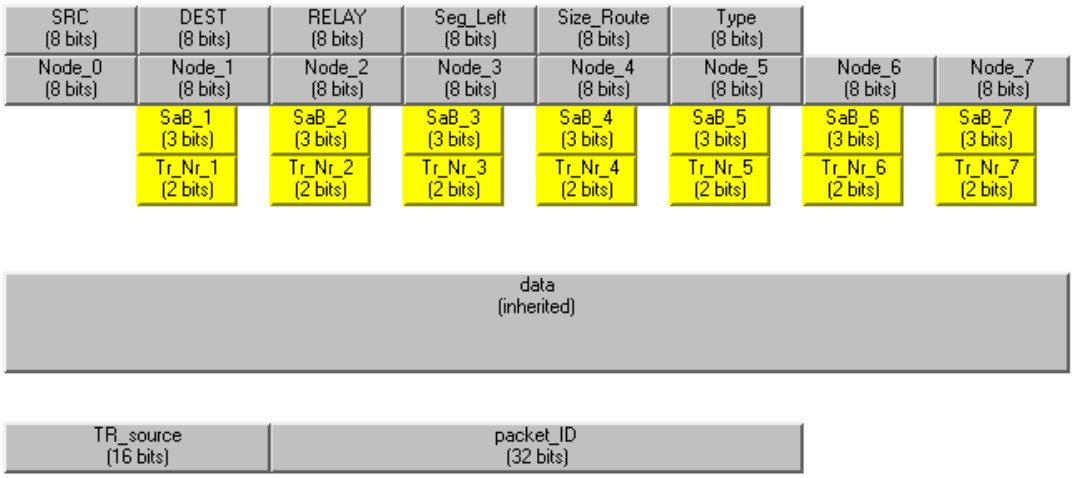

Σχήμα Β.6.4: *Το μοντέλο διαδικασίας για το DSR με ενσωματωμένη την Εμπιστοσύνη Κόμβων.*

2. Για το μηχανισμό εξάπλωσης των διαδόσεων, όπως αναφέραμε και στο κεφ. 4 αποφασίσαμε να χρησιμοποιήσουμε τα πακέτα δεδομένων του DSR. Για την αρχική δομή (format) τους παραπέμπουμε στο [21]. Για να υλοποιηθεί κατά αποδοτικό τρόπο, καταλήξαμε ότι τόσο η τιμή της εκτίμησης, όσο και του αριθμού των συναλλαγών έπρεπε να κβαντιστούν σε ένα ελάχιστο αριθμό από bits. Για την εκτίμηση, ο αριθμός bits που χρησιμοποιήσαμε είναι 3, όπου η κβαντισμένη τιμή 0 σημαίνει «καμία συναλλαγή με τον κόμβο», ενώ οι τιμές 1 ως και 6 απεικονίζονται ομοιόμορφα στο διάστημα [0,1] της αρχικής τιμής της εκτίμησης. Το πλήθος των συναλλαγών κβαντίστηκε σε 2 bit, με το 0 να σημαίνει «*μικρό πλήθος από συναλλαγές*» και βαθμιαία αυξάνει μέχρι την τιμή 3 που σημαίνει ένα μεγάλο πλήθος από συναλλαγές. Έτσι, το πακέτο δεδομένων του μοντέλου DSR διαμορφώθηκε όπως στο σχήμα Β.6.5

```
0) id: 796 nxt: 13 seenAck: 1 txTime: 13.92321 ackTime: 13.92761 fwdTime: -1.00000
1) id: 802 nxt:  1 seenAck: 1 txTime: 14.01516 ackTime: 14.01626 fwdTime: 14.01796
2) id: 830 nxt:  4 seenAck: 1 txTime: 14.39806 ackTime: 14.39917 fwdTime: 14.40041
```

```
3) id: 834 nxt: 13 seenAck: 1 txTime: 14.40827 ackTime: 14.40975 fwdTime: -1.00000
4) id: 840 nxt:  1 seenAck: 1 txTime: 14.50298 ackTime: 14.50408 fwdTime: 14.50537
5) id: 874 nxt: 13 seenAck: 1 txTime: 14.95068 ackTime: 14.95178 fwdTime: -1.00000
6) id: 683 nxt: 13 seenAck: 1 txTime: 12.18307 ackTime: 12.18417 fwdTime: -1.00000
7) id: 687 nxt: 13 seenAck: 1 txTime: 12.25579 ackTime: 12.25690 fwdTime: -1.00000
8) id: 759 nxt: 13 seenAck: 1 txTime: 13.37514 ackTime: 13.37625 fwdTime: -1.00000
9) id: 764 nxt:  4 seenAck: 1 txTime: 13.49567 ackTime: 13.49677 fwdTime: 13.49797
```

Πλαίσιο Β.6.1: *Ο πίνακας Προωθήσεων, είναι οργανωμένος ως κυκλικός ενταμιευτής και περιέχει πληροφορίες για κάθε πακέτο που έστειλε ένας κόμβος σε έναν ενδιάμεσο του ζητώντας του να το προωθήσει. Συγκεκριμένα περιλαμβάνει το αναγνωριστικό του πακέτου, την διεύθυνση του ενδιάμεσου κόμβου, αν έχει ληφθεί επιβεβαίωση, το χρόνο αποστολής, το χρόνο λήψης της επιβεβαίωσης και το χρόνο που λήφθηκε το πακέτο ξανά από την εκπομπή προώθησης με το μηχανισμό αδιάκριτης λήψης. Στον συγκεκριμένο πίνακα μπορούμε άμεσα να δούμε ότι ο κόμβος 13 φέρεται εγωιστικά…*




Σχήμα Β.6.5: *Το πακέτο του μοντέλου DSR με εμπιστοσύνη κόμβων που κατασκευάσαμε στο OPNET. Η επιπλέον πλεονάζουσα πληροφορία είναι 35bits, δηλαδή ποσοστιαία, ανά πακέτο δεδομένων αντιστοιχεί σε μία αύξηση κατά 22.5% της επικεφαλίδας.*

3. Με δεδομένη την παραπάνω επιλογή για τον κβαντισμό της πληροφορίας στην εξάπλωση των διαδόσεων, επιλέξαμε τη συνάρτηση F για τον υπολογισμό να είναι απλά ο πολλαπλασιασμός της $f\left(S_A^t(X)\right)$ με την $S_x^t(B)$, όπου η $f$ είναι η απεικόνιση των κβαντισμένων τιμών της εκτίμησης σε τιμές βαρών στο [0,1], κατά τον πίνακα Β.6.1.

| Κβαντισμένες τιμές της εκτίμησης $S_A^t(X)$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|

| $f\left(S_A^t(X)\right)$ | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 | 1 |
|---|---|---|---|---|---|---|

Πίνακας Β.6.1: *η απεικόνιση f που χρησιμοποιήσαμε στην υλοποίησή μας.*

# 7. Αποτελέσματα

Έχοντας υλοποιήσει ολόκληρο τον μηχανισμό παρακολούθησης των τεσσάρων υπηρεσιών και το μηχανισμό εξάπλωσης των διαδόσεων, κάναμε μία σειρά από πειράματα για να ελέγξουμε τα αποτελέσματα που έδινε η προτεινόμενη μετρική της εμπιστοσύνης.

Εδώ καταγράφουμε, τις παρατηρήσεις μας για τον καθένα από τους προτεινόμενους τρόπους παρακολούθησης και βαθμολόγησης των επιμέρους υπηρεσιών:

## 7.1 Προώθηση

Σε όλες τις περιπτώσεις όπου ένας εγωιστικά συμπεριφερόμενος κόμβος δεν προωθούσε πακέτο δεδομένων DSR ο μηχανισμός παρακολούθησης το αντιλαμβανόταν άμεσα, μετά από την πάροδο του προκαθορισμένου χρόνου αναμονής προώθησης. Έτσι, ο κόμβος που είχε ζητήσει την προώθηση βαθμολογούσε με την τιμή 0 την υπηρεσία προώθησης για τον εγωιστή κόμβο.

Σε ελάχιστες περιπτώσεις παρατηρήθηκε κόμβοι που δεν συμπεριφέρονταν εγωιστικά έπαιρναν κάποια χρονική στιγμή μία μηδενική τιμή. Με συγκεκριμένα πειράματα καταφέραμε να εντοπίσουμε την πηγή του σφάλματος: Υπάρχει η περίπτωση ένας ενδιάμεσος κόμβος να έχει έναν σχετικά γεμάτο ενταμιευτή αποστολής και να λάβει ένα πακέτο για να το προωθήσει στον προορισμό του. Ο κόμβος το τοποθετεί στο τέλος της ουράς του ενταμιευτή αποστολής και μέχρι αυτός να αδειάσει παρέρχεται ο προκαθορισμένος χρόνος αναμονής προώθησης στον αποστολέα του πακέτου. Ο αποστολέας δεν έχει ακούσει τον ενδιάμεσο να προωθεί το πακέτο που του ζήτησε, άρα τον βαθμολογεί με μηδενική τιμή για αυτήν την περίπτωση. Παρόλα αυτά, χάρη στον τρόπο υπολογισμού της Εκτίμησης Υπηρεσίας, τέτοια «στιγμιαία» σφάλματα δεν είχαν επιπτώσεις στην τελική τιμή της.

## 7.2 Ανακάλυψη Διαδρομής

Σε περιπτώσεις ακίνητων, στατικών δικτύων η υπηρεσία αυτή έχει νόημα για πολύ σύντομο χρονικό διάστημα και πολύ λίγες συναλλαγές. Επίσης για κόμβους οι οποίοι έχουν μονάχα έναν γείτονα που τους συνδέει με το υπόλοιπο δίκτυο, η υπηρεσία αυτή έδινε αποτελέσματα που ήταν ισχυρά εξαρτημένα από την τοπολογία του δικτύου.

## 7.3 RSS

Από τη βαθμολογία της υπηρεσίας του RSS παρατηρήσαμε ότι μπορούσαμε μέσω της τιμής της να ξεχωρίσουμε άμεσα κόμβους οι οποίοι βρίσκονται σε μικρή απόσταση από κόμβους που βρίσκονται μακριά. Γενικά η βαθμολογία αυτή ρυθμίστηκε κατά τρόπο ώστε ένας κόμβος που επικοινωνεί έναν άλλο με ζεύξη που βρίσκεται στο όριο της ευαισθησίας των δεκτών τους[4] να του αποδίδει βαθμό εκτίμησης RSS πολύ χαμηλό (κοντά στο 0).

## 7.4 Καθυστερήσεις

Χωρίς κανένα πρόβλημα, η βαθμολόγηση των καθυστερήσεων οδηγούσε τιμές σε εκτίμησης υπηρεσίας που ήταν στο διάστημα 0.9 έως 1 όταν οι καθυστερήσεις ήταν μικρές ενώ αντίθετα για μεγαλύτερες τιμές καθυστερήσεων έπεφτε γρήγορα σε μικρότερες τιμές.

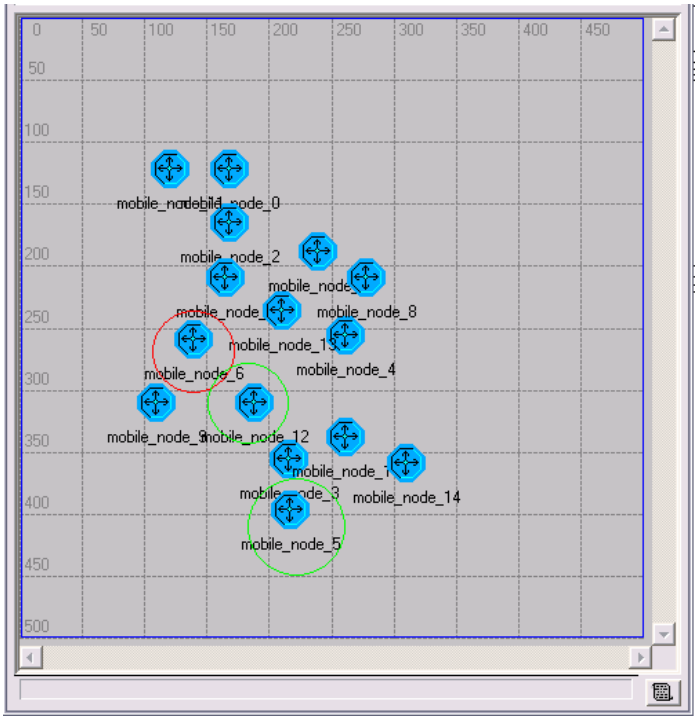
Ο μηχανισμός εξάπλωσης των διαδόσεων αποδείχθηκε ότι κατά την υλοποίηση μας επιφόρτιζε το σύστημα με ένα ελάχιστο ποσό πλεονάζουσας πληροφορίας. Συγκεκριμένα παρατηρήσαμε ότι για ακίνητα δίκτυα, όπου η πλεονάζουσα πληροφορία κυμαίνεται στην τάξη του 25% για πακέτα των 512bits η αύξηση αυτού του ποσοστού ήταν +2%.

Δυστυχώς, διαπιστώσαμε ότι η μετρική που ορίσαμε δεν ανταποκρινόταν πλήρως στις προσδοκίες μας. Συγκεκριμένα διαπιστώσαμε ότι σε πολλές περιπτώσεις, κόμβοι που δεν είχαν προγραμματιστεί να εμφανίσουν εγωιστική συμπεριφορά ή που δεν

(4) *Οι υπολογισμοί έγιναν με βάση το μοντέλο δύο κλίσεων [22] και με ευαισθησία λήψης -94 dB*

ανήκαν σε ζεύξεις που κόβονταν ποτέ, διαγράφονταν από τις caches και χαρακτηρίζονταν αναξιόπιστοι.

Το παράδειγμα που ακολουθεί παρατίθεται μία χαρακτηριστική περίπτωση σφάλματος. Στο σχήμα Β.7.1 βλέπουμε την τοπολογία του δικτύου που μελετάμε. Οι κόμβοι είναι ακίνητοι και όλοι συμμετέχουν κανονικά στους μηχανισμούς του DSR. Το σενάριο που εκτελέστηκε και του οποίου τα αποτελέσματα βλέπουμε στο πλαίσιο Β.7.1 έχει ως εξής:




Σχήμα Β.7.1: *Ο κόμβος 6 ακούει τη μετάδοση ενός πακέτου από τον 12 στον 5 και υπολογίζει μια νέα τιμή για την Εμπιστοσύνη του στον 5.*

Ο κόμβος 12 στέλνει στον κόμβο 5 ένα πακέτο δεδομένων που πλέον έχει τη μορφή του σχήματος 6.5. Στο πακέτο αυτό περιέχεται στο πεδίο SaB_1 η κβαντισμένη εκτίμηση του κόμβου 12 για τον 5 και έχει την τιμή 1, η οποία έχει αποδοθεί πιθανότατα λόγω της μεγάλης απόστασης μεταξύ τους που σημαίνει ότι θα υπάρχει σίγουρα χαμηλό RSS και πιθανότατα μεγάλες καθυστερήσεις. Παρατηρούμε επίσης ότι η τιμή αυτή έχει υπολογιστεί με βάση μικρό πλήθος συναλλαγών, που έχει κβαντιστεί στην τιμή 0.

Το πακέτο αυτό λαμβάνεται από τον κόμβο 6 με τον μηχανισμό αδιάκριτης λήψης (πλαίσιο 7.1, γραμμές 1-5). Ο κόμβος 6 τώρα μπορεί να υπολογίσει μία καινούρια φήμη μέσω του 12 για τον 5, άρα και μια καινούρια τιμή για την Εμπιστοσύνη του σε αυτόν

```
<1>  [0.116246]  6: I am in <<< MAC DELAY >>>
<2>  [0.116246]  6: Got delay from 12 for relay 5 dest is 5 DELAY = 0.001632
<3>  [0.116246]  6: The received packet is IN TR, distance(12, 6) = 70.310476
<4>  [0.116246]  6: I am in <<< MAC LAYER ARRIVAL >>>
<5>  [0.116246]  6: I have just received a data packet
<6>                 [src][dst] == [12][5]
<7>     CALCULATING:
<8>     ------------
<9>     >>> SxB[12][5] = 1.000000
<10>    >>> nrT_r =  0
<11>    calculating Sab for 12
<12>    CalulateSab(12):
<13>    w_for = 0.000000 w.rou = 0.000000 w.del = 0.500000 w.rss = 0.500000
<14>    f.val = 0.000000 r.val = 0.000000 d.val = 0.980104 s.val = 0.294390
<15>    CalulateSab(12): Sab.val = 0.637247
<16>    CalulateSab: final.val = 4
<17>    TempSax.transNr = 0
<18>    >>> SaX = 4.000000
<19>    >>> SxB = 1.000000
<20>    (1.0-( (6.0-(double)TempSaX.val) *0.1))= 0.800000
<21>    >>> Rnom = 0.133333
<22>    >>> R = 0.133333
<23>    calculating Sab for 5
<24>    CalulateSab: returning NO_TRANSACTION_AVAILABLE
<25>    >>> L.val(5) = 0.000000
<26>    >>> L.transNr = 0
<27> [0.116246]  6: !!! Killing 5 from my route cache !!!
<28> [0.116246]  6: my Trusts are:
<29>     0: 0.550000 at 0.000000
<30>     1: 0.550000 at 0.000000
<31>     2: 0.550000 at 0.000000
<32>     3: 0.550000 at 0.000000
<33>     4: 0.550000 at 0.000000
<34>     5: 0.133333 at 0.116246
<35>     6: 0.550000 at 0.000000
<36>     7: 0.550000 at 0.000000
<37>     8: 0.550000 at 0.000000
<38>     9: 0.550000 at 0.000000
<39>    10: 0.550000 at 0.000000
<40>    11: 0.550000 at 0.000000
<41>    12: 0.550000 at 0.000000
<42>    13: 0.550000 at 0.000000
<43>    14: 0.550000 at 0.000000
```

Πλαίσιο 7.1: *Τα αποτελέσματα από τον υπολογισμό της εμπιστοσύνης στο σενάριο του σχήματος ?!@. Βλέπουμε όλες τις ενέργειες του κόμβου 6 από τη χρονική στιγμή 0.116246s που ακούει το πακέτο από τον κόμβο 12 προς τον κόμβο 5.*

(γραμμές 7-26). Επειδή όμως δεν έχει ποτέ άμεσες αλληλεπιδράσεις με τον 5 (γραμμές 24-26) πρακτικά η τιμή της φήμης που θα υπολογίσει είναι και αυτή της τελικής εμπιστοσύνης. Έτσι, ο

κόμβος 6 υπολογίζει την φήμη του 5 που του φτάνει από τον 12, με δεδομένο ότι η εκτίμηση που έχει για τον 12 είναι ικανοποιητική (γραμμή 18). Η τιμή για την φήμη του 5 υπολογίζεται να είναι πολύ χαμηλή (γραμμή 22), οπότε και ο κόμβος 6 αποφασίζει, εσφαλμένα, ότι πρέπει ο 5 να βγει από την cache διαδρομών του.

## 8. Συμπεράσματα

1. Ο τρόπος ορισμού της εμπιστοσύνης αποδείχθηκε κατά την πειραματική διαδικασία δυσκίνητος: οι πολλές παράμετροι που χρησιμοποιούνταν για να ρυθμίσουν τη βαρύτητα της κάθε ποσότητας που λαμβάνει μέρος σε ένα σταθμισμένο άθροισμα καθιστούσαν τον έλεγχο της τελικής βαρύτητας αξίας τους εξαιρετικά δύσκολο και χρονοβόρο.

2. Η βαθμοδότηση που χρησιμοποιήσαμε για αξιολογήσουμε τη συμμετοχή ενός κόμβου στη διαδικασία ανακάλυψης διαδρομής δεν απέδωσε, διότι αφ' ενός είχε να κάνει με την τοπολογία του δικτύου και όχι με την συμπεριφορά των κόμβων, αφ' εταίρου είναι ασταθής με τον τρόπο που την χρησιμοποιήσαμε: ένας κόμβος μπορεί να αποδώσει τιμή εκτίμησης ίση με 1 σε έναν γείτονα του εάν τον αναζητήσει ως στόχο σε μία ανακάλυψη διαδρομής και στην επόμενη ακριβώς συναλλαγή να του αποδώσει μία πολύ χαμηλή τιμή εάν ο γείτονας απαντήσει με μία μεγάλη διαδρομή πηγής που έχει αποθηκευμένη στην cache του.

   Μία τέτοια μετρική θα μπορούσε να χρησιμοποιηθεί σε μία διαφορετική υλοποίηση του DSR όπου θα αποθηκεύονταν πολλαπλές διαδρομές πηγής ανά προορισμό αλλά και η εμπιστοσύνη θα χρησιμοποιούταν για να διαχειριστεί διαδρομές.

3. Η μετρική για την προώθηση πακέτων έχει σαφώς καλύτερη συμπεριφορά, ιδιαίτερα όταν ένας κόμβος φέρεται εγωιστικά από την πρώτη του εμφάνιση του μέσα στο δίκτυο. Η περίπτωση των εσφαλμένων αρνητικών (false negatives) παρατηρήσεων που παρουσιάσαμε στην παράγραφο με τα αποτελέσματα δεν δημιουργεί προβλήματα. Παρόλα αυτά μας έδωσε ένα έναυσμα να αναζητήσουμε

τρόπο για να την εξαλείψουμε, αλλά και να μελετήσουμε πιο συγκεντρωμένα το ζήτημα της προώθησης πακέτων.

4. Ενώ η αρχική ιδέα για την συμμετοχή της ποιότητας της ζεύξης στην εμπιστοσύνη ενός κόμβου φαινόταν να προσδίδει μία νέα διάσταση στην εμπιστοσύνη, αποδείχθηκε ότι η αξιολόγηση του φυσικού μέσου δεν πρέπει να μετέχει σε διαδικασίες διάδοσης φημών με τον ίδιο τρόπο όπως οι συμπεριφορές των κόμβων. Πάλι και εδώ η πρόταση είναι ότι κάτι τέτοιο θα είχε καλύτερη εφαρμογή σε επίπεδο διαδρομών και όχι κόμβων, όπως και η μετρική για την συμμετοχή στην Ανακάλυψη Διαδρομών.

Συνοψίζοντας, πιο υποσχόμενο περιβάλλον για τον μηχανισμό επιβολής συνεργασίας μέσω Εμπιστοσύνης φαίνεται να είναι μία υλοποίηση του DSR με δυνατότητα αποθήκευσης πολλαπλών διαδρομών πηγής ανά προορισμό, στο οποίο η Εμπιστοσύνη θα έχει ρόλο στο κόστος της διαδρομής και θα χρησιμοποιείται ως μηχανισμός επιλογής καταλληλότερης διαδρομής και όχι απλά ως μηχανισμός απόφασης παύσης μίας διαδρομής.

Σε ένα περιβάλλον όμως όπως αυτό που χρησιμοποιήσαμε για την εργασία μας, οι μετρήσεις και οι συμπεριφορές των ζεύξεων πρέπει να είναι πλήρως διαχωρισμένες από αυτές που αφορούν στην συμπεριφορά των κόμβων και την διάθεση συμμετοχής τους στο πρωτόκολλο δρομολόγησης. Ο λόγος είναι ότι οι πρώτες χαρακτηρίζουν ζεύξεις ενώ οι δεύτερες συμπεριφορές κόμβων.

Έτσι οδηγηθήκαμε στην ανάπτυξη των δύο μηχανισμών που παρουσιάζονται στα επόμενα κεφάλαια: Ενός μηχανισμού που αναγνωρίζει ζεύξεις που πρόκειται να κοπούν (τόσο λόγω αυξανόμενου θορύβου / παρεμβολών *κλπ*, ή λόγω της κινητικότητας των κόμβων) και ενός μηχανισμού για την ανακάλυψη και απομόνωση κόμβων που δεν προωθούν πακέτα. Στο κεφάλαιο της μελλοντικής εργασίας προτείνουμε μία σειρά από προβλήματα που αφήσαμε ανοιχτά με αυτό το κομμάτι της εργασίας μας.

# Γ΄ ΜΕΡΟΣ: ΔΥΟ ΜΗΧΑΝΙΣΜΟΙ ΒΕΛΤΙΩΣΗΣ ΤΟΥ DSR

## 1. Εισαγωγή

Στην ενότητα αυτή παρουσιάζονται δύο μηχανισμοί που αναπτύξαμε, για την ενίσχυση του DSR, βασιζόμενοι στην εμπειρία μας από την προηγούμενη ενότητα. Ο πρώ-τος, που παρουσιάζεται στο κεφάλαιο 2, είναι ένας μηχανισμός για την πρόβλεψη απώλειας ζεύξης και σχεδιάστηκε για να εφαρμοστεί σε δυναμικό περιβάλλον με σκοπό να προλαβαίνει τις απώλειες δεδομένων που παρουσιάζονται, όταν συμβεί ένα σφάλμα διαδρομής στον DSR. Ο δεύτερος, που παρουσιάζεται στο κεφάλαιο 3, είναι ένας μηχανισμός συνολικής αντιμετώπισης κόμβων οι οποίοι επιδεικνύουν εγωιστική συμπεριφορά, απορρίπτοντας πακέτα που οφείλουν να προωθήσουν. Αποτελείται από ένα μηχανισμό ανακάλυψης τέτοιων κόμβων, που συνδυάζεται με τρεις προτεινόμενες στρατηγικές απομόνωσης.

## 2. Ο Μηχανισμός Πρόβλεψης Απώλειας Ζεύξης

Στο κεφάλαιο αυτό, στην πρώτη παράγραφο περιγράφεται ο μηχανισμός πρό-βλεψης απώλειας μίας ζεύξης. Η επόμενη παράγραφος παρουσιάζει την υλοποίηση για το μηχανισμό αυτό που κάναμε βασιζόμενοι πάνω στο μοντέλο του DSR για το OPNET. Στην παράγραφο 2.3 παρουσιάζονται τα πειράματα που εκτελέστηκαν στο OPNET και το κεφάλαιο κλείνει με τα αποτελέσματα και τα συμπεράσματα στα οποία καταλήξαμε για το μηχανισμό που προτείνουμε.

### 2.1 Σκοπός & Γενική Περιγραφή του μηχανισμού

Η κεντρική ιδέα αυτού το μηχανισμού είναι η δυνατότητα πρόβλεψης της απώλειας μίας ζεύξης, με σκοπό να προλαμβάνονται τα Σφάλματα Διαδρομής στο DSR. Στηριζόμενοι στο ίδιο σύνολο υποθέσεων που είδαμε στο κεφάλαιο 2 του Β' μέρους της εργασίας και εκμεταλλευόμενοι την εμπειρία που είχαμε αποκτήσαμε από την

δουλειά μας σε εκείνο το μέρος της εργασίας, καταλήξαμε σε ένα μηχανισμό που αποτελείται από ένα σύστημα παρακολούθησης των ζεύξεων και ένα μηχανισμό για τη διάδοση των αποτελεσμάτων του συστήματος στο δίκτυο. Και εδώ, επιδίωξη μας ήταν η ενσωμάτωση ολόκληρου του μηχανισμού που αναπτύξαμε στο DSR. Με το σκεπτικό αυτό, ο μηχανισμός που σχεδιάσαμε έχει ως εξής:

Όταν ένα κόμβος λάβει ένα πακέτο, γνωρίζει την τιμή του RSS του[5]. Η υπόθεση που κάνουμε είναι ότι παρακολουθώντας στο χρόνο την τη συμπεριφορά της τιμής RSS ανάμεσα σε δύο κόμβους μπορούμε να εξάγουμε συμπεράσματα για την μελλοντική συμπεριφορά της ζεύξης.

Η απλούστερη μέθοδος πρόβλεψης, την οποία και υλοποιήσαμε, είναι η παρακολούθηση της τιμής του RSS και της παραγώγου της. Η ιδέα είναι αρκετά απλή: όποτε ένας κόμβος λαμβάνει ένα πακέτο, μετράται η τιμή του RSS και όταν αυτή βρεθεί κάτω από ένα κατώφλι, τότε ελέγχεται η τιμή της παραγώγου του RSS. Εάν η παράγωγος είναι αρνητική, τότε αυτό λαμβάνεται ως ένδειξη ότι η ζεύξη, που βρίσκεται ήδη σε χαμηλό επίπεδο αξιοπιστίας λόγω του χαμηλού RSS, τείνει να χειροτερέψει ακόμα περισσότερο, οπότε πιθανότατα θα κοπεί σύντομα προκαλώντας σφάλμα διαδρομής. Αντίθετα, εάν τιμή του RSS είναι χαμηλή αλλά η παράγωγος είναι μη αρνητική, τότε η ζεύξη θεωρείται αξιόπιστη για το σύντομο μέλλον.

Τα πειράματα που εκτελέσαμε με αυτόν τον σχετικά απλό μηχανισμό έδειξαν ότι με σχεδόν απόλυτη επιτυχία εντοπίζονται ζεύξεις ανάμεσα σε κόμβους που απομακρύνονται και αποτελούν την σχεδόν αποκλειστική αιτία σφαλμάτων διαδρομής σε ένα περιβάλλον όπου οι κόμβοι συνεργάζονται πλήρως στο επίπεδο του DSR.

Όπως στο μηχανισμό εξάπλωσης διαδόσεων που είδαμε στο Β' μέρος της εργασίας στο κεφάλαιο 4, έτσι και εδώ, επιλέξαμε να περιορίσουμε την παραπάνω παρακολούθηση του RSS στα πακέτα δεδομένων. Επιπλέον, σε κάθε πακέτο δεδομένων, όπως θα δούμε παρακάτω στην παράγραφο της υλοποίησης του μηχανισμού, μεταφέρεται η δυαδική αξιοπιστία των ζεύξεων που χρησιμοποιούνται κατά την διαδρομή πηγής που ακολουθείται.

---

(5) *Οι κάρτες ασύρματου δικτύου IEEE 802.11b πρέπει να μετράνε την λαμβανόμενη ισχύ για να υποστηρίζουν την οπισθοχώρηση (fallback) σε ρυθμούς μικρότερους των 11Mbps (βλ. Α' Μέρος §1.5).*

Συγκεκριμένα, κάθε κόμβος αξιολογεί την ζεύξη μέσω της οποίας έφτασε το πακέτο σε αυτόν και εισάγει την πληροφορία αυτή στο πακέτο δεδομένων (*με τον τρόπο αυτό κάθε κόμβος που θα εντοπίσει μία επίφοβη ζεύξη ενημερώνει τους επόμενους κόμβους στην διαδρομή πηγής*). Στη συνέχεια, ελέγχει την αντίστοιχη πληροφορία που αφορά στις προηγούμενες ζεύξεις, η οποία έχει εισαχθεί από τους κόμβους από τους οποίους έχει ήδη περάσει το πακέτο. Εάν διαπιστωθεί ότι κάποιος κόμβος έκρινε μία ζεύξη ως *επίφοβη για απώλεια στο σύντομο μέλλον* τότε ο κόμβος που επεξεργάζεται το πακέτο ελέγχει την cache διαδρομών και διαγράφει όσες διαδρομές πηγής περιλαμβάνουν την ζεύξη αυτή.

Εάν ο κόμβος που επεξεργάζεται το πακέτο είναι ο πρώτος στη διαδρομή πηγής που θα βρει μια ζεύξη επίφοβη για απώλεια, τότε, εκτός της υποχρέωσης του να ενημερώσει τους κόμβους που έπονται στην διαδρομή πηγής, πρέπει να ενημερώσει και τους προ-ηγούμενους και συγκεκριμένα την πηγή του πακέτου δεδομένων. Εδώ βρίσκεται και η πρώτη «τροποποίηση» που κάναμε στο DSR. Χωρίς να έχει κοπεί η ζεύξη που περιγράφεται στην διαδρομή πηγής, ο κόμβος στέλνει ένα πακέτο Σφάλματος Διαδρομής. Αν και δεν υπάρχει ακόμα σφάλμα, το πακέτο αυτό παρόλο που θα μπορούσαμε να το χαρακτηρίσουμε πιο εύστοχα *πακέτο προειδοποίησης σφάλματος* (warning) εξακολουθούμε να το χαρακτηρίζουμε πακέτο σφάλματος διαδρομής, καθώς όπως θα δούμε παρακάτω υλοποιείται με ένα από τα υπάρχοντα πακέτα σφάλματος. Το πακέτο αυτό όπως θα περιγράψουμε την υλοποίηση έχει μία ιδιαιτερότητα που το κάνει να ξεχωρίζει από ένα κανονικό πακέτο σφάλματος διαδρομής toy DSR, οπότε παρόλο που βγαίνουμε εκτός πρωτοκόλλου, δεν χρειάζεται να ορίσουμε κάποιον νέο τύπο πακέτου.

Όταν ένας κόμβος λάβει ένα πακέτο σφάλματος διαδρομής που προκλήθηκε από το μηχανισμό πρόβλεψης απώλειας ζεύξεων τότε, εάν ο παραλήπτης είναι η πηγή από την οποία ξεκίνησε το πακέτο δεδομένων που προκάλεσε το «σφάλμα» (α) διαγράφει όλες τις διαδρομές που χρησιμοποιούν την επίφοβη ζεύξη και (β) ακολουθώντας το μηχανισμό συντήρησης διαδρομής, στέλνει ένα πακέτο Αίτησης Διαδρομής από Σφάλμα (*βλ.* Β' μέρος §6.1.β.1), στο οποίο όμως τώρα θα ενσωματώνεται η πληροφορία για τη ζεύξη που προκάλεσε αυτήν την Αίτηση Διαδρομής. Αυτό γίνεται, με σκοπό να

*μην* απαντήσει ένας κόμβος ο οποίος δεν άκουσε το πακέτο σφάλματος και έχει ακόμα στην cache του αποθηκευμένη μία διαδρομή που χρησιμοποιεί την επίφοβη ζεύξη. Εκτός από την επίφοβη ζεύξη αυτό το πακέτο της Αίτησης Διαδρομής από Σφάλμα μπορεί να περιλαμβάνει και όλες τις υπόλοιπες ζεύξεις οι οποίες είχαν κριθεί επίφοβες μέσα σε ένα χρονικό παράθυρο, με το σκεπτικό ότι ενδέχεται να μην έχουν ακόμα διαγραφεί από όλες τις caches ακόμα.

## 2.2 Υλοποίηση πάνω στο μοντέλο OPNET του DSR

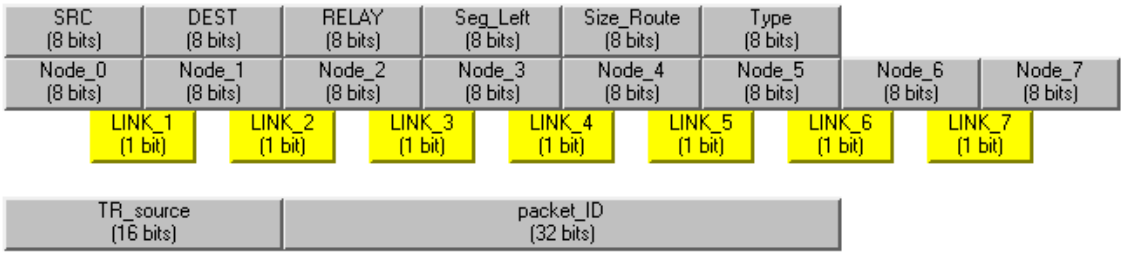
Για την υλοποίηση του μηχανισμού αυτού δεν απαιτήθηκε η προσθήκη νέων καταστάσεων στο μοντέλο διαδικασίας του μοντέλου DSR του WCTG του NIST που είδαμε στο σχήμα Β.6.3. Ριζικές αλλαγές έγιναν στον κώδικα των συναρτήσεων που χειρίζονται τα πακέτα δεδομένων, ώστε να υποστηρίζεται ο σύστημα παρακολούθησης των ζεύξεων, αλλά και να στέλνεται το πακέτο σφάλματος που παράγεται από το μηχανισμό ετούτο. Αλλαγές επίσης έγιναν στον κώδικα που χειρίζεται τα πακέτα των Αιτήσεων Διαδρομών, ώστε να πραγματοποιείται ο έλεγχος για τις επίφοβες ζεύξεις που περιγράψαμε στην προηγούμενη παράγραφο. Τέλος χρειάστηκαν οι ακόλουθες τροποποιήσεις των πακέτων του μοντέλου του DSR.

### 2.2.α *Τροποποιήσεις Πακέτων*

Όπως περιγράψαμε στην παράγραφο 2.1, χρησιμοποιήσαμε για το μηχανισμό αυτό ορισμένα πακέτα τα οποία διαφέρουν από αυτά που ορίζονται μέσα στο πρωτόκολλο, και κατ' επέκταση στο μοντέλο του WCTG για DSR.

#### 2.2.α.1 Το Νέο Πακέτο Δεδομένων

Στα πακέτα δεδομένων, όπως ορίζονται στο μοντέλο προσθέσαμε ένα πεδίο για κάθε ζεύξη (*βλ.* σχήμα Γ.2.1). κάθε τέτοιο πεδίο (LINK_xx) απαιτεί 1 bit μονάχα και σηματοδοτεί εάν η ζεύξη κρίνεται επίφοβη ή όχι. Η τιμή του πεδίου που χαρακτηρίζει τη ζεύξη ανάμεσα στους κόμβους Χ και Υ τίθεται από τον κόμβο Υ και η προκαθορισμένη του τιμή είναι 0, ενώ εάν ο κόμβος Υ κρίνει τη ζεύξη του με τον Χ ως επίφοβη, όπως παρουσιάσαμε στην προηγούμενη παράγραφο, τότε θέτει το πεδίο στην τιμή 1.

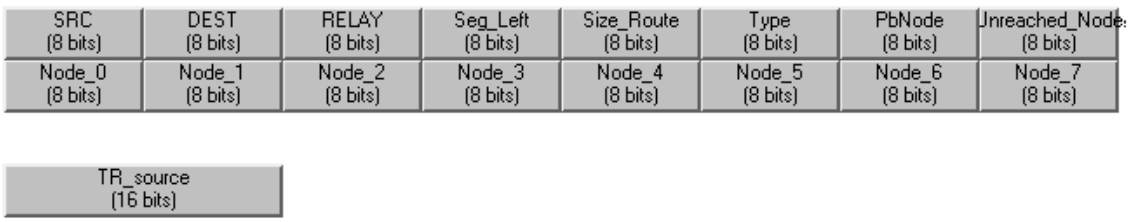



Σχήμα Γ.2.1: *Η επικεφαλίδα του πακέτου δεδομένων που χρησιμοποιήσαμε για το μηχανισμό πρόβλεψης απώλειας ζεύξης.*

## 2.2.α.2 Το Πακέτο Σφάλματος

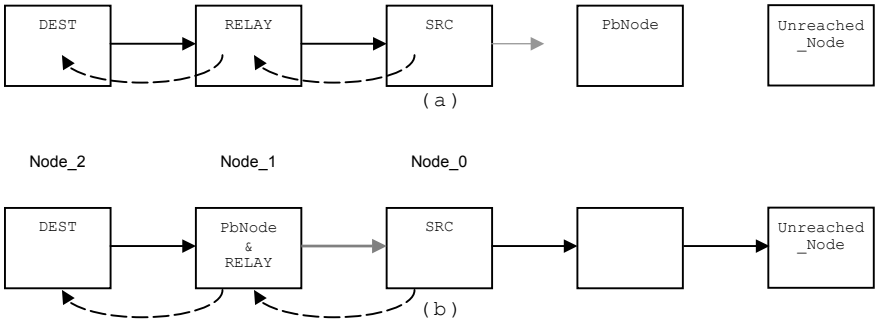
Το πακέτο σφάλματος δεν χρειάστηκε καμία απολύτως αλλαγή στα πεδία του. Η επικεφαλίδα του αρχικού πακέτου, την οποία χρησιμοποιήσαμε και εμείς, παρουσιάζεται στο σχήμα Γ.2.2.

Στο DSR, όταν συμβεί ένα σφάλμα διαδρομής θα σταλεί αυτό το πακέτο, στο οποίο το πεδίο SRC έχει την διεύθυνση του κόμβου που εντόπισε το σφάλμα διαδρομής, DEST είναι ο προορισμός του πακέτου σφάλματος –ισοδύναμα η πηγή του πακέτου δεδομένων που προκάλεσε το σφάλμα, RELAY είναι ο κόμβος στον οποίο απευθύνεται αυτό το πακέτο, PbNode είναι ο κόμβος που δεν επιβεβαίωσε το πακέτο δεδομένων. Άρα η ζεύξη που ορίζουν ο SRC με τον PbNode είναι η ζεύξη που έχει πλέον κοπεί. Τέλος Unreached_Node είναι ο κόμβος για τον οποίο προοριζόταν το πακέτο δεδομένων, άρα ο κόμβος για τον οποίο η πηγή του πακέτου δεδομένων, με τη λήψη αυτού του πακέτου σφάλματος, θα πρέπει να εκκινήσει το μηχανισμό ανακάλυψης διαδρομής. Τέλος τα πεδία Node_xx είναι η διαδρομή πηγής του πακέτου σφάλματος (δηλαδή ο στο Node_0 βρίσκεται ο SRC και στο τελευταίο έγκυρο πεδίο Node_xx βρίσκεται αντίστοιχα ο DEST).




Σχήμα Γ.2.2: *Το πακέτο σφάλματος του μοντέλου DSR.*

Αυτό που παρατηρήσαμε είναι ότι στον DSR ο PbNode βρίσκεται πάντα δεξιότερα από τον SRC στη διαδρομή πηγής του πακέτου δεδομένων που προκάλεσε το σφάλμα (*βλ.* σχήμα Γ.2.3.α.). Έτσι ο PbNode δεν εμφανίζεται μέσα στην διαδρομή πηγής του πακέτου σφάλματος. Αντίθετα, με τον τρόπο που ορίσαμε το μηχανισμό πρόβλεψης απώλειας ζεύξεων στην προηγούμενη παράγραφο, ο κόμβος που πρέπει να στείλει το πακέτο σφάλματος (δηλαδή ο SRC) βρίσκεται δεξιότερα, στην διαδρομή πηγής του πακέτου δεδομένων, από αυτόν που θα χαρακτηριστεί ως PbNode (*βλ.* σχήμα Γ.2.3.β.). Αυτό αφ' ενός σημαίνει ότι ο μηχανισμός που ορίσαμε υπονοούσε ότι η επίφοβη ζεύξη θα «ζει» ακόμα αρκετό χρόνο, ώστε να περάσει πάνω της το πακέτο σφάλματος, αφ' εταίρου, ότι τα πεδία Node_1 και PbNode ταυτίζονται. Χάρη στην τελευταία παρατήρηση, δεν καθί-σταται αναγκαία η δημιουργία καινούριου πακέτου για να υλοποιηθούν τα μηνύματα σφάλματος του μηχανισμού ετούτου.




Σχήμα Γ.2.3: (α) *Σφάλμα Διαδρομής DSR: Ο PbNode δεν έστειλε στον SRC επιβεβαίωση, προκαλώντας την μετάδοση ενός πακέτου Σφάλματος Διαδρομής. Η διαδρομή πηγής του πακέτου Σφάλματος Διαδρομής φαίνεται με τη διακεκομμένη γραμμή. Επάνω στους κόμβους είναι σημειωμένα τα πεδία του πακέτου Σφάλματος Διαδρομής.*

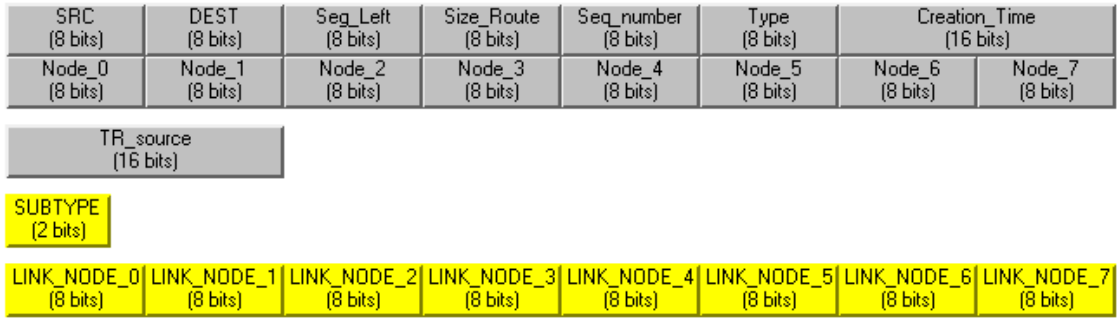
(β) *Σφάλμα Διαδρομής μηχανισμού Πρόβλεψης Απώλειας Διαδρομών: Ο SRC έκρινε ότι η ζεύξη του με τον PbNode είναι επίφοβη και έστειλε ένα πακέτο σφάλματος με τα πεδία όπως φαίνονται επάνω στους κόμβους. Και στις δύο περιπτώσεις η διαδρομή πηγής του πακέτου σφάλματος είναι η ίδια, όπως φαίνεται από τις διακεκομμένες γραμμές και τα αντίστοιχα πεδία Node_xx ανάμεσα στα δύο σχήματα.*

### 2.2.α.3 Το Νέο πακέτο Αίτησης Διαδρομής

Το πακέτο Αίτησης Διαδρομής, σύμφωνα με το μηχανισμό που περιγράψαμε στην παράγραφο 2.1, μπορεί να περιλαμβάνει τις ζεύξεις εκείνες που θεωρούνται επίφοβες για τον κόμβο που το έστειλε αρχικά. Η κάθε ζεύξη περιγράφεται από το ζευγάρι των

κόμβων που συνδέει. Έτσι στο μοντέλο του DSR του OPNET επεκτείναμε το πακέτο της Αίτησης Διαδρομής, ώστε να έχει τα πεδία LINK_NODE_0 έως LINK_NODE_7, που ορίζουν τέσσερις ζεύξεις (*βλ.* σχήμα Γ.2.4).

Ο μηχανισμός αυτός θυμίζει αρκετά την τεχνική της αυξημένης διάδοσης μηνυμάτων σφάλματος διαδρομής που ορίζεται στο πρωτόκολλο του DSR (βλ. Α' μέρος §4.5.γ). Η διαφορά είναι ότι η πρόταση μας με το να εισάγει μόνο κόμβους που ανά ζεύγος ορίζουν μία επίφοβη ζεύξη, είναι αισθητά πιο οικονομική στην πλεονάζουσα πληροφορία που εισάγει, από ότι η επισύναψη ολόκληρου του πακέτου σφάλματος διαδρομής που την προκάλεσε. Αυτό υπονοεί ότι με ένα τέτοιου τύπου πακέτο θα μπορούσε να υλοποιηθεί και η τεχνική της αυξημένης διάδοσης μηνυμάτων σφάλματος διαδρομής.




Σχήμα Γ.2.4: *Η επικεφαλίδα του πακέτου δεδομένων που χρησιμοποιήσαμε για το μηχανισμό πρόβλεψης απώλειας ζεύξης.*

Πρέπει να σημειωθεί ότι επιλέξαμε στατικό μέγιστο αριθμό επίφοβων ζεύξεων ανά κόμβο, παρόλο που σε πολλές περιπτώσεις, όπως διαπιστώσαμε πειραματικά, οι επίφοβες ζεύξεις ανά κόμβο μπορεί να είναι σαφώς λιγότερες. Η επιλογή αυτή έγινε διότι η δυναμική δημιουργία πεδίων στην έκδοση του OPNET που χρησιμοποιούμε προϋποθέτει ότι όλα τα πεδία στο πακέτο πρέπει να είναι δυναμικά, πράγμα που σημαίνει ότι έπρεπε να αλλαχθούν στον κώδικα του μοντέλου όλες οι συναρτήσεις που χειρίζονται πακέτα –πρακτικά δηλαδή όλος ο κώδικας, πράγμα το οποίο κρίναμε εξαιρετικά επίπονο και χρονοβόρο για το όφελος που θα απέδιδε στις προσομοιώσεις μας.

## 2.3 Περιγραφή πειραμάτων

Τα πειράματα προσομοιώθηκαν σε ένα 500x500$m^2$ ελεύθερο χώρο. Χρησιμο-ποιήθηκαν 8 κόμβοι για να προσομοιωθεί ένα αραιό δίκτυο και 24 για ένα πυκνό δίκτυο. Οι σταθμοί εκπέμπουν με ισχύ 100mW. Θεωρήσαμε ως μοντέλο διάδοσης η/μ κυμάτων το μοντέλο δύο κλίσεων και ευαισθησία λήψης τα -94dB. Έτσι, η ακτίνα κάλυψης ενός σταθμού είναι τα 100m. Η πηγή κάθε κόμβου παράγει μικρά (128bit), μεσαία (512bit) και μεγάλα (1024bit) πακέτα δεδομένων (payload). Το μεσοδιάστημα ανάμεσα σε δύο πακέτα της ίδιας πηγής έχει εκθετική συνάρτηση πυκνότητας πιθανότητας με μέση τιμή 0,25s.

Η κινητικότητα των κόμβων περιγράφεται με το μοντέλο μπιλιάρδου, στο οποίο ένας κόμβος επιλέγει μία τυχαία κατεύθυνση, την οποία ακολουθεί με προκαθορισμένη ταχύτητα -κοινή για όλους τους κόμβους. Όταν ο κόμβος φτάσει στα όρια του χώρου προσομοίωσης «ανακλάται», επιλέγοντας μία νέα τυχαία κατεύθυνση. Έχοντας κατά νου το μοντέλο κίνησης τυχαίου προορισμού (Random Waypoint), καθώς και τα προβλήματα που έχουν αναφερθεί για αυτό [23], τροποποιήσαμε το μοντέλο μπιλιάρδου ώστε κάθε κόμβος σε τυχαία στιγμή να σταματάει για ένα μικρό διάστημα, ώστε συνολικά να κινείται κατά το 80% του χρόνου προσομοίωσης Με τον τρόπο αυτό έχουμε καταφέρει να διατηρήσουμε μια σταθερή, προκαθορισμένη μέση ταχύτητα στο δίκτυο, ενώ παράλληλα δίνουμε μία μεγαλύτερη ρεαλιστικότητα στο μοντέλο. Έτσι στα πειράματα μας ορίσαμε ακίνητα δίκτυα (ως σημείο αναφοράς), δίκτυα με μικρή κινητικότητα (όλοι οι κόμβοι κινούμενοι με ταχύτητα 0,5m/s) και δίκτυα με μεγάλη κινητικότητα (όλοι οι κόμβοι κινούμενοι με ταχύτητα 5m/s, ταχύτητα δηλαδή των 18km/h).

Στα αρχικά μας πειράματα παρατηρήσαμε ότι σε ένα στατικό δίκτυο με απλό DSR οι caches διαδρομών των κόμβων γεμίζουν μέσα σε λιγότερο από 30sec, με αποτέλεσμα από εκεί και έπειτα, να μην χρειάζονται πακέτα Αίτησης/Απάντησης Διαδρομής και συνεπώς η μόνη πλεονάζουσα πληροφορία που μεταδίδεται να είναι η επικεφαλίδα των πακέτων δεδομένων, δηλαδή 160bits/πακέτο, που αντιστοιχούν θεωρητικά σε πλεονασμό 55,55%, 23.81% και 13.51% για μικρά, μεσαία και μεγάλα πακέτα αντίστοιχα. Έτσι, τα πειράματα που παρουσιάζονται παρακάτω έχουν χρόνο εκτέλεσης 5min. Στο χρόνο

αυτό, ακόμα και με την ταχύτητα των 0.5m/s ένας κόμβος διανύει σε ευθεία 120m, οπότε, μπορούμε με βεβαιότητα να πούμε ότι θα υπάρχουν ζεύξεις που θα κοπούν.

Με βάση τα παραπάνω εκτελέστηκαν πειράματα στα οποία μελετήθηκαν:

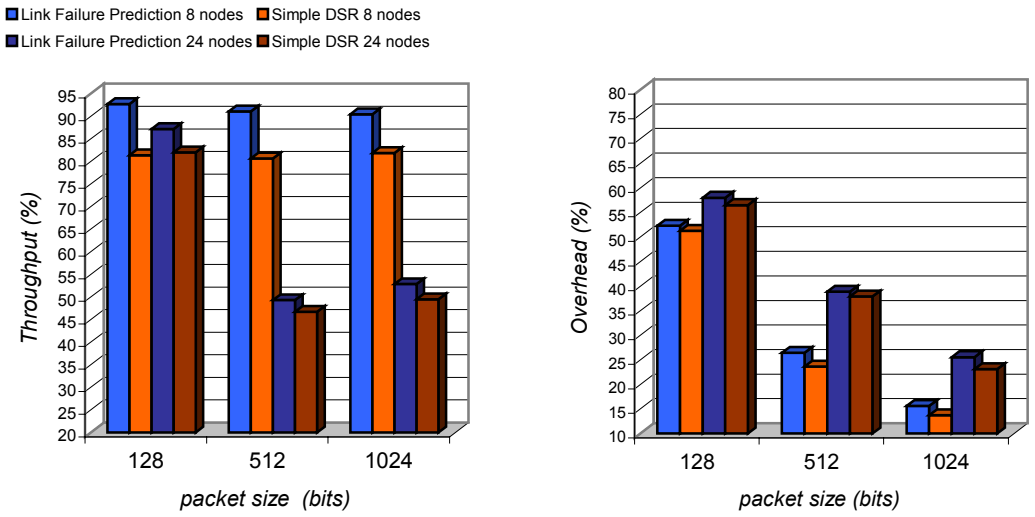
- το ποσοστό της πλεονάζουσας πληροφορίας:
  *Overhead* = [(*control bits*)+(*data header bits*) / (*total bits transported*)] x 100%, όπου ως control bits υπολογίζονται ολόκληρα τα πακέτα Αιτησης/Απάντησης και Σφάλματος Διαδρομής του DSR.).

- το ποσοστό του throughput μετρημένου σε πακέτα ανά κόμβο του δικτύου.
  Ως 100% λαμβάνεται η μέση τιμή του ρυθμού παραγωγής πακέτων από την πηγή κάθε κόμβου, δηλαδή 4 πακέτα ανά δευτερόλεπτο.

## 2.4 Αποτελέσματα - Συμπεράσματα

Το σύστημα παρακολούθησης και ανακάλυψης επίφοβων ζεύξεων σε όλα τα πειράματα είχε απόλυτη επιτυχία: σε όλα τα πειράματα ανακάλυπτε ορθά κάθε ζεύξη που λόγω κίνησης θα κοβόταν. Σε δίκτυό με χαμηλή κινητικότητα αυτό συνέβη μέχρι και περίπου 25 δευτερόλεπτα προτού κοπεί η ζεύξη. Δεν παρατηρήσαμε περίπτωση όπου ο μηχανισμός έκρινε μία ζεύξη ως επίφοβη χωρίς αυτή να είναι.

Ολοκληρωμένος ο μηχανισμός μας, σε δίκτυα μικρής κινητικότητας είχε αρκετά θετική επίδραση στο throughput το οποίο αύξησε έως και κατά 11 ποσοστιαίες μονάδες. Ο επιπλέον πλεονασμός που εισήγαγε ήταν της τάξης του +1% έως +3%. Τα αποτελέσματα φαίνονται συγκεντρωτικά στο σχήμα Γ.2.5.

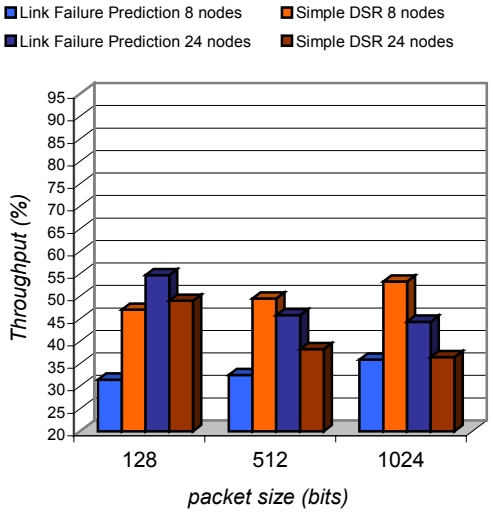


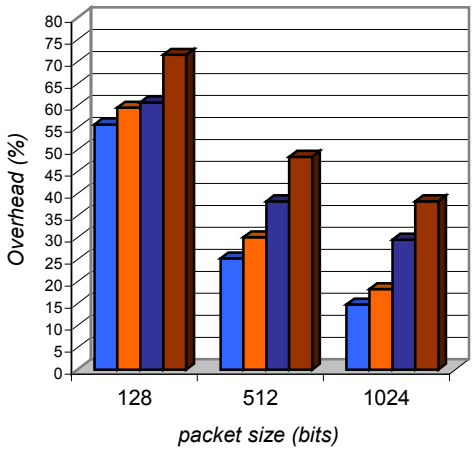

Σχήμα Γ.2.5: *Δίκτυα με μικρή κινητικότητα: Η μέση ταχύτητα κόμβου είναι 0.5m/s. (α) Το throughput για διάφορα μεγέθη πακέτων δεδομένων, σε αραιό και πυκνό δίκτυο με και χωρίς το μηχανισμό πρόβλεψης απώλειας ζεύξης. (β) Η πλεονάζουσα πληροφορία ομοίως.*

Σε δίκτυα με μεγάλες ταχύτητες (*βλ.* σχήμα Γ.2.6), παρατηρήσαμε ότι ο μηχανισμός μας δεν είχε την αναμενόμενη επίδραση στο throughput στα αραιά δίκτυα, σε αντίθεση με τα πυκνά δίκτυα των 24 κόμβων, όπου τα αποτελέσματα ήταν αρκετά καλά: αύξηση throughput έως και 7,8 ποσοστιαίες μονάδες. Επίσης, απροσδόκητη, με βάση τα προηγούμενα αποτελέσματα μας, ήταν και η ελάττωση της πλεονάζουσας πληροφορίας που επιτεύχθηκε.

Συμπερασματικά, ο μηχανισμός πρόβλεψης απώλειας ζεύξης, παρά την απλότητα που τον χαρακτηρίζει, επιφέρει εν γένει θετικά αποτελέσματα, καθώς εξαιρουμένης μίας μόνο περίπτωσης, επιτυγχάνει να αυξήσει το throughput, χωρίς να επιφέρει υπολογίσιμες αυξήσεις στην πλεονάζουσα πληροφορία που εισάγει. Εντούτοις, πιστεύουμε ότι ο μηχανισμός αυτός θα δρούσε με σαφώς ευεργετικότερα αποτελέσματα εάν το μοντέλο του DSR υποστήριζε caches με πολλαπλές διαδρομές ανά προορισμό. Σε αυτήν την περίπτωση η πλεονάζουσα πληροφορία θα ελαττωνόταν στο ελάχιστο, διότι κάθε ανακάλυψη μίας επίφοβης ζεύξης δεν θα συνεπαγόταν άμεσα την κλήση του μηχανισμού ανακάλυψης διαδρομής. Επίσης οι συνολικές καθυστερήσεις που εισάγονται από το μηχανισμό

ανακάλυψης διαδρομής από σφάλμα θα ελαττώνονταν με αποτέλεσμα την αύξηση του throughput.




(α)

(β)

Σχήμα Γ.2.6: *Δίκτυα με έντονη κινητικότητα: Η μέση ταχύτητα κόμβου εδώ είναι 5m/s. (α) Το throughput για διάφορα μεγέθη πακέτων δεδομένων, σε αραιό και πυκνό δίκτυο με και χωρίς το μηχανισμό πρόβλεψης απώλειας ζεύξης. (β) Η πλεονάζουσα πληροφορία ομοίως.*

## 3. Ο Μηχανισμός αντιμετώπισης κόμβων με εγωιστική συμπεριφορά.

## 3.1 Εγωισμός στο DSR

Στο προηγούμενο μέρος της εργασίας μας, ισχυρά επηρεασμένοι από τις σχετικές εργασίες που μελετήσαμε αρχικά, χρησιμοποιήσαμε ένα μοντέλο εγωισμού για τον DSR στο οποίο, ο εγωιστικά συμπεριφερόμενος κόμβος μπορούσε να μη μετέχει στην διαδικασία προώθησης πακέτων *ή* στην διαδικασία ανακάλυψης διαδρομής. Το μοντέλο αυτό κρίναμε ότι είναι υπερβολικά απλοϊκό και δεν αντανακλά σε μία συμπεριφορά που θα είχε νόημα για έναν κόμβο. Η εγωιστική συμπεριφορά δεν θα έπρεπε να ενέχει στοιχεία κακίας, εντούτοις, ένας κόμβος που δεν προωθεί πακέτα ενώ συμμετέχει στην ανακάλυψη διαδρομής προσφέρει εν γνώση του στο δίκτυο διαδρομές πηγής οι οποίες δεν καταλήγουν στον προορισμό τους και μάλιστα κατά μη αναγνωρίσιμο από το DSR τρόπο.

Μελετώντας διεξοδικά το πρωτόκολλο, υπό το πρίσμα ότι η εγωιστική συμπεριφορά που θέλουμε να αντιμετωπίσουμε δεν θα οφείλεται σε κακία αλλά σε μία προσπάθεία αυτοσυντήρησης (πχ: Ένας κόμβος που έχει χαμηλή μπαταρία επιλέγει να γίνει εγωιστής για να «ζήσει» περισσότερο), καταλήξαμε στο παρακάτω μοντέλο για την εγωιστική συμπεριφορά.

- Ένας κόμβος θα εμφανίζει εγωιστική συμπεριφορά σε τυχαία χρονική στιγμή, και θα την διατηρεί για ένα σχετικά μεγάλο χρονικό διάστημα. Δηλαδή δεν θα απορρίπτει ένα ποσοστό από τα πακέτα που πρέπει να εξυπηρετήσει όταν ο κόμβος αποφασίσει να γίνει εγωιστής ακολουθεί τη συμπεριφορά αυτή σε όλα τα πακέτα που καλείται να εξυπηρετήσει.
- Η αντιμετώπιση του προς όλους τους υπόλοιπους κόμβους θα είναι κοινή, δεν υπάρχουν δηλαδή «ομάδες φίλων κόμβων» και ο εγωιστικά φερόμενος κόμβος δεν θα αποφασίζει με βάση τον αποστολέα του πακέτου δεδομένων που χρειάζεται προώθηση ή του πακέτου αίτησης διαδρομής που έλαβε.
- Ένας κόμβος που αποφάσισε να επιδείξει εγωιστική συμπεριφορά θα παύει να προωθεί πακέτα δεδομένων. Όποιο πακέτο δεδομένων φτάσει στον κόμβο αυτό χωρίς να τον έχει ως στόχο θα απορρίπτεται άμεσα.
- Ένας κόμβος που αποφάσισε να επιδείξει εγωιστική συμπεριφορά θα παύει στέλνει Απαντήσεις Διαδρομής. Εξαίρεση θα αποτελούν:

- Οι αιτήσεις εκείνες που τον φέρουν ως στόχο τους: Με τον τρόπο αυτό ο κόμβος διατηρεί την «ύπαρξη» του μέσα στο δίκτυο μέσω διαδρομών που τον φέρουν ως προορισμό. Ο λόγος είναι ότι ο κόμβος μπορεί να περιμένει δεδομένα από κάποιον άλλο μέσα στο δίκτυο.
- Οι χαριστικές απαντήσεις (gratuitous route replies, *βλ.* Μέρος Α' §4.5.β) αλλά μόνο στην περίπτωση που ο εγωιστής κόμβος είναι ο στόχος του πακέτου δεδομένων που τις προκάλεσε: Οι χαριστικές απαντήσεις, ανανεώνουν την διαδρομή πηγής σε μία μικρότερη (σε πλήθος βημάτων). Ο κόμβος λοιπόν δίνοντας χαριστικές απαντήσεις, ελαττώνει τα βήματα της διαδρομής με την οποία κάποιος επικοινωνεί με αυτόν άρα ελαττώνει την από άκρου εις άκρο καθυστέρηση.

Σημειώνουμε ότι ο εγωιστής κόμβος παύει και την προώθηση πακέτων δεδομένων και την συμμετοχή του στην ανακάλυψη διαδρομής. Η αιτιολόγηση είναι ότι αν πάψει να προωθεί πακέτα δεδομένων αλλά συνεχίσει να απαντάει σε αιτήσεις διαδρομών, τότε απαντώντας σε μία αίτηση διαδρομής για την οποία δεν είναι στόχος δίνει μία διαδρομή στην οποία είναι ενδιάμεσος. Η συμπεριφορά αυτή μπορεί καλύτερα να χαρακτηριστεί ως κακία παρά ως εγωισμός, γιατί εν γνώση του ο κόμβος προσφέρει μία διαδρομή που δεν θα φτάσει στον προορισμό της. Αντίθετα, εάν ένας κόμβος προωθεί πακέτα, χωρίς να διαφημίζει διαδρομές, τότε δεν θα έχει ουσιαστικό όφελος, γιατί ήδη θα μετέχει σε ορισμένες διαδρομές από το παρελθόν –μη απαντώντας σε διαδρομές όμως από την αρχή της εισαγωγής του στο δίκτυο, επιτυγχάνει να θεωρείται ως περιφερειακός κόμβος και αυτή είναι μία συμπεριφορά που δεν ανιχνεύεται παρά μόνο με χρήση του μηχανισμού αδιάκριτης λήψης και παράλληλα οργάνωση με μορφή γράφων των cache διαδρομών.

- Τέλος ο εγωιστής κόμβος θα μετέχει ορθά την Συντήρηση Διαδρομών. Η λογική είναι ότι όταν θα στείλει σε κάποιον κόμβο ένα πακέτο σφάλματος ως αποτέλεσμα ο παραλήπτης του θα διαγράψει την παλιά διαδρομή πηγής που χρησιμοποιούσε τον εγωιστή κόμβο. Όταν στη συνέχεια μεταδώσει την Αίτηση Διαδρομής από Σφάλμα, ο εγωιστής δεν θα απαντήσει, οπότε παύει να βρίσκεται ως ενδιάμεσος σε τουλάχιστον μία διαδρομή ενός τουλάχιστον κόμβου. Με τον τρόπο αυτό ο εγωιστής γλιτώνει και την επεξεργασία πακέτων δεδομένων τα οποία θα απέρριπτε στο

μέλλον. Αν αντίθετα δεν συμμετείχε στην Συντήρηση Διαδρομών προωθώντας τα πακέτα Σφάλματος, τότε θα παρέμενε σε μία κομμένη διαδρομή, όπου η πηγή της δεν θα γνώριζε ότι έχει κοπεί και συνεπώς θα εξακολουθούσε να στέλνει πακέτα μέσω αυτής, άρα να απασχολεί τον εγωιστή κόμβο. Η περίπτωση αυτή είναι βέβαια σπάνια, γιατί ο εγωιστής κόμβος θα κληθεί να προωθήσει ένα πακέτο σφάλματος μονάχα αν όταν δεν ήταν εγωιστής είχε προωθήσει κάποιο πακέτο δεδομένων το οποίο ανακάλυψε το σφάλμα, στη συνέχεια η συμπεριφορά του κόμβου άλλαξε και έγινε εγωιστική και αργότερα έφτασε σε αυτόν το πακέτο του σφάλματος. Η γενική περίπτωση είναι ότι ο εγωιστής κόμβος δεν θα κληθεί να προωθήσει ένα πακέτο σφάλματος διαδρομής, καθώς δεν θα έχει προωθήσει πακέτο δεδομένων.

## 3.2 Ανακάλυψη εγωιστικά συμπεριφερόμενων κόμβων

Έχοντας κατά νου το παραπάνω μοντέλο εγωιστικής συμπεριφοράς ενός κόμβου στο DSR, καθώς και τον μηχανισμό βαθμολόγησης της εκτίμησης προώθησης που είχαμε αναπτύξει για στο δεύτερο μέρος της εργασίας (§6.2 κ' §7.1), ο μηχανισμός για την ανακάλυψη ενός κόμβου με εγωιστική συμπεριφορά αναπτύχθηκε σε παρόμοιο μοτίβο.

Η κεντρική ιδέα είναι εδώ ότι ένας κόμβος που δεν θα προωθήσει ένα πακέτο δεδομένων είναι εγωιστής. Άρα όπως και στο Β' μέρος όταν ένας κόμβος στείλει για προώθηση ένα πακέτο, παρακολουθεί το μέσο με το μηχανισμό αδιάκριτης, για ένα χρονικό διάστημα (*βλ.* Β' μέρος Πλαίσιο 6.1). Εδώ όμως σε αντίθεση με το μηχανισμό που κατασκευάσαμε στο Β' μέρος μία εσφαλμένη παρατήρηση, όπως την περιγράψαμε στην §7.1, θα είχε το αποτέλεσμα να χαρακτηριστεί εγωιστής ένας κόμβος που δεν έχει εγωιστική συμπεριφορά, απλά έτυχε να έχει στον ενταμιευτή αποστολής του μεγάλη ουρά.

Για να αποφευκτεί κάτι τέτοιο εισάγαμε ένα *πακέτο διερεύνησης* (probe packet –*βλ.* παρακάτω §3.4.β.1). Το πακέτο αυτό έχει ως παραλήπτη τον ίδιο τον αποστολέα και ως ενδιάμεσο τον κόμβο που θέλουμε να εξετάσουμε. Έτσι, αν ένας κόμβο ο οποίος έστειλε επιτυχώς ένα πακέτο για προώθηση, περιμένει το προκαθορισμένο χρονικό διάστημα για την αδιάκριτη λήψη της επανεκπομπής του πακέτου από τον ενδιάμεσο και στο διάστημα αυτό δεν ακούσει το

πακέτο του να επανεκπέμπεται τότε, προκειμένου να βεβαιωθεί ότι ο ενδιάμεσος είναι πράγματι εγωιστής, μπαίνει σε μια διαδικασία διερεύνησης, κατά την οποία στέλνει περιοδικά στον «ύποπτο» κόμβο πακέτα διερεύνησης. Η έναρξη της διαδικασίας διερεύνησης δεν πρέπει να είναι άμεση, ώστε να αποφευχθεί η περίπτωση όπου ο ενταμιευτής αποστολής του ενδιάμεσου δεν θα έχει αδειάσει όταν θα πρέπει να προωθήσει ένα πακέτο διερεύνησης. Η διαδικασία αυτή αν και εισάγει πλεονάζουσα πληροφορία (όλα τα πακέτα διερεύνησης πρέπει να μετρώνται ως πλεονασμός) μπορεί να πραγματοποιηθεί επιτυχώς ακόμη και από μονάχα ένα πακέτο όπως διαπιστώσαμε πειραματικά, το οποίο μάλιστα είναι αρκετά περιορισμένου μεγέθους.

Όταν περατωθεί η διαδικασία αυτή, ο κόμβος που την ξεκίνησε γνωρίζει εάν ο γείτονας του είναι εγωιστής. Στην περίπτωση που η απάντηση είναι θετική, τότε την καταγράφει, μαζί με το χρόνο παρατήρησης σε έναν *πίνακα εγωισμού* (selfishness table), τον οποίο συμβουλεύεται σε κάθε πακέτο δεδομένων που αναλαμβάνει να προωθήσει. Ο χρόνος παρατήρησης έχει το νόημα ότι η εγγραφή αυτή δεν πρέπει να είναι μόνιμη, αλλά να διατηρείται για ένα συγκεκριμένο χρόνο μετά το πέρας του οποίου ο γείτονας θα πάψει να θεωρείται εγωιστής. Προφανώς εάν ο κόμβος έχει ακόμη μετά το πέρας αυτού το χρόνου διατηρήσει την εγωιστική του συμπεριφορά, αυτό θα διαπιστωθεί με την επόμενη προώθηση πακέτου δεδομένων...

## 3.3 Τακτικές αντίδρασης στον εγωισμό κόμβου

Στην περίπτωση που θα διαπιστωθεί από κάποιον με βεβαιότητα ότι ένας άλλος κόμβος είναι πράγματι εγωιστής, τότε για τον κόμβο που έκανε τη διαπίστωση ορίσαμε και μελετήσαμε τρεις τακτικές αντίδρασης.

Και οι τρεις τακτικές μας έχουν ένα κοινό χαρακτηριστικό στην αντιμετώπιση των εγωιστών: Όταν σε έναν κόμβο φτάσει ένα πακέτο δεδομένων που χρειάζεται προώθηση, ο κόμβος αυτός ανεξάρτητα από την τακτική που θα ακολουθήσει, το πρώτο βήμα που κάνει είναι να ελέγξει εάν η διαδρομή πηγής του πακέτου περιλαμβάνει στα ενδιάμεσα (πλην πηγής και στόχου) βήματα κάποιον κόμβο που βρίσκεται στον πίνακα εγωισμού του. Εάν συμβαίνει κάτι τέτοιο,

τότε ο κόμβος γνωρίζει ότι η διαδρομή αυτή θα αποτύχει, οπότε, οφείλει να στείλει στην πηγή ένα μήνυμα *σφάλματος διαδρομής από εγωισμό* (Selfish Route Error) και να σταματήσει το πακέτο.

Ένα πακέτο σφάλματος διαδρομής από εγωισμό, κύριο σκοπό έχει να καταδείξει τον πρώτο εγωιστή κόμβο κατά μήκος μίας διαδρομής πηγής, επίσης σκοπό έχει να ενημερώσει την πηγή του πακέτου δεδομένων ότι ο στόχος πλέον δεν είναι προσβάσιμος μέσω της διαδρομής του πακέτου δεδομένων. Το πακέτο σφάλματος διαδρομής από εγωισμό δρομολογείται με μία διαδρομή πηγής που είναι η αντίστροφη από έως τώρα διαδρομή πηγής του πακέτου δεδομένων που το προκάλεσε. Έτσι, ένας κόμβος που θα λάβει ένα τέτοιο πακέτο, αυτό που κάνει είναι να ελέγξει την cache διαδρομών του και να αποβάλλει από αυτήν όσες διαδρομές χρησιμοποιούν *ως ενδιάμεσο* τον κόμβο που το πακέτο σφάλματος είχε χαρακτηρίσει ως εγωιστή. Ο παραλήπτης του πακέτου σφάλματος, επίσης θέτει στον πίνακα εγωισμού του για τον εγωιστή κόμβο το χρόνο παρατήρησης να είναι η χρονική στιγμή που έλαβε το πακέτο σφάλματος. Εάν ο παραλήπτης είναι και ο στόχος στη διαδρομή πηγής του πακέτου σφάλματος (άρα ήταν η πηγή του πακέτου δεδομένων που προκάλεσε το σφάλμα), τότε ο κόμβος αυτός θα ξεκινήσει μία ανακάλυψη διαδρομής για τον προορισμό, στην οποία θα ζητάει μία διαδρομή για το στόχο του, η οποία όμως δεν πρέπει να περιλαμβάνει κανέναν από τους κόμβους που έχει στον πίνακα εγωισμού του.

Εκτός από αυτούς τους γενικούς κανόνες, οι κόμβοι του δικτύου μπορούν να αντιμετωπίζουν με τρεις τρόπους κλιμακούμενης «σκληρότητας» στους εγωιστές κόμβους:

### 3.3.α *Αφελής Αντιμετώπιση*

Σε αυτήν την τακτική, ο κόμβος που διαπιστώνει ότι άλλος κόμβος είναι εγωιστής τον αντιμετωπίζει με αρκετή επιείκεια, αποφεύγοντας μονάχα να τον χρησιμοποιήσει ως ενδιάμεσο. Συγκεκριμένα:

- Δεν χρησιμοποιεί εγωιστή κόμβο ως ενδιάμεσο στην cache διαδρομών του.
- Προωθεί προς τον εγωιστή οποιοδήποτε πακέτο έχει στόχο αυτόν.

- Αποδέχεται και εξυπηρετεί οποιοδήποτε πακέτο δεδομένων πηγάζει από εγωιστή.

Με την τακτική αυτή δεν μπορεί κανείς να ισχυριστεί ότι ενθαρρύνεται / επιβάλλεται κατά οποιονδήποτε τρόπο η συνεργασία. Αντίθετα, ένας εγωιστής κόμβος εξακολουθεί να είναι μέσα στο δίκτυο, ανταλλάσσοντας ό,τι πληροφορία χρειάζεται, χωρίς να βαρύνεται με την υποχρέωση να προωθεί πακέτα.

### 3.3.β *Δίκαιη Αντιμετώπιση*

Στην τακτική αυτή, ένας κόμβος που χαρακτηρίζει έναν δεύτερο κόμβο ως εγωιστή, από το σημείο αυτό και μετά, εκτός του ότι αποφεύγει να τον χρησιμοποιήσει ως ενδιάμεσο, παύει επίσης να προωθεί πακέτα δεδομένων που πηγάζουν από εκείνον, δηλαδή:

- Δεν χρησιμοποιεί τον εγωιστή ως ενδιάμεσο κόμβο στην cache διαδρομών του.
- Προωθεί προς τον εγωιστή οποιοδήποτε πακέτο έχει στόχο αυτόν.
- Δεν εξυπηρετεί πακέτα δεδομένων που πηγάζουν από εγωιστή κόμβο.

Με αυτήν την τακτική αυτή, μερικώς απομονώνεται ο εγωιστής, καθώς δεν μπορεί πια να στείλει δεδομένα. Η λογική της τακτικής αυτής στηρίζεται στην ανταποδοτικότητα [12].

### 3.3.γ *Σκληρή αντιμετώπιση*

Στην τακτική αυτή, ένας κόμβος που χαρακτηρίζει έναν δεύτερο κόμβο ως εγωιστή κάνει από το σημείο αυτό και μετά, ό,τι μπορεί για να τον απομονώσει. Έτσι:

- Δεν χρησιμοποιεί τον εγωιστή ως ενδιάμεσο κόμβο στην cache διαδρομών του.
- Δεν εξυπηρετεί πακέτα δεδομένων που πηγάζουν από εγωιστή κόμβο.
- Αντιμετωπίζει πακέτα με στόχο τον εγωιστή ως και εάν να τον είχαν ενδιάμεσο.

Με την τακτική αυτή προσπαθούμε να δώσουμε τα ισχυρότερα αντικίνητρα για εγωιστική συμπεριφορά. Ο σκοπός εδώ είναι να

απομονωθεί κατά το δυνατό το συντομότερο ο εγωιστής κόμβος με έναν κατ' απαίτηση (on demand) μηχανισμό.

## 3.4 Υλοποίηση πάνω στο μοντέλο OPNET του DSR

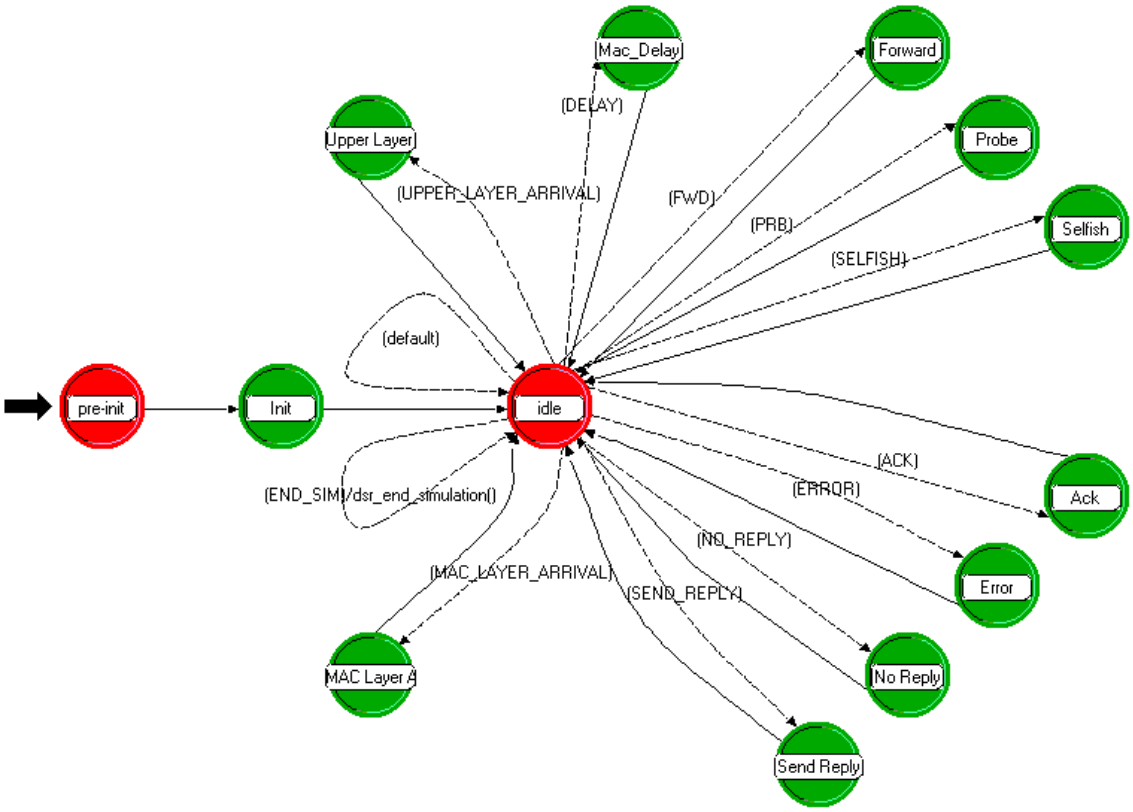
### 3.4.α *Προσθήκες στο μοντέλο διαδικασίας*

Για να υλοποιηθεί ο μηχανισμός που περιγράψαμε σε αυτήν την παράγραφο, έγιναν σημαντικές προσθήκες στο μοντέλο διαδικασίας του μοντέλου DSR του WCTG του NIST που είδαμε στο σχήμα Β.6.3. Συγκεκριμένα το νέο μοντέλο όπως τελικά προέκυψε φαίνεται στο σχήμα Γ.3.1.

Ο μηχανισμός ανακάλυψης κόμβων με εγωιστική συμπεριφορά περιγράφεται στις νέες καταστάσεις Forward, Probe και Selfish. Στην τελευταία από τις τρεις γίνονται και οι διαδικασίες που είναι κοινές στην περίπτωση που διαπιστωθεί ότι ένας κόμβος είναι εγωιστής (*βλ.* §3.3).

Forward: Κατά όμοιο τρόπο με την κατάσταση Forward που είχαμε ορίσει στο Β' μέρος της εργασίας μας (*βλ.* Β' μέρος §6.3), ελέγχεται ένας πίνακας προωθήσεων (*βλ.* πλαίσιο Β.6.1). Στην περίπτωση που διαπιστωθεί ότι ένας κόμβος δεν προώθησε κάποιο πακέτο, μεταβαίνουμε στην κατάσταση Probe. Από την κατάσταση αυτή τέλος φεύγουμε, μεταβαίνοντας στην κατάσταση Selfish.

Probe: Στην κατάσταση αυτή στέλνουμε τα πακέτα διερεύνησης προς έναν «ύποπτο» κόμβο. Ενώ αρχικά πειραματιστήκαμε με περισσότερα του ενός πακέτα διερεύνησης, τα οποία στέλναμε είτε σε κανονικά χρονικά διαστήματα, είτε με εκθετική καθυστέρηση, διαπιστώσαμε τελικά ότι η απλούστερη λύση ήταν και η καλύτερη: αρκεί ένα πακέτο διερεύνησης το οποίο στέλνεται 1 sec αργότερα από την διαπίστωση της Forward.




Σχήμα Γ.3.1: *Το μοντέλο διαδικασίας για το DSR με τον προτεινόμενο μηχανισμό αντιμετώπισης εγωισμού.*

Selfish: Στην κατάσταση αυτή ελέγχουμε τα αποτελέσματα που είχε η κατάσταση probe. Εάν διαπιστωθεί ότι ο κόμβος που διερευνήσαμε είναι πράγματι εγωιστής, τότε, στην κατάσταση αυτή:

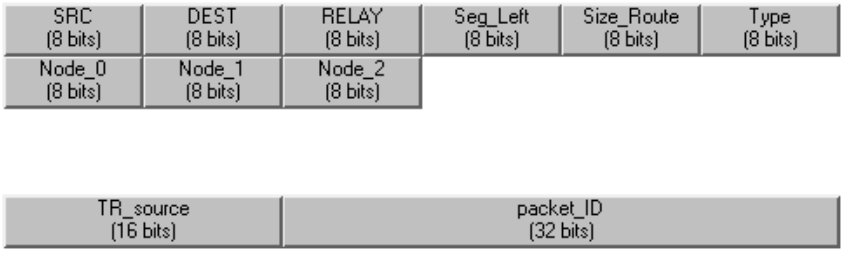
1. Εισάγεται ο εγωιστής κόμβος στον Πίνακα Εγωισμού του κόμβου που έκανε την διαπίστωση.
2. Διαγράφεται από τις cache διαδρομών του κόμβου που έκανε την διαπίστωση όλες τις διαδρομές που φέρουν τον εγωιστή κόμβο ως ενδιάμεσο.
3. Αποστέλλεται το πακέτο σφάλματος διαδρομής από εγωισμό στην πηγή του πακέτου δεδομένων που χάθηκε στον εγωιστή κόμβο.

### 3.4.β *Τροποποιήσεις Πακέτων*

Για να υλοποιηθεί ολόκληρος ο μηχανισμός αντιμετώπισης εγωισμού κατασκευάσαμε / τροποποιήσαμε τα παρακάτω πακέτα:

### 3.4.β.1 Το νέο πακέτο Διερεύνησης (probe packet)

Το πακέτο Διερεύνησης υλοποιήθηκε ως ένα πακέτο δεδομένων. Σκοπός μας ήταν να ελαχιστοποιήσουμε τόσο την επιπλέον πλεονάζουσα πληροφορία που μετακινείται λόγω αυτού το νέου πακέτου, αλλά και να διευκολύνουμε κατά το δυνατό την υλοποίηση. Προφανώς το πακέτο διερεύνησης δεν χρειάζεται πεδίο δεδομένων. Επίσης, όπως περιγράψαμε την λειτουργία του στην παράγραφο 3.2, έγινε προφανές, ότι το μήκος διαδρομής του είναι πάντοτε 3 (πηγή → «ύποπτος» κόμβος → πηγή). Έτσι κατασκευάσαμε το πακέτο που φαίνεται στο σχήμα Γ.3.2.

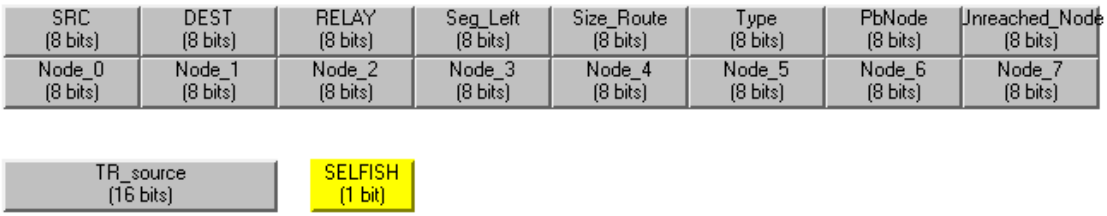



Σχήμα Γ.3.2: *Το νέο πακέτο διερεύνησης*

### 3.4.β.2 Το Πακέτο Σφάλματος από Εγωισμό

Το «σφάλμα» που προκαλείται από έναν εγωιστή κόμβο είναι σχεδόν πανομοιότυπο με ένα σφάλμα διαδρομής που οφείλεται σε μία κομμένη ζεύξη. Η ουσιαστική διαφορά ενός τέτοιου πακέτου σφάλματος από ένα πακέτο σφάλματος διαδρομής, είναι ότι αυτό εδώ δεν έχει σκοπό να καταδείξει τη ζεύξη που έχει κοπεί, αλλά τον εγωιστή κόμβο που πρέπει να αντιμετωπιστεί. Παρατηρήσαμε ότι το πακέτο σφάλματος διαδρομής, όπως είχε οριστεί στο αρχικό μοντέλο ήταν σχεδόν επαρκές: χρειαζόταν μονάχα την προσθήκη ενός μονόμπιτου πεδίου για την ένδειξη εάν το σφάλμα αυτό είχε προκληθεί από εγωισμό ή όχι. Με τον τρόπο αυτό ο έλεγχος του τύπου σφάλματος ουσιαστικά μεταφέρεται από το πεδίο του τύπου πακέτου (type) στο πεδίο SELFISH (*βλ.* σχήμα Γ.3.3). Με δεδομένο λοιπόν ότι η προσθήκη αυτή εισήγαγε αμελητέα επιπρόσθετη πληροφορία, δεν υλοποιήσαμε το μήνυμα αυτό με νέο τύπο πακέτου, αλλά στο αρχικό πακέτο σφάλματος διαδρομής του μοντέλου του DSR

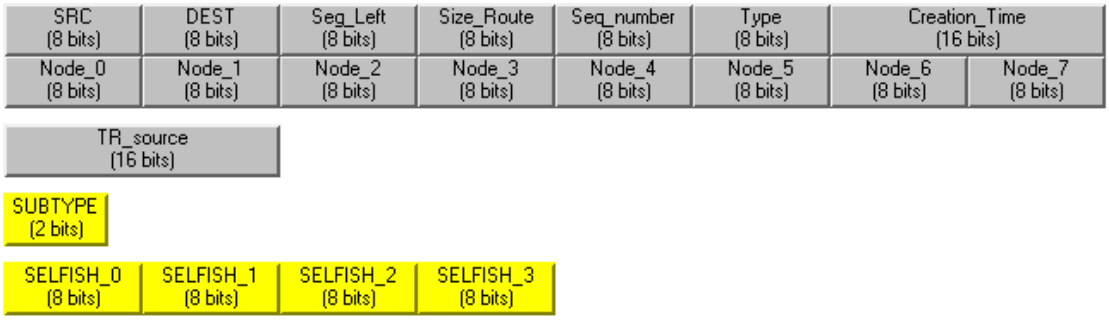
εισάγαμε το επιπλέον πεδίο. Έτσι το πακέτο σφάλματος έγινε όπως φαίνεται στο σχήμα Γ.3.3.




Σχήμα Γ.3.3: *Το πακέτο σφάλματος στο μοντέλο DSR με το μηχανισμό αντιμετώπισης εγωιστικής συμπεριφοράς.*

### 3.4.β.3 Το Νέο Πακέτο Αίτησης Διαδρομής

Το πακέτο Αίτησης Διαδρομής τροποποιήθηκε ώστε να περιλαμβάνει τους κόμβους που βρίσκονται μέσα στον πίνακα εγωισμού του κόμβου που κόμβου που το στέλνει. Θεωρήσαμε στην υλοποίηση μας ότι οι εγωιστές κόμβοι δεν θα ξεπερνάνε τους 4, οπότε το πακέτο τελικά διαμορφώθηκε όπως φαίνεται στο σχήμα Γ.3.4.




Σχήμα Γ.3.4: *Το νέο πακέτο αίτησης διαδρομής στο μοντέλο DSR με το μηχανισμό αντιμετώπισης εγωιστικής συμπεριφοράς.*

## 3.5 Αποτελέσματα-Συμπεράσματα

Με τις ίδιες παραμέτρους όπως και στον προηγούμενο μηχανισμό στήσαμε τα πειράματα μας, με επιπλέον παράγοντές:

1. το πλήθος των κόμβων με εγωιστική συμπεριφορά: για το πυκνό δίκτυο των 24 κόμβων, οι κόμβοι αυτοί ήταν 0,1,2 ή 4, ενώ στο αραιό δίκτυο των 8 κόμβων οι κόμβοι με εγωιστική συμπεριφορά ήταν 0,1, ή 2.
2. την τακτική με την οποία αντιμετωπίζεται ένας κόμβος με εγωιστική συμπεριφορά: Εκτελέσαμε πειράματα χωρίς κανένα μηχανισμό, με αφελή, δίκαιη και σκληρή αντιμετώπιση, όπως ορίσαμε την καθεμία στην παράγραφο 3.3.

Εκτελέσαμε 252 πειράματα με διαφορετικές παραμέτρους. Σε όλα από αυτά η ανακάλυψη εγωιστών κόμβων είχε απόλυτη επιτυχία: η εγωιστική συμπεριφορά αναγνωριζόταν πρακτικά άμεσα από τους γείτονες ενός εγωιστή κόμβου και χάρη στο μηχανισμό του πακέτου διερεύνησης δεν παρατηρήθηκαν εσφαλμένες παρατηρήσεις.

Έτσι, μελετήσαμε το ποσοστό της πλεονάζουσας πληροφορίας και το ποσοστό του throughput ανά κόμβο, όπως και στον μηχανισμό πρόβλεψης απώλειας ζεύξης, που παρουσιάσαμε στο κεφάλαιο 2. Παρακάτω, παρουσιάζουμε τα αποτελέσματα μας κάνοντας ένα διαχωρισμό μεταξύ στατικών και κινητών δικτύων.

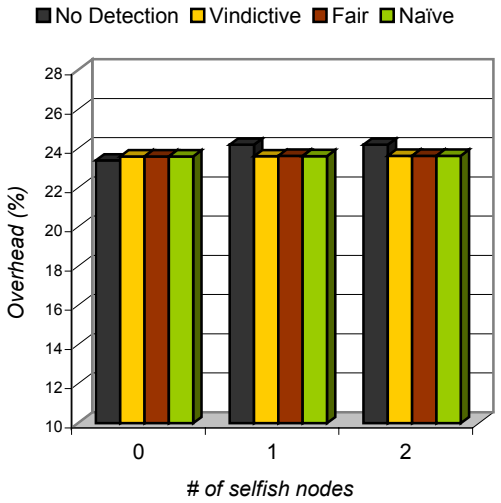
### 3.5.α *Στατικά Δίκτυα*

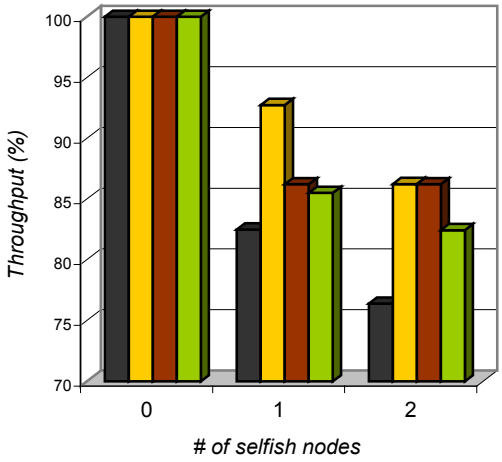
Διατηρώντας σταθερό το μέγεθος πακέτου παρατηρήσαμε:

1. *Ελάττωση της πλεονάζουσας πληροφορίας:*
ο μηχανισμός μας ελάττωσε την πλεονάζουσα πληροφορία, που εισάγουν με την εμφάνιση τους οι εγωιστές κόμβοι, έως και κατά 2 ποσοστιαίες μονάδες (*βλ.* σχήμα Γ.3.5.α,γ). Ο μηχανισμός μας επιδρά εντονότερα στα πυκνά δίκτυα, και η επίδρασή του είναι ανεξάρτητη από την τακτική αντιμετώπισης των εγωιστών. Αξίζει να σημειωθεί ότι στην περίπτωση μη ύπαρξης κόμβων με εγωιστική συμπεριφορά, το ποσοστό της πλεονάζουσας πληροφορία που προστίθεται από το μηχανισμό ανακάλυψης, είναι ανάλογο με αυτό που αφαιρείται όταν υπάρχουν κόμβοι με εγωιστική συμπεριφορά.

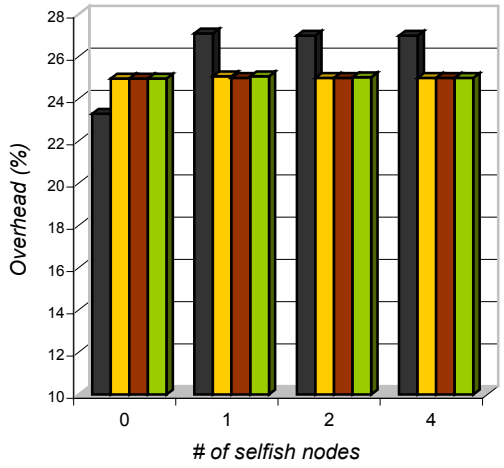
2. *Αύξηση του throughput:*
ο μηχανισμός μας ελαττώνει την αρνητική επίδραση που έχουν οι κόμβοι με εγωιστική συμπεριφορά στο throughput του δικτύου. Όπως παρατηρήσαμε, με το μηχανισμό μας «περισώζουμε» έως και σχεδόν

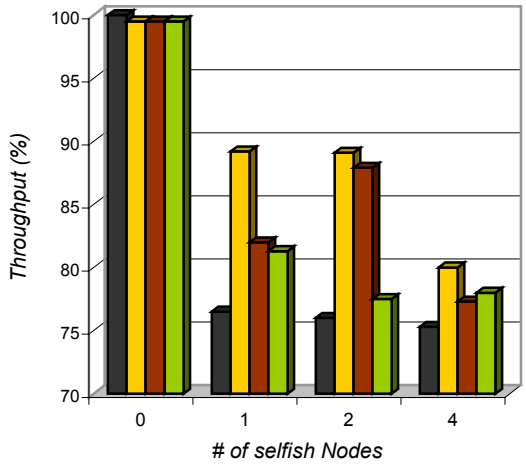
13% του ολικού throughput. Καλύτερη τακτική ως προς το throughput εμφανίζεται η σκληρή πολιτική, ιδιαίτερα σε πυκνά δίκτυα. Σε κάθε περίπτωση, απουσία κόμβων με εγωιστική συμπεριφορά ο μηχανισμός της ανακάλυψης ουσιαστικά δεν επιβαρύνει το throughput (-0.3%).




(α) (β)

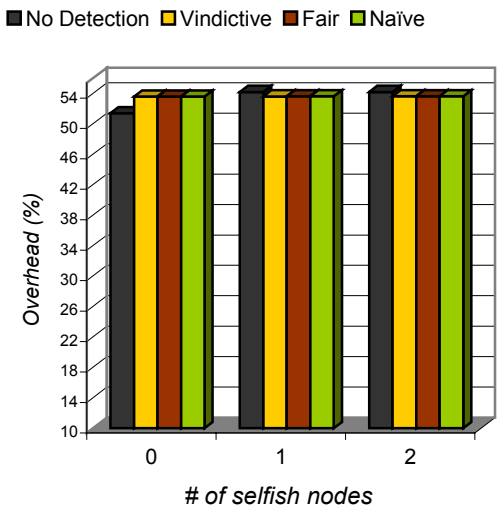


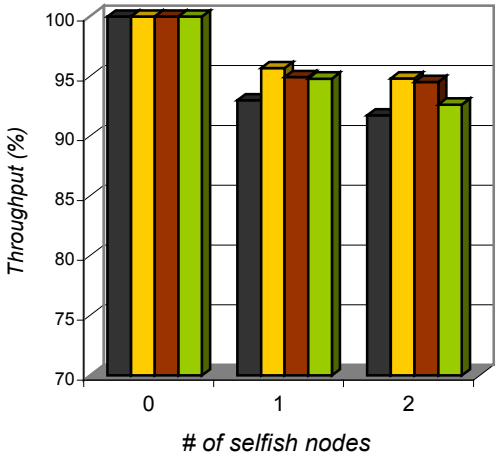




(γ) (δ)

Σχήμα Γ.3.5: *Στατικά δίκτυα με:* (α),(β) *8 κόμβους,* (γ),(δ) *24 κόμβους. Το μέγεθος πακέτου πηγής για τα παραπάνω πειράματα είναι 512 bits.*

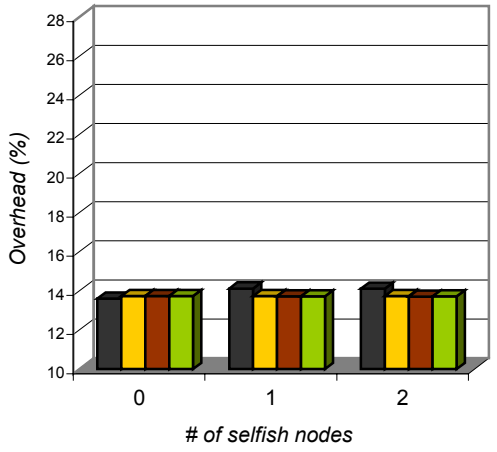
Όπως φαίνεται στο σχήμα Γ.3.5 παραπάνω, ο μηχανισμός ανακάλυψης και αντιμετώπισης εγωισμού επιδρά σε αραιό και σε πυκνό στατικό δίκτυο με ανάλογο τρόπο. Έτσι παρακάτω παρουσιάζουμε τα αποτελέσματα για αραιό δίκτυο με μεταβάλλοντας το μέγεθος του πακέτου δεδομένων.

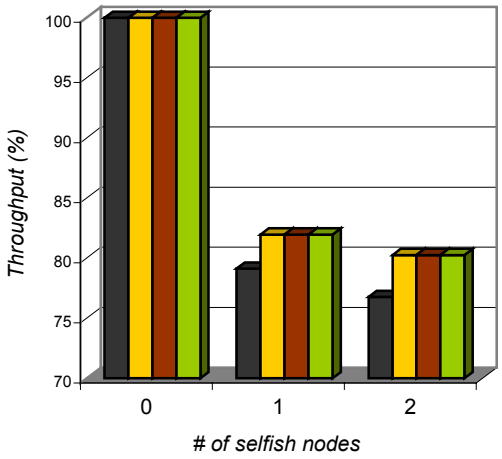

No Detection
Vindictive
Fair
Naïve
Overhead (%)
54
50
46
42
38
34
30
26
22
18
14
10
0
1
2
# of selfish nodes


Throughput (%)
100
95
90
85
80
75
70
0
1
2
# of selfish nodes

(α)

(β)




(γ)

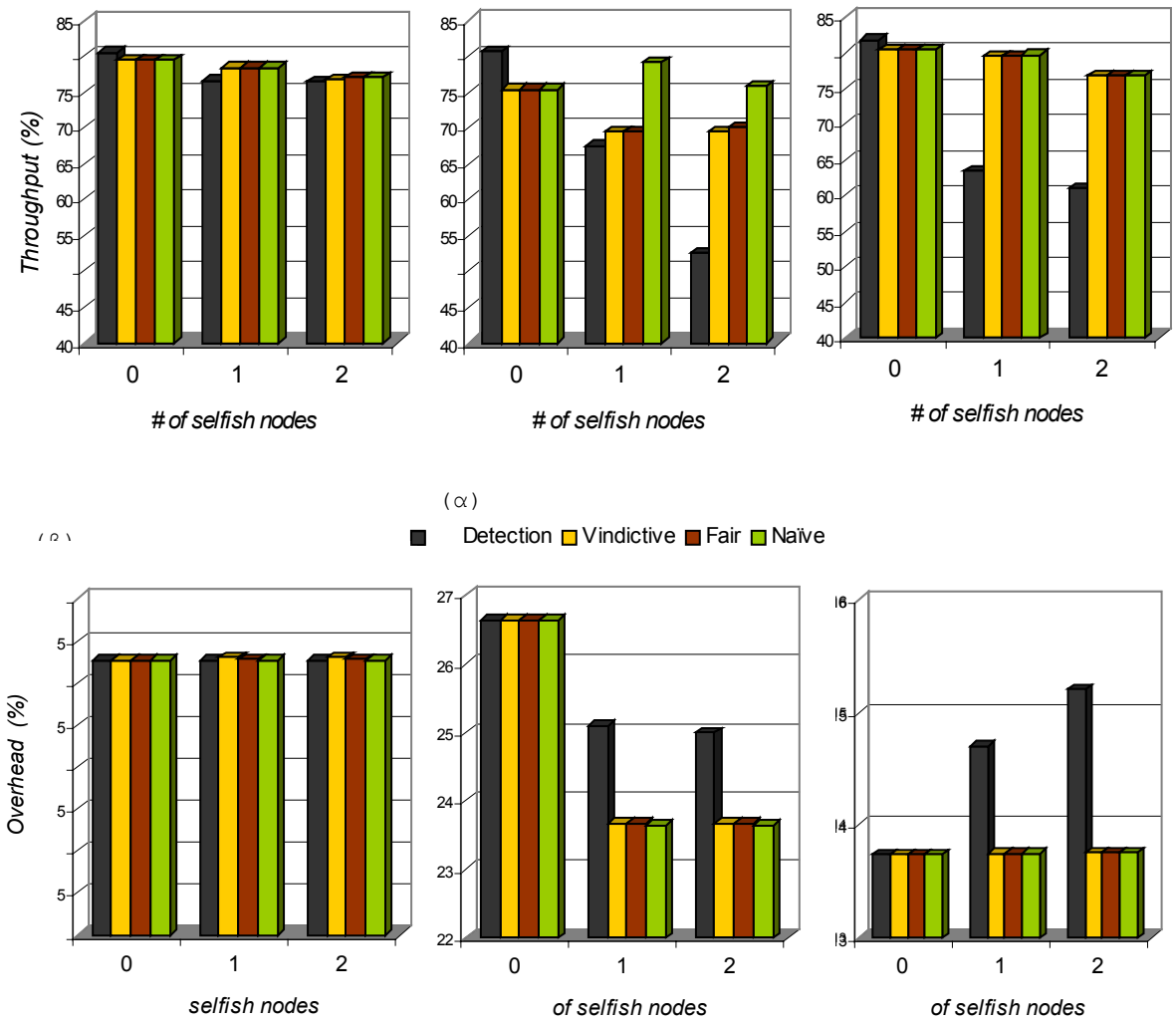
(δ)

Σχήμα Γ.3.6: *Στατικά δίκτυα 8 κόμβων με μέγεθος πακέτου:* (α),(β) *128bits*, (γ),(δ) *1024bits*.

Η ταύτιση που παρατηρείται στο (δ) αν και αρχικά εντυπωσιακή, μπορεί να χαρακτηριστεί ως αναμενόμενη, καθώς λαμβάνοντας τις σχετικές διαφορές των βελτιώσεων που επιφέρει η κάθε τακτική με αναφορά την τιμή χωρίς το μηχανισμό, παρατηρούμε μία τάση ελάττωσης τους από τα δίκτυα των πακέτων των 128 και 256 bits.

### 3.5.β *Κινούμενα Δίκτυα*

Για χαμηλή κινητικότητα (0.5 m/s) εκτελέσαμε σε ένα αραιό δίκτυο πειράματα για τα διάφορα μεγέθη πακέτων. Τα αποτελέσματα φαίνονται στο σχήμα Γ.3.7:



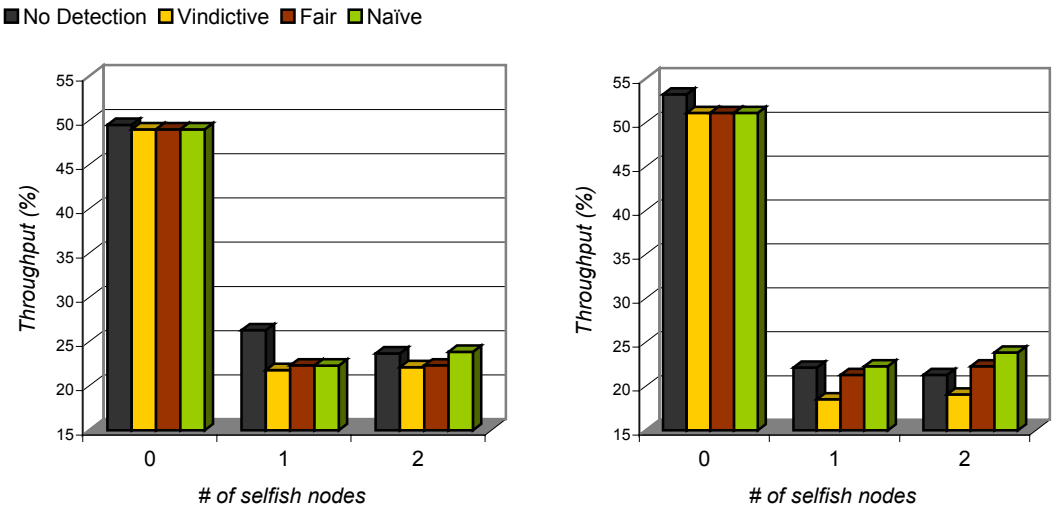

Σχήμα Γ.3.7: *Δίκτυα με χαμηλή κινητικότητα: Μέση ταχύτητα 0.5m/s. Η επάνω σειρά γραφημάτων απεικονίζει το throughput για μεγέθη πακέτων πηγής* (α) 128bits, (β) 512bits (α) 1024bits. Η κάτω σειρά απεικονίζει την πλεονάζουσα πληροφορία για τα αντίστοιχα μεγέθη πακέτων.

Συνοψίζουμε τις παρατηρήσεις μας στη λίστα που ακολουθεί:

1. Δεν υπάρχουν οφέλη αλλά ούτε και ζημιές από το μηχανισμό για τα μικρά πακέτα.
2. Παρατηρείται πρακτικά πλήρης σύγκλιση της σκληρής με τη δίκαιη τακτική

3. Και οι τρεις τακτικές αντιμετώπισης εγωιστών έχουν τα ίδια ακριβώς αποτελέσματα στην πλεονάζουσα πληροφορία που εισάγουν σε κάθε περίπτωση.
4. Έχουμε ελάττωση της πλεονάζουσας πληροφορίας σε μεσαία και μεγάλα πακέτα.
5. Η γραφική παράσταση (3.7(β)) είναι η μόνη περίπτωση σε όσα πειράματα κάναμε, όπου η αφελής αντιμετώπιση εγωιστών κόμβων είχε τα θετικότερα αποτελέσματα.

Τέλος για έντονη κινητικότητα (5 m/s) εκτελέσαμε σε ένα αραιό δίκτυο πειράματα για τα διάφορα μεγέθη πακέτων. Τα πιο ενδεικτικά αποτελέσματα φαίνονται στο σχήμα 3.8:




Σχήμα 3.7: *Δίκτυα με έντονη κινητικότητα: Μέση ταχύτητα 5m/s. (α) πακέτα των 512 bits, (α) πακέτα των 1024 bits.*

Παρατηρούμε ότι εδώ είναι η μόνη περίπτωση που ο μηχανισμός αντιμετώπισης του εγωισμού δεν έχει θετικά αποτελέσματα. Επίσης βλέπουμε ότι η αφελής αντιμετώπιση εγωιστών κόμβων έχει τα καλύτερα αποτελέσματα. Η αιτιολόγηση είναι ότι με αυτήν την αντιμετώπιση ένας εγωιστής κόμβος απολαμβάνει μεγαλύτερο throughput, από ότι στις άλλες περιπτώσεις και λόγω της έντονης κίνησης που δρα καταστροφικά για το δίκτυο ακόμα και αυτό το ελάχιστο παραπάνω κέρδος για αυτούς τους λίγους κόμβους αντανακλάται στο throughput ολόκληρου του δικτύου.

Συμπερασματικά, χάρη στα με τα πακέτα διερεύνησης, ο μηχανισμός ανακάλυψης εγωιστών κόμβων είχε απόλυτη επιτυχία. Η απλούστερη δυνατή χρήση τους (αποστολή ενός μονάχα πακέτου διερεύνησης 2 δευτερόλεπτα μετά από την λήξη του timeout για την προώθηση πακέτου από τον «ύποπτο» κόμβο) αποδείχτηκε πειραματικά επαρκής, γλιτώνοντας μας από πρόσθετη πλεονάζουσα πληροφορία και κίνηση στο δίκτυο. Τέλος ο συνολικός μηχανισμός αντιμετώπισης εγωισμού είχε τα καλύτερα αποτελέσματα σε πυκνά, στατικά δίκτυα, τα οποία αποτελούν και το πιο πιθανό σενάριο για κόμβους με εγωιστική συμπεριφορά [24]. Σε αυτά, η σκληρή τακτική αντιμετώπισης εγωιστών κόμβων, που ουσιαστικά τους απομακρύνει απομονώνοντας τους από το δίκτυο, αποδείχτηκε η πιο επικερδής αντιμετώπιση. Σε δίκτυα με χαμηλή κινητικότητα, οι τρεις τακτικές αντιμετώπισης συνέκλιναν σε κοινά θετικά αποτελέσματα, δείχνοντας ότι σε αυτήν την περίπτωση η ανακάλυψη εγωιστών και διαγραφή τους από την cache διαδρομών είναι η ουσιαστική συνεισφορά ολόκληρου του μηχανισμού.

## 4. Μελλοντική εργασία

Έχοντας κατασκευάσει δύο μηχανισμούς που αντιμετωπίζουν με επιτυχία τα καίρια προβλήματα της κινητικότητας και της εγωιστικής συμπεριφοράς κόμβων ενός κινητού αδόμητου δικτύου με το πρωτόκολλο DSR, σκοπεύουμε να επιστρέψουμε στο 2° μέρος της εργασίας μας και να ασχοληθούμε με το θέμα της Διαχείρισης Εμπιστοσύνης Κόμβων σε αδόμητα δίκτυα.

Εκτενής μελέτη απαιτείται, ώστε να μοντελοποιηθεί η Εμπιστοσύνη σε ένα τέτοιο δίκτυο και να αναπτυχθεί ένα αποδοτικό σχήμα διαχείρισης της. Παράλληλα οφείλουμε χρησιμοποιώντας θεωρία παιγνίων, να μελετήσουμε και να μοντελοποιήσουμε περισσότερες συμπεριφορές κόμβων οι οποίοι προσπαθούν να εκμεταλλευτούν στο έπακρο τις όποιες αδυναμίες ενός αδόμητου δικτύου με σκοπό είτε εγωιστικά να αυξήσουν τα δικά τους οφέλη, ή κακόβουλα να επιτεθούν ενεργά στο δίκτυο.

Τέλος, όπως προέκυψε από το σύνολο της εργασίας μας, η πλατφόρμα πάνω στην οποία μπορεί να αναπτυχθεί τέτοια μελέτη είναι ένα νέο

μοντέλο του DSR στο OPNET, το οποίο θα έχουμε κατασκευάσει ενδεχομένως εξ' αρχής ώστε να έχει τις ακόλουθες ιδιότητες:

- Μεγαλύτερη πιστότητα στο πρωτόκολλο DSR, όπως αυτό ορίζεται στο τελευταίο internet draft [8].
- Υποστήριξη πολλαπλών cache διαδρομών ανά προορισμό σε κάθε κόμβο, με καλύτερη οργάνωση –Η οργάνωση των διαδρομών ως *γράφων* φαίνεται να είναι η πιο δελεαστική και από πλευρά καθαρής πρόκλησης αλλά και δυνατοτήτων που παρέχει.
- Βελτιωμένο, ρεαλιστικότερο μοντέλο κινητικότητας.

# ΒΙΒΛΙΟΓΡΑΦΙΑ


1. IEEE Computer Society LAN/MAN Standards Committee,"Wireless LAN medium access control (MAC) and physical layer (PHY) specifications." IEEE Std.802.11-1997. IEEE, NewYork, NY1997.
2. D. J. Baker and A. Ephremides, "The Architectural Organization of a Mobile Radio Network via a Distributed Algorithm," *IEEE Trans. on Commun.*, vol. COM-19, pp. 1694-1701, November 1981.
3. R. E. Kahn, et. al., "Advances in Packet Radio Technology," Proceedings of the IEEE, Vol. 66, No. 11, pp. 1468-1496, Nov. 1978.
4. H. Takagi and Kleinrock, "Optimal transmission ranges for randomly distributed packet radio terminals", IEEE Trans Comm, March 1984.
5. C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers." *Comp. Commun. Rev.*, Oct. 1994, pp. 234-44
6. V. Park, S. Corson, Temporally-Ordered Routing Algorithm (TORA) Version 1, functional Specification, 26, November 1997
7. C. Perkins, Ad hoc On Demand Distance Vector (AODV) Routing, IETF Internet Draft, 20 November 1997.
8. D. Johnson, D. Maltz, Y. Hu, *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)*, IETF Internet Draft, 15 April 2003.
9. Ad Hoc Routing Protocols:

   http://www.update.uu.se/~davidl/msthesis/html/node4.htm
10. D. B. Johnson, Routing in ad hoc Networks of mobile hosts, proc. of the IEEE workshop on Mobile Computing Systems and Applications Dec. 1994.
11. T.D. Dyer,R.V. Boppana, A Comparison of TCP Performance over Three Routing Protocols for Mobile Ad Hoc Networks, Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing, October 2001.
12. S. Buchegger, J. Le Boudec, Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes: Fairness in dynamic ad-

hoc networks), In proceedings of the third ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, Switzerland, June, 2002.

13. About GloMoSim: http://pcl.cs.ucla.edu/projects/glomosim/

14. P. Michiardi, R. Molva. Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks. European Wireless Conference, 2002.

15. Michiardi, R. Molva, CORE: A Collaborative Reputation mechanism to enforce node cooperation in mobile ad hoc networks. Institut Eurecom, Research Report No RR-02-062, December 2001.

16. P.Resnik et. al. Reputation Systems, Communications of The ACM, vol. 43. no. 12. Dec. 2000.

17. Li Xiong , Ling Liu, A reputation-based trust model for peer-to-peer ecommerce communities [Extended Abstract], Proceedings of the 4th ACM conference on Electronic commerce, June 2003, San Diego, CA, USA.

18. Developing a model using opnet:

http://www.ee.ucl.ac.uk/dcs/commercial/opnet/modeling_in_opnet.html#Network

19. Λυκούργου Ευδοκία, Opnet Modeler 8.0.C, Εγχειρίδιο του Ασύρματου Μοντέλου στο Opnet. Πτυχιακή Εργασία, Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης, 2002.

20. The Opnet Modeler 8.0 Online Documentation, Opnet Technologies Inc. 2001.

21. Simulation Model for the DSR MANET Routing Protocol:

http://www.antd.nist.gov/wctg/prd_dsrfiles.html

22. T. S. Rappaport, Wireless Communications Principles and Practice, Prentice Hall, Upper Saddle River, NJ.1996 1st ed.

23. J. Yoon et al., Random Waypoint Considered Harmful, IEEE
Infocom 2003, March 2003, San Francisco, CA, USA.

24. The Grid Ad Hoc Networking Project:

http://www.pdos.lcs.mit.edu/grid/