ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ

Μοντελοποίηση και Ανάλυση Έξυπνων Τεχνικών Διάδοσης Κακόβουλου Λογισμικού με Χρήση Τοπολογικών Ιδιοτήτων Δυναμικών και Αυτοργανούμενων (Ad-Hoc) Δικτύων Ευρείας Κλίμακας

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

του

Βασίλειου Α. Καρυώτη

Αθήνα, Ιούνιος 2009

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ

Μοντελοποίηση και Ανάλυση Έξυπνων Τεχνικών Διάδοσης Κακόβουλου Λογισμικού με Χρήση Τοπολογικών Ιδιοτήτων Δυναμικών και Αυτοργανούμενων (Ad-Hoc) Δικτύων Ευρείας Κλίμακας

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

του

Βασίλειου Α. Καρυώτη

Συμβουλευτική Επιτροπή : Συμεών Παπαβασιλείου
Βασίλειος Μάγκλαρης
Ευστάθιος Συκάς

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή την 29η Ιουνίου, 2009.

.....	.....	.....
Συμεών Παπαβασιλείου	Βασίλειος Μάγκλαρης	Ευστάθιος Συκάς
Επίκ. Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.
.....	.....	.....
Μιχαήλ Θεολόγου	Ανδρέας-Γεώργιος Σταφυλοπάτης	Μιλτιάδης Αναγνώστου
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

.....
Δημήτριος Καλογεράς
Ερευνητής Ε.Π.Ι.Σ.Ε.Υ.

Αθήνα, Ιούνιος 2009

.....

Βασίλειος Α. Καρυώτης

Διδάκτωρ Ηλεκτρολόγος Μηχανικός και Μηχανικός Ηλεκτρονικών Υπολογιστών Ε.Μ.Π.

Το έργο υλοποιήθηκε στο πλαίσιο του Μέτρου 8.3 του Ε.Π. Ανταγωνιστικότητα Γ΄ Κοινοτικό Πλαίσιο Στήριξης και συγχρηματοδοτείται κατά:

* 75% της Δημόσιας Δαπάνης από την Ευρωπαϊκή Ένωση – Ευρωπαϊκό Κοινωνικό Ταμείο.
* 25% της Δημόσιας Δαπάνης από το Ελληνικό Δημόσιο – Υπουργείο Ανάπτυξης – Γενική Γραμματεία Έρευνας και Τεχνολογίας.

The project is co-funded by the European Social Fund (75%) and National Resources (25%).

Περίληψη

Η διάδοση κακόβουλου λογισμικού έχει αναχθεί σε καίριο ζήτημα των σύγχρονων δικτυακών υποδομών κάνοντας την εμφάνισή του σε διάφορα επίπεδα. Σημαντική εργασία για την περιγραφή της διάδοσης έχει αφιερωθεί στη βιβλιογραφία για τις περιπτώσεις των ενσύρματων δικτύων που αποτελούν και το πιο μεγάλο τμήμα της τρέχουσας υποδομής, καθώς όμως αυξάνεται η διείσδυση των ασύρματων αυτοργανούμενων δικτύων, μεγαλώνει αντίστοιχα και το ενδιαφέρον για αυτές τις περιπτώσεις δικτύων.

Η παρούσα εργασία επικεντρώνεται στη μελέτη της διάδοσης κακόβουλου λογισμικού σε ασύρματα αυτοργανούμενα δίκτυα ευρείας κλίμακας και εξετάζει την επίδραση της τοπολογίας στην εξέλιξη της διασποράς σε διάφορους τύπους δικτυών. Για το σκοπό αυτό προτείνεται ενα πρωτοποριακό μοντέλο περιγραφής της διάδοσης κακόβουλου λογισμικού, το οποίο βασίζεται στη θεωρία κλειστών δικτύων ουρών αναμονής. Το προτεινόμενο μοντέλο συγκεκριμενοποιείται για την περίπτωση ασύρματων αυτοργανούμενων δικτύων επιτρέποντας την εξαγωγή αναλυτικών αποτελεσμάτων για τον αναμενόμενο αριθμό μολυσμένων κόμβων στο δίκτυο και τον αναμενόμενο συνολικό ρυθμό μόλυνσης κόμβων. Τέτοια χρονικά–ανεξάρτητα μετρικά αξιολόγησης σε συνδυασμό με το χρονικά–εξαρτώμενο μετρικό της Αποδοτικότητας Μόλυνσης που εισάγεται, χρησιμοποιούνται για την αξιολόγηση της επίδοσης υπό διάφορες στρατηγικές διάδοσης και διαφορετικούς τύπους δικτύων.

Με σκοπό τη μελέτη της επίδρασης διαφόρων στρατηγικών διασποράς κακόβουλου λογισμικού, ώστε να διαφανούν υποσχόμενες κατευθύνσεις για τη σχεδίαση αποδοτικών αντίμετρων, εισάγονται και αναλύονται έξυπνες στρατηγικές επίθεσης που στηρίζονται στον Έλεγχο Τοπολογίας και εκμεταλλεύονται κατάλληλα τα τοπικά τοπολογικά χαρακτηριστικά ενός δικτύου και τους διαθέσιμους πόρους κάθε κόμβου για την αποδοτικότερη διασπορά απειλών σε ασύρματα αυτοργανούμενα δίκτυα. Για τις περιπτώσεις όπου ένα συγκεκριμένο τμήμα κακόβουλου λογισμικού επιχειρείται να διαδοθεί καθολικά σε ένα δίκτυο, εισάγονται και αναλύονται τυχαιοποιημένες τεχνικές διασποράς ιών υπολογιστών που βασίζονται σε Τυχαίους Περίπατους.

Συνολικά από την ανάλυση και μελέτη του γενικού πλαισίου για τη μοντελοποίηση της διάδοσης κακόβουλου λογισμικού και των αποδοτικών τεχνικών διασποράς, γίνεται φανερή η σημασία που έχει η τοπολογία ενός αυτοργανούμενου δικτύου σε τοπική κλίμακα και ο τρόπος που μπορεί αυτό να γίνει αντικείμενο εκμετάλλευσης από κακόβουλους χρήστες για να αυξήσουν την αποδοτικότητά τους, αλλά αντίστοιχα και από τους νόμιμους διαχειριστές των εν λόγω δικτύων για να θωρακίσουν περαιτέρω τις υποδομές τους.

Μέσα από το πλαίσιο που παρουσιάζεται στην παρούσα διατριβή, η περιγραφή και ανάλυση της διάδοσης κακόβουλου λογισμικού με στοχαστικές μεθόδους φαίνεται αρκετά αποδοτική και πολλά υποσχόμενη για το μέλλον, ειδικότερα υπό το πρίσμα της αύξησης των επιθέσεων σε όγκο και ευφυΐα που αναμένεται καθώς αυξάνονται οι αντίστοιχες υποδομές. Αντίστοιχα, ο έλεγχος ισχύος υπό την έκφανση του Ελέγχου Τοπολογίας εμφανίζεται ως μια κατάλληλη μέθοδος για την αντιμετώπιση πολλών προβλημάτων και τελικά την αποδοτικότερη προστασία αυτοργανούμενων δικτύων ευρείας ή μικρότερης κλίμακας.

Λέξεις Κλειδιά

Ασύρματα αυτοργανούμενα δίκτυα, διάδοση κακόβουλου λογισμικού, δίκτυα ουρών αναμονής, στρατηγικές επίθεσης, Έλεγχος Τοπολογίας, Τυχαίοι Περίπατοι, τοπολογικά χαρακτηριστικά

Abstract

The propagation of malicious software (malware) has become one of the major issues in contemporary networking infrastructures, emerging at various levels and occasions. Significant work for studying malware spreading has been performed, dealing mainly with wired networks which constitute the most significant part of today's modern infrastructures. However, as the penetration of wireless ad hoc and sensor networks increases, the interest for corresponding studies in wireless networks increases as well.

This thesis focuses on the study of malware propagation in large scale wireless ad hoc and sensor networks, emphasizing on the impact of network topology on the outcome of malware spreading in various types of networks. A novel framework that is based on the theory of closed queuing networks is proposed for describing the malware spreading process. The proposed model is made explicit for the case of ad hoc and sensor networks, leading to analytical expressions for the expected number of infected nodes and the expected total node infection rate in the network. Such time-independent metrics, combined with a proposed time-dependent one, namely Infection Efficiency, are used for evaluating malware propagation under different attack strategies and different types of network.

More specifically, in order to analyze the impact of various attack strategies, malware propagation methods that are based on Topology Control are designed and analyzed. Such techniques exploit local topological network characteristics and available node resources for spreading malware more efficiently in wireless ad hoc networks. In the event that a specific malware module is desired to be propagated completely over a network, randomized spreading techniques that are based on Random Walks are proposed and compared in order to identify the most appropriate ones on a per network type case.

Overall, through the analysis and study of the proposed framework for modeling malware propagation and the efficient malware spreading strategies, the importance of topology of a wireless ad hoc network becomes evident, as well as the means to exploit it from a malicious user point of view, or make the network more robust from an administrator's perspective.

Through the framework proposed in this thesis, the analysis and study of malware propagation by means of stochastic approaches and more specifically queuing theory seems promising for future extensions and further studies, especially as the frequency of such attacks keeps increasing, both in terms of quantity and intelligence. Similarly, power control and Topology Control respectively, appear to be appropriate methods for dealing with several emerging problems and consequently for more efficient protection of any–scale wireless ad hoc and sensor networks.

Keywords

Wireless ad hoc networks, malware propagation, queuing networks, attack strategies, Topology Control, Random Walks, topological characteristics

Ευχαριστίες

Στο σημείο αυτό θα ήθελα να εκφράσω τις ευχαριστίες μου σε εκείνους που συνέβαλαν με τον τρόπο τους στην ολοκλήρωση αυτής της διδακτορικής διατριβής. Η εκπόνησή της δεν έλαβε χώρα μόνο κατά τη διάρκεια των τεσσάρων χρόνων στη Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών του Ε.Μ.Π., αλλά ουσιαστικά προετοιμάστηκε σε όλους τους ακαδημαϊκούς χώρους που έτυχε να βρεθώ, από τη Βαρβάκειο Πρότυπο Σχολή στο Ψυχικό, μέχρι το Πανεπιστήμιο Πενσυλβάνιας στη Φιλαδέλφεια των Η.Π.Α.

Κυριότερα θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Συμεών Παπαβασιλείου, για την καθοδήγηση που παρείχε και εμπιστοσύνη που έδειξε στο πρόσωπό μου στη διάρκεια των τεσσάρων χρόνων που δουλεύουμε μαζί. Στη συνεργασία μας υπήρξε πάντα λογικός, ρεαλιστής, δείχνοντας τον δέοντα σεβασμό για τη δουλειά και την προσπάθεια που απαιτήθηκε για την παρούσα εργασία. Υπήρξε για μένα παραπάνω από επιβλέπων καθηγητής και θεωρώ ότι αποτελεί πρότυπο Δασκάλου για την ελληνική και παγκόσμια πραγματικότητα.

Στη συνέχεια θα ήθελα να ευχαριστήσω τον καθηγητή κ. Βασίλη Μάγκλαρη για το εισαγωγικό μάθημα των Συστημάτων Αναμονής, το οποίο όπως αποδείχθηκε αποτέλεσε τη βάση για την παρούσα εργασία, για ορισμένες ιδέες που μου έδωσε καθώς και για τη φιλοξενία του στο εργαστήριο NETMODE που ίδρυσε. Επίσης, τον καθηγητή Α.Π.Θ. κ. Πάνο Αργυράκη για τη συνεργασία που είχαμε με τον ίδιο και την ερευνητική του ομάδα.

Επιπρόσθετα οφείλω ένα μεγάλο ευχαριστώ στους καθηγητές του Πανεπιστήμιου Πενσυλβάνιας με τους οποίους είχα την ευκαιρία να θητεύσω και να συνεργαστώ. Το μάθημά τους, η στάση τους και η δουλειά τους, αναζοπύρωσαν το ενδιαφέρον μου για πρωταρχικές και θεμελιακές μαθηματικές γνώσεις και την αναζήτηση των ουσιαστικών και λογικών αιτίων των πραγμάτων. Κάτι τέτοιο δεν θα μπορούσε να συμβεί αν δεν υπήρχε μια ομάδα καθηγητών της Βαρβακείου Σχολής που λειτουργούσε με τον ίδιο ακριβώς τρόπο και στον ίδιο βαθμό. Τους ευχαριστώ θερμά για τα ισχυρά γνωστικά θεμέλια που μου παρείχαν.

Σημαντική συμβολή στην όλη μου προσπάθεια διαδραμάτισαν οι στενοί φίλοι και συνεργάτες Κώστας Βαλαγιαννόπουλος και Τιμόθεος Καστρινογιάννης. Μέσα

από τις γενικότερες συζητήσεις που είχαμε τα τελευταία δέκα και τέσσερα χρόνια αντίστοιχα, λύθηκαν προβλήματα, αγωνίες και άγχη, ενώ προέκυψαν δημοσιεύσεις, φιλοσοφικές απόψεις και στάσεις ζωής.

Θα ήθελα επίσης να ευχαριστήσω όλους του διπλωματικούς φοιτητές με τους οποίους συνεργάστηκα στη διάρκεια των τεσσάρων χρόνων, Μαρία, Μικέ, Τάσσο, Θεοδόση, Έλενα, Βάλια και Βιβή. Οι συζητήσεις που κάναμε, οι προβληματισμοί τους, οι αγωνίες τους και οι δυσκολίες που αντιμετώπισαν υπήρξαν για μένα πεδίο προβληματισμού, έμπνευσης και κριτήριο της γνώσης μου.

Τέλος, οφείλω να ευχαριστήσω τους γονείς μου, Αστέριο και Αρετή, δίχως τους οποίους δεν θα είχα φτάσει μέχρι εδώ. Υπήρξαν για μένα ζωντανά παραδείγματα και τους είμαι ευγνώμων για την επιμονή τους να μου δίνουν μακροπρόθεσμα εφόδια και αξίες, αντί προσωρινών συντομεύσεων και σαθρών υποβοηθήσεων.

To v. p.

Best results are yet to come…

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Διαγραμμάτων

Κατάλογος Πινάκων

Κεφάλαιο 1

Εισαγωγή

Τα τελευταία χρόνια παρατηρούνται συχνά κακόβουλες επιθέσεις σε δίκτυα επικοινωνιών και υπολογιστών διαφόρων τύπων, με συνέπειες που διαφέρουν ριζικά σε είδος, έκταση και κόστος [1]. Για παράδειγμα, αρκετά δίκτυα τραπεζών έχουν υποστεί επιθέσεις με αποτέλεσμα ευαίσθητα δεδομένα να διαρρεύσουν σε επικίνδυνους χρήστες, ενώ σε άλλες περιπτώσεις απλοί χρήστες έχουν δεχθεί μαζικά επιθέσεις με αποτέλεσμα τη δυσλειτουργία των συστημάτων τους, τη διαρροή προσωπικών στοιχείων ή και την προσωρινή παύση λειτουργίας των υπολογιστών τους. Κυβερνητικοί οργανισμοί έχουν δεχτεί σκόπιμα πλήγματα τόσο σε ερασιτεχνικό όσο και επαγγελματικό ή στρατιωτικό επίπεδο. Η διάδοση κακόβουλου λογισμικού απασχολεί σήμερα τόσο τον απλό χρήστη, όσο και ολόκληρες ομάδες ειδικών που ασχολούνται με την προστασία κρίσιμων υποδομών και συστημάτων.

Η εκρηκτική αύξηση διακίνησης κακόβουλων προγραμμάτων λογισμικού (malware) που παρατηρήθηκε τα τελευταία χρόνια οδήγησε στην εντατικοποίηση της έρευνας για τη μοντελοποίηση και αντιμετώπιση των επιθέσεων σε ακαδημαϊκά και βιομηχανικά πλαίσια. Οι διαφορετικοί τύποι κακόβουλου λογισμικού επικεντρώνονταν μέχρι πρόσφατα σε ενσύρματα δίκτυα υπολογιστών και κυριότερα σε υπολογιστές συνδεδεμένους στο Διαδίκτυο (Internet), το οποίο μεταξύ άλλων αποτελεί σήμερα το πιο συνηθισμένο μέσο παραγωγής και διάδοσης κακόβουλου λογισμικού [2],[3]. Παράλληλα όμως και άλλοι τύποι δικτύων, κυρίως ασύρματων κινητών (με ή χωρίς κεντρική δομή), αυξάνουν τη διείσδυσή τους στην καθημερινή ζωή διαδραματίζοντας ρόλο δικτύων πρόσβασης με αυξημένη σημαντικότητα για τους χρήστες τους και τις εφαρμογές που καλούνται να εξυπηρετήσουν [4],[5]. Ασύρματα αυτοργανούμενα δίκτυα χρησιμοποιούνται πλέον σε πληθώρα καθημερινών ή πιο εξειδικευμένων εφαρμογών παρέχοντας δικτυακές υποδομές πρόσβασης χαμηλού κόστους που μπορούν να λειτουργήσουν άμεσα, όπως σε περιπτώσεις αντιμετώπισης έκτακτων αναγκών και καταστροφών [6], σε δίκτυα παρακολούθησης δασών για πυρκαϊές [7], σε εφαρμογές δικτύων που χτίζονται πάνω σε ανθρώπους (αισθητήρες και μικρο-υπολογιστές που φοριούνται) [8] και

εφαρμογές ασύρματων δικτύων που χρησιμοποιούνται για την παρακολούθηση ασθενών [9]. Ως επακόλουθο, εντάθηκαν οι κακόβουλες επιθέσεις λογισμικού που παρατηρούνται και σε αυτά τα δίκτυα με ρυθμούς που αυξάνουν απότομα και διευρύνονται ανάλογα με τον τύπο των δικτύων που πλήττουν και τις δυνατότητες των συσκευών που χρησιμοποιούνται [10],[11]. Όπως αναμενόταν, το ενδιαφέρον για τη μοντελοποίηση της διάδοσης κακόβουλου λογισμικού έχει επεκταθεί και ενταθεί στην περίπτωση μη παραδοσιακών τύπων δικτύων, όπως είναι τα ασύρματα αυτοργανούμενα (ad hoc networks) [12] και τα δίκτυα αισθητήρων (sensor networks) [13],[14]. Καθώς τα τελευταία εξαπλώνονται σημαντικά σε κρίσιμες υποδομές και καθημερινές εφαρμογές [15],[16], το ενδιαφέρον για πιο στοχευμένες μελέτες και πιο ουσιαστικά αποτελέσματα στην περιγραφή των επιθέσεων και τη σχεδίαση αντίμετρων για την αντιμετώπισή τους γίνεται εντονότερο.

Μέχρι στιγμής έχουν εμφανιστεί πολλοί διαφορετικοί τύποι κακόβουλου λογισμικού και επιθέσεων. Οι πιο χαρακτηριστικοί αφορούν σε οικογένειες λογισμικού που εκμεταλλεύονται αδυναμίες ή ατέλειες του λειτουργικού συστήματος ενός μηχανήματος και μπορούν να δημιουργήσουν αντίγραφα του εαυτού τους. Τα κακόβουλα αντίγραφα μπορούν να ενσωματωθούν σε τμήματα λογισμικού και να μεταφερθούν είτε μέσω ηλεκτρονικού ταχυδρομείου, είτε ως προγράμματα εγκατάστασης ή μέσω κοινά χρησιμοποιούμενων αρχείων (ιοί υπολογιστών – computer viruses) [17],[18]. Σε άλλες περιπτώσεις, ένα τμήμα κακόβουλου λογισμικού μπορεί να λειτουργεί πιο αυτόνομα και να ανακαλύπτει μόνο του αδυναμίες/ατέλειες σε διάφορα συστήματα, τις οποίες εκμεταλλεύεται αυτόβουλα για να τα μολύνει (λογισμικό τύπου worm) [19],[20]. Οι ιοί τύπου worm δεν χρειάζεται να ενσωματωθούν σε άλλα προγράμματα/αρχεία για να μεταφερθούν, ενώ ταυτόχρονα έχουν επιπτώσεις στο δίκτυο που χρησιμοποιούν για την εξάπλωσή τους, καταλαμβάνοντας μέρος του διατιθέμενου εύρους ζώνης του. Άλλες κατηγορίες κακόβουλου λογισμικού περιλαμβάνουν προγράμματα που φαινομενικά φαίνονται αθώα (trojan horses, rootkits, spyware, adware) [21], αλλά στην πραγματικότητα εκτελούν κακόβουλες ενέργειες εν αγνοία του χρήστη του μηχανήματος, όπως η καταγραφή κωδικών πρόσβασης, εγκατάσταση προγραμμάτων χωρίς συγκατάθεση χρήστη, παρακολούθηση επισκέψεων και ενεργειών που εκτελεί το μηχάνημα και αποστολή των δεδομένων στις πηγές του κακόβουλου λογισμικού.

Σημαντικά επίσης διαφέρουν και οι συνέπειες διαφορετικών τύπων επιθέσεων. Έτσι μπορούν να περιλαμβάνουν απλή μείωση της αποδοτικότητας του κόμβου, διαρροή προσωπικών και ευαίσθητων δεδομένων, καταστροφή δεδομένων ή ακόμα και μερική ή ολική αδυναμία λειτουργίας του αντίστοιχου μηχανήματος [11],[13]. Σε κάθε περίπτωση όμως το κοινό στοιχείο μεταξύ των διαφόρων τύπων κακόβουλου λογισμικού είναι το γεγονός ότι καθίσταται δύσκολο ή σχεδόν αδύνατο για το χρήστη να εκτελέσει την κανονική του εργασία και το σύστημά του μπορεί να θεωρηθεί πρακτικά μη-διαθέσιμο για την περίοδο που έχει μολυνθεί.

Η εμφάνιση κακόβουλου λογισμικού δεν γίνεται συνήθως μεμονωμένα, αλλά παρουσιάζεται με τη μορφή οργανωμένων σχεδίων από ένα ή περισσότερους κακόβουλους χρήστες [22]. Η κάθε επίθεση διακρίνεται από συγκεκριμένες τάσεις και πρότυπα λειτουργίας, τα οποία χαρακτηρίζουν τη διάδοση μονοσήμαντα και μπορούν να χρησιμοποιηθούν για την κατηγοριοποίηση των στρατηγικών που υλοποιούνται κατά περίπτωση [23]. Ειδικότερα, λόγω της μεγαλύτερης χρήσης ενσύρματων δικτύων, έχει αφιερωθεί σημαντική προσπάθεια στην αναγνώριση και περιγραφή προτύπων συμπεριφοράς κατά τη διασπορά κακόβουλου λογισμικού σε τέτοια δίκτυα και ειδικότερα για τις περιπτώσεις ιών τύπου worm [24],[25]. Ταυτόχρονα, έχουν γίνει προσπάθειες ώστε αυτά τα μοντέλα για τη διάδοση κακόβουλου λογισμικού να αξιοποιηθούν στη μελέτη μεθόδων για την αντιμετώπιση των αντίστοιχων απειλών, λαμβάνοντας κατάλληλα αντίμετρα, προκαταβολικά [26],[27] ή δυναμικά κατά τη διάρκεια μιας επίθεσης [28],[29].

1.1 Συμβολή και Διάρθρωση της Διατριβής

Από τα παραπάνω, γίνεται φανερή η σπουδαιότητα και αναγκαιότητα της ορθής και αποδοτικής περιγραφής μιας διαδικασίας διάδοσης κακόβουλου λογισμικού σε ασύρματα αυτοργανούμενα δίκτυα και δίκτυα αισθητήρων, λαμβάνοντας υπόψη τα ιδιαίτερα χαρακτηριστικά αυτών των δικτύων. Αντικείμενο της παρούσας εργασίας είναι η αναλυτική περιγραφή της διάδοσης κακόβουλου λογισμικού ειδικά σε ασύρματα αυτοργανούμενα δίκτυα και δίκτυα αισθητήρων με χρήση στοχαστικών διαδικασιών (Stochastic Processes). Ειδικότερα το προτεινόμενο πλαίσιο μοντελοποίησης στηρίζεται σε μεθόδους της θεωρίας αναμονής (Queuing Theory). Πιο συγκεκριμένα, μελετάται η διάδοση κακόβουλου λογισμικού γενικευμένου τύπου σε ασύρματα δίκτυα μεταδόσεων πολλαπλών βημάτων (multihop networks) και επιχειρείται η ακριβής ανάλυση της διάδοσης πρώτα σε επίπεδο κόμβου δικτύου και

στη συνέχεια συνολικά σε επίπεδο δικτύου. Συνεπώς στα πλαίσια της διατριβής αυτής δεν δίνεται έμφαση στον τύπο κακόβουλου λογισμικού που έχει να αντιμετωπίσει ένα δίκτυο, αλλά στη μόλυνση κόμβων καθ' αυτή (από οποιοδήποτε τύπο απειλής). Απώτερος σκοπός είναι η εξαγωγή συμπερασμάτων και αναλυτικών εκφράσεων που περιγράφουν τη μέση και συνολική συμπεριφορά – αντίδραση του δικτύου αναφορικά με διάφορα σχήματα γενικευμένων κακόβουλων επιθέσεων.

Η μελέτη ξεκινά από τη σκοπιά του επιτιθέμενου, επιχειρώντας να καταλήξει σε αποδοτικά σχήματα επίθεσης, με έμφαση στην κατανόηση της βλάβης που μπορεί να προκαλέσει μια έξυπνη στρατηγική μόλυνσης. Τελικός στόχος είναι η εκτίμηση της δυνατής έκτασης της βλάβης που μπορεί να προκληθεί από μια μέθοδο επίθεσης και συνεκτίμηση των αποτελεσμάτων για τη σχεδίαση όσο το δυνατόν πιο έξυπνων και αποδοτικών αντίμετρων. Το προτεινόμενο πλαίσιο μοντελοποίησης μπορεί να χρησιμοποιηθεί για διάφορους τύπους δικτύων. Ωστόσο, στη συγκεκριμένη εργασία η μελέτη συγκεκριμενοποιείται στον τύπο των αυτοργανούμενων ad hoc δικτύων και δικτύων αισθητήρων.

Παράλληλα οι στρατηγικές επίθεσης που αναλύονται ανήκουν σε δύο κύριες κατηγορίες. Στην πρώτη περιγράφονται γενικότερες μέθοδοι που θα μπορούσαν να χρησιμοποιηθούν σε ασύρματα δίκτυα χωρίς κεντρική δομή χωρίς να συγκεκριμενοποιούνται για κάποιο ειδικό τύπο κακόβουλου λογισμικού. Οι ενέργειες που προδιαγράφονται για την βελτίωση της αποδοτικότητας της επίθεσης είναι γενικού τύπου και θα μπορούσαν να εφαρμοστούν σε οποιοδήποτε σύνολο ή υποσύνολο τμημάτων κακόβουλου λογισμικού είναι διαθέσιμο στους κακόβουλους χρήστες. Αντίθετα, στη δεύτερη κατηγορία, οι προτεινόμενες μέθοδοι αφορούν σε συγκεκριμένες απειλές – τύπους κακόβουλου λογισμικού, έχουν πιο καθορισμένους αντικειμενικούς στόχους και περιορισμένη ελευθερία στον τρόπο λειτουργίας τους.

Η συνδρομή της εργασίας στην περιοχή της διάδοσης κακόβουλου λογισμικού μπορεί να συνοψισθεί στα ακόλουθα κύρια στοιχεία:

- Προτάθηκε ενα πρωτοποριακό στοχαστικό πλαίσιο για τη μοντελοποίηση της διάδοσης κακόβουλου λογισμικού το οποίο βασίζεται στη θεωρία δικτύων κλειστών ουρών αναμονής. Η μοντελοποίηση της διάδοσης κακόβουλου λογισμικού στηρίζεται για πρώτη φορά στο στοιχείο της αναμονής και το προτεινόμενο πλαίσιο μπορεί να χρησιμοποιηθεί εν δυνάμει στην ανάλυση της

διάδοδης γενικευμένου τύπου κακόβουλου λογισμικού σε οποιοδήποτε τύπο δικτύου. Αρχικά δίνεται ένα μοντέλο αναμονής M/M/1 για την αναπαράσταση ενός κόμβου με συνδέσεις από/προς κακόβουλους ή μολυσμένους γείτονες, το οποίο επεκτείνεται σε ένα δίκτυο πολλαπλών ουρών με ανάδραση για το συνολικό δίκτυο ασύρματων κόμβων που υπόκειται σε επίθεση. Με χρήση του θεωρήματος Norton από τη θεωρία κυκλωμάτων, το σύνθετο κλειστό δίκτυο ουρών απλοποιείται σε ένα απλό κλειστό δίκτυο δύο εν σειρά συνδεδεμένων ουρών, το οποίο προσφέρεται για ανάλυση και εξαγωγή χρήσιμων συμπερασμάτων.

- Το απλό μοντέλο δικτύου δύο κλειστών ουρών συγκεκριμενοποιήθηκε ειδικά για ασύρματα δίκτυα χωρίς κεντρική δομή (αυτοργανούμενα τύπου ad hoc και δίκτυα αισθητήρων), οδηγώντας σε αναλυτικές εκφράσεις για τον αναμενόμενο αριθμό μολυσμένων νόμιμων κόμβων και τον αναμενόμενο συνολικό ρυθμό μόλυνσης νόμιμων κόμβων που δεν έχουν μολυνθεί ακόμα. Κάτι τέτοιο έγινε εφικτό για πρώτη φορά για ασύρματα αυτοργανούμενα δίκτυα, λόγω των διαθέσιμων τεχνικών ανάλυσης που παρέχει το προτεινόμενο μοντέλο διάδοσης κακόβουλου λογισμικού που στηρίζεται στη θεωρία αναμονής.

- Αναγνωρίστηκαν για πρώτη φορά οι παράμετροι που υπεισέρχονται στη διάδοση κακόβουλου λογισμικού και κυριότερα ο τρόπος που αλληλοσχετίζονται, επηρεάζουν και ελέγχουν τη συμπεριφορά της διάδοσης στο συγκεκριμένο τύπο δικτύου που μελετάται. Χαρακτηριστικά, αναδείχθηκε η σημαντικότητα της τοπολογίας και κυριότερα των τοπικών τοπολογικών παραμέτρων και ιδιοτήτων (ακτίνα μετάδοσης, πυκνότητα κόμβων, περιοχή κάλυψης) στην εξέλιξη της διάδοσης, γεγονός που συμβαδίζει με τη διαίσθηση που συνοδεύει τα ασύρματα δίκτυα πολυ-βηματικού (multihop) χαρακτήρα σχετικά με την επίδραση των τοπικών αλληλεπιδράσεων σε διαδικασίες που χαρακτηρίζουν το δίκτυο συνολικά.

- Με βάση τα συμπεράσματα για τις παραμέτρους του προβλήματος που προέκυψαν, σχεδιάστηκαν έξυπνες τεχνικές διάδοσης κακόβουλου λογισμικού ειδικά για ασύρματα δίκτυα χωρίς κεντρική δομή και πολυ-βηματικού χαρακτήρα. Οι τεχνικές αυτές βασίζονται στη φιλοσοφία του Ελέγχου Τοπολογίας και εκμεταλλεύονται τη δυνατότητα μεταβολής της εκπομπής ισχύος για να ρυθμίσουν δυναμικά τη διάρκεια ζωής των κόμβων τους και επομένως την Αποδοτικότητα Μόλυνσής τους. Το ενδιαφέρον επικεντρώθηκε στη σχεδίαση μεθόδων που λειτουργούν στο φυσικό επίπεδο (με βάση την ενέργεια), το στρώμα Ελέγχου

Πρόσβασης στο Μέσο (MAC) και το στρώμα Δικτύου. Οι σχεδιαζόμενες τεχνικές συγκρίνονται μεταξύ τους ώστε να προκύψουν οι κατά περίπτωση επικρατέστερες. Η σχετική επεξεργασία των αποτελεσμάτων καταδεικνύει τις επικρατέστερες μεθόδους για διαφορετικούς τύπους δικτύων και συνθήκες περιβάλλοντος λειτουργίας. Χρησιμοποιώντας τον Έλεγχο Τοπολογίας για τη σχεδίαση τεχνικών διάδοσης κακόβουλου λογισμικού, αναδείχθηκε και ποσοτικοποιήθηκε η δυνατότητα χρήσης ελέγχου ισχύος (power control), ως εργαλείου για αύξηση της αποδοτικότητας της διασποράς ή αντίθετα αντιμετώπισης έξυπνων επιθέσεων. Πρόσφατες εργασίες χρησιμοποιούν πλέον την ιδέα του ελέγχου ισχύος για να σχεδιάσουν μηχανισμούς ανίχνευσης και αντιμετώπισης επιθέσεων σε ασύρματα δίκτυα χωρίς κεντρική δομή.

- Παράλληλα εξετάστηκαν τυχαιοποιημένες τεχνικές διάδοσης κακόβουλου λογισμικού, οι οποίες προορίζονται για περιπτώσεις που ο στόχος είναι η διασπορά μιας απειλής σε όλους τους κόμβους του δικτύου τουλάχιστον μια φορά. Οι μέθοδοι αυτές στηρίζονται στις διαδικασίες Τυχαίων Περίπατων και χρησιμοποιούν κυρίως τοπική τοπολογική πληροφορία για την εκτέλεση της λειτουργίας τους. Το στοιχείο που εισάγεται είναι η προσθήκη αλμάτων πολλαπλών βημάτων μεταξύ κόμβων που επισκέπτεται ο Τυχαίος Περίπατος και η δημιουργία υβριδικών σχημάτων Τυχαίων Περίπατων με βελτιωμένες επιδόσεις. Τα σχήματα που αναλύονται συγκρίνονται μεταξύ τους με βάση διάφορες παράμετρους απόδοσης και κόστους και συμπεραίνονται τα επικρατέστερα για διαφορετικούς τύπους αυτοργανούμενων δικτύων (ad hoc, αισθητήρων, πλέγματος και αυτοκινητιστικά).

Η διάρθρωση του περιεχομένου της διατριβής και της θεματολογίας που παρουσιάστηκε παραπάνω ακολουθεί την εξής δομή:

Στο κεφάλαιο 2 καταγράφεται συνοπτικά η προγενέστερη εικόνα στην ερευνητική περιοχή της διάδοσης κακόβουλου λογισμικού. Περιλαμβάνεται μια σύνοψη των σχετικών εργασιών καθώς και μια ποιοτική σύγκριση μεταξύ των προσεγγίσεων που έχουν χρησιμοποιηθεί στη βιβλιογραφία αναφορικά με την αποτελεσματικότητα και καταλληλότητα τους για τη μοντελοποίηση διάδοσης κακόβουλου λογισμικού σε ασύρματα δίκτυα χωρίς κεντρική υποδομή. Το υλικό αυτό φιλοδοξεί να αποτελέσει ένα κατάλληλο υπόβαθρο για μια σύντομη, αλλά

περιεκτική εισαγωγή στο πρόβλημα της διασποράς κακόβουλου λογισμικού με έμφαση τα ασύρματα δίκτυα χωρίς κεντρική δομή.

Στο κεφάλαιο 3 παρουσιάζεται το μοντέλο δικτύου επικοινωνιών που θεωρείται στην παρούσα μελέτη, και συγκεκριμένα το επικοινωνιακό μοντέλο μεταξύ κόμβων που καθορίζει σε συνδυασμό με το θεωρούμενο μοντέλο κινητικότητας τις σχέσεις γειτονίας νόμιμων – κακόβουλων κόμβων και επομένως την εξέλιξη της διασποράς κακόβουλου λογισμικού. Παράλληλα, δίνεται ο τυπικός ορισμός του προβλήματος στο οποίο εστιάζει η παρούσα εργασία και το πλαίσιο – έκταση μελέτης του. Στη συνέχεια εισάγεται και περιγράφεται αναλυτικά το προτεινόμενο μοντέλο διάδοσης κακόβουλου λογισμικού, με χρήση θεωρίας αναμονής, από το επίπεδο κόμβου, μέχρι την ολική περιγραφή που αφορά στο δίκτυο και το απλοποιημένο μοντέλο δύο εν σειρά ουρών με ανάδραση. Το μοντέλο συγκεκριμενοποιείται με αναλυτικά αποτελέσματα για αυτοργανούμενα ad hoc δίκτυα και δίκτυα αισθητήρων. Με αυτό τον τρόπο παρέχονται χρονικά ανεξάρτητα μετρικά αξιολόγησης μιας επίθεσης κακόβουλου λογισμικού και παράλληλα εισάγεται ένα χρονικά–εξαρτώμενο μετρικό (Αποδοτικότητα Μόλυνσης) που μπορεί να χρησιμοποιηθεί για τη μελέτη της επίδρασης της κατανάλωσης ενέργειας στη διάδοση κακόβουλου λογισμικού.

Το κεφάλαιο 4 περιλαμβάνει αριθμητικά αποτελέσματα και αποτελέσματα προσομοιώσεων για την εξοικείωση με την προβλεπόμενη συμπεριφορά της διάδοσης σε ασύρματα δίκτυα και την αναγνώριση των παραμέτρων που ελέγχουν την εξέλιξη της διάδοσης, όπως και του συγκεκριμένου τρόπου με τον οποίο αυτό συμβαίνει. Στη συνέχεια, με βάση τα συμπεράσματα που προκύπτουν αξιολογούνται οι δυνατότητες μιας βέλτιστης στρατηγικής γενικού τύπου με χρήση θεωρίας βελτιστοποίησης, ώστε να αναγνωριστεί το εύρος της επίδρασης ενός συνόλου κακόβουλων χρηστών.

Το κεφάλαιο 5 παρουσιάζει τις έξυπνες τεχνικές διάδοσης κακόβουλου λογισμικού, οι οποίες βασίζονται στην προσέγγιση του Ελέγχου Τοπολογίας και αποσκοπούν ειδικά για χρήση σε ασύρματα αυτοργανούμενα δίκτυα ευρείας κλίμακας. Οι μέθοδοι που προτείνονται συνοδεύονται από τη σχετική ανάλυση λειτουργίας τους. Επίσης παρατίθενται αποτελέσματα προσομοιώσεων για τη σύγκριση μεταξύ των προτεινόμενων μεθόδων και την αξιολόγηση της καταλληλότητας κάθε προσέγγισης.

Στο κεφάλαιο 6 παρατίθενται οι τυχαιοποιημένες τεχνικές διάδοσης κακόβουλου λογισμικού από ένα κακόβουλο χρήστη προς όλους τους κόμβους ενός δικτύου που βασίζονται σε Τυχαίους Περίπατους. Παρατίθενται αποτελέσματα προσομοιώσεων με σκοπό τον προσδιορισμό της πιο αποδοτικής τεχνικής για διαφορετικούς τύπους ασύρματων δικτυών χωρίς κεντρική υποδομή, λαμβάνοντας υπόψη τα ιδιαίτερα χαρακτηριστικά λειτουργίας των δικτύων και απόδοσης/κόστους των τεχνικών Τυχαίου Περίπατου.

Τέλος, το κεφάλαιο 7 παρουσιάζει συνολικά συμπεράσματα που προέκυψαν από την μελέτη που διεξήχθη στα πλαίσια της παρούσας διατριβής, τόσο σε θεωρητικό επίπεδο, όσο και πρακτικό για τη σχεδίαση ρεαλιστικών συστημάτων. Στη συνέχεια σκιαγραφούνται κατευθύνσεις για μελλοντική εργασία και επέκταση των μεθόδων και των μοντέλων που προτάθηκαν με σκοπό τη συνέχιση της εργασίας και την αξιοποίησή της στα πλαίσια ακριβέστερων και αποδοτικότερων σχεδιασμών.

Κεφάλαιο 2

Διάδοση Κακόβουλου Λογισμικού σε Δίκτυα Υπολογιστών και Επικοινωνιών

Το σύνολο των προσπαθειών που επιχειρούν να περιγράψουν με ακρίβεια τη διάδοση κακόβουλου λογισμικού και να εμβαθύνουν στη μελέτη των επιθέσεων και της αντιμετώπισής τους επικεντρώνονταν μέχρι πρόσφατα σε περιπτώσεις ενσύρματων τοπικών δικτύων και το Διαδίκτυο. Σταδιακά, όμως και με την αύξηση της διείσδυσης των ασύρματων δικτύων πρόσβασης (κυψελωτά ή χωρίς κεντρική δομή), η συχνότητα εμφάνισης κακόβουλου λογισμικού σε περιπτώσεις ασύρματων δικτύων, έστρεψε το ενδιαφέρον των ερευνητών και προς το συγκεκριμένο τύπο δικτύων πρόσβασης.

Στο τρέχον κεφάλαιο παρουσιάζονται οι πιο σημαντικές κατηγορίες προσεγγίσεων μοντελοποίησης της διάδοσης κακόβουλου λογισμικού που έχουν προταθεί για δίκτυα υπολογιστών και επικοινωνιών. Η κατηγοριοποίηση των μεθόδων που παρατίθενται βασίζεται στο μαθηματικό φορμαλισμό που προτείνει ή υιοθετεί η κάθε τεχνική. Στη συνέχεια οι προσεγγίσεις που παρουσιάζονται συγκρίνονται με βάση τα χαρακτηριστικά τους προκειμένου να διαπιστωθεί η καταλληλότητα τους για χρήση σε ασύρματα αυτοργανούμενα δίκτυα και δίκτυα αισθητήρων, στα οποία επικεντρώνει η παρούσα μελέτη.

Με γνώμονα τα κύρια χαρακτηριστικά των μεθόδων που έχουν ήδη προταθεί, δίνεται έμφαση στους βασικούς άξονες που θα έπρεπε να ακολουθηθούν για τη σχεδίαση νέων και εξυπνότερων μεθόδων διάδοσης κακόβουλου λογισμικού. Για το σκοπό αυτό παρουσιάζονται συνοπτικά, αλλά με την αναγκαία λεπτομέρεια τα μοντέλα και τα αναλυτικά εργαλεία που έχουν καθιερωθεί και χρησιμοποιηθεί μέχρι τώρα. Η παρουσίαση δεν εστιάζει σε μία μόνο κατηγορία δικτύων, αλλά ασχολείται με όλους τους τύπους, προκειμένου να γίνει κατανοητό το εύρος εφαρμογής κάθε μεθόδου και οι περιορισμοί που τη διέπουν. Παράλληλα, γίνεται πιο ξεκάθαρος ο διαχωρισμός μεταξύ τεχνικών που αφορούν μόνο σε ενσύρματα ή ασύρματα δίκτυα

και εντοπίζονται εκείνες οι μέθοδοι που θα μπορούσαν να χρησιμοποιηθούν και για τους δύο τύπους, με ή χωρίς αναγκαίες τροποποιήσεις.

Στη συνέχεια διακρίνονται τρεις κύριες κατηγορίες προσεγγίσεων κάθε μία από τις οποίες αντιμετωπίζεται ξεχωριστά. Αρχικά παρουσιάζονται τα μοντέλα διάδοσης που στηρίζονται σε προσεγγίσεις εμπνευσμένες από τον κλάδο της επιδημιολογίας. Ακολουθούν στοχαστικά μοντέλα διαφόρων τύπων και τέλος, περιγράφονται στοχαστικά μοντέλα τύπου Markov. Ορισμένες από τις τεχνικές που παρατίθενται αποτελούν συνδυασμούς δύο ή και των τριών κατηγοριών που διαμορφώθηκαν, η παρουσίασή τους όμως γίνεται με βάση την κύρια ιδέα στην οποία στηρίζεται το εκάστοτε μοντέλο και την αντίστοιχη κατηγορία στην οποία αυτή ανήκει.

2.1 Επιδημιολογικά Μοντέλα Διάδοσης

Η διάδοση κακόβουλου λογισμικού σε δίκτυα υπολογιστών και επικοινωνιών παρουσιάζει πολλές ομοιότητες με τη διάδοση ασθενειών και βιολογικών ιών σε έμβιους οργανισμούς, όπως οι άνθρωποι, ομάδες φυτών, ζώων ή διάφορων κυτταρικών οργανισμών [30]. Σημαντική προσπάθεια έχει γίνει στον αντίστοιχο κλάδο της βιολογίας–παθολογίας (επιδημιολογία) ήδη από τον δέκατο όγδοο αιώνα (Daniel Bernoulli, [30]) με σκοπό αφενός την ακριβή περιγραφή της διάδοσης τέτοιων απειλών και αφετέρου την επιτυχημένη αντιμετώπισή τους όταν ξεσπάσουν. Ως επακόλουθο, οι πρώτες προσπάθειες για μοντελοποίηση διάδοσης κακόβουλου λογισμικού χρησιμοποίησαν μεθόδους από την επιδημιολογία [31],[32], με τις κατάλληλες τροποποιήσεις και μεταβάλλοντας τις υπεισερχόμενες παραμέτρους αντίστοιχα, ώστε να μελετηθεί η διάδοση κακόβουλου λογισμικού στο Διαδίκτυο και τοπικά ενσύρματα δίκτυα.

Αρχικά το ενδιαφέρον για επιδημιολογική αντιμετώπιση του κακόβουλου λογισμικού εστίαζε σε ενσύρματα δίκτυα και το Διαδίκτυο, κυρίως λόγω της γενικότερης απουσίας ασύρματων μέσων. Ωστόσο, καθώς η διείσδυση των τελευταίων αυξάνεται και το ενδιαφέρον μετατοπίζεται και προς αυτή την κατεύθυνση τουλάχιστον για τα δίκτυα πρόσβασης, οι επιδημιολογικές τεχνικές προσαρμόστηκαν και εφαρμόστηκαν αντίστοιχα για χρήση και σε ασύρματα δίκτυα. Στη συνέχεια παρουσιάζονται και οι δύο προσεγγίσεις, επικεντρώνοντας στις λεπτομέρειες που διαφοροποιούνται λόγω της φύσης των δικτύων που μελετάται η διάδοση.

Στην επιδημιολογία μελετώνται κλειστές ομάδες πληθυσμών, αντιστοιχίζοντας τις ομάδες αυτές σε γράφους δικτύων. Τα μέλη του πληθυσμού απεικονίζονται ως κόμβοι και οι δυνατές αλληλεπιδράσεις μεταξύ τους ως συνδέσεις μεταξύ κόμβων. Σημαντικό βήμα για την ορθή μοντελοποίηση τέτοιων συστημάτων είναι ο τρόπος που τα μέλη–κόμβοι επηρεάζονται από τις ασθένειες/απειλές που κυκλοφορούν και η συμπεριφορά τους αφού μολυνθούν. Η συγκεκριμένη προδιαγραφή για κάθε δίκτυο, ανεξαρτήτως τύπου και περιβάλλοντος εφαρμογής του, αναφέρεται με τον όρο μοντέλο μόλυνσης κόμβων. Έτσι θεωρώντας ότι όλοι οι κόμβοι ξεκινούν στην κατάσταση μη-μόλυνσης, τα μέλη του πληθυσμού μεταβαίνουν στην κατάσταση μόλυνσης μόλις προσβληθούν από μια επίθεση και μετά ανάλογα με το είδος της επίθεσης και το μοντέλο μόλυνσης, οι κόμβοι επανακάμπτουν στην αρχική τους κατάσταση, παραμένουν μολυσμένοι (και είτε μολύνουν άλλους γειτονικούς κόμβους, είτε μένουν ανενεργοί) ή ανακάμπτουν ανοσοποιημένοι και δεν προσβάλλονται ξανά, εκτελώντας κανονικά την αρχική λειτουργία τους [31],[32].

Στα επιδημιολογικά μοντέλα η κύρια παράμετρος είναι ο αριθμός των μολυσμένων κόμβων ως συνάρτηση του χρόνου. Πρόκειται για μοντέλα συνεχούς χρόνου, όπου το σύστημα μελετάται για ένα συγκεκριμένο χρονικό διάστημα και το ζητούμενο είναι ο καθορισμός ενός συστήματος συνήθων διαφορικών εξισώσεων που να περιγράφουν τη μεταβολή των μολυσμένων κόμβων μέσα στο χρονικό διάστημα παρατήρησης. Όλα τα μεγέθη που υπεισέρχονται στην περιγραφή του συστήματος θεωρούνται ότι έχουν συνεχή εξάρτηση του πραγματικού χρόνου συστήματος, αν και όπως θα διαφανεί κάτι τέτοιο μπορεί να μην ισχύει απόλυτα στην πραγματικότητα. Οι λύσεις που λαμβάνονται είναι επίσης συνεχείς συναρτήσεις του χρόνου, παρόλα αυτά όμως φαίνεται να έχουν αρκετά καλή συμφωνία με τα πραγματικά δεδομένα.

Για να περιγραφεί πλήρως η συμπεριφορά του συστήματος σε σχέση με μια δεδομένη επίθεση είναι αναγκαίος ο προσδιορισμός δύο μακροσκοπικών ρυθμών σε σχέση με το σύνολο του πληθυσμού του δικτύου. Ο ένας είναι ο ρυθμός μόλυνσης κόμβων στο δίκτυο και ο δεύτερος είναι ο ρυθμός ανάκαμψης κάθε κόμβου ή αντίστοιχα ο ρυθμός απομάκρυνσης κόμβων (όταν οι κόμβοι δεν μπορούν να ανακάμψουν), ανάλογα με το θεωρούμενο μοντέλο μόλυνσης κόμβων. Στην πράξη τέτοιες ποσότητες δεν είναι διαθέσιμες τη στιγμή που λαμβάνει χώρα μια επίθεση ή τουλάχιστον είναι γνωστές κάποιες τιμές οι οποίες μπορεί να αλλάξουν δραστικά μέχρι το πέρας της. Το γεγονός αυτό περιορίζει αναγκαστικά την εφαρμογή τέτοιων

μεθόδων για αντιμετώπιση επιθέσεων σε πραγματικό χρόνο και τις καθιστά περισσότερο ακριβείς για μοντελοποίηση των επιθέσεων μετά την ολοκλήρωσή τους. Φυσικά, σε ενδεχόμενη επανάληψη μιας επίθεσης με τους ίδιους όρους και συνθήκες η ακρίβεια αυξάνει σημαντικά.

Η αλληλοσυσχέτιση των θεωρούμενων ρυθμών με την κύρια μεταβλητή του προβλήματος και το είδος της θεωρούμενης διαφορικής εξίσωσης εξαρτάται σε μεγάλο βαθμό από το είδος του δικτύου υπολογιστών που μελετάται και περισσότερο από τη συμπεριφορά των χρηστών του δικτύου στις επιθέσεις που δέχονται. Στην πιο απλή περίπτωση, δεν υπάρχει δυνατότητα ένας κόμβος που δέχεται κακόβουλο λογισμικό να το μεταδώσει με τη σειρά του στους γείτονές του. Επιπρόσθετα ο κόμβος δεν επανέρχεται στην αρχική του κατάσταση. Από την άλλη ένας κόμβος μπορεί να μεταδίδει το λογισμικό που δέχεται σε γειτονικούς κόμβους, χωρίς ο ίδιος να μπορεί να ανακάμψει, και το ίδιο συμβαίνει με τους γείτονες που μολύνει. Επίσης μπορεί ο μολυσμένος κόμβος να μη μεταδίδει παραπέρα τις απειλές που δέχεται, αλλά να μπορεί να επιστρέψει στην αρχική του κατάσταση, ενώ τέλος, ένας κόμβος μπορεί να είναι σε θέση να ανακάμπτει, αλλά μέχρι εκείνο το σημείο να γίνεται αντικείμενο εκμετάλλευσης από τις πηγές κακόβουλου λογισμικού και να χρησιμοποιείται για να μολύνει γειτονικούς του κόμβους.

Στην περίπτωση κόμβων που μπορούν να ανακάμψουν από μολύνσεις που δέχονται, το επιδημιολογικό μοντέλο δίνεται από το ζεύγος των διαφορικών εξισώσεων:

$$\begin{aligned} \frac{ds(t)}{dt} &= -\frac{k\lambda s(t)i(t)}{N} + \frac{i(t)}{D} \\ \frac{di(t)}{dt} &= \frac{k\lambda s(t)i(t)}{N} - \frac{i(t)}{D} \end{aligned} \qquad (1)$$

όπου $s(t)+i(t)=N$ είναι ο συνολικός αριθμός κόμβων δικτύου, $i(t)$ είναι ο τρέχων αριθμός μολυσμένων κόμβων στο δίκτυο, $s(t)$ ο αριθμός μη-μολυσμένων κόμβων, D είναι η μέση διάρκεια μόλυνσης (μέσο χρονικό διάστημα παρατήρησης), k είναι ο αριθμός των συνδέσεων (βαθμός) κόμβου με μολυσμένους γείτονες και λ είναι η πιθανότητα μόλυνσης για μια ζεύξη μεταξύ μολυσμένου, μη-μολυσμένου κόμβου. Στο σύστημα εξισώσεων (1), το δίκτυο θεωρείται ομογενές (η κατανομή του βαθμού κόμβου είναι μέγιστη στη μέση τιμή και μειώνεται εκθετικά εκατέρωθέν της), αλλά οι αλληλεπιδράσεις κόμβων είναι τυχαίες. Μια τέτοια θεώρηση είναι ρεαλιστική για τη

μελέτη διάδοσης ασθενειών και ιών όπως αυτοί της γρίπης [31]. Στην περίπτωση δικτύων υπολογιστών και επικοινωνιών, η υπόθεση ομογενούς δικτύου ισχύει μόνο για ορισμένους τύπους δικτύων, όπως είναι τα δίκτυα εφαρμογών υπέρθεσης (overlay networks) και τα ομότιμα δίκτυα (peer-to-peer, P2P) [33]. Ωστόσο, για άλλους τύπους απέχει σημαντικά από την πραγματικότητα, ειδικά για τα ασύρματα χωρίς κεντρική υποδομή, όπως είναι τα αυτοργανούμενα και τα δίκτυα αισθητήρων [34]. Κάτι τέτοιο είναι αναγκαίο να ληφθεί υπόψη και να γίνουν οι αναγκαίες τροποποιήσεις στην περίπτωση τέτοιων δικτύων, όπως θα φανεί στη συνέχεια.

Πολύ σημαντικό μέγεθος που προκύπτει από την επίλυση του συστήματος (1) είναι ο ρυθμός αναπαραγωγής κακόβουλου λογισμικού (μέσος αριθμός μολύνσεων που παράγει ένας μολυσμένος κόμβος) $R_0 = k\lambda D$. Αν $R_0 < 1$, η ασθένεια τείνει τελικά προς εξαφάνιση, ενώ για $R_0 > 1$ η ασθένεια βαίνει προς επιδημία (ο πληθυσμός καθολικά μολυσμένος). Για $R_0 = 1$, το σύστημα βρίσκεται σε μια ενδημική κατάσταση που ο αριθμός των μολυσμένων κόμβων έχει μια τιμή που δεν μεταβάλλεται σημαντικά (καθόλου κατά μέσο όρο).

Σε ανομοιογενείς πληθυσμούς (όπου η τιμή του k δεν είναι ίδια για όλους τους κόμβους), ο ρυθμός αναπαραγωγής τροποποιείται στη μορφή $R_0 = \rho_0 \left(1 + \frac{\sigma^2}{\langle k \rangle} \right)$, όπου τώρα ρ_0 είναι ο μέσος αριθμός μολύνσεων που παράγονται από ένα μολυσμένο κόμβο, $\langle k \rangle$ είναι ο μέσος βαθμός κόμβου και σ^2 είναι η μεταβλητότητά του. Η δεύτερη παραλλαγή του ρυθμού αναπαραγωγής για ανομοιογενείς πληθυσμούς είναι καταλληλότερη για τη μοντελοποίηση μεταδιδόμενων νοσημάτων σε ανθρώπους, κάτι που έχει επιβεβαιωθεί και εμπειρικά [31].

Τα επιδημιολογικά μοντέλα όπως το σύστημα εξισώσεων (1) επηρεάζονται σε μεγάλο βαθμό από τις διασυνδέσεις μεταξύ των μελών του πληθυσμού υπό μελέτη, κυρίως μέσω του βαθμού κόμβου και της μεταβλητότητας που παρουσιάζει. Διαφορετικοί τύποι δικτύων, εμφανίζουν διαφορετική συμπεριφορά αναφορικά με τις συνδέσεις των κόμβων τους και ειδικότερα την κατανομή του βαθμού κόμβου [34]. Έτσι το υποκείμενο μοντέλο δικτύου επηρεάζει σημαντικά τα τελικά αποτελέσματα και την έκβαση της συμπεριφοράς της εκάστοτε απειλής. Στην περίπτωση ομογενούς δικτύου, επικεντρώνοντας μόνο στον αριθμό των μολυσμένων κόμβων, και

σημειώνοντας ότι το σύστημα διαφορικών εξισώσεων έχει γραφεί ως συνάρτηση της πυκνότητας μολυσμένων κόμβων $\rho(t)=\frac{i(t)}{N}$, επιβάλλοντας τη συνθήκη στασιμότητας $\frac{\partial\rho(t)}{\partial t}=0$, για μεγάλες τιμές του χρόνου λαμβάνουμε την εξίσωση $\rho\left[-1+\lambda\langle k\rangle(1-\rho)\right]=0$. Η τελευταία καθορίζει ένα επιδημικό κατώφλι $\lambda_c=\frac{1}{\langle k\rangle}$, έτσι ώστε:

$$\begin{aligned}&\rho=0, \qquad \lambda<\lambda_c\\ &\rho=\frac{\lambda-\lambda_c}{\lambda},\ \lambda\geq\lambda_c\end{aligned} \tag{2}$$

Επομένως, σε ομογενή δίκτυα όπου οι κόμβοι ανακάμπτουν, υπάρχει ένα θετικό επιδημικό κατώφλι (τιμή του ρυθμού μόλυνσης) κάτω από το οποίο η απειλή εκμηδενίζεται, ενώ πάνω από αυτή την τιμή η απειλή μετατρέπεται σε πανδημία [31],[32].

Η κατάσταση αλλάζει άρδην στην περίπτωση δικτύων με εκθετική κατανομή κόμβων (scale-free/exponential networks) [35]. Η διαφορική εξίσωση τροποποιείται για να ληφθεί:

$$\frac{d\rho_k(t)}{dt}=-\rho_k(t)+\lambda k\left[1-\rho_k(t)\right]\Theta\left[\{\rho_k(t)\}\right] \tag{3}$$

όπου $\Theta\left[\{\rho_k(t)\}\right]$ είναι η πιθανότητα μια τυχαία επιλεγμένη ζεύξη να περιλαμβάνει ένα μολυσμένο κόμβο. Λύση της παραπάνω με εφαρμογή της συνθήκης στασιμότητας, και υπολογισμό της $\Theta\left[\{\rho_k(t)\}\right]$ για την περίπτωση τυχαίων δικτύων με εκθετική κατανομή κόμβων οδηγεί στο επιδημικό κατώφλι $\lambda_c=\frac{\langle k\rangle}{\langle k^2\rangle}$, το οποίο για δίκτυα με εκθέτες $2<\gamma\leq 3$ δίνει $\lambda_c=0$ [32]. Επομένως για δίκτυα τέτοιου τύπου, δεν παρουσιάζεται επιδημικό κατώφλι και άρα η έκβαση της απειλής εξαρτάται από την πυκνότητα κόμβων του δικτύου και το ρυθμό μόλυνσης νόμιμων κόμβων, οδηγώντας είτε σε πλήρη εξαφάνισή της ή σε πλήρη επικράτησή της. Μόνο για τιμές των εκθετών $\gamma>4$ ή πεπερασμένους πληθυσμούς μικρού μεγέθους, αρχίζει η εμφάνιση επιδημικών κατωφλίων και σε αυτά τα δίκτυα [32]. Ένα σημαντικό αποτέλεσμα που μπορεί να εξαχθεί από τα παραπάνω, είναι ότι για δίκτυα τέτοιου

τύπου, τυχαία επιλογή κόμβων ώστε να ανοσοποιηθούν με σκοπό να εμποδίζουν τη περαιτέρω διάδοση του κακόβουλου λογισμικού δεν λειτουργεί αποδοτικά. Αντίθετα, στοχευμένες στρατηγικές ανοσοποίησης με κριτήρια όπως η τοπολογία ή η κίνηση κόμβων δικτύου είναι πιο ουσιαστικές και αποτελεσματικές.

Θεωρώντας ότι οι μη-μολυσμένοι κόμβοι μπορούν να μεταβούν μόνο στην κατάσταση μόλυνσης το επιδημιολογικό μοντέλο για πεπερασμένο μέγεθος πληθυσμού γίνεται:

$$\frac{di(t)}{dt} = \lambda i(t)\big[N - i(t)\big] \tag{4}$$

και αντίστοιχα μπορεί να προκύψει μια παρόμοια έκφραση για τον αριθμό των μη-μολυσμένων κόμβων.

Η γενίκευση που ακολουθεί αφορά σε συστήματα που οι μη-μολυσμένοι κόμβοι περνούν στην κατάσταση της μόλυνσης μόλις δεχθούν μια επιτυχημένη απειλή και παραμένουν σε αυτή μέχρι να απομακρυνθούν εντελώς από το δίκτυο. Σε αυτό το θεωρούμενο σύστημα οι κόμβοι δεν ανακάμπτουν στην αρχική μη-μολυσμένη κατάστασή τους. Το επιδημιολογικό μοντέλο για αυτή την περίπτωση αναφέρεται ως Kermack-McKendrick [36],[37],[38]:

$$\begin{aligned} \frac{dj(t)}{dt} &= \lambda j(t)\big[N - j(t)\big] \\ \frac{dr(t)}{dt} &= \gamma i(t) \\ j(t) &= i(t) + r(t) = N - s(t) \end{aligned} \tag{5}$$

όπου $i(t)$ είναι ο αριθμός των μολυσματικών κόμβων, $r(t)$ ο αριθμός των κόμβων που απομακρύνονται, $j(t)$ ο αριθμός των συνολικά μολυσμένων κόμβων ($j(t) = i(t) + r(t)$), $s(t)$ ο αριθμός των μη-μολυσμένων κόμβων, λ είναι ο ρυθμός μόλυνσης κόμβων και γ ο ρυθμός απομάκρυνσης μολυσμένων κόμβων. Ο διαχωρισμός μολυσματικών – απομακρυσμένων κόμβων γίνεται για να διακρίνει τους κόμβους που ενώ είναι μολυσμένοι μπορούν να μολύνουν άλλους μη-μολυσμένους γείτονές του, από εκείνους τους κόμβους που είναι μολυσμένοι και δεν διαδραματίζουν κανένα ρόλο στο δίκτυο (πρακτικά έχουν απομακρυνθεί). Από τη λύση του συστήματος προκύπτει ότι με $\rho \equiv \frac{\gamma}{\lambda}$, $\frac{di(t)}{dt} > 0$ αν και μόνο αν $s(t) > \rho$, ώστε να προκύπτει ένα επιδημικό κατώφλι, όπως σε προηγούμενες περιπτώσεις.

Η παρουσία επιδημικού κατωφλίου που καθορίζει τη συμπεριφορά των συστημάτων που περιγράφηκαν παραπάνω υποδηλώνει μια χαρακτηριστική τάση για το δίκτυο στο οποίο πραγματοποιείται η διάδοση. Συγκεκριμένα, στην εκκίνηση της διάδοσης η αύξηση των μολυσμένων κόμβων είναι σχεδόν ασήμαντη, σύντομα όμως γίνεται εκθετική, ώστε τελικά στην αρχική φάση της διάδοσης να παρατηρείται ραγδαία αύξηση [36],[39]. Ο ρυθμός της αύξησης εξαρτάται από τις συσχετίσεις μεταξύ των κόμβων δικτύου, οι οποίες με τη σειρά τους καθορίζονται από την τοπολογία που διαμορφώνεται από τα ιδιαίτερα χαρακτηριστικά (κανάλι, μηχανισμός μόλυνσης κόμβων) του συστήματος που μελετάται.

Οι παραπάνω προσεγγίσεις μπορούν να εφαρμοστούν σε διάφορες κατηγορίες συστημάτων, προερχόμενα από διαφορετικές επιστημονικές περιοχές (βιολογία, δίκτυα υπολογιστών, ειδησεογραφικά δίκτυα). Ειδικά για την περίπτωση δικτύων υπολογιστών και επικοινωνιών έχουν γίνει διάφορες προσαρμογές, ώστε να υπάρχει συμβατότητα με τα ιδιαίτερα χαρακτηριστικά που εμφανίζει η διάδοση κακόβουλου λογισμικού σε δίκτυα υπολογιστών. Στην περίπτωση του ιού τύπου worm CodeRed2 (Random Constant Scanning – RCS), το λογισμικό διαρκώς προσπαθεί να βρεί νέα θύματα χωρίς τοπολογικούς περιορισμούς και δυνητικά όλοι οι μη-μολυσμένοι κόμβοι μπορούν να μολυνθούν ανά πάσα στιγμή από οποιοδήποτε μολυσμένο κόμβο [36]. Το μοντέλο που εκφράζεται από τις σχέσεις (5), χρειάζεται τροποποίηση προκειμένου να χρησιμοποιηθεί στην περίπτωση του CodeRed2 και συγκεκριμένα πρέπει να ληφθεί υπόψη η λήψη μέτρων από μη-μολυσμένους κόμβους που μαθαίνουν την απειλή που κυκλοφορεί στο δίκτυο και προετοιμάζονται κατάλληλα, δηλαδή λαμβάνουν τα αναγκαία μέτρα, ώστε ακόμα και επικοινωνία να υπάρξει με κακόβουλους ή μολυσμένους κόμβους να μην επιτρέψουν στο κακόβουλο τμήμα λογισμικού να λειτουργήσει. Αυτό μπορεί να γίνει θεωρώντας ότι ένας αριθμός μη-μολυσμένων κόμβων απομακρύνεται από το σύνολο των κόμβων που μπορεί να μολυνθούν $q(t)$ (κόμβοι σε καραντίνα – quarantined nodes). Σε αυτή την περίπτωση $s(t)+i(t)+r(t)+q(t)=N$ και το μοντέλο (5) γίνεται:

$$\frac{di(t)}{dt}=\lambda(t)\left[N-r(t)-i(t)-q(t)\right]i(t)-\frac{dr(t)}{dt} \qquad (6)$$

το οποίο αναφέρεται ως μοντέλο δύο-παραγόντων (two-factor model) [36],[40]. Το παραπάνω μοντέλο δύο-παραγόντων έχει μελετηθεί αρκετά και δείχνει να συμφωνεί με ακρίβεια με στοιχεία που αφορούν στην πραγματική λειτουργία του λογισμικού

CodeRed2. Ουσιαστικά αποτελεί ένα γενικότερο μοντέλο για ιούς τύπου worm που διαδίδονται στο Διαδίκτυο, ωστόσο έχει τον περιορισμό ότι περιγράφει τη διάδοση ως μια συνεχή διαδικασία σε ένα συνεχές χρονικό διάστημα, κάτι που δεν αληθεύει για πραγματικό λογισμικό, μιας και όπως έχει ήδη αναφερθεί η διάδοση μπορεί να περιλαμβάνει πολλά ενδιάμεσα διαστήματα διακοπής και εκκίνησης της διαδικασίας [37].

Με βάση το παραπάνω μοντέλο δύο-παραγόντων έχει προταθεί μια τεχνική ανοσοποίησης, με βάση την οποία κάθε κόμβος που θεωρείται ύποπτος τίθεται σε καραντίνα και απομακρύνεται από το δίκτυο. Αυτή η τεχνική αναφέρεται ως Δυναμική Καραντίνα [39]. Μια τέτοια πρακτική είναι κατάλληλη για την αντιμετώπιση περιπτώσεων άγνωστων επιθέσεων. Ορίζοντας λ_1, λ_2 τους ρυθμούς τοποθέτησης σε καραντίνα των μολυσματικών (κόμβοι που έχουν μολυνθεί και διαδίδουν οι ίδιοι πλέον κακόβουλο λογισμικό) και μη-μολυσμένων κόμβων αντίστοιχα, τότε $r(t) = \frac{\lambda_1 T}{1+\lambda_1 T} i(t)$ και $q(t) = \frac{\lambda_2 T}{1+\lambda_2 T} s(t)$, όπου T είναι ο χρόνος τοποθέτησης κόμβων σε καραντίνα. Μελετώντας τη διάδοση των απειλών που κυκλοφορούν στο δίκτυο υπό διαφορετικά καθεστώτα συμπεριφοράς κόμβων σε σχέση με το μοντέλο μόλυνσης, στην περίπτωση του απλού επιδημικού μοντέλου, η διάδοση γίνεται όπως και πριν με τη διαφορά μιας ελαφράς καθυστέρησης στο ρυθμό διάδοσης. Για την περίπτωση του μοντέλου Kermack-McKendrick, η Δυναμική Καραντίνα μειώνει σημαντικά τη δυνατότητα ενός ιού worm να εξελιχθεί σε επιδημία, παρόλο που δεν είναι σε θέση να αποτρέπει την εκκίνηση της διάδοσης. Στην περίπτωση που τροποποιηθεί το μοντέλο ώστε να απομακρύνονται μόνο μολυσματικοί κόμβοι, η Δυναμική Καραντίνα εξασφαλίζει με σιγουριά ότι δεν θα ξεσπάσει πανδημία στο δίκτυο [39].

Το κλασικό επιδημικό μοντέλο έχει επεκταθεί και σε περιπτώσεις κατευθυντικών δικτύων με αντίστοιχους υποκείμενους γράφους [41]. Κάτι τέτοιο είναι χρήσιμο σε περιπτώσεις δικτύων εφαρμογών στις οποίες δεν είναι δυνατή η αμφίδρομη επικοινωνία μεταξύ χρηστών, είτε λόγω του περιβάλλοντος, είτε λόγω της ποιότητας ζεύξης μεταξύ τους. Υποθέτοντας κατευθυντικούς γράφους διαφόρων τύπων (τυχαίους, πλέγματα και ιεραρχικούς) και επεκτείνοντας το κλασικό ντετερμινιστικό επιδημιολογικό μοντέλο, μέσω της πιθανότητας $p(I,t)$ που

υποδηλώνει την ύπαρξη I μολυσμένων κόμβων στη χρονική στιγμή t, μπορεί να υπολογισθεί η πιθανότητα εξαφάνισης κακόβουλου λογισμικού:

$$p_{\infty}(I) = \frac{e^{-(I-I_{\max})^2/2N\rho'}}{\sqrt{2\pi N\rho'}} \tag{7}$$

όπου ρ' είναι το ντετερμινιστικό επιδημικό κατώφλι, $I_{\max}$ ο μέγιστος αριθμός μολυσμένων κόμβων που μπορεί να επιτευχθεί και N ο συνολικός αριθμός κόμβων δικτύου. Η μελέτη των αποτελεσμάτων σε κατευθυντικούς γράφους επιβεβαιώνει την ύπαρξη επιδημικών κατωφλίων και σε αυτή την περίπτωση, αν και ελαφρά τροποποιημένων, συνήθως με αυξημένες τιμές σε σχέση με το κλασικό επιδημικό κατώφλι. Κάτι τέτοιο είναι αρκετά ενθαρρυντικό από τη σκοπιά του διαχειριστή δικτύου, υπό την έννοια ότι η διάδοση κακόβουλου λογισμικού στα δίκτυα υπολογιστών που μελετήθηκαν γίνεται πιο αργά σε σχέση με βιολογικούς πληθυσμούς, ως απόρροια των λιγότερων συνδέσεων που εγγενώς παρατηρούνται μεταξύ τυχαία επιλεγμένων κόμβων αυτών των δικτύων.

2.2 Επιδημιολογικά Μοντέλα για Ασύρματα Αυτοργανούμενα Δίκτυα

Ειδικότερα για την περίπτωση των αυτοργανούμενων (ad hoc) δικτύων έχουν προταθεί διάφορες μέθοδοι από τη σκοπιά της επιδημιολογίας για την εξαγωγή αντίστοιχων αποτελεσμάτων. Μια σχετικά απλή προσπάθεια για την εφαρμογή των επιδημιολογικών μοντέλων που παρουσιάστηκαν παραπάνω έχει προταθεί στο [42]. Επεκτείνοντας το μοντέλο δύο-παραγόντων και θεωρώντας ότι μολυσμένοι κόμβοι που παραμένουν στην κατάσταση μόλυνσης πάνω από χρόνο δ επανακάμπτουν, το οποίο μεταφράζεται ως $r(t) = j(t-\delta)$, για χρονικό διάστημα μεγαλύτερο του δ, έχουμε:

$$\lim_{\varepsilon\to 0}\frac{dj(\delta+\varepsilon)}{dt} - \frac{dj(\delta-\varepsilon)}{dt} = -\lambda j(0)\left[1-j(\delta)\right] \tag{8}$$

Από αυτή τη σχέση μπορούν να μελετηθούν αρκετές διαφορετικές λύσεις στη μόνιμη κατάσταση (δηλαδή για $t\to\infty$), να προκύψουν αντίστοιχες τιμές για το επιδημιολογικό κατώφλι $j_c(0)$ και να κατανοηθεί η μέση συμπεριφορά του υπο-μελέτη συστήματος. Με τον όρο μέση συμπεριφορά εννοείται η λειτουργία που εμφανίζει το δίκτυο συνολικά στη διάρκεια μιας επίθεσης, όπως προκύπτει από τη μελέτη των αναμενόμενων τιμών των μεγεθών που μελετώνται. Η ορθότητα του

μοντέλου δοκιμάστηκε με επιτυχία μέσω προσομοιώσεων για ασύρματα κινητά αυτοργανούμενα δίκτυα που ακολουθούν το μοντέλο κινητικότητας τυχαίων προορισμών (Random Waypoint) [43], το πρωτόκολλο δρομολόγησης AODV [44] και το πρωτόκολλο πρόσβασης στο μέσο 802.11 (CSMA/CA DCF) [45], ενώ προέκυψε ότι υπό προϋποθέσεις οι μέθοδοι καταπολέμησης της διάδοσης αναφορικά με το χρησιμοποιούμενο μοντέλο είχαν το αντίθετο αποτέλεσμα.

Μια διαφορετική προσέγγιση επιτυγχάνει να ενσωματώσει στην ανάλυση μεγαλύτερο πλήθος των ιδιαίτερων χαρακτηριστικών των αυτοργανούμενων (ad hoc) δικτύων [46]. Κατασκευάζεται ένας κατευθυνόμενος τυχαίος γεωμετρικός γράφος με βάση μια σταθερή ακτίνα μετάδοσης (που εξαρτάται από την ισχύ εκπομπής, το θόρυβο υποβάθρου και την ευαισθησία του δέκτη) και καθορίζονται οι σχέσεις γειτονίας μεταξύ των κόμβων δικτύου. Επομένως, η κατανομή του βαθμού κόμβου είναι διωνυμική και συνεπώς το μέγιστό της επιτυγχάνεται στη μέση τιμή της. Η πρόσβαση στο μέσο γίνεται με βάση το πρωτόκολλο 802.11. Κόμβοι που μολύνονται θεωρούνται ότι ανακάμπτουν μετά από κάποιο χρονικό διάστημα ανοσοποιημένοι, έτσι ώστε να μην υπάρχει περίπτωση να μολυνθούν ξανά. Η δρομολόγηση γίνεται ακολουθώντας πολλαπλά βήματα, έτσι ώστε ένας κόμβος να μπορεί να κατευθύνει τις απειλές του όχι μόνο σε γειτονικούς, αλλά και πιο απομακρυσμένους μη-μολυσμένους κόμβους. Η μελέτη του συστήματος έγινε με προσομοιώσεις Monte-Carlo [47], για διάφορες τιμές της πυκνότητας κόμβων και ακτίνας μετάδοσης. Όπως στην περίπτωση των ενσύρματων δικτύων, ένα επιδημικό κατώφλι λ_c εμφανίστηκε σε σχέση με την τιμή λ/μ, όπου μ είναι ο ρυθμός ανοσοποίησης των μολυσμένων κόμβων, το οποίο όμως αυξάνεται με την εισαγωγή του μηχανισμού 802.11, σε σχέση με δίκτυα που δεν τον χρησιμοποιούν. Το επιδημικό κατώφλι έχει τη μορφή $\lambda_c = \frac{\kappa_c}{\langle k \rangle} = \frac{\kappa_c}{\pi(N/L^2)r^2}$, όπου L^2 είναι η επιφάνεια του δικτύου (υποθέτοντας τετραγωνική μορφή με πλευρά L) και r η ακτίνα μετάδοσης των κόμβων. Ο λόγος της αύξησης που παρουσιάζει το επιδημικό κατώφλι είναι οι τοπικές εξαρτήσεις που εμφανίζονται σε αυτά τα δίκτυα (τυχαίοι γεωμετρικοί γράφοι) και επηρεάζουν το ρυθμό αναπαραγωγής μολύνσεων και το μέσο αριθμό νέων μολύνσεων κατ' επέκταση. Ο μηχανισμός πρόσβασης 802.11 εισάγει επιπρόσθετες χρονικές καθυστερήσεις και εξαρτήσεις, με αποτέλεσμα το επιδημικό κατώφλι να αυξάνεται. Αντίθετα, για αυξανόμενη πυκνότητα δικτύου, το επιδημικό κατώφλι μειώνεται,

δηλαδή η διάδοση καθίσταται ευκολότερη για δίκτυα με περισσότερους κόμβους ανά μονάδα επιφανείας και επομένως με περισσότερους γείτονες για κάθε κόμβο τοπικά. Πιο ενδιαφέροντα είναι τα αποτελέσματα για τη δυναμική της διάδοσης. Πιο συγκεκριμένα, η αρχική αύξηση της διασποράς είναι σημαντικά πιο αργή της εκθετικής που παρατηρείται στην περίπτωση ενσύρματων δικτύων, αποκλειστικά λόγω της επίδρασης της τοπολογίας, η οποία περιορίζει (εξαιτίας παρεμβολών) την επίδοση των γειτονικών μολυσμένων κόμβων (μεταξύ τους ανταγωνισμός για την πρόσβαση στο μέσο).

2.3 Στοχαστικά Μοντέλα Διάδοσης

Αν και τα επιδημιολογικά μοντέλα επιβεβαιώνονται πολύ καλά από τις μετρήσεις που έγιναν σε πραγματικές επιθέσεις, αποτελούν ντετερμινιστικά εργαλεία συνεχούς χρόνου, τα οποία μπορούν να χρησιμοποιηθούν για την ανάλυση μιας επίθεσης αφού αυτή έχει ολοκληρωθεί και είναι εφικτό να εξαχθούν οι ρυθμοί μόλυνσης και ανάκαμψης των κόμβων του δικτύου. Η χρησιμότητα τους περιορίζεται στις περιπτώσεις όπου μια επίθεση επαναλαμβάνεται, οπότε είναι δυνατόν να αναγνωρισθεί στα πρώτα στάδιά της και να χρησιμοποιηθούν τα συμπεράσματα που έχουν προκύψει.

Στον αντίποδα, μοντέλα στοχαστικής φύσεως, τα οποία δεν εξαρτώνται από το χρόνο ή τον λαμβάνουν υπόψη στη ανάλυση έμμεσα, μπορούν να εφαρμοστούν κατά τη διάρκεια της επίθεσης και επομένως καθίστανται πιο ελκυστικά για σύγχρονα απαιτητικά συστήματα. Για το σκοπό αυτό αναπτύχθηκαν μέθοδοι που βασίζονται σε στοχαστικές μεθόδους και κυριότερα σε στοχαστικές διαδικασίες.

Πιο χαρακτηριστική προσέγγιση αποτελεί το μοντέλο Αναλυτικής Διάδοσης Ιών Τύπου Worm (Analytical Active Worm Propagation – AAWP) που προτάθηκε για ενεργό κακόβουλο λογισμικό που εκτελεί τυχαίες σαρώσεις διευθύνσεων μηχανημάτων IP σε ενσύρματα τοπικά δίκτυα και το Διαδίκτυο [48]. Σε αυτή την περίπτωση οποιοσδήποτε κόμβος του δικτύου μπορεί να μολυνθεί, ανεξάρτητα από την απόσταση σε βήματα συνδέσεων του υποκείμενου γράφου δικτύου. Κάτι τέτοιο καθιστά το μοντέλο καταλληλότερο για δίκτυα εφαρμογών ή ενσύρματα που αναπαρίστανται με πλήρεις γράφους (όλοι οι κόμβοι συνδέονται με όλους). Θεωρώντας λοιπόν μια δεδομένη χρονική στιγμή, m_i επιρρεπείς κόμβους (συμπεριλαμβανομένων των μολυσμένων) και n_i μολυσμένους εντός του δικτύου με

ρυθμό σάρωσης s, στην επόμενη χρονική στιγμή, $(m_i - n_i)\left[1-\left(1-\frac{1}{2^{32}}\right)^{sn_i}\right]$ κόμβοι θα μολυνθούν κατα μέσο όρο (επειδή οι δυνατές διευθύνσεις σε ένα δίκτυο, άρα και οι δυνατοί στόχοι στην περίπτωση χρήσης πρωτοκόλλου διευθυνσιοδότησης IPv4 είναι 2^{32}, $\frac{1}{2^{32}}$ είναι η πιθανότητα να επιλεχθεί ένας συγκεκριμένος κόμβος για επίθεση). Ο αριθμός των μολυσμένων κόμβων την επόμενη χρονική στιγμή προκύπτει:

$$n_{i+1} = (1-d-p)n_i + \left[(1-p)^i N - n_i\right]\left[1-\left(1-\frac{1}{2^{32}}\right)^{sn_i}\right] \quad (9)$$

όπου p είναι ο ρυθμός ανοσοποίησης των κόμβων και d ο ρυθμός ανάκαμψης (χωρίς ανοσοποίηση), N ο αριθμός των κόμβων που μπορεί να μολυνθούν και $n_0 = h$ ο αριθμός των μολυσμένων κόμβων στην αρχή της διάδοσης κακόβουλου λογισμικού. Η διαφορά σε σχέση με τα κλασικά επιδημιολογικά μοντέλα είναι ότι πλέον το σύστημα είναι διακριτού χρόνου, λαμβάνονται υπόψη οι χρόνοι μόλυνσης, ο ρυθμός ανοσοποίησης και η περίπτωση μόλυνσης του ίδιου κόμβου την ίδια στιγμή από διαφορετικές πηγές. Κατά συνέπεια το συγκεκριμένο μοντέλο εμφανίζεται πληρέστερο και πιο κοντά στην πραγματική λειτουργία διάδοσης κακόβουλου λογισμικού για τα ενσύρματα δίκτυα για τα οποία είναι κατάλληλο. Συγκρίσεις μέσω προσομοιώσεων με επιδημιολογικά μοντέλα όπως τα παραπάνω, δείχνουν ότι το μοντέλο Αναλυτικής Διάδοσης Ιών Τύπου Worm δίνει πιο ρεαλιστικά αποτελέσματα. Μεταξύ άλλων, προβλέπει το μη-αναμενόμενο αποτέλεσμα κατά το οποίο τμήματα λογισμικού τύπου worm με μεγάλη λίστα σάρωσης διευθύνσεων (άρα περισσότερους εν δυνάμει στόχους) μπορούν να ανιχνευθούν ευκολότερα, παρόλο που διαδίδονται γρηγορότερα.

Η ανίχνευση τέτοιων απειλών είναι εξίσου σημαντική και μπορεί να γίνει παρατηρώντας παθητικά τη ροή της κίνησης σε ένα τοπικό δίκτυο και εφαρμόζοντας μεθόδους από τη θεωρία ανίχνευσης–εκτίμησης σημάτων [49]. Σε αυτή την περίπτωση θεωρείται το βασικό επιδημιολογικό μοντέλο με κόμβους που μολύνονται και δεν ανακάμπτουν. Πάνω σε αυτό το μοντέλο δημιουργείται ένα στοχαστικό μοντέλο διαδικασιών σημείων (Point Processes, [50]) για τους χρόνους που τα κακόβουλα τμήματα λογισμικού σαρώνουν το χώρο διευθύνσεων για νέα θύματα και

το αντίστοιχο αποτέλεσμα (επιτυχία–αποτυχία) κάθε σάρωσης–επίθεσης. Οι συγκεκριμένες διαδικασίες σημείων αφορούν στο χρόνο, αλλα θα μπορούσαν να χρησιμοποιηθούν εξίσου μέθοδοι χωρικών διαδικασιών σημείων σε μία διάσταση (one dimensional spatial point processes). Θεωρώντας ένα συγκεκριμένο ποσοστό κίνησης υποβάθρου στο τοπικό δίκτυο εν είδη θορύβου υποβάθρου (ανεπιθύμητη κίνηση σάρωσης στο υποδίκτυο που δεν οφείλεται όμως στο κακόβουλο λογισμικό) μπορεί να δημιουργηθεί το διατεταγμένο σύνολο των χρόνων σάρωσης στο υποδίκτυο $\{t_1, t_2, t_3, ...\}$ που αποτελεί το σύνολο των παρατηρήσεων. Θεωρώντας επίσης $\{d_1, d_2, d_3, ...\}$ τους δείκτες των διευθύνσεων μηχανημάτων που επισκέπτεται το κακόβουλο λογισμικό σε ένα στιγμιότυπο σάρωσης, τότε αν $p(t)$ είναι ο αριθμός των σαρώσεων που έχουν λάβει χώρα μέχρι χρόνο t και $i(p)$ ο αριθμός των μολυσμένων μηχανημάτων για $p(t)$ συνολικές σαρώσεις, τότε:

$$i(p) = n_s - (n_s - i_0)e^{-\frac{p}{n}} \tag{10}$$

Χρησιμοποιώντας το αποτέλεσμα της (10), μπορεί να υπολογιστεί τόσο η ακολουθία χρονικών στιγμών $\{t_1, t_2, t_3, ...\}$, όσο και το $p(t)$:

$$\begin{aligned} t(p) &= \frac{n}{\beta n_s}\left[\frac{p}{n} + \ln\left(\frac{\beta\left(n_s - (n_s - i_0)e^{-\frac{p}{n}}\right)}{\beta i_0}\right)\right] \\ p(t) &= \beta n_s t + n\ln\left[\frac{i_0 + (n_s - i_0)e^{-\frac{p}{n}}}{n_s}\right] \end{aligned} \tag{11}$$

Με βάση αυτές τις παρατηρήσεις, ορίζεται ένα πρόβλημα εξέτασης υπόθεσης (hypothesis testing), στο οποίο η απόφαση που εξετάζεται είναι αν το σύνολο των παρατηρήσεων οφείλεται σε κακόβουλο λογισμικό και κίνηση υποβάθρου (υπόθεση H_1) ή μόνο σε κίνηση υποβάθρου (υπόθεση H_0). Υιοθετώντας μεθόδους ακολουθιακής ανάλυσης (sequential analysis) και πιο συγκεκριμένα ακολουθιακή εξέταση πιθανότητας αναλογίας (sequential probability ratio test, SPRT [51]) μπορεί να ληφθούν αποφάσεις για την ανίχνευση κακόβουλου λογισμικού με χρήση συγκεντρωτικών αθροισμάτων (cumulative sum – CUSUM [52]) επί των

παρατηρήσεων. Οι αποφάσεις λαμβάνονται συναρτήσει παραμέτρων όπως ο χρόνος διακοπής (stopping time – αριθμός παρατηρήσεων που χρησιμοποιούνται για την εξέταση υπόθεσης) και το μέσο πλήθος παρατηρήσεων (average run length – ARL) για την επίτευξη συγκεκριμένου σφάλματος στην εξέταση υπόθεσης. Από την ανάλυση της μεθόδου συνάγεται το ήδη γνωστό συμπέρασμα από τη μέθοδο Αναλυτικής Διάδοσης Ιών Τύπου Worm ότι όσο πιο επιθετικό είναι το κακόβουλο λογισμικό, τόσο ευκολότερο είναι να ανιχνευθεί.

Άλλες μέθοδοι στηρίζονται στα ιδιαίτερα χαρακτηριστικά που παρουσιάζει η διάδοση κακόβουλου λογισμικού τύπου worm, όπως είναι η σταθερή εκθετική αύξηση του ρυθμού διάδοσης απειλών στα πρώτα στάδια για τα ενσύρματα δίκτυα και το Διαδίκτυο. Υποθέτωντας ότι οι κόμβοι που μολύνονται δεν ανακάμπτουν και δυνητικά όλοι οι νόμιμοι κόμβοι είναι ευάλωτοι σε επιθέσεις από μολυσματικούς κόμβους (πλήρης γράφος συστήματος), η διάδοση του λογισμικού χωρίζεται σε τρεις φάσεις, στο στάδιο της αργής εκκίνησης, τη φάση γρήγορης διάδοσης και το τελικό στάδιο αργού τερματισμού [53]. Η προτεινόμενη μέθοδος ανίχνευσης (στοχαστικής φύσης) επικεντρώνει στην πρώτη φάση διάδοσης, υιοθετώντας τη διακριτή έκφραση του επιδημιολογικού μοντέλου για τη φάση αυτή. Το διακριτό επιδημιολογικό μοντέλο έχει λύση $\mathrm{I}_{\mathrm{t}} = \left(1 + a\Delta\right)\mathrm{I}_{\mathrm{t-1}}$, όπου I_t είναι ο αριθμός των μολυσμένων κόμβων στη χρονική στιγμή t, $a = \lambda N$ είναι ο πραγματικός ρυθμός μόλυνσης και Δ είναι το στοιχειώδες χρονικό διάστημα μεταξύ παρατηρήσεων του συστήματος. Η κατάλληλη επιλογή του Δ είναι σημαντική για την αποδοτική λειτουργία της μεθόδου σε πρακτικά συστήματα. Η λύση αυτή αναφέρεται ως εκθετική–αυτοπαλινδρομική (exponential–autoregressive) λύση του επιδημιολογικού μοντέλου, υποδηλώνοντας ταυτόχρονα ιδιότητες που συνεπάγεται για τη συμπεριφορά του μεγέθους που μελετάται. Εναλλακτικά, εφαρμόζοντας τη συνάρτηση λογαρίθμου και στα δύο μέλη της λύσης, μπορεί να χρησιμοποιηθεί ένα μετασχηματισμένο μοντέλο, το οποίο αναφέρεται ως μετασχηματισμένο γραμμικό μοντέλο, $\mathrm{I}_{\mathrm{t}} = \left(1 + a\Delta\right)\mathrm{I}_{\mathrm{t-1}} - \beta\Delta I_{t-1}^2$ και λόγω του λογαρίθμου εξομαλύνει τη μεταβλητότητα του αριθμού των μολυσμένων κόμβων, διευκολύνοντας την παρατήρησή του. Για την υλοποίηση της μεθόδου χρησιμοποιείται ένα σύστημα παρατήρησης με δρομολογητές στα άκρα τοπικών δικτύων, για τη συγκέντρωση δεδομένων σε κάθε χρονική στιγμή, όπως ο αριθμός των σαρώσεων που πραγματοποιήθηκαν, ο συνολικός αριθμός μολυσμένων κόμβων, η κατανομή σάρωσης και ο ρυθμός σάρωσης. Το σύστημα βασίζεται σε κατώφλια,

δίνοντας κατάλληλα σήματα όταν αυτά ξεπεραστούν από την παρατηρούμενη κίνηση. Έτσι μπορεί να εκτιμηθεί ο παρατηρούμενος αριθμός των μολυσμένων κόμβων, ο οποίος δεν είναι αναγκαστικά ανάλογος του I_t. Χρησιμοποιώντας φίλτρα Kalman [54], μπορεί να γίνει αποδοτικά η ανίχνευση λογισμικού worm στην αρχική φάση της διάδοσης. Επίσης μπορεί να εκτιμηθεί το μέγεθος του πληθυσμού που κινδυνεύει περισσότερο. Ουσιαστικά, με την παραπάνω μέθοδο, ανιχνεύεται η τάση που ακολουθεί η μέθοδος και όχι το ξέσπασμα της διάδοσης.

2.4 Μοντέλα Διάδοσης Markov

Παρόλο που οι στοχαστικές μέθοδοι παρέχουν μεγαλύτερη γενικότητα και εφαρμογή σε σχέση με τα αμιγώς επιδημιολογικά μοντέλα, βασίζονται κυρίως σε παρατηρήσεις της κίνησης που ρέει στο εκάστοτε δίκτυο. Ταυτόχρονα η διάδοση κακόβουλου λογισμικού παρουσιάζει μεν στοχαστική συμπεριφορά, αλλά εμφανίζει και συσχετίσεις μεταξύ γειτονικών καταστάσεων. Τέτοιες συσχετίσεις μπορούν να μοντελοποιηθούν καλύτερα με στοχαστικές διαδικασίες Markov, όπως φαίνεται στα μοντέλα που ακολουθούν.

Η πιο άμεση επέκταση είναι ένα στοχαστικό επιδημιολογικό μοντέλο με διαδικασίες Markov [55]. Θεωρώντας ένα μοντέλο μόλυνσης όπου οι κόμβοι δεν μπορούν να ανακάμψουν μετά από τις μολύνσεις που δέχονται, το ζεύγος $\{s(t), i(t)\} = \{s, i\}$ των μη-μολυσμένων και μολυσμένων κόμβων αντίστοιχα μπορεί να θεωρηθεί ως κατάσταση του συστήματος. Για το θεωρούμενο μοντέλο μόλυνσης – ανάκαμψης κόμβων, η κατάσταση $(0, N)$ είναι απορροφητική (absorbing), με την έννοια ότι όταν το σύστημα μεταβεί σε αυτή δεν την εγκαταλείπει ποτέ, όπως θα συνέβαινε στην πραγκατικότητα όταν μολύνονταν όλοι οι κόμβοι του δικτύου. Θεωρώντας ένα μοντέλο Markov συνεχούς χρόνου για το σύστημα, ο ρυθμός μετάβασης από την κατάσταση (s, i) στην $(s-1, i+1)$ είναι ίσος με $\frac{\lambda}{N} s(t) i(t)$. Αυτή η στοχαστική διαδικασία μπορεί να μοντελοποιηθεί σαν μια διαδικασία αλμάτων–Markov εξαρτώμενη από την πυκνότητα των γεγονότων (density–dependent Markov jump process) με ρυθμό μετάβασης μεταξύ διαδοχικών καταστάσεων:

$$q_{(s_a,i_a)(s_b,i_b)} = \begin{cases} \frac{\lambda}{N} s_a i_a & (s_b = s_a - 1) \wedge (i_b = i_a + 1) \\ 0 & \delta\iota\alpha\phi. \end{cases} \quad (12)$$

Οι τιμές των μεγεθών των πληθυσμών στο στοχαστικό μοντέλο (στη στάσιμη κατάσταση) τείνουν στις τιμές που προβλέπεται από το ντετερμινιστικό μοντέλο και τελικά οι μεταβολές είναι ασυμπτωτικά τύπου Gauss. Ο χρόνος παραμονής στην κατάσταση (s_j, i_j) του συστήματος είναι εκθετικά κατανεμημένος με μέση τιμή $\frac{N}{\lambda(n_s - i_j)i_j}$ και μεταβλητότητα $\left(\frac{N}{\lambda(n_s - i_j)i_j}\right)^2$ με $i(t) + s(t) = n_s \le N$. Ο χρόνος μετάβασης από μια κατάσταση σε μια άλλη μη-γειτονική μπορεί επίσης να υπολογιστεί ως $T_{i_a i_b} = \sum_{i_j = i_a}^{i_b - 1} T_{ij}$, ο οποίος δεν είναι υποχρεωτικά εκθετικός. Κατ' επέκταση μπορεί να υπολογιστεί:

$$E\left[T_{1\frac{n_s}{2}}\right] = \frac{N}{\lambda n_s}\left[C + \ln(n_s - 1) + f(n)\right] \to \frac{N}{\lambda n_s}\ln(n_s - 1) \quad (13)$$

με $C \neq 0$ σταθερά, $f(n) \in O(1/n)$ και η τιμή που συγκλίνει το όριο να είναι τελικά αυτή που προβλέπεται από το ντετερμιστικό επιδημικό μοντέλο.

Με βάση αυτό το στοχαστικό μοντέλο μπορεί να δημιουργηθεί ένα υβριδικό που βασίζεται στο ντετερμινιστικό απλό επιδημικό μοντέλο για την περιγραφή της μακροσκοπικής διάδοσης, ενώ οι χρόνοι σάρωσης παράγονται στοχαστικά [55]. Χρησιμοποιώντας την τυχαία μεταβλητή που περιγράφει το συνολικό αριθμό μολύνσεων που έχουν γίνει στο δίκτυο μέχρι μια χρονική στιγμή στη διαφορική επιδημιολογική εξίσωση, μπορεί να εξαχθεί αναλυτικά ο χρόνος που συμβαίνει η κάθε σάρωση και μέσω αυτού η σειρά των χρόνων σάρωσης από το κακόβουλο λογισμικό και επομένως η πλήρης εξέλιξη της διάδοσης. Θεωρώντας $p(t)$ το συνολικό αριθμό προσπαθειών μόλυνσης που έχουν λάβει χώρα μέχρι και το χρονικό στιγμιότυπο t του συστήματος, τότε $\frac{dp}{dt} = \beta i$ (όπου β ο ρυθμός σάρωσης μηχανημάτων). Συνδυάζοντας με το ντετερμινιστικό επιδημιολογικό μοντέλο $\frac{di}{dt} = \frac{\beta}{n} si$ (i είναι ο αριθμός μολυσμένων κόμβων, s ο αριθμός εκείνων που

μπορούν να μολυνθούν και n ο συνολικός αριθμός κόμβων δικτύου), προκύπτει το στοχαστικό επιδημιολογικό μοντέλο:

$$\frac{dt}{dp} = \frac{1}{\beta\left[n_s - (n_s - i_0)e^{-p/n} \right]} \tag{14}$$

με λύση:

$$t(p) = \frac{n}{\beta n_s}\left[\frac{p}{n} + \log\left(\frac{n_s - (n_s - i_0)e^{-p/n}}{i_0} \right) \right] \tag{15}$$

όπου n_s είναι ο δυνατός αριθμός μηχανημάτων που μπορούν να μολυνθούν και i_0 ο αριθμός των αρχικά μολυσμένων κόμβων.

Αντίστοιχες προσπάθειες που επικεντρώνονται στη διάδοση κακόβουλου λογισμικού στο Διαδίκτυο χρησιμοποιούν αλληλεπιδρώμενες αλυσίδες Markov (Interactive Markov Chains – IMCs) [56]. Κάθε κόμβος μεταβαίνει στις επιτρεπτές καταστάσεις του με βάση μια εσωτερική διαδικασία Markov, ωστόσο οι ρυθμοί μετάδοσης εξαρτώνται και από τις καταστάσεις των γειτονικών κόμβων. Το συνολικό σύστημα εξελίσσεται με βάση μια γενική αλυσίδα Markov με χώρο καταστάσεων το γινόμενο των καταστάσεων των επιμέρους κόμβων. Ένα προσεγγιστικό μοντέλο (αναφέρεται γενικά ως μοντέλο επίδρασης – influence model) χρησιμοποιείται για την ανάλυση της σύνθετης αλυσίδας του αρχικού ακριβούς μοντέλου. Το μοντέλο επίδρασης είναι μια διαδικασία Markov διακριτού χρόνου, το οποίο περιγράφει την εξέλιξη του συστήματος μέσω του διανύσματος καταστάσεων κάθε κόμβου και του πίνακα μεταβάσεων. Οι μεταβάσεις έχουν σταθμιστεί με μια παράμετρο βάρους που αντιστοιχεί στο ποσοστό επίδρασης που ασκεί ο κάθε ένας κόμβος στους άλλους (πόσο επηρεάζει δηλαδή την κατάστασή τους και άρα τις αντίστοιχες μεταβάσεις). Στα βάρη αυτά μπορούν εν δυνάμει να ενσωματωθούν τα τοπολογικά χαρακτηριστικά των δικτύων που μελετώνται. Οι μη-μολυσμένοι κόμβοι δεν ανακάμπτουν όταν μολυνθούν, ενώ γίνεται και η θεώρηση αρχικά ανοσοποιημένων κόμβων που δεν μολύνονται καθόλου. Για το μοντέλο επίδρασης οι κόμβοι επηρεάζονται από τους γειτονικούς μόνο αν βρίσκονται στην κατάσταση μη-μόλυνσης. Η εξέλιξη της κατάστασης ενός κόμβου περιγράφεται από το σύστημα εξισώσεων:

$$
\begin{aligned}
P_{I_j}[k+1] &= P_{I_j}[k] + \sum_{i=1}^{N} w_{i,j} c_j P_{I_i S_j}[k] \\
P_{M_j}[k+1] &= P_{M_j}[k] + \sum_{i=1}^{N} w_{i,j} (1-c_j) P_{I_i S_j}[k] \\
P_{S_j}[k+1] &= 1 - P_{I_j}[k+1] - P_{M_j}[k+1]
\end{aligned}
\tag{16}
$$

όπου $w_{i,j}$ είναι τα βάρη του μοντέλου επίδρασης, c_j η πιθανότητα ένας κόμβος να μολυνθεί από την αλληλεπίδραση με ένα άλλο, P_{S_j}, P_{I_j} και P_{M_j} οι πιθανότητες να υπάρχουν τη δεδομένη χρονική στιγμή j μη-μολυσμένοι, μολυσμένοι και ανοσοποιημένοι κόμβοι αντίστοιχα. Το πρόβλημα της εύρεσης του τελικού αριθμού μολυσμένων κόμβων ανάγεται σε ένα πρόβλημα συνεχούς διήθησης (continuum percolation problem), το οποίο παρουσιάζει φαινόμενα κατωφλίου σε σχέση με την πιθανότητα c_j (επιδημικό κατώφλι) και υπολογίζεται ο αριθμός των τελικά μολυσμένων κόμβων για την περίπτωση δικτύων τύπου μικρόκοσμου (small-scale networks). Το προτεινόμενο μοντέλο μπορεί να χρησιμοποιηθεί και για την ανάλυση της μεταβατικής συμπεριφοράς της διάδοσης.

Η επίδραση της τοπολογίας είναι πολύ σημαντική για τη διάδοση κακόβουλου λογισμικού για κάθε τύπο δικτύου [57]. Για την αντίστοιχη μελέτη υποτίθεται ότι οι μη-μολυσμένοι κόμβοι που μολύνονται, ανακάμπτουν και επιστρέφουν στην αρχική τους κατάσταση. Η κατάσταση του συστήματος περιγράφεται από ένα δυαδικό διάνυσμα που αντιπροσωπεύει την κατάσταση κάθε κόμβου. Οι σχέσεις γειτονίας μεταξύ των κόμβων δίνονται από τον πίνακα γειτονίας $\underline{A}$. Υποθέτοντας ότι ένας κόμβος μπορεί να μολυνθεί από ένα γείτονά του με ρυθμό λ και ανακάμπτει με ρυθμό μ, το σύστημα μπορεί να περιγραφεί από μια διαδικασία Markov που διαθέτει μια απορροφητική κατάσταση, η οποία αργά ή γρήγορα θα επιτευχθεί. Ο χρόνος μετάβασης σε αυτή την κατάσταση είναι πολύ σημαντικός και αποδεικνύεται ότι όταν $\rho(\underline{A}) < \frac{\mu}{\lambda}$ ($\rho(\underline{A})$ είναι το μέγιστο ιδιοδιάνυσμα του $\underline{A}$), τότε ο μέσος χρόνος ζωής του διαδιδόμενου κακόβουλου λογισμικού κλιμακώνεται φθίνοντας ασυμπτωτικά ως $E[\tau] = O(\log N)$. Αντίθετα, όταν ο λόγος $\frac{\mu}{\lambda}$ είναι μικρότερος από μια γενίκευση του ισοπεριμετρικού αριθμού του γράφου δικτύου, τότε $E[\tau] = \Omega\left(e^{N^a}\right), a > 0$ και το λογισμικό παραμένει για αρκετό χρόνο ενεργό στο δίκτυο (εκθετικό σε σχέση με τον

αριθμό των κόμβων). Αναγκαίες συνθήκες σε κλειστή αναλυτική μορφή έχουν αναπτυχθεί στο [57] για διάφορα μοντέλα γράφων όπως οι αστέρες, οι υπερ-κύβοι, οι πλήρεις γράφοι, οι τυχαίοι γράφοι και οι γράφοι νόμων δύναμης (εκθετική κατανομή βαθμού κόμβου). Από τη σχετική μελέτη προέκυψε ότι στην περίπτωση γράφων τύπου αστέρα και νόμου δύναμης, αφενός οι συνθήκες και τα όρια της συμπεριφοράς της διάδοσης που υπολογίστηκαν δεν είναι ακριβή (tight), αφετέρου η διάδοση είναι ευαίσθητη στον αρχικό αριθμό μολυσμένων κόμβων.

Σε επέκταση του μοντέλου που προτάθηκε στο [57], στα [58],[59] αναπτύσσεται ένα προσεγγιστικό μοντέλο του ακριβούς μοντέλου Markov με 2^N καταστάσεις, το οποίο βασίζεται στη θεωρία μέσου πεδίου (mean field theory) και προτείνει ένα μοντέλο N-αμοιβαίως σχετιζόμενων αλυσίδων Markov (N-intertwined Markov chains). Το τελευταίο σχετίζει παράμετρους της τοπολογίας δικτύου (μέγιστο ιδιοδιάνυσμα πίνακα γειτονίας και βαθμό κόμβου) στη διαδικασία της διασποράς κακόβουλου λογισμικού, μέσω της σχέσης:

$$\tau_c = \frac{1}{\lambda_{\max}(\underline{A})} \tag{17}$$

όπου τ_c είναι το επιδημικό κατώφλι και $\lambda_{\max}(\underline{A})$ το μεγαλύτερο ιδιοδιάνυσμα του πίνακα γειτονίας $\underline{A}$. Συγκρίνοντας την επίδραση της προσέγγισης με το ακριβές σύστημα Markov με 2^N καταστάσεις, διαπιστώνεται η ακρίβεια του προσεγγιστικού μοντέλου και τίθενται τα όρια εφαρμογής του σε πραγματικά δίκτυα, κυρίως ενσύρματα. Μεταξύ των συμπερασμάτων που μπορεί να ληφθούν, πέρα από το γεγονός ότι το μέγιστο ιδιοδιάνυσμα ελέγχει την εξέλιξη της διασποράς μέσω της (17), είναι το γεγονός ότι για κανονικούς γράφους (regular graphs) το μοντέλο N-αμοιβαίως σχετιζόμενων αλυσίδων Markov καταλήγει στο βασικό επιδημιολογικό μοντέλο με μερικές απλοποιήσεις. Παράλληλα, με βάση τη σχέση (17) μελετήθηκε ο χρόνος εξαφάνισης κακόβουλου λογισμικού για δίκτυα γραμμών και πλέγματος (line/mesh networks).

Κεφάλαιο 3

Μοντέλο Διάδοσης Κακόβουλου Λογισμικού

3.1 Καθορισμός Προβλήματος – Μοντέλο Συστήματος

Όπως προαναφέρθηκε, η παρούσα εργασία εστιάζει στη μελέτη της διάδοσης κακόβουλου λογισμικού σε ασύρματα δίκτυα τα οποία δεν διαθέτουν αυστηρά καθορισμένη τοπολογία ή κεντρική υποδομή. Πιο συγκεκριμένα, θεωρούμε ένα ασύρματο αυτοργανούμενο δίκτυο τύπου ad hoc ή δίκτυο αισθητήρων χωρίς κεντρική υποδομή, στο οποίο όλοι οι κόμβοι είναι ισότιμοι (peers) αναφορικά με τις δικτυακές λειτουργίες (δρομολόγηση, πρόσβαση στο μέσο, αποστολή/λήψη πακέτων).

Όλες οι προσεγγίσεις μοντελοποίησης, ανάλυσης και χρησιμοποίησης αποτελεσμάτων για τη διάδοση κακόβουλου λογισμικού σε ποικίλα δίκτυα υπολογιστών που παρουσιάστηκαν νωρίτερα είχαν κύριο αντικειμενικό σκοπό την ανίχνευση των απειλών που κυκλοφορούσαν στο δίκτυο. Δεν έγινε κάποια προσπάθεια μελέτης των ίδιων των απειλών, προκειμένου να διαπιστωθούν τα ιδιαίτερα χαρακτηριστικά τους σε σχέση με τις παραμέτρους του δικτύου και επομένως να σχεδιασθούν καλύτερα αποδοτικά αντίμετρα. Στην παρούσα εργασία, αρχικά προτείνουμε ένα νέο πλαίσιο μοντελοποίησης της διάδοσης, το οποίο μπορεί με γενικό τρόπο να περιγράψει τη διάδοση διαφόρων απειλών σε διαφορετικούς τύπους δικτύων και στη συνέχεια μελετάμε γενικές κατηγορίες έξυπνων μεθόδων επίθεσης σε ασύρματα δίκτυα, προκειμένου να γίνει αντιληπτό το μέγεθος της επίδρασής τους στο δίκτυο και οι παράγοντες που την ελέγχουν.

Το δίκτυο περιλαμβάνει N ασύρματους κόμβους, ο καθένας με ακτίνα διάδοσης R. Επίσης θεωρούμε την ύπαρξη επιπρόσθετων $M \leq N$ κακόβουλων χρηστών, ο καθένας από τους οποίους έχει ακτίνα μετάδοσης r. Οι κακόβουλοι χρήστες έχουν τη δυνατότητα να μεταβάλλουν αν χρειαστεί/θέλουν την ακτίνα εκπομπής τους, έμμεσα μεταβάλλοντας την ισχύ εκπομπής τους και κατά συνέπεια τη γειτονιά τους, με χρήση κατάλληλων αλγορίθμων Ελέγχου Τοπολογίας (Topology Control, TC) [60]. Ο Έλεγχος Τοπολογίας αποτελεί ένα μηχανισμό συμβιβασμού μεταξύ της προσφερόμενης ισχυρής συνδετικότητας δικτύου που εξασφαλίζεται με

μεγάλη ισχύ εκπομπής (και αντίστοιχη υψηλή κατανάλωση ενέργειας) και εξοικονόμησης ενεργειακών πόρων με χαμηλά επίπεδα παρεμβολής που συνοδεύουν τις χαμηλότερες ακτίνες μετάδοσης. Κατά βάση αποτελεί μια διαστρωματική τεχνική ελέγχου της υποκείμενης τοπολογίας δικτύου, όπου το στρώμα Ελέγχου Πρόσβασης στο Μέσο (MAC) αλληλεπιδρά με το στρώμα Δικτύου (Network) και αντίστροφα. Οι κακόβουλοι χρήστες μπορούν να εκμεταλλευτούν τις δυνατότητες που προσφέρει ο Έλεγχος Τοπολογίας, ώστε να αυξήσουν την αποδοτικότητα της διασποράς κακόβουλου λογισμικού χρησιμοποιώντας τα ιδιαίτερα χαρακτηριστικά που παρουσιάζουν τα αυτοργανούμενα δίκτυα.

Το κανάλι μετάδοσης θεωρείται ντετερμινιστικό και μόνο απώλειες διάδοσης λαμβάνονται υπόψη. Έτσι η λαμβανόμενη ισχύς από ένα κόμβο εξαρτάται μόνο από την απόσταση του δεδομένου κόμβου από τον εκπομπό και τη σταθερά απωλειών διάδοσης του μέσου α. Κατα συνέπεια, από τη σκοπιά του μοντέλου δικτύου, δύο κόμβοι θεωρούνται γείτονες όταν ο ένας βρίσκεται εντός της ακτίνας μετάδοσης του άλλου και το ανάποδο. Αν και αυτή η αντιστοίχιση φαίνεται αρκετά απότομη ως φυσική διαδικασία και όχι τόσο ρεαλιστική, είναι αρκετά δυνατή σχετικά με τη μοντελοποίηση της γειτονιάς ενός ασύρματου αυτοργανούμενου δικτύου [61]. Έχει χρησιμοποιηθεί κατά κόρον στη βιβλιογραφία και η επέκτασή της είναι άμεση ώστε να λαμβάνονται υπόψη κανάλια μεταβλητής φύσεως. Ακόμα και τότε η περιοχή κάλυψης του κάθε ασύρματου κόμβου μπορεί να θεωρηθεί κυκλική, με μια ακτίνα μετάδοσης κατάλληλα προσαρμοσμένη (η αρχική ακτίνα μετάδοσης πολλαπλασιάζεται με ένα διορθωτικό παράγοντα) ώστε να αντιστοιχεί κατά μέσο όρο, όσο γίνεται καλύτερα σε ένα πραγματικό σύστημα [62].

Οι κακόβουλοι κόμβοι έχουν τη δυνατότητα να κινούνται στην περιοχή δικτύου, η οποία θεωρείται επίπεδη και τετραγωνικής μορφής με πλευρά L. Θεωρούμε ότι οι κινούμενοι κακόβουλοι χρήστες ακολουθούν το μοντέλο κινητικότητας τυχαίου περίπατου με αναδίπλωση στην περίπτωση που φτάσουν στα όρια της περιοχής δικτύου (random walk with wrapping) [43]. Αντίθετα, οι νόμιμοι χρήστες του δικτύου θεωρούνται ακίνητοι. Εναλλακτικά, θα μπορούσαν να θεωρηθούν ότι κινούνται και αυτοί ακολουθώντας το ίδιο μοντέλο κινητικότητας με τους κακόβουλους, αλλά προκειμένου να μπορέσουμε να απομονώσουμε την επίδραση των επιτιθέμενων και να διαπιστωθεί η συμβολή της κινητικότητας των κακόβουλων στη διάδοση κακόβουλου λογισμικού θεωρούμε στατικό δίκτυο για τους

νόμιμους κόμβους. Επιπλέον η στατικότητα των νόμιμων κόμβων δεν επηρεάζει τη γενικότητα της ανάλυσης. Πιο συγκεκριμένα, η αρχική τοποθέτηση και των δύο ομάδων κόμβων γίνεται με τυχαίο και ομοιόμορφα κατανεμημένο τρόπο στην περιοχή δικτύου. Το μοντέλο κινητικότητας τυχαίου περίπατου με αναδίπλωση που θεωρήθηκε παραπάνω, εξασφαλίζει ότι στη μόνιμη κατάσταση, η χωρική κατανομή των κόμβων στην περιοχή δικτύου είναι ομοιόμορφη [43]. Επομένως, αν η αρχική τοποθέτηση των κόμβων του δικτύου είναι τυχαία και ομοιόμορφα κατανεμημένη, τότε μακροσκοπικά και κατά μέσο όρο, δεν υπάρχει διαφορά είτε οι κόμβοι του δικτύου κινούνται, είτε είναι στατικοί.

Αναφορικά με τη συμπεριφορά των κόμβων στις επιθέσεις μπορει κανείς να διακρίνει δύο γενικές περιπτώσεις. Οι κόμβοι που μολύνονται, επηρεάζονται μόνο τοπικά, παραμένουν ουσιαστικά ανεξάρτητοι και δεν μεταδίδουν σε γειτονικούς κόμβους το κακόβουλο λογισμικό που λαμβάνουν. Τα δίκτυα αυτής της κατηγορίας αναφέρονται ως δίκτυα μη-διασποράς (non-propagative). Στη δεύτερη περίπτωση οι κόμβοι που μολύνονται καταλαμβάνονται μερικώς ή ολικώς από τους αρχικούς παραγωγούς κακόβουλου λογισμικού και αρχίζουν να διαδίδουν με τη σειρά τους απειλές στους γειτονικούς ή και πιο απομακρυσμένους γείτονες. Σε αυτές τις περιπτώσεις τα δίκτυα χαρακτηρίζονται ως δίκτυα διασποράς κακόβουλου λογισμικού (propagative networks).

Στην παρούσα εργασία θα μελετηθούν και οι δύο κατηγορίες δικτύων καθώς υπό το πρίσμα των ασύρματων δικτύων χωρίς κεντρική υποδομή, κάθε μια περίπτωση δικτύου διάδοσης κακόβουλου λογισμικού αντιστοιχεί σε διαφορετικό περιβάλλον εφαρμογής. Ειδικότερα, η πρώτη κατηγορία μοντέλων δικτύων (δίκτυα μη-διασποράς) περιγράφει με ακρίβεια τις περιπτώσεις δικτύων αισθητήρων, όπου υπάρχουν άφθονοι κόμβοι, κάθε ένας όμως είναι περιορισμένων υπολογιστικών δυνατοτήτων και αντίστοιχης φύσεως πρέπει να είναι το κακόβουλο λογισμικό που δέχονται/κυκλοφορεί στο δίκτυο. Επομένως και οι κακόβουλοι χρήστες δεν χρειάζεται να έχουν περισσότερη υπολογιστική πολυπλοκότητα, αφού μπορούν με το πλήθος τους (και το αντίστοιχο χαμηλό κόστος) να καλύψουν συνολικά τις μειωμένες υπολογιστικές δυνατότητες. Έτσι σε ένα δίκτυο μη-διασποράς παρόλο που οι κόμβοι μπορεί να μολυνθούν δεν μεταδίδουν παραπέρα τις μολύνσεις που δέχονται. Αντίθετα, η κατηγορία των δικτύων διασποράς είναι καταλληλότερη για την περιγραφή αυτοργανούμενων δικτύων τύπου ad hoc, όπου ο κάθε κόμβος έχει

περισσότερες υπολογιστικές δυνατότητες (πρακτικά όσες και ενός σταθερού προσωπικού υπολογιστή), δίνοντας ταυτόχρονα τη δυνατότητα στους επιτιθέμενους να βρούν περισσότερες αδυναμίες και επομένως να χρησιμοποιήσουν τους κόμβους που μολύνουν προς όφελός τους.

Με βάση τα μοντέλα που ακολουθούνται για την ασύρματη μετάδοση και κινητικότητα κόμβων, το ασύρματο δίκτυο που μελετάται μπορεί να αναπαρασταθεί με ένα τυχαίο γεωμετρικό γράφο (random geometric graph, [63]), είτε πρόκειται για δίκτυο τύπου ad hoc, είτε για δίκτυο αισθητήρων. Ένα τέτοιο μοντέλο τοπολογίας αποτελεί μια ενδιάμεση λύση μεταξύ εντελώς τυχαίων τοπολογιών οι οποίες συνήθως απαντώνται στα δίκτυα υπέρθεσης (overlay networks) που περιγράφονται με ακρίβεια από τυχαίους γράφους (random graphs, [64]) και δίκτυα που δημιουργούνται με βάση διάφορες συσχετίσεις και περιορισμούς μεταξύ των κόμβων τους (ντετερμινιστικοί γράφοι). Ένας τυχαίος γεωμετρικός γράφος, περιγράφει με ακρίβεια την τυχαιότητα θέσης των κόμβων λόγω της κίνησης τους, την τυχαιότητα στη δημιουργία συνδέσεων λόγω του μεταβαλλόμενου ασύρματου καναλιού, αλλά και τη συσχέτιση που προκύπτει από τις γεωμετρικές αποστάσεις και το θεωρούμενο συνεχές μοντέλο διάδοσης κυμάτων μεταξύ γειτονικών κόμβων. Δηλαδή περιγράφει με ακρίβεια το συνδυασμό γεωμετρικής πληροφορίας (τοποθεσία) με την τυχαιότητα του ασύρματου μέσου μετάδοσης.

Κάθε νόμιμος κόμβος μπορεί να είναι σε μία από δύο δυνατές καταστάσεις ανά πάσα χρονική στιγμή, την κατάσταση μη-μόλυνσης (susceptible) και μόλυνσης (infected) αντίστοιχα. Η επιτρεπτή αλληλουχία καταστάσεων κάθε νόμιμου κόμβου είναι καθοριστική για τη συμπεριφορά του δικτύου συνολικά και την τελική έκβαση μιας οργανωμένης επίθεσης. Χωρίς βλάβη της γενικότητας μπορούμε να θεωρήσουμε ότι οι κόμβοι του δικτύου ξεκινούν στην κατάσταση μη-μόλυνσης (susceptible). Εάν ένας κόμβος μολυνθεί περνά στην κατάσταση μόλυνσης (infected). Στη συνέχεια, αν υπάρχει η δυνατότητα ο κόμβος να ακολουθήσει ένα σύνολο ενεργειών ώστε να απομακρύνει το κακόβουλο λογισμικό, μπορεί να επιστρέψει στην αρχική κατάσταση μη-μόλυνσης (susceptible). Στη συνέχεια θα ακολουθηθεί η ίδια διαδικασία, είτε επειδή ο κόμβος δεν παίρνει κάποια μέτρα για να προστατευθεί, είτε γιατί νέες απειλές εμφανίζονται και δεν είναι δυνατόν να αντιμετωπιστούν εν τη γενέση τους. Σε αυτό το μοντέλο κόμβου η αλληλουχία καταστάσεων είναι susceptible – infected – susceptible (SIS) και το μοντέλο αναφέρεται ως SIS-μοντέλο μόλυνσης κόμβων [65].

Υπάρχουν βέβαια και περιπτώσεις νόμιμων κόμβων που όταν μολυνθούν από κακόβουλο λογισμικό δεν μπορούν να ανακάμψουν στην αρχική μη-μολυσμένη κατάσταση. Ο κόμβος είτε παύει εντελώς να λειτουργεί ή συνεχίζει να λειτουργεί και να είναι μολυσμένος. Ανάλογα με τη φύση των επιθέσεων και την εκάστοτε μελέτη ο κόμβος που μολύνεται και δεν επανακάμπτει ουσιαστικά είναι σαν να διαγράφεται από το δίκτυο. Τότε η διαδοχή των καταστάσεων κάθε κόμβου δικτύου δίνεται από την αλληλουχία susceptible – infected – removed (SIR), όπου η τελευταία κατάσταση υποδηλώνει ότι ο κόμβος πρακτικά ή ουσιαστικά έχει απομακρυνθεί από το δίκτυο και άρα δεν λογαριάζεται στην υπόλοιπη κατάσταση του δικτύου. Το μοντέλο αυτό αναφέρεται ως SIR-μοντέλο μόλυνσης κόμβων [65]. Για την περίπτωση που ο κόμβος μολύνεται και δεν διαγράφεται (δεν απομακρύνεται από το δίκτυο) η αλληλουχία των καταστάσεων θα είναι susceptible – infected (SI). Σε αυτές τις περιπτώσεις ο κόμβος παραμένει μολυσμένος στο δίκτυο και ανάλογα με τον τύπο δικτύου αναφορικά με τη διασπορά κακόβουλου λογισμικού (διασποράς ή μη-διασποράς), δεν θα κάνει τίποτα (οπότε είναι σαν το δίκτυο να είναι τύπου SIR), ή θα μολύνει γειτονικούς του κόμβους, επομένως αργά ή γρήγορα το δίκτυο συνολικά θα μεταβεί σε μια πανδημική κατάσταση όπου όλοι οι κόμβοι θα είναι μολυσμένοι.

Οι δύο παραπάνω παράμετροι μοντέλου για το είδος και τη συμπεριφορά των (ασύρματων) νόμιμων κόμβων του δικτύου μπορούν να χρησιμοποιηθούν για τον πλήρη χαρακτηρισμό ενός δικτύου που δέχεται επίθεση. Έτσι σε ένα δίκτυο διασποράς SIS (propagative SIS) οι κόμβοι ακολουθούν πολλαπλούς κύκλους μολύνσεων–ανακάμψεων και ταυτόχρονα μπορούν να διασκορπίζουν παραπέρα το κακόβουλο λογισμικό που λαμβάνουν. Αντίθετα, σε ένα δίκτυο μη-διασποράς SIS (non-propagative SIS), οι κόμβοι ακολουθούν την ίδια συμπεριφορά με το πρώτο με τη διαφορά ότι δεν μεταδίδουν παραπέρα το λογισμικό που λαμβάνουν. Το ίδιο ισχύει και για τα SIR δίκτυα. Για παράδειγμα, σε ένα δίκτυο διασποράς SIR (propagative SIR) ένας κόμβος που μολύνεται, διασκορπίζει με τη σειρά του κακόβουλο λογισμικό σε γειτονικούς κόμβους μέχρι τελικά για κάποιο λόγο να απομακρυνθεί από το δίκτυο ή να πάψει να λειτουργεί (κατάσταση Removed). Παρόμοια σε ένα δίκτυο μη-διασποράς SIR (non-propagative SIR), οι κόμβοι μολύνονται και περιμένουν μέχρι να απομακρυνθούν, χωρίς ωστόσο να συμμετέχουν παραπέρα στη διάδοση κακόβουλου λογισμικού.

Στην παρούσα εργασία επικεντρωνόμαστε σε δίκτυα τύπου SIS προκειμένου να μελετήσουμε τη μακροσκοπική και πιο γενική συμπεριφορά του δικτύου, όπου κάθε κόμβος δύναται να μολύνεται και να επανακάμπτει στην αρχική του κατάσταση ανάλογα με τις διαφορετικές επιθέσεις (ιοί, worms, trojan horses, spyware, rootkits) που κυκλοφορούν στο δίκτυο. Κάτι τέτοιο αντιστοιχεί στη γενικότερη περίπτωση διάδοσης και μελέτης του δικτύου σε βάθος χρόνου, όπως συμβαίνει στη διάρκεια ζωής ενός μηχανήματος, το οποίο αναμένεται να δεχθεί επιθέσεις όλων των τύπων και εντάσεων. Επίσης, υποθέτουμε τόσο δίκτυα διασποράς, όσο και μη-διασποράς, ώστε να καλύψουμε τις περιπτώσεις αυτοργανούμενων ad hoc και δικτύων αισθητήρων, δηλαδή τους δύο κύριους τύπους ασύρματων δικτύων πολλαπλών βημάτων χωρίς κεντρική δομή. Παρόμοια δίκτυα όπως τα αυτοκινητιστικά (vehicular) και τα δίκτυα πλέγματος (grid) μπορούν επίσης να υπαχθούν στη μία ή την άλλη κατηγορία, ανάλογα με τη συγκεκριμένη εφαρμογή που καλούνται να εξυπηρετήσουν. Τα SIR δίκτυα είναι καταλληλότερα για τη μελέτη μεμονωμένων απειλών ή ενός πεπερασμένου συνόλου απειλών, αντιστοιχώντας στη μελέτη ενός δικτύου σε μια περιορισμένη χρονική περίοδο, κάτι το οποίο ξεφεύγει από το στόχο της συγκεκριμένης εργασίας.

Σκοπός της παρούσας διατριβής και του προτεινόμενου μοντέλου είναι, μεταξύ άλλων, η εισαγωγή ενός γενικού πλαισίου, ανεξάρτητου από το είδος και τον τύπο του δικτύου, το οποίο να μπορεί να χρησιμοποιηθεί εύκολα και με ακρίβεια για τη μελέτη και την ανάλυση της συμπεριφοράς της διάδοσης κακόβουλου λογισμικού σε δίκτυα υπολογιστών οποιουδήποτε τύπου. Στόχος δεν είναι η μελέτη μιας συγκεκριμένης απειλής, τη στιγμή μάλιστα που υπάρχουν αρκετές επιτυχημένες μέθοδοι που μελετούν μεμονωμένους τύπους κακόβουλου λογισμικού που έκαναν την εμφάνισή τους στο παρελθόν. Αντίθετα, η απουσία γενικού πλαισίου για τη μελέτη της συνολικής συμπεριφοράς των απειλούμενων δικτύων σε βάθος χρόνου και ανεξαρτήτως τύπου επιθέσεων, καθιστά αναγκαία τη γενικευμένη μελέτη τέτοιων προβλημάτων. Σε αυτήν την κατεύθυνση επικεντρώνεται η παρούσα μελέτη.

Για την αξιολόγηση της προτεινόμενης μεθόδου και για να φανεί πιο εύληπτα η δυναμική που έχει ένα τέτοιο γενικότερο πλαίσιο μοντελοποίησης, εξειδικεύουμε την ανάλυση για την περίπτωση ασύρματων δικτύων πολλαπλών βημάτων, όπως τα αυτοργανούμενα δίκτυα τύπου ad hoc και τα δίκτυα αισθητήρων. Παράλληλα, δίνεται μια εκτίμηση για το μέγεθος της ζημιάς που θα μπορούσε να γίνει σε αυτά τα δίκτυα

(παρατηρώντας τα δίκτυα μακροσκοπικά) στην περίπτωση που η συχνότητα των επιθέσεων γινόταν παρόμοια με τα ενσύρματα (κάτι που αναμένεται στα επόμενα χρόνια, δεδομένης της αύξησης της διείσδυσης ασύρματων δικτύων στην αγορά).

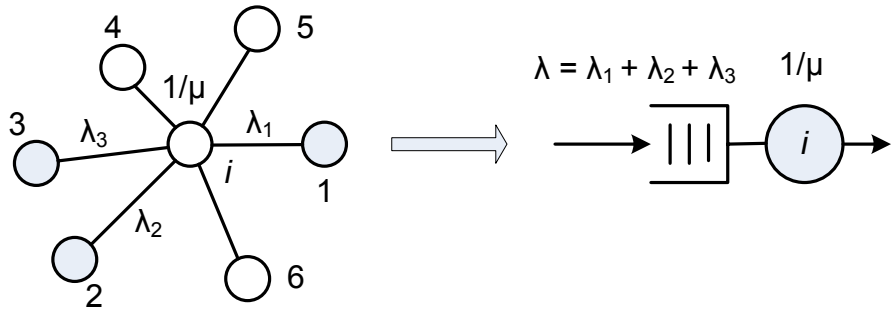
Ταυτόχρονα ένα τέτοιο πλαίσιο δίνει τη δυνατότητα για τη μελέτη έξυπνων στρατηγικών επίθεσης από τη μεριά των κακόβουλων χρηστών, προκειμένου να οριοθετηθούν οι συνέπειες που έχουν τέτοιες επιθέσεις, ώστε να ληφθούν υπόψη κατά τη σχεδίαση αποδοτικών αντίμετρων. Όπως θα διαφανεί από την ακόλουθη μελέτη και το προτεινόμενο πλαίσιο, ακολουθείται μια πιθανοκρατική φιλοσοφία προκειμένου το πρόβλημα να μελετηθεί συνολικά και στη μέγιστη δυνατή γενικότητά του, λαμβάνοντας υπόψη απροσδιόριστους παράγοντες, όπως η συμπεριφορά των κακόβουλων χρηστών, οι τυχαίες θέσεις των κινητών κόμβων και οι σχέσεις γειτονίας που προκύπτουν μεταξύ τους.

3.2 Αναμονητικό Μοντέλο Διάδοσης Κακόβουλου Λογισμικού

Το κύριο χαρακτηριστικό στη διάδοση κακόβουλου λογισμικού, όπως παρουσιάστηκε μέχρι τώρα, είναι το γεγονός ότι ένας ασύρματος (ή ενσύρματος) κόμβος που βρίσκεται στην κανονική του κατάσταση (susceptible) μολύνεται κάποια χρονική στιγμή, περνώντας στην κατάσταση όπου προσπαθεί να ανακάμψει από την επίθεση που δέχεται (infected). Τόσο η πρώτη διαδικασία της μόλυνσης, όσο και η δεύτερη της ανάκαμψης εμπεριέχουν το στοιχείο της αναμονής, η πρώτη για την άφιξη μιας μόλυνσης και η δεύτερη για την ολοκλήρωση της διαδικασίας καθαρισμού του κόμβου. Μάλιστα στη γενική περίπτωση αυτές οι διαδικασίες αναμονής είναι μη-ελεγχόμενες και καθορίζονται από ένα τυχαίο συνδυασμό παραγόντων που έχουν να κάνουν τόσο με τα ιδιαίτερα χαρακτηριστικά του μέσου μετάδοσης, όσο και με τη συμπεριφορά των κακόβουλων κόμβων. Συνεπώς το σύστημα συνολικά αποκτά στοχαστική και αναμονητική συμπεριφορά.

Η παραπάνω παρατήρηση μας οδηγεί στην αντιστοίχιση ενός κόμβου δικτύου με τις ασύρματες συνδέσεις του σε μια ουρά αναμονής με ένα εξυπηρετητή. Έχοντας πολλαπλές ασύρματες συνδέσεις με γειτονικούς κόμβους, ένας χρήστης μπορεί να δεχθεί πολλαπλές επιθέσεις ανάλογα με την κατάσταση (susceptible/infected) των γειτόνων του. Η ουρά αντιπροσωπεύει τις διαφορετικές επιθέσεις που μπορεί να πλήξουν τον κόμβο, ταυτόχρονα ή σε διαφορετικές χρονικές στιγμές και μπορούν να συνυπάρχουν μέχρι ο χρήστης να αντιληφθεί την παρουσία τους στο μηχάνημά του

και να ακολουθήσει τις αναγκαίες ενέργειες για την αντιμετώπιση των μολύνσεων. Ο κόμβος καθαυτός αντιστοιχίζεται στον εξυπηρετητή της ουράς, ο οποίος στην προκείμενη περίπτωση απασχολείται όταν ο χρήστης θέσει σε λειτουργία τους μηχανισμούς αντιμετώπισης, επιχειρώντας να απομακρύνει ένα ή περισσότερα στοιχεία του κακόβουλου λογισμικού. Το περιγραφόμενο αναμονητικό μοντέλο βασίζεται στην παραδοχή ενός SIS μοντέλου μολύνσεων δικτύου. Οι κόμβοι ξεκινούν στην κατάσταση μη-μόλυνσης (άδεια ουρά, άεργος εξυπηρετητής), μολύνονται από μία ή περισσότερες επιθέσεις (ενεργός εξυπηρετητής και άδεια ή κατειλημμένη ουρά αντίστοιχα) και επανέρχονται στην αρχική κατάσταση μη-μόλυνσης όταν δεν υπάρχουν αφίξεις, αδειάσει η ουρά και τελειώσει ο εξυπηρετητής. Η εξυπηρέτηση (διαδικασία ανάκαμψης) μπορεί θεωρητικά να κρατήσει άπειρο χρόνο, αυτό όμως συμβαίνει με μικρή πιθανότητα (που καθορίζεται από τη στοχαστική διαδικασία εξυπηρέτησης της θεωρούμενης ουράς).



Σχήμα 1 – Αντιστοίχιση κόμβου δικτύου και κακόβουλων γειτόνων σε ουρά M/M/1

Στην παρούσα μελέτη, ως πρώτο στάδιο μελέτης και αξιολόγησης του προτεινόμενου μοντέλου διάδοσης κακόβουλου λογισμικού για ένα κόμβο και ακολουθώντας ανάλογες πρακτικές της βιβλιογραφίας [56], υποθέτουμε ότι η διαδικασία άφιξης κακόβουλου λογισμικού (αριθμός διαφορετικών τμημάτων κακόβουλου λογισμικού που λαμβάνεται) σε ένα κόμβο από κάθε μια ασύρματη σύνδεση με ένα γειτονικό μολυσμένο κόμβο είναι Poisson κατανεμημένη και άρα οι ενδιάμεσοι χρόνοι μεταξύ διαδοχικών αφίξεων κακόβουλου λογισμικού είναι εκθετικά κατανεμημένοι με παράμετρο λ_k για τη σύνδεση k. Επομένως η συνολική διαδικασία άφιξης στην ουρά αποτελεί υπέρθεση πολλαπλών διαδικασιών Poisson (ανάλογα με τον αριθμό των συνδέσεων που έχει ο κόμβος i με μολυσμένους γείτονες) και άρα πρόκειται για μια νέα διαδικασία Poisson με ρυθμό το άθροισμα των επιμέρους ρυθμών $\lambda_i = \sum_k \lambda_k$. Αντίστοιχα, θεωρούμε ότι διαδοχικές

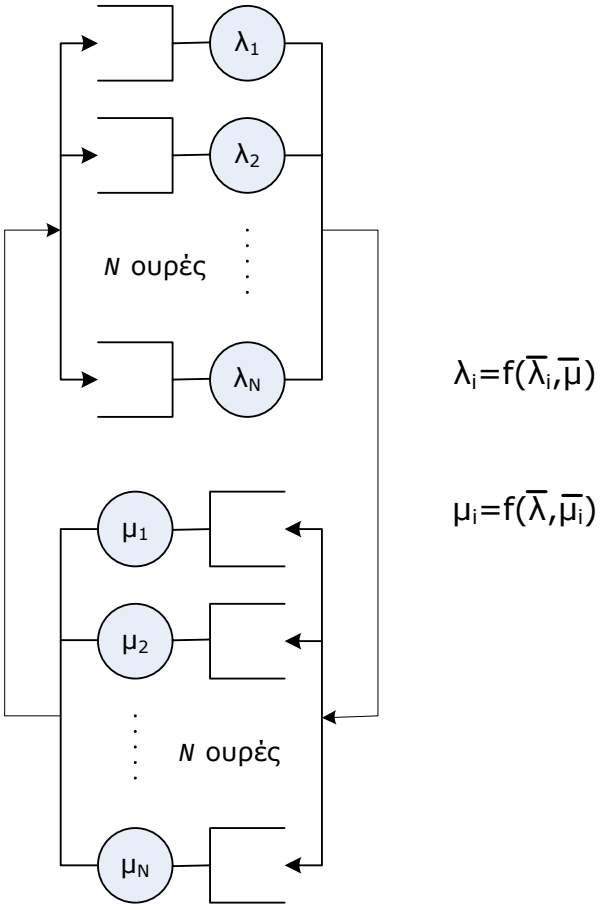
εξυπηρετήσεις (χρόνος αντιμετώπισης διαφορετικών τύπων κακόβουλου λογισμικού) είναι εκθετικά κατανεμημένες με ρυθμό μ_i για τον κόμβο i. Με βάση αυτές τις παραδοχές, ο κάθε κόμβος με τις συνδέσεις του, αντιστοιχίζεται σε μια ουρά M/M/1, όπως φαίνεται στο Σχήμα 1. Στο εικονιζόμενο στιγμιότυπο, ο κόμβος i έχει στη γειτονιά του τρεις κακόβουλους γείτονες $\{1,2,3\}$. Σε κάθε ζεύξη με καθένα από αυτούς, λαμβάνει κακόβουλο λογισμικό με ρυθμό λ_k, $k \in \{1,2,3\}$. Ο ρυθμός ανάκαμψης λαμβάνεται ως $1/\mu$. Ο κόμβος i αντιστοιχίζεται σε μια ουρά αναμονής M/M/1 με συνολικό ρυθμό μόλυνσης $\lambda = \lambda_1 + \lambda_2 + \lambda_3$ και τον ίδιο ρυθμό ανάκαμψης $1/\mu$.

Το μοντέλο ουράς M/M/1 για ένα κόμβο και τους μολυσμένους γείτονές του, μπορεί να επεκταθεί και να χρησιμοποιηθεί για την περιγραφή της συμπεριφοράς όλων των κόμβων του δικτύου. Σε κάθε στιγμιότυπο της εξέλιξης της κατάστασης του δικτύου, οι νόμιμοι κόμβοι του μπορούν να διαχωριστούν σε δύο ομάδες, τους μολυσμένους και αυτούς που είναι στην κατάσταση μη-μόλυνσης. Μπορούμε λοιπόν να θεωρήσουμε αντίστοιχα δύο ομάδες ουρών, κάθε μια από τις οποίες περιέχει τόσες ουρές αναμονής, όσοι οι κανονικοί κόμβοι του δικτύου. Η μία ομάδα αναπαριστά τους κόμβους που είναι μολυσμένοι, ενώ η δεύτερη τους κόμβους που δεν είναι, όπως φαίνεται στο Σχήμα 2. Επειδή ένας συγκεκριμένος κόμβος μπορεί να είναι μόνο σε μια ομάδα κάθε χρονική στιγμή, ενεργή μπορεί να είναι μόνο η ουρά που αντιστοιχεί στον κόμβο στη συγκεκριμένη ομάδα. Έτσι για ένα κόμβο που είναι μολυσμένος, μόνο η αντίστοιχη ουρά του στην ομάδα των μολυσμένων είναι ενεργή (ο εξυπηρετητής είναι ενεργός), ενώ η αντίστοιχη στην ομάδα των μη-μολυσμένων κόμβων είναι ανενεργή (άδεια ουρά, ανενεργός εξυπηρετητής).

Το μοντέλο κλειστών ουρών στο Σχήμα 2 είναι από τη φύση του αρκετά σύνθετο και η ανάλυσή του καθίσταται πολύπλοκη, αν όχι αδύνατη. Υποθέτοντας $\overline{\lambda} = \left(\lambda_1\ \lambda_2 \ldots \lambda_N\right)^{\mathrm{T}}$ το διάνυσμα των ρυθμών μόλυνσης των κόμβων του δικτύου και $\overline{\lambda}_i = \left(\lambda_1\ \lambda_2 \ldots \lambda_{i-1}\ \lambda_{i+1} \ldots \lambda_N\right)^{\mathrm{T}}$ το διάνυσμα των ρυθμών μόλυνσης των κόμβων του δικτύου εκτός του ρυθμού μόλυνσης του κόμβου *i*, και αντίστοιχα $\overline{\mu} = \left(\mu_1\ \mu_2 \ldots \mu_N\right)^{\mathrm{T}}$ το διάνυσμα των ρυθμών ανάκαμψης των κόμβων και $\overline{\mu}_i = \left(\mu_1\ \mu_2 \ldots \mu_{i-1}\ \mu_{i+1} \ldots \mu_N\right)^{\mathrm{T}}$ το διάνυσμα των ρυθμών ανάκαμψης των κόμβων εκτός του ρυθμού του κόμβου *i*, ο

κάθε ένας από αυτούς τους ρυθμούς εξαρτάται και από όλους τους άλλους ρυθμούς, έτσι ώστε $\forall i \in \{1,2,\ldots,N\}$:

$$\begin{aligned} \lambda_i &= f\left(\overline{\lambda}_i, \overline{\mu}\right) \\ \mu_i &= f\left(\overline{\lambda}, \overline{\mu}_i\right) \end{aligned} \tag{18}$$



Σχήμα 2 – Κλειστό μοντέλο ουρών αναμονής για το συνολικό δίκτυο

Παρόλα αυτά, το μοντέλο κλειστών ουρών στο Σχήμα 2 περιλαμβάνει τη μέγιστη δυνατή λεπτομέρεια για την περιγραφή της συμπεριφοράς του δικτύου (π.χ. κατάσταση κάθε κόμβου σε κάθε χρονική στιγμή, ρυθμοί αλλαγής καταστάσεων). Για την ανάλυσή του και προκειμένου να εξαχθούν χρηστικά συμπεράσματα, μπορεί να χρησιμοποιηθεί μια μέθοδος απλοποίησης του μοντέλου, θυσιάζοντας ταυτόχρονα, ένα μέρος της αρχικά προσφερόμενης περιγραφικής λεπτομέρειας.

Ειδικότερα, εφαρμόζοντας το θεώρημα Norton από την θεωρία κυκλωμάτων (δυαδικό του θεωρήματος Thevenin) μπορούμε να συμπτύξουμε τις ουρές κάθε

επιμέρους ομάδας σε μια ουρά με ισοδύναμο ρυθμό εξυπηρέτησης, θεωρώντας κάθε ουρά ως στοιχείο κυκλώματος και τις συνδέσεις μεταξύ ουρών ως καλωδιώσεις [66]. Η προσέγγιση του ισοδύναμου Norton επιτρέπει την παραμετρική μελέτη σύνθετων δικτύων ουρών που ικανοποιούν συγκεκριμένες συνθήκες. Η διαδικασία της σύμπτυξης περιλαμβάνει τη 'βραχυκύκλωση' ενός υποσυστήματος ουρών (όπως στη θεωρία κυκλωμάτων ένα κομμάτι κυκλώματος βραχυκυκλώνεται μεταξύ δύο ακροδεκτών) και τον υπολογισμό του συνολικού ρυθμού εξυπηρέτησης, της ρυθμαπόδοσης του βραχυκυκλωμένου υποσυστήματος ή άλλων μεγεθών που ενδιαφέρουν. Η μέθοδος της βραχυκύκλωσης μπορεί να εφαρμοστεί μόνο σε κλειστά δίκτυα ουρών 'τύπου γινομένου', το οποίο ισχύει για το εν λόγω θεωρούμενο σύστημα, όπως θα φανεί από τις λεπτομέρειες της ανάλυσης και τις αντίστοιχες εργοδικές πιθανότητες καταστάσεων [66],[67].

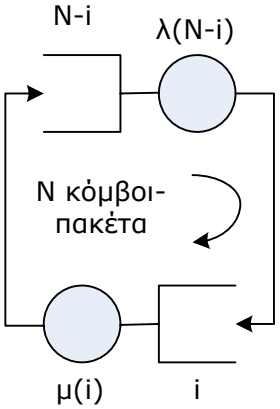
Για το σύστημα παράλληλων ουρών M/M/1, το ισοδύναμο Norton αποτελείται από δύο ουρές αναμονής σε εν σειρά σύνδεση, έτσι ώστε η έξοδος της μίας να αποτελεί είσοδο της άλλης. Η κάθε ομάδα παράλληλων ουρών αντικαθίσταται από μια ουρά με ισοδύναμο ρυθμό εξυπηρέτησης. Πλέον αυτές οι ουρές δεν αντιστοιχίζονται σε συγκεκριμένους κόμβους, αλλά οι κόμβοι του δικτύου αντιστοιχούν στα πακέτα που κυκλοφορούν στο κλειστό δίκτυο των δύο ουρών. Να σημειωθεί σε αυτό το σημείο ότι στη συνέχεια της ανάλυσης και χωρίς βλάβη της γενικότητας θεωρούμε ότι οι ουρές επεξεργάζονται πακέτα δικτύων τηλεπικοινωνιών και αναφερόμαστε σε πακέτα και κόμβους του δικτύου που υπόκεινται σε επίθεση εξίσου.

Όπως στο αρχικό μοντέλο υπήρχαν δύο ομάδες παράλληλων ουρών, στο ισοδύναμο Norton υπάρχουν δύο ουρές, μία για τους μολυσμένους και μια για τους μη-μολυσμένους. Κάθε ένας κόμβος ξεκινά από την ουρά μη-μολυσμένων και όταν δεχθεί μια επιτυχημένη επίθεση, μεταβαίνει στην ουρά των μολυσμένων, αναμένοντας για όσο χρόνο αντιστοιχεί η διαδικασία ανάκαμψης που ακολουθεί. Μόλις ολοκληρωθεί η αναμονή/εξυπηρέτηση στην ουρά των μολυσμένων, ο κόμβος μεταβαίνει στην ουρά των μη-μολυσμένων, όπου αναμένει την επόμενη επιτυχημένη επίθεση, εκκινώντας έτσι ένα νέο κύκλο. Η ανακύκλωση ανάμεσα στις δύο ουρές συμβαίνει για όλους τους κόμβους και με τυχαίο τρόπο, ανάλογα με τις θεωρούμενες συνθήκες δικτύου και τη συμπεριφορά των κακόβουλων και νόμιμων μολυσμένων κόμβων.

Ειδικότερα για την περίπτωση της θεώρησης ουρών M/M/1, με τις αντίστοιχες εκθετικές εξυπηρετήσεις, η σύμπτυξη των παράλληλων ουρών είναι εύκολη και γίνεται με την άθροιση των επιμέρους ρυθμών εξυπηρέτησης κάθε ουράς (ιδιότητα ελαχίστου πολλαπλών εκθετικών κατανομών), όπως προκύπτει και από την εφαρμογή του θεωρήματος Norton για παράλληλα συνδεδεμένα στοιχεία δικτύου. Η επίλυση του ισοδύναμου Norton μπορεί να γίνει με τυπικές μεθόδους ανάλυσης συστημάτων γεννήσεων–θανάτων και μαρκοβιανών αλυσίδων για την επίτευξη αναλυτικών εκφράσεων για τα μεγέθη που ενδιαφέρουν. Οι λεπτομέρειες της επίλυσης εξαρτώνται από το θεωρούμενο σύστημα (διασποράς/μη-διασποράς) και τις τοπολογικές ιδιότητές του. Στη συνέχεια παρατίθενται οι αναλύσεις για τις δύο θεωρούμενες περιπτώσεις δικτύων διάδοσης κακόβουλου λογισμικού.

3.3 Επίλυση Παρουσία Πολλαπλών Κακόβουλων Κόμβων σε Περιβάλλον Δικτύων Μη-Διασποράς

Αρχικά θεωρείται η περίπτωση ενός δικτύου μη-διασποράς (non-propagative), στο οποίο οι επιθέσεις που δέχεται ένας νόμιμος κόμβος δεν μεταδίδονται από αυτόν σε γειτονικούς κόμβους του ασύρματου δικτύου. Επομένως, μόνο κακόβουλοι χρήστες μπορούν να μολύνουν άλλους νόμιμους κόμβους. Όπως αναφέρθηκε, μια τέτοια θεώρηση περιγράφει καλύτερα την περίπτωση ενός δικτύου αισθητήρων, όπου συνυπάρχουν N κόμβοι δικτύου και $M \leq N$ κακόβουλοι κόμβοι.



Σχήμα 3 – Ισοδύναμο Norton για δίκτυο μη-διασποράς με πολλαπλούς κακόβουλους χρήστες

Το ισοδύναμο Norton μοντέλο όπως περιγράφηκε παραπάνω φαίνεται στο Σχήμα 3 και αναφέρεται στο δίκτυο που σχηματίζουν οι νόμιμοι κόμβοι του δικτύου. Θεωρώντας ότι η κάτω ουρά του σχήματος αποτελεί την ουρά των μολυσμένων

κόμβων, εάν υπάρχουν i κόμβοι σε αυτή σε μια χρονική στιγμή, θα υπάρχουν $N-i$ κόμβοι στην ουρά των μη-μολυσμένων κόμβων (πάνω ουρά). Οι ρυθμοί εξυπηρέτησης της εκάστοτε ουράς εξαρτώνται από τον αριθμό των κόμβων–πελατών στην αναμονή. Χωρίς βλάβη της γενικότητας εστιάζουμε στην ουρά των μολυσμένων κόμβων. Η κατάστασή της περιγράφει τον αριθμό των κόμβων δικτύου που είναι μολυσμένοι στο δεδομένο στιγμιότυπο του συστήματος. Λόγω των θεωρήσεων των εκθετικών κατανομών η κατάσταση αυτής της ουράς μπορεί να περιγραφεί από μια αλυσίδα γεννήσεων–θανάτων που διαθέτει μοναδική εργοδική κατανομή πιθανοτήτων [66],[67],[68]. Η ανάλυση της ουράς με εξισώσεις ισορροπίας καταστάσεων δίνει την αναδρομική έκφραση των εργοδικών πιθανοτήτων καταστάσεων του συστήματος:

$$\pi(i) = \pi(0) \cdot \prod_{j=1}^{i} \frac{\lambda(N-i+j)}{\mu(j)} \tag{19}$$

όπου $\pi(0)$ είναι η πιθανότητα το σύστημα να βρίσκεται στην κατάσταση όπου δεν υπάρχουν μολυσμένοι κόμβοι στο σύστημα. Εφαρμόζοντας τη συνθήκη κανονικοποίησης $\sum_{i=1}^{N} \pi(i) = 1$, η έκφραση (19) γίνεται:

$$\pi(0) \cdot \sum_{i=0}^{N} \prod_{j=1}^{i} \frac{\lambda(N-i+j)}{\mu(j)} = 1 \tag{20}$$

Υποτίθεται ότι όλοι οι κόμβοι έχουν τον ίδιο ρυθμό μολύνσεως από μια ασύρματη σύνδεση λ, δηλαδή $\lambda_i = \lambda, \forall i \in \{1,2,\ldots,N\}$ και αντίστοιχα τον ίδιο ρυθμό ανάκαμψης μ, δηλαδή $\mu_i = \mu, \forall i \in \{1,2,\ldots,N\}$. Σε αυτή την περίπτωση ο συνολικός ρυθμός ανάκαμψης κόμβων στο σύστημα στο δεδομένο στιγμιότυπο, προκύπτει $\mu(i) = \sum_i \mu_i = i \cdot \mu$. Το επόμενο γεγονός ανάκαμψης είναι αυτό που θα λάβει χώρα στον ελάχιστο χρόνο που καθορίζεται από τις i διαδικασίες ανάκαμψης (μία για κάθε μολυσμένο κόμβο). Επομένως, ο συνολικός ρυθμός εξυπηρέτησης δίνεται από το ελάχιστο i εκθετικών (σταθερών) ρυθμών εξυπηρέτησης, εξαιτίας της θεώρησης της εκθετικής κατανομής των διαδικασιών ανάκαμψης. Ο συνολικός ρυθμός μόλυνσης προκύπτει πιο σύνθετα επειδή εξαρτάται από τους γείτονες του κάθε μη-μολυσμένου κόμβου. Έτσι:

$$\lambda(N-i+j)=\sum_{m=1}^{N-i+j}k_m\lambda_m=\lambda\frac{\sum_{m=1}^{N-i+j}k_m}{N-i+j}(N-i+j) \tag{21}$$

όπου k_m είναι ο αριθμός των γειτονικών κακόβουλων κόμβων ενός νόμιμου κόμβου του δικτύου. Αθροίζοντας αυτόν τον αριθμό $\sum k_m$ και διαιρώντας με τον αριθμό των προσθεταίων προκύπτει ο μέσος αριθμός κακόβουλων χρηστών K στη γειτονιά ενός κόμβου. Επομένως, η έκφραση (21) δίνει το συνολικό στιγμιαίο ρυθμό μόλυνσης του δικτύου $\lambda(N-i+j)=\lambda K(N-i+j)$. Χρησιμοποιώντας αυτές τις εκφράσεις, η σχέση (20), παίρνει τη μορφή:

$$\pi(0)\cdot\sum_{i=0}^{N}\left[\binom{N}{i}\left(\frac{\lambda K}{\mu}\right)^i\right]=1 \tag{22}$$

Με εφαρμογή του θεωρήματος της διωνυμικής κατανομής, η πιθανότητα να μην υπάρχουν μολυσμένοι κόμβοι στο δίκτυο προκύπτει:

$$\pi(0)=\frac{1}{\left(1+\frac{\lambda K}{\mu}\right)^N} \tag{23}$$

Επομένως, η τελική έκφραση για τις εργοδικές πιθανότητες καταστάσεων έχει την κλειστή έκφραση:

$$\pi(i)=\frac{1}{\left(1+\frac{\lambda K}{\mu}\right)^N}\binom{N}{i}\left(\frac{\lambda K}{\mu}\right)^i=\pi'\left(N-i\right) \tag{24}$$

όπου $\pi'\left(N-i\right)$ είναι οι εργοδικές πιθανότητες καταστάσεων για την ουρά των μη-μολυσμένων κόμβων.

Με χρήση της σχέσης (24) η πιθανότητα το δίκτυο να είναι πλήρως μολυσμένο (πιθανότητα πανδημίας) δίνεται από την έκφραση:

$$\pi(N)=\frac{\left(\frac{\lambda K}{\mu}\right)^N}{\left(1+\frac{\lambda K}{\mu}\right)^N} \tag{25}$$

Η μέση πυκνότητα κακόβουλων γειτόνων από τη σκοπιά του κόμβου δικτύου μπορεί εύκολα να υπολογιστεί, λαμβάνοντας υπόψη την αρχικά ομοιόμορφη κατανομή τους και τη διατήρησή της από το μοντέλο κινητικότητας που ακολουθείται (τυχαίος περίπατος – random walk, [43]). Το συγκεκριμένο μέγεθος μπορεί να υπολογιστεί άμεσα σε δίκτυα μη-διασποράς παρουσία κακόβουλων χρηστών και δίνεται από την έκφραση:

$$K = \frac{\pi R^2}{L^2} \cdot M = \pi M \left(\frac{R}{L} \right)^2 \tag{26}$$

Η παραπάνω σχέση προκύπτει ως το ποσοστό των κακόβουλων κόμβων που αντιστοιχούν στην περιοχή κάλυψης ενός κόμβου δικτύου και αντιπροσωπεύει τη συμβολή της τοπολογίας στην επίδραση που έχει το κακόβουλο λογισμικό στο δίκτυο.

Από τα παραπάνω μπορεί να υπολογιστεί ο μέσος αριθμός μολυσμένων κόμβων στο δίκτυο, $E[i] = \sum_{i=1}^{N} i \cdot \pi(i)$ (που αντιστοιχεί στο μέσο αριθμό πακέτων της ουράς των μολυσμένων κόμβων), σε κλειστή μορφή:

$$E[i] = \frac{\lambda N K}{\mu + \lambda K} \tag{27}$$

και με αντικατάσταση της έκφρασης (26) στην (27) προκύπτει:

$$E[i] = \frac{\lambda \pi M N \left(\frac{R}{L} \right)^2}{\mu + \lambda \pi M \left(\frac{R}{L} \right)^2} \tag{28}$$

Αντίστοιχα, μπορεί να υπολογιστεί ο μέσος συνολικός ρυθμός μόλυνσης κόμβων στο δίκτυο, ο οποίος αντιστοιχεί στη μέση ρυθμαπόδοση (throughput) της ουράς των μη-μολυσμένων κόμβων, $E'[\gamma] = \sum_{i=1}^{N} \lambda(i) \cdot \pi'(i)$, ο οποίος μπορεί να υπολογισθεί ως:

$$E'[\gamma] = \sum_{i=1}^{N} \lambda(i) \cdot \pi'(i) = \lambda K \sum_{i=1}^{N} i \cdot \pi'(i) = \lambda K E'[i] = \lambda K \left(N - E[i] \right) \tag{29}$$

το οποίο τελικά δίνει:

$$E'[\gamma] = \frac{\lambda \mu N K}{\mu + \lambda K} \tag{30}$$

Με αντικατάσταση της έφρασης (26) στην (30), τελικά ο μέσος συνολικός ρυθμός μόλυνσης κόμβων στο δίκτυο προκύπτει:

$$E'[\gamma] = \frac{\lambda \mu \pi M N \left(\frac{R}{L}\right)^2}{\mu + \lambda \pi M \left(\frac{R}{L}\right)^2} \tag{31}$$

Οι παραπάνω εκφράσεις έχουν προκύψει ακολουθώντας την ανάλυση από τη σκοπιά του χρήστη δικτύου. Για αυτό το λόγο στις τελικές σχέσεις εμφανίζεται η ακτίνα μετάδοσης των νόμιμων κόμβων δικτύων. Αντίστοιχη ανάλυση μπορεί να γίνει ακολουθώντας την πορεία των υπολογισμών από τη σκοπιά του κακόβουλου κόμβου. Σε αυτή την περίπτωση, οι σχέσεις (19), (20) και ο ρυθμός εξυπηρέτησης $\mu(i) = i \cdot \mu$ παραμένουν αναλλοίωτα. Ο μέσος ρυθμός μόλυνσης τροποποιείται στη μορφή:

$$\lambda(N - i + j) = \sum_{m=1}^{M} k'_m \lambda_m = \lambda \frac{\sum_{m=1}^{M} k'_m}{M} M = \lambda K' M \tag{32}$$

όπου k'_m είναι το πλήθος μη-μολυσμένων γειτόνων (κόμβων δικτύου) ενός κακόβουλου χρήστη και K' το μέσο πλήθος γειτονικών μη-μολυσμένων κόμβων δικτύου. Το τελευταίο μέγεθος δίνεται από την έκφραση:

$$K' = \frac{\pi r^2}{L^2} \cdot \left(N - i + j\right) \tag{33}$$

και επομένως:

$$\lambda(N - i + j) = \lambda \pi M \left(\frac{r}{L}\right)^2 \left(N - i + j\right) \tag{34}$$

Με βάση την τελευταία, η έκφραση (20) γίνεται:

$$\pi(0) \cdot \sum_{i=0}^{N} \left[\binom{N}{i} \left(\frac{\lambda \pi M}{\mu} \cdot \left(\frac{r}{L}\right)^2 \right)^i \right] = 1 \tag{35}$$

η οποία με εφαρμογή του θεωρήματος διωνυμικής κατανομής δίνει σε κλειστή μορφή την πιθανότητα απουσίας μολυσμένων κόμβων στο δίκτυο:

$$\pi(0) = \frac{1}{\left(1+\frac{\lambda\pi M}{\mu}\left(\frac{r}{L}\right)^2\right)^N} \tag{36}$$

Οι εργοδικές πιθανότητες καταστάσεων προκύπτουν άμεσα με αντικατάσταση:

$$\pi(i) = \frac{1}{\left(1+\frac{\lambda\pi M}{\mu}\left(\frac{r}{L}\right)^2\right)^N}\binom{N}{i}\left(\frac{\lambda\pi M}{\mu}\left(\frac{r}{L}\right)^2\right)^i = \pi'\left(N-i\right) \tag{37}$$

και η αντίστοιχη πιθανότητα πανδημίας δίνεται ως εξής:

$$\pi(N) = \frac{\left(\frac{\lambda\pi M}{\mu}\left(\frac{r}{L}\right)^2\right)^N}{\left(1+\frac{\lambda\pi M}{\mu}\left(\frac{r}{L}\right)^2\right)^N} \tag{38}$$

Με παρόμοιο τρόπο μπορούν να εξαχθούν το μέσο πλήθος μολυσμένων κόμβων στο δίκτυο, καθώς και ο μέσος συνολικός ρυθμός μόλυνσης κόμβων, τα οποία τελικά δίνονται από τις εκφράσεις:

$$E[i] = \frac{\lambda\pi MN\left(\frac{r}{L}\right)^2}{\mu+\lambda\pi M\left(\frac{r}{L}\right)^2} \tag{39}$$

και

$$E'[\gamma] = \frac{\lambda\mu\pi MN\left(\frac{r}{L}\right)^2}{\mu+\lambda\pi M\left(\frac{r}{L}\right)^2} \tag{40}$$

Η ομοιότητα μεταξύ των σχέσεων (28)-(39) και (31)-(40) είναι εμφανής με μόνη αλλαγή την παράμετρο της ακτίνας μετάδοσης, ανάλογα με την σκοπιά που ακολουθεί η ανάλυση. Κάτι τέτοιο είναι αναμενόμενο, αν ληφθούν υπόψη οι τελικές κατανομές των κόμβων (δικτύου – κακόβουλων). Η μια κατανομή είναι δυϊκή της άλλης και λόγω της ανεξάρτητης και ίδιας χωρικής κατανομής των δύο ομάδων

κόμβων το πρόβλημα αποδεικνύεται ισοδύναμο από όποια σκοπιά και να ιδωθεί. Μόνο η τοπολογία που έχει δημιουργηθεί από τις αλληλεπιδράσεις των κόμβων έχει επίδραση στο μέσο αριθμό μολυσμένων κόμβων και το μέσο συνολικό ρυθμό μόλυνσης κόμβων, όπως φαίνεται και από τις παραπάνω αναλυτικές εκφράσεις και τις παραμέτρους δικτύου που υπάρχουν σε αυτές. Κάτι τέτοιο είναι αναμενόμενο σε αυτοργανούμενα ad hoc δίκτυα και δίκτυα αισθητήρων, όπου λόγω της έλλειψης κεντρικής υποδομής, οι κόμβοι λειτουργούν αυτόνομα με βάση την τοπικά διαθέσιμη πληροφορία που κατέχουν. Επομένως, οι τοπικές αλληλεπιδράσεις (τοπολογική γειτονιά) έχει μεγαλύτερη επίδραση στη συνολική συμπεριφορά του συστήματος.

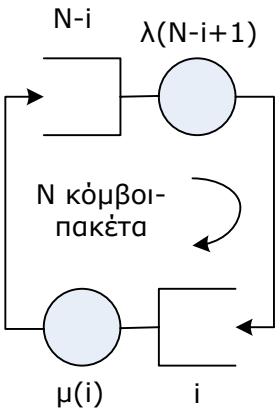
Επιπρόσθετα οι αναλυτικές εκφράσεις που προέκυψαν ως συναρτήσεις των παραμέτρων του συστήματος μπορούν να χρησιμοποιηθούν ως παράμετροι ανάδρασης και ελέγχου της μίας ή άλλης ουράς, ανάλογα με τη σκοπιά που λαμβάνει η ανάλυση. Το σύστημα των δύο κλειστών ουρών μπορεί να θεωρηθεί ως ένα κλειστό σύστημα αυτομάτου ελέγχου, στο οποίο η μία ουρά ελέγχει την άλλη [69]. Λαμβάνοντας τη σκοπιά των κακόβουλων χρηστών, μπορεί να γίνει η θεώρηση ότι η ουρά μολυσμένων κομβων αποτελεί τον ελεγκτή του συστήματος και η ουρά των μη-μολυσμένων κόμβων το ελεγχόμενο τμήμα. Βέλτιστες ή υπο-βέλτιστες και αποδοτικές πολιτικές ελέγχου μπορούν να εφαρμοστούν από την ουρά-ελεγκτή, οι οποίες αντιστοιχούν σε στρατηγικές επίθεσης που επηρεάζουν την ελεγχόμενη ουρά (ουρά μη-μολυσμένων κόμβων δικτύου).

3.4 Επίλυση σε Περιβάλλον Δικτύων Διασποράς

Θεωρώντας ένα δίκτυο διασποράς κακόβουλου λογισμικού (propagative network), η ανάλυση μπορεί να ακολουθήσει παρόμοια πορεία με την περίπτωση των δικτύων μη-διασποράς, με κατάλληλες τροποποιήσεις, ώστε να βρεθούν αναλυτικές εκφράσεις κλειστού τύπου για τα μεγέθη που ενδιαφέρουν.

Αρχικά, σε ένα δίκτυο διασποράς θεωρούμε την ύπαρξη ενός μόνο κακόβουλου χρήστη, μιας και οι μολυσμένοι κόμβοι δικτύου μπορούν πλέον να διαδραματίσουν κατά τη διάρκεια της μόλυνσής τους το ρόλο των κακόβουλων. Στην αντίθετη περίπτωση ύπαρξης πολλαπλών κακόβουλων κόμβων, η ανάλυση θα παρέμενε αναλλοίωτη, τα αποτελέσματα όμως θα ήταν αρκετά στραμμένα προς τη μεριά των κακόβουλων χρηστών. Δηλαδή, το αποτέλεσμα της δράσης τους θα ήταν δυσανάλογα μεγάλο. Διαισθητικά, κάτι τέτοιο είναι αναμενόμενο, αφού αν θεωρήσει κάποιος

παρα πολλούς κακόβουλους χρήστες και λίγους κόμβους δικτύου, τότε με μεγάλη πιθανότητα οι περισσότεροι νόμιμοι κόμβοι θα ήταν στη μολυσμένη κατάσταση. Το ανάποδο φυσικά θα συνέβαινε στην περίπτωση πολύ λίγων κακόβουλων κόμβων. Ωστόσο, ακόμα και με ένα κακόβουλο χρήστη, ρυθμίζοντας κατάλληλα το ρυθμό μόλυνσης κόμβου λ μπορούν να ληφθούν ρεαλιστικά συμπεράσματα για τη συμπεριφορά του συστήματος. Τελικά θα φανεί ότι η επίδραση ενός και μόνου κακόβουλου χρήστη μπορεί να είναι περισότερο από υπολογίσιμη, επιβεβαιώντας προηγούμενα συμπεράσματα παλαιότερων μελετών [12].



Σχήμα 4 – Ισοδύναμο Norton για δίκτυο διασποράς με μοναδικό κακόβουλο χρήστη

Το ισοδύναμο Norton ενός ασύρματου δικτύου διασποράς με ένα κακόβουλο χρήστη φαίνεται στο Σχήμα 4. Ο συνολικός στιγμιαίος ρυθμός μόλυνσης κόμβων εξαρτάται από τον κακόβουλο κόμβο (ή τους κακόβουλους στην περίπτωση πολλαπλών κόμβων), όπως και στην περίπτωση των δικτύων μη-διασποράς. Ωστόσο στο Σχήμα 4 επισημαίνεται η εξάρτηση του συνολικού ρυθμού μόλυνσης από τον κακόβουλο χρήστη, ώστε να γίνεται άμεσα κατανοητό γιατί η κατάσταση χωρίς μολυσμένους κόμβους ($\pi(0)$) δεν είναι απορροφητική (absorbing). Σε αυτή την περίπτωση, ακόμα και όταν όλοι οι κόμβοι είναι μη-μολυσμένοι (οπότε ο ρυθμός μόλυνσης που οφείλεται στους μολυσμένους κόμβους δικτύου είναι μηδενικός), ο συνολικός ρυθμός μόλυνσης δεν είναι μηδενικός, εξαιτίας της επίδρασης του κακόβουλου χρήστη.

Η ανάλυση της μόνιμης κατάστασης του συστήματος ακολουθεί την ίδια μεθοδολογία με τα δίκτυα μη-διασποράς. Επικεντρώνοντας στην ουρά των μολυσμένων κόμβων και αναλύοντας τη σχετική αλυσίδα καταστάσεων, η αναδρομική έκφραση των εργοδικών πιθανοτήτων καταστάσεων δίνεται από:

$$\pi(i) = \pi(0) \cdot \prod_{j=1}^{i} \frac{\lambda(N+1-i+j)}{\mu(j)} \tag{41}$$

Με εφαρμογή της συνθήκης κανονικοποίησης $\sum_{i=1}^{N} \pi(i) = 1$, η έκφραση (41) γίνεται:

$$\pi(0) \cdot \sum_{i=0}^{N} \prod_{j=1}^{i} \frac{\lambda(N+1-i+j)}{\mu(j)} = 1 \tag{42}$$

Ο συνολικός ρυθμός ανάκαμψης προκύπτει όπως στην προηγούμενη ανάλυση $\mu(i) = \sum_i \mu_i = i \cdot \mu$, ενώ ο συνολικός ρυθμός μόλυνσης υπολογιζόμενος από τη σκοπιά των κόμβων δικτύου είναι:

$$\lambda(N+1-i+j) = \sum_{m=1}^{N-i+j} k_m \lambda_m = \lambda \frac{\sum_{m=1}^{N-i+j} k_m}{N-i+j} (N-i+j) = \lambda K(i)(N-i+j) \tag{43}$$

όπου k_m είναι όπως πριν ο αριθμός των μολυσμένων κόμβων (συμπεριλαμβανομένου και του κακόβουλου χρήστη) στη γειτονιά του κόμβου δικτύου m και $K(i)$ είναι το στιγμιαίο μέσο πλήθος μολυσμένων κόμβων στη γειτονιά ενός κόμβου δικτύου, το οποίο εξαρτάται πλέον από τον αριθμό των μολυσμένων κόμβων i στην εκάστοτε χρονική στιγμή. Υιοθετώντας τη σκοπιά ενός κόμβου δικτύου, το μέγεθος αυτό υπολογίζεται:

$$K(i) = \frac{\pi R^2}{L^2}\left(N - \left(N-i+j\right)+1\right) = \frac{\pi R^2}{L^2}\left(i-j+1\right) \tag{44}$$

όπου $\left(i-j+1\right)$ είναι ο συνολικός αριθμός μολυσματικών χρηστών (συμπεριλαμβανομένου του κακόβουλου χρήστη) στη δεδομένη χρονική στιγμή. Χρησιμοποιώντας την έκφραση (44), η έκφραση (43) του συνολικού στιγμιαίου ρυθμού μολύνσεων του δικτύου γίνεται:

$$\lambda(N+1-i+j) = \lambda\pi\left(\frac{R}{L}\right)^2 \left(i-j+1\right)(N-i+j) \tag{45}$$

Με χρήση της (45), η σχέση (42) γίνεται:

$$\pi(0) \cdot \sum_{i=0}^{N} \prod_{j=1}^{i} \left[\frac{\lambda\pi}{\mu}\left(\frac{R}{L}\right)^2 \frac{\left(i-j+1\right)(N-i+j)}{j} \right] = 1 \tag{46}$$

Θέτοντας $a^{-1} \triangleq \frac{\lambda\pi}{\mu}\left(\frac{R}{L}\right)^2$ η παραπάνω έκφραση παίρνει τη μορφή:

$$\pi(0)\cdot\sum_{i=0}^{N}\prod_{j=1}^{i}\left[\frac{1}{a}\cdot\frac{(i-j+1)(N-i+j)}{j}\right]=1 \tag{47}$$

Η σχέση (47) μπορεί να απλοποιηθεί και να γραφεί στη μορφή:

$$\frac{\pi(0)\cdot N!}{a^N}\cdot\sum_{k=0}^{N}\frac{a^k}{k!}=1 \tag{48}$$

Καθώς ο αριθμός των κόμβων δικτύου τείνει στο άπειρο ($N\to\infty$), το άθροισμα στην έκφραση (48) συγκλίνει στο ανάπτυγμα σε δυναμοσειρά του e^a. Επομένως, στο όριο για $N\to\infty$, η πιθανότητα μη-ύπαρξης μολυσμένων κόμβων στο δίκτυο μπορεί να προσεγγιστεί από την έκφραση:

$$\pi(0)\cong\frac{a^N}{N!}\cdot e^{-a} \tag{49}$$

Η αναλυτική έκφραση των εργοδικών πιθανοτήτων καταστάσεων γίνεται με χρήση της σχέσης (49):

$$\pi(i)=\frac{a^{N-i}}{(N-i)!}\cdot e^{-a}=\pi'(N-i) \tag{50}$$

Από την τελευταία έφραση προκύπτει ότι η πιθανότητα πανδημίας είναι $\pi(N)=e^{-a}$, η οποία εξαρτάται μόνο από τις άμεσα σχετιζόμενες παραμέτρους με την επίθεση (λ και μ) και από τα ιδιαίτερα χαρακτηριστικά του δικτύου και πιο συγκεκριμένα το ποσοστό ασύρματης κάλυψης ενός κόμβου δικτύου σε σχέση με τη συνολική έκταση της περιοχής του δικτύου.

Σε αυτό το σημείο είναι αναγκαίο να σημειωθεί ότι για τις τιμές των παραμέτρων a και N που χρησιμοποιούνται στην πράξη, το σφάλμα που υπεισέρχεται στη σχέση (49) είναι πολύ μικρό, σχεδόν αμελητέο, όπως θα φανεί στο επόμενο κεφάλαιο. Επιπρόσθετα, η συνάρτηση αθροίσματος στη σχέση (48), μπορεί να θεωρηθεί γνωστή με τιμές που δίνονται από διαθέσιμους πίνακες, επομένως, η έκφραση (49) μπορεί να χρησιμοποιηθεί αναλυτικά και να οδηγήσει στη (50) χωρίς την ανάγκη προσέγγισης με την εκθετική συνάρτηση e^{-a}.

Ο μέσος αριθμός πελατών στην ουρά μολυσμένων κόμβων αντιστοιχεί στο μέσο πλήθος μολυσμένων κόμβων στο δίκτυο και μπορεί εύκολα να υπολογισθεί:

$$E[i] = e^{-a}\left(Ne^{a} - a\sum_{k=1}^{N-1}\frac{a^{k-1}}{(k-1)!}\right) \cong N - a = N - \frac{\frac{\mu}{\lambda\pi}}{\left(\frac{R}{L}\right)^2} \tag{51}$$

Παρόμοια μπορεί να υπολογιστεί ο μέσος συνολικός ρυθμός μόλυνσης κόμβων δικτύου που αντιστοιχεί στη μέση ρυθμαπόδοση της ουράς των μη-μολυσμένων κόμβων, $E'[\gamma] = \sum_{i=1}^{N} \lambda(i)\cdot\pi'(i)$:

$$E'[\gamma] = \sum_{i=1}^{N}\left[c(i-1)(N+2-i)\pi'(i)\right] \tag{52}$$

Όπου $c \triangleq \lambda\pi\left(\frac{R}{L}\right)^2$. Η σχέση (52) μπορεί να γραφεί στη μορφή:

$$E'[\gamma] = c\cdot\sum_{i=1}^{N}\left\{\left[(N+3)i - i^2 - (N+2)\right]\pi'(i)\right\} \tag{53}$$

και χρησιμοποιώντας το γεγονός ότι $e^{-a}\cdot\sum_{i=1}^{N} i^2\frac{a^i}{i!} = a(1+a)$ στην (53), η τελική έκφραση για το μέσο ρυθμό μόλυνσης κόμβων γίνεται:

$$E'[\gamma] = c\left[a(N+2-a) - (N+2)\left(1-\pi'(0)\right)\right] \tag{54}$$

3.5 Μετρικό Αποδοτικότητας Μόλυνσης (Infection Efficiency)

Τα παραπάνω μεγέθη που υπολογίστηκαν με βάση το προτεινόμενο μοντέλο διάδοσης κακόβουλου λογισμικού βασιζόμενο σε κλειστά δίκτυα ουρών αναμονής, προέκυψαν από ανάλυση για τη μόνιμη κατάσταση του δικτύου. Επομένως, αποτελούν μετρικές που είναι ανεξάρτητες του χρόνου και εξαρτώνται αποκλειστικά από τα δομικά χαρακτηριστικά του δικτύου (ακτίνα μετάδοσης, πυκνότητα κόμβων, μοντέλο κινητικότητας) και τις παραμέτρους των επιθέσεων (ρυθμός μόλυνσης/ανάκαμψης νόμιμων κόμβων).

Σε πολλές περιπτώσεις είναι αναγκαίο να αξιολογηθεί η συμπεριφορά διάδοσης κακόβουλου λογισμικού για ένα δίκτυο σε ένα συγκεκριμένο χρονικό διάστημα, κατά το οποίο εμφανίζονται ενδεχομένως και μεταβατικά φαινόμενα. Τα τελευταία

εμφανίζονται κατά την εκκίνηση της λειτουργίας ενός δικτύου, όπου απαιτείται ένα χρονικό διάστημα μέχρι ο μέσος αριθμός κόμβων να αυξηθεί και να φτάσει στην περιοχή της μέσης τιμής του. Επίσης προς το τέλος της διάρκειας ζωής του δικτύου, κατά το οποίο λόγω έλλειψης ενεργειακών πόρων, κάποιοι ασύρματοι κόμβοι παύουν να λειτουργούν, αναγκαστικά ο αριθμός των κόμβων που είναι μολυσμένοι κατά μέσο όρο θα είναι μικρότερος από τον αρχικά προβλεπόμενο (αφού μειώνεται ο διαθέσιμος πληθυσμός κόμβων δικτύου).

Για την αξιολόγηση της συμπεριφοράς της διάδοσης κακόβουλου λογισμικού στη δεύτερη περίπτωση προτείνεται ένα μέγεθος που περιγράφει το συνολικό αποτέλεσμα της επίθεσης στη διάρκεια του χρόνου που μελετάται το δίκτυο. Επικεντρώνοντας στον αριθμό των κόμβων που είναι μολυσμένοι σε κάθε χρονική στιγμή (συμβολίζεται με $i(t)$), θεωρούμε ότι αυτό το μέγεθος είναι ενδεικτικό της αποτελεσματικότητας μιας επίθεσης σε μια δεδομένη χρονική στιγμή. Ακόμα και για δίκτυα μη-διασποράς οι μολυσμένοι κόμβοι είναι πρακτικά μη-διαθέσιμοι για να επιτελέσουν την προβλεπόμενη λειτουργία τους (είτε γιατί το είδος της επίθεσης τους καθιστά ανενεργούς, είτε γιατί όλοι ή μέρος των πόρων τους έχει διατεθεί για την αντιμετώπιση της επίθεσης).

Επομένως, ένα συνδυασμένο μετρικό του αριθμού των μολυσμένων κόμβων με τη χρονική διάρκεια του διαστήματος παρατήρησης είναι κατάλληλο ως ένα χρονικά-ενδεικτικό μέτρο αποδοτικότητας επίθεσης. Η Αποδοτικότητα Μόλυνσης (Infection Efficiency, I_E) ορίζεται ως το ολοκλήρωμα του αριθμού των μολυσμένων κόμβων για το διάστημα παρατήρησης του δικτύου

$$I_E = \int_{t=0}^{T} i(t)dt \tag{55}$$

όπου T είναι η συνολική διάρκεια παρατήρησης του συστήματος για την οποία υπολογίζεται η Αποδοτικότητα Μόλυνσης. Διαισθητικά η Αποδοτικότητα Μόλυνσης προκύπτει ως το γινόμενο του αριθμού των μολυσμένων κόμβων επί τη διάρκεια του συγκεκριμένου χρονικού διαστήματος. Θεωρώντας διαστήματα μικρής χρονικής διάρκειας, στο όριο όπου τα διαστήματα γίνονται πολύ μικρά και πολλά το πλήθος, το άθροισμα των εκάστοτε γινομένων συγκλίνει στο ολοκλήρωμα (55). Η Αποδοτικότητα Μόλυνσης παρέχει ένα συνδυασμένο μέτρο της στιγμιαίας ζημιάς

που προκαλεί μια ομάδα κακόβουλων χρηστών και της χρονικής περιόδου που η επίθεση λαμβάνει χώρα.

Κεφάλαιο 4

Ανάλυση – Αξιολόγηση Συμπεριφοράς Αναμονητικού Μοντέλου Διάδοσης Κακόβουλου Λογισμικού

Στο τρέχον κεφάλαιο μελετάται περαιτέρω η συμπεριφορά και οι δυνατότητες που παρουσιάζει η διάδοση κακόβουλου λογισμικού γενικού τύπου με βάση τα αναλυτικά αποτελέσματα του προτεινόμενου μοντέλου. Αρχικά παρατίθενται αριθμητικά αποτελέσματα προκειμένου να αναγνωριστεί η επίδραση των εμπλεκόμενων παραγόντων και στη συνέχεια με χρήση θεωρίας βελτιστοποίησης εκτιμώνται τα όρια της επίδοσης που δυνητικά έχει μια στρατηγική διάδοσης κακόβουλου λογισμικού με βάση τις συμβατές ενέργειες που επιτρέπεται να εφαρμόσει από τη φύση του συστήματος. Επιπρόσθετα παρουσιάζονται αποτελέσματα προσομοιώσεων για την επιβεβαίωση της ορθότητας του προτεινόμενου μοντέλου και την αξιολόγηση των παραμέτρων του με βάση και το χρονικά–εξαρτώμενο μετρικό επίδοσης της Αποδοτικότητας Μόλυνσης.

4.1 Αριθμητικά Αποτελέσματα και Αποτελέσματα Προσομοιώσεων

Σε αυτή την ενότητα, παραθέτουμε ενδεικτικά διαγράμματα με αριθμητικά αποτελέσματα και αποτελέσματα προσομοιώσεων, προκειμένου να διαφανούν εποπτικά οι σημαντικοί παράμετροι που επηρεάζουν την εκκίνηση, λειτουργία και εξέλιξη της διάδοσης κακόβουλου λογισμικού σε ασύρματα δίκτυα πολλαπλών βημάτων. Σκοπός είναι να διαφανεί τόσο η συμπεριφορά των δικτύων που δέχονται επιθέσεις, όσο και οι παράμετροι που ελέγχουν τη διάδοση κακόβουλου λογισμικού και την επηρεάζουν άμεσα ή έμμεσα.

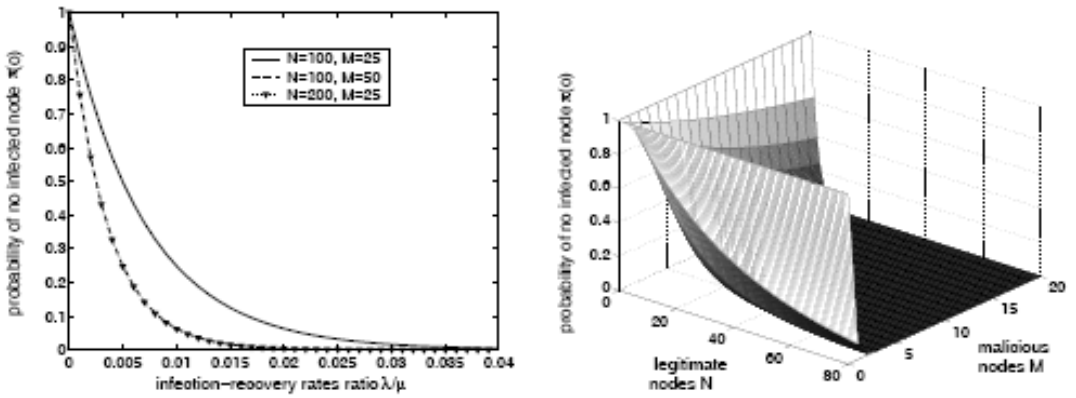
Τα αποτελέσματα διαχωρίζονται σε δύο κατηγορίες αναφορικά με τις περιπτώσεις που μελετήθηκαν παραπάνω με αναλυτικές μεθόδους, τα δίκτυα μη-διασποράς και τα δίκτυα διασποράς. Για την αξιολόγηση της συμπεριφοράς των συστημάτων χρησιμοποιούνται τόσο τα χρονικά–ανεξάρτητα μετρικά των

αναμενόμενων τιμών μολυσμένων κόμβων και ρυθμού μόλυνσης κόμβων, όσο και το χρονικά–εξαρτώμενο μετρικό της Αποδοτικότητας Μόλυνσης.

4.1.1 Δίκτυα Μη-Διασποράς Παρουσία Πολλαπλών Κακόβουλων Χρηστών

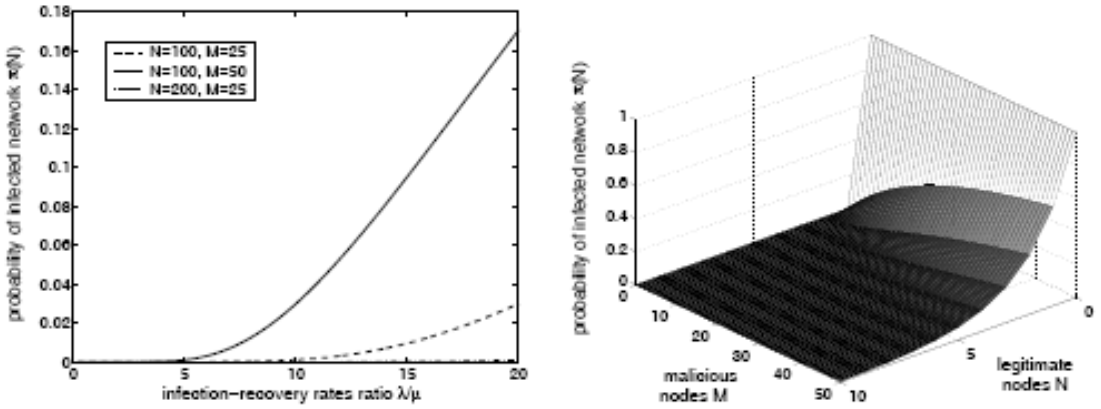
Στα δίκτυα μη-διασποράς, όπως ήδη αναφέρθηκε, οι νόμιμοι κόμβοι δεν μεταδίδουν σε γειτονικούς νόμιμους κόμβους το κακόβουλο λογισμικό που λαμβάνουν. Πρόκειται για περιπτώσεις δικτύων με κόμβους χαμηλών υπολογιστικών δυνατοτήτων και χαμηλό κόστος, όπως τα δίκτυα αισθητήρων. Για τη μελέτη τους υποτίθεται αντίστοιχα ένα σύνολο κακόβουλων χρηστών, επίσης χαμηλού κόστους και υπολογιστικών πόρων, ώστε να γίνει εμφανής η επίδρασή τους στη διασπορά του απειλητικού λογισμικού στο δίκτυο.

Στο Διάγραμμα 1 παρουσιάζεται η πιθανότητα απουσίας μολυσμένων κόμβων στο δίκτυο, (a) συναρτήσει του λόγου λ/μ, και (b) του αριθμού νόμιμων κόμβων και κακόβουλων χρηστών. Η τιμή της πιθανότητας είναι γενικά χαμηλή και μειώνεται πολύ γρήγορα όσο κάθε μια παράμετρος αυξάνει, αύξηση η οποία αντιστοιχεί, είτε σε εντονότερες επιθέσεις, είτε σε περισσότερες δυνατότητες μόλυνσης (μεγαλύτερο/πυκνότερο δίκτυο).



(a) $\pi(0)$ vs λ/μ (b) $\pi(0)$ vs N, M

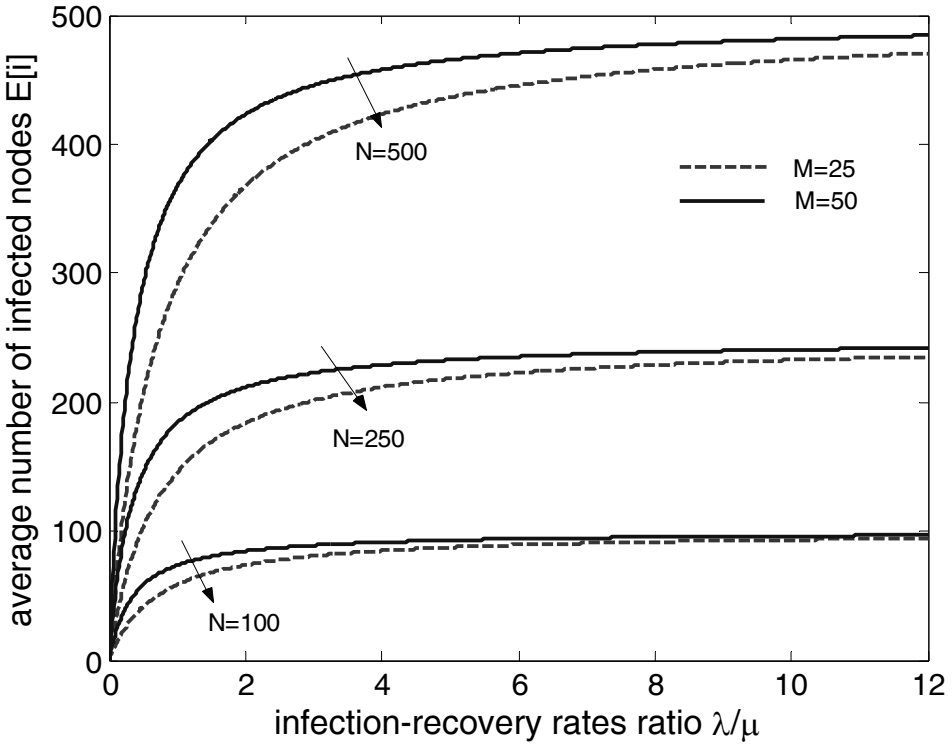
Διάγραμμα 1 – Πιθανότητα απουσίας μολυσμένων κόμβων $\pi(0)$ συναρτήσει του λόγου λ/μ, νομιμων κόμβων N και κακόβουλων κόμβων M



(a) $\pi(N)$ vs λ/μ (b) $\pi(N)$ vs N, M

Διάγραμμα 2 – Πιθανότητα πανδημίας $\pi(N)$ συναρτήσει του λόγου λ/μ, νόμιμων κόμβων N και κακόβουλων κόμβων M

Στο Διάγραμμα 2 φαίνεται η πιθανότητα πανδημίας, δηλαδή η πιθανότητα να μολυνθούν όλοι οι κόμβοι του δικτύου σε ένα δεδομένο χρονικό στιγμιότυπο. Πρόκειται για ένα σημαντικό μέγεθος, το οποίο είναι ενδεικτικό της επίδρασης μιας στρατηγικής επίθεσης, αλλά και των παραγόντων που θα μπορούσαν να καταστήσουν μια στρατηγική αποδοτική στο μέγιστο βαθμό. Οι τάσεις που παρατηρούνται είναι αντίστροφες σε σχέση με την πιθανότητα απουσίας μολυσμένων κόμβων $\pi(0)$.

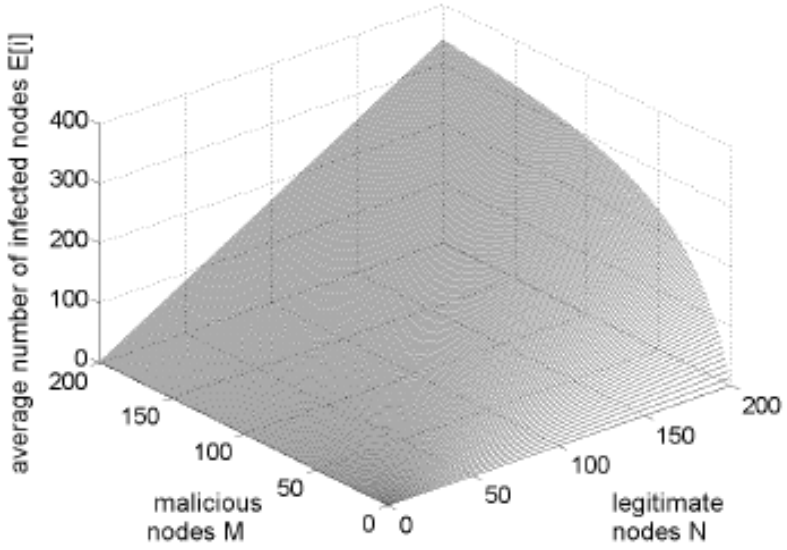


Διάγραμμα 3 – Μέσος αριθμός μολυσμένων κόμβων $E[i]$ συναρτήσει του λόγου λ/μ

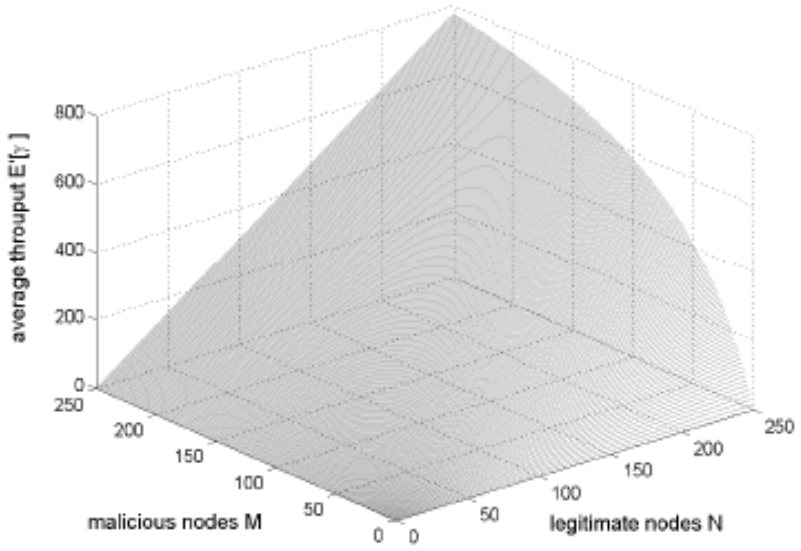
Στο Διάγραμμα 3 φαίνεται το μέσο πλήθος μολυσμένων κόμβων ως συνάρτηση του λόγου του ρυθμού μόλυνσης προς το ρυθμό ανάκαμψης κόμβου λ/μ, για διαφορετικούς συνδυασμούς κόμβων δικτύου N, και κακόβουλων χρηστών M. Η περιοχή δικτύου για όλα τα αποτελέσματα θεωρείται τετραγωνική με πλευρά $L = 1500m$, ενώ όλοι οι κόμβοι δικτύου θεωρούνται στη γενική περίπτωση ότι έχουν ακτίνα $R = 200m$, εκτός και αν αναφέρεται διαφορετικά. Το μέσο πλήθος μολυσμένων κόμβων αυξάνει όσο μεγαλώνει το πλήθος κόμβων δικτύου ή ο αριθμός κακόβουλων χρηστών και όσο αυξάνει ο ρυθμός μόλυνσης σε σχέση με το ρυθμό ανάκαμψης. Ωστόσο, υπάρχει ένα κατώφλι του ρυθμού λ/μ, πέρα από το οποίο δεν υπάρχει σημαντική αύξηση του μεγέθους, ενώ το κόστος για την επίτευξη μεγαλύτερου λ/μ μεγαλώνει σημαντικά.

Το γεγονός αυτό είναι σημαντικό για τους κακόβουλους χρήστες, ώστε να μειώσουν το κόστος της επίθεσής τους και να διατηρήσουν την επίδοσή τους σε υψηλό επίπεδο σε σχέση με τη μέγιστη δυνατή επιτευκτή. Κάτι τέτοιο προκύπτει από τη διαφαινόμενη βαρύτητα του κάθε παράγοντα στην έκβαση της εξέλιξης των αναμενόμενων μεγεθών μολυσμένων κόμβων. Έτσι ο λόγος των ρυθμών μόλυνσης–ανάκαμψης μπορεί να οδηγήσει σε σημαντικά οφέλη, κυρίως όταν βρίσκεται στην περιοχή κάτω της μονάδας. Για υψηλότερες τιμές, περαιτέρω αυξήσεις παύουν να έχουν τα άμεσα αποτελέσματα που έχουν για τις χαμηλότερες.

Στο Διάγραμμα 4 παρουσιάζεται η μεταβολή του μέσου αριθμού μολυσμένων κόμβων σε σχέση με τον αριθμό των κόμβων δικτύου και των κακόβουλων χρηστών, για $\lambda/\mu = 0.5$. Από το διάγραμμα γίνεται φανερή η διαφορετική επίδραση των δύο παραμέτρων και πιο συγκεκριμένα η γραμμική σχέση αναφορικά με τους κόμβους του δικτύου και η εκθετική αναφορικά με τους κακόβουλους χρήστες. Ως αποτέλεσμα, μια αύξηση του αριθμού των κακόβουλων χρηστών οδηγεί σε μεγαλύτερη αύξηση του μέσου αριθμού μολυσμένων κόμβων σε σχέση με την αντίστοιχη αύξηση που θα προκαλούσε μια αντίστοιχη αύξηση του αριθμού των νόμιμων κόμβων δικτύου. Επιπρόσθετα, η πρώτη αλλαγή είναι πιο εφικτή για τη σχεδίαση έξυπνων στρατηγικών.



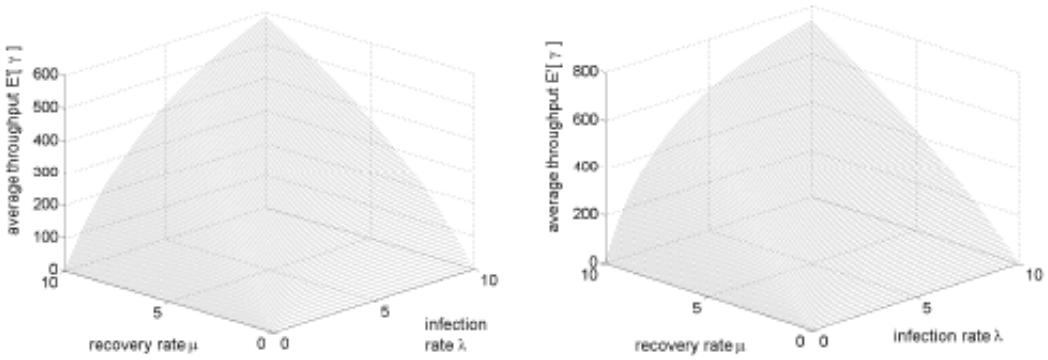
Διάγραμμα 4 – Μέσος αριθμός μολυσμένων κόμβων $E[i]$ συναρτήσει κόμβων δικτύου N , κακόβουλων κόμβων M



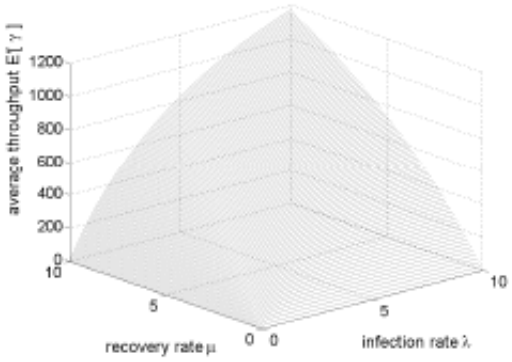
Διάγραμμα 5 – Μέσος συνολικός ρυθμός μόλυνσης κόμβων δικτύου $E'[\gamma]$ συναρτήσει κακόβουλων χρηστών M και κόμβων δικτύου N

Στο Διάγραμμα 5 παρουσιάζεται η αντίστοιχη συνάρτηση για την περίπτωση του μέσου συνολικού ρυθμού μόλυνσης κόμβων δικτύου. Οι εξαρτήσεις από το μέσο αριθμό μολυσμένων κόμβων είναι παρόμοιες με την περίπτωση του μέσου πλήθους μολυσμένων κόμβων (Διάγραμμα 4). Αύξηση του αριθμού των κακόβουλων κόμβων προκαλεί μεγαλύτερη βλάβη (μεγαλύτερο μέσο ρυθμό μόλυνσης) από την αντίστοιχη

αύξηση του αριθμού των κόμβων δικτύου, καθιστώντας αυτή την παράμετρο πιο κρίσιμη. Αντίστοιχα διαγράμματα προκύπτουν συναρτήσει των ρυθμών λ και μ για διαφορετικούς συνδυασμούς νόμιμων κόμβων – κακόβουλων χρηστών (Διάγραμμα 6). Από τα αντίστοιχα διαγράμματα γίνεται εμφανής η πιο σημαντική επίδραση του ρυθμού λ, η οποία είναι άμεσα ελέγξιμη από τον κακόβουλο χρήστη, παρόλο που η αύξησή της πάνω από ένα κατώφλι μπορεί να επιφέρει μεγάλο κόστος σε αυτόν.



(a) N=100, M=25 (b) N=100, M=50

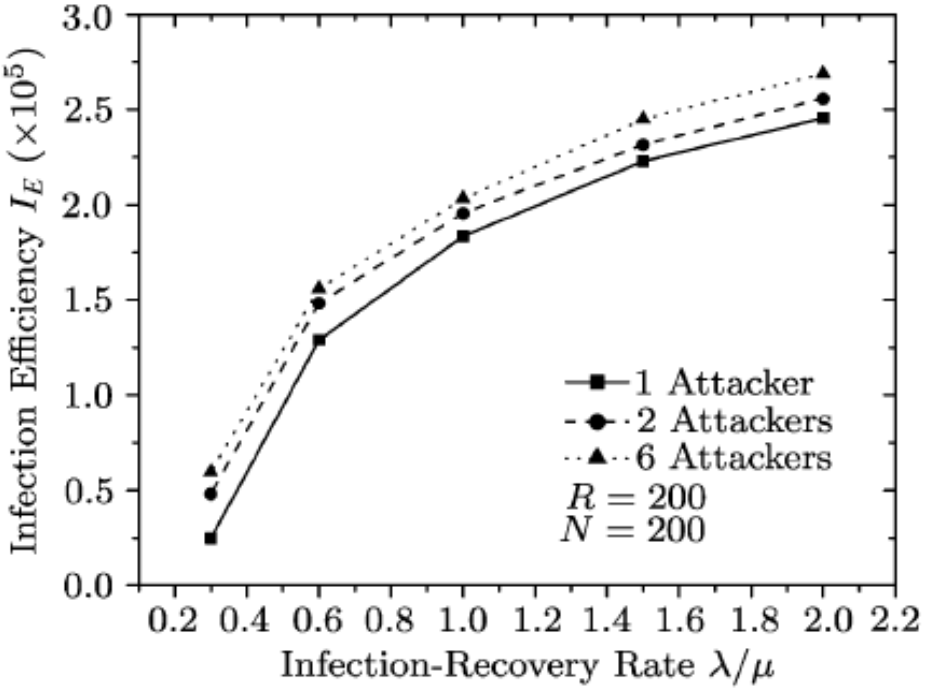


(c) N=200, M=25

Διάγραμμα 6 – Μέσος συνολικός ρυθμός μόλυνσης κόμβων δικτύου $E'[\gamma]$ συναρτήσει ρυθμού μόλυνσης λ και ρυθμού ανάκαμψης μ

Στο σημείο αυτό πρέπει να επισημανθεί η φυσική ερμηνεία της αλλαγής του αριθμού κόμβων δικτύου και κακόβουλων χρηστών για το σύστημα. Η αύξηση του αριθμού των κόμβων δικτύου δεν ελέγχεται από τους κακόβουλους χρήστες και συνήθως νοείται σε μικρή κλίμακα για το ίδιο δίκτυο (προσθήκη/αφαίρεση μικρού ποσοστού κόμβων) ή σε μεγαλύτερη κλίμακα (με ολοκληρωτική αλλαγή δικτύου). Από την άλλη προσθήκη/αφαίρεση ενός μικρού ποσοστού κακόβουλων χρηστών είναι σχεδόν πάντα εφικτή και ελέγξιμη. Επομένως το δεύτερο σενάριο φαίνεται πιο

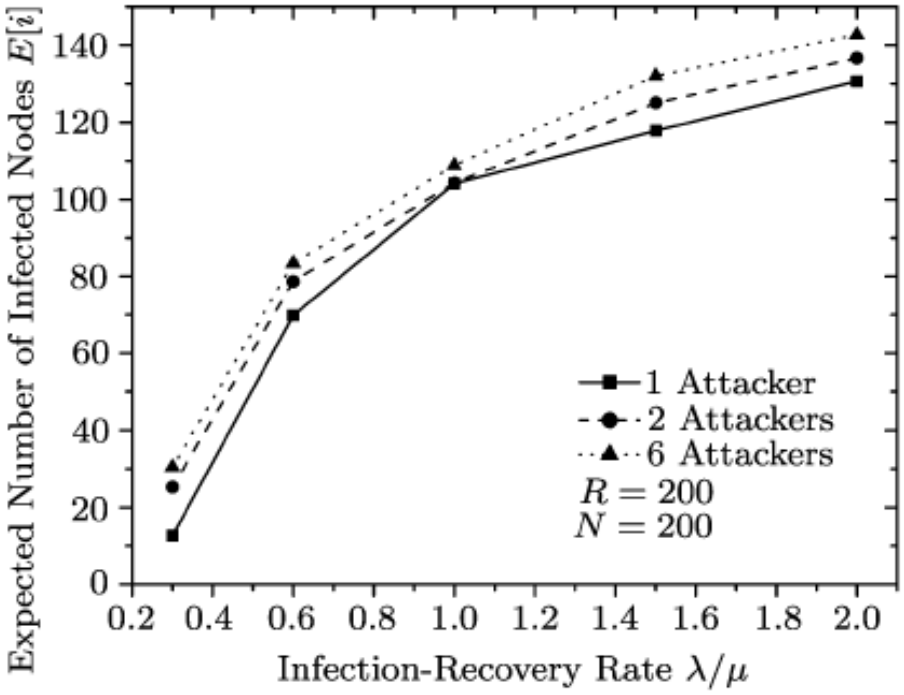
ρεαλιστικό για τον καθορισμό και εφαρμογή έξυπνων στρατηγικών επίθεσης σε ασύρματα δίκτυα αισθητήρων.



Διάγραμμα 7 – Αποδοτικότητα Μόλυνσης I_E για δίκτυα μη-διασποράς και πολλαπλούς κακόβουλους χρήστες (προσομοίωση)

Στο Διάγραμμα 7 παρουσιάζονται αποτελέσματα προσομοιώσεων για την Αποδοτικότητα Μόλυνσης με τη βοήθεια του περιβάλλοντος NS2 για 1, 2 και 6 κακόβουλους χρήστες σε δίκτυο $N = 200$ κόμβων συναρτήσει του λόγου λ/μ. Όπως αναμένεται, αύξηση του αριθμού των κακόβουλων χρηστών οδηγεί σε αύξηση της Αποδοτικότητας Μόλυνσης και το ίδιο συμβαίνει με το λόγο λ/μ. Ωστόσο, η δεύτερη παράμετρος είναι αρκετά σημαντικότερη, αφού ακόμα και μικρές αυξήσεις του λ/μ μπορεί να οδηγήσουν σε πολύ μεγάλες αυξήσεις της αποδοτικότητας μιας ομάδας κακόβουλων χρηστών. Από το Διάγραμμα 7 διαφαίνεται μια τάση παρόμοια με αυτή που παρουσιάζουν τα αριθμητικά αποτελέσματα για τον αναμενόμενο αριθμό μολυσμένων κόμβων και τον αναμενόμενο ρυθμό μόλυνσης κόμβων. Η Αποδοτικότητα Επίθεσης αυξάνει γρήγορα για μικρές μεταβολές των παραμέτρων όσο η τιμή του λόγου λ/μ είναι μικρή, ενώ όσο μεγαλώνει η τιμή του λόγου αυτού, χρειάζονται σημαντικές μεταβολές για να παρατηρηθεί μια αλλαγή στην Αποδοτικότητα Μόλυνσης. Επομένως, εμφανίζεται ένα κατώφλι για το λόγο λ/μ, πάνω από το οποίο δεν έχει νόημα να γίνει προσπάθεια αύξησης της τιμής του λ/μ,

μιας και το κόστος για να γίνει κάτι τέτοιο θα είναι μεγαλύτερο από το λαμβανόμενο όφελος για τους κακόβουλους χρήστες.



Διάγραμμα 8 – Μέσος αριθμός μολυσμένων κόμβων $E[i]$ συναρτήσει λ / μ για δίκτυα μη-διασποράς (προσομοίωση)

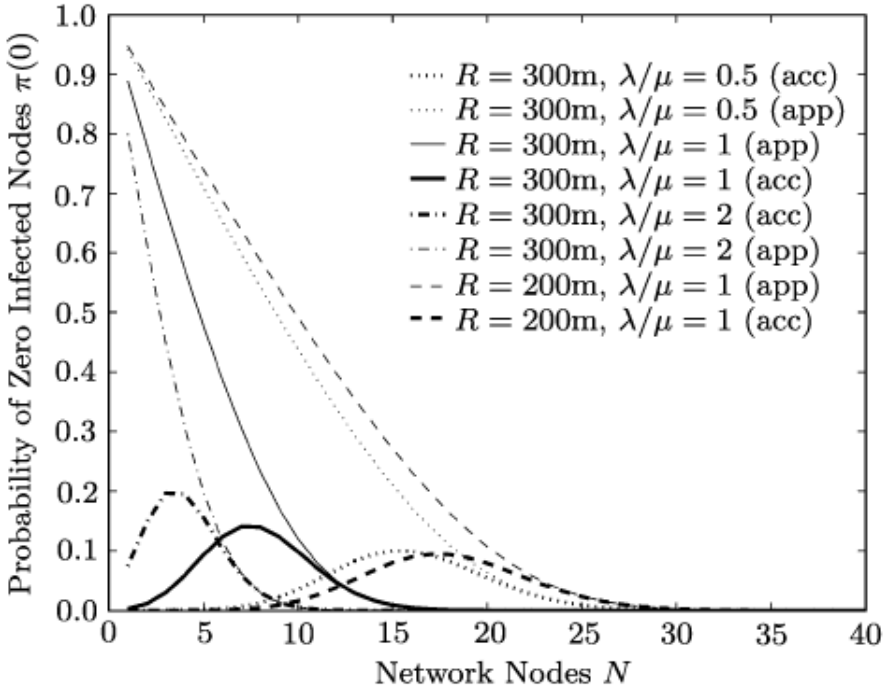
Στο Διάγραμμα 8 φαίνεται ο μέσος αριθμός μολυσμένων κόμβων για την περίπτωση 1, 2 και 6 κακόβουλων χρηστών, όπως προέκυψε από τις αντίστοιχες προσομοιώσεις. Επισημαίνεται η ομοιότητα των καμπυλών του διαγράμματος με την περίπτωση του αριθμητικού αποτελέσματος που δόθηκε στο Διάγραμμα 3 στο αντίστοιχο εύρος μεταβολής παραμέτρων για το λόγο λ / μ. Απόλυτη σύγκριση με το Διάγραμμα 3, δείχνει ότι οι τιμές στην περίπτωση των προσομοιώσεων είναι χαμηλότερες, γεγονός που οφείλεται σε διάφορες παραδοχές που έχουν γίνει για την αναλυτική θεώρηση του συστήματος και αντίστοιχες προσεγγίσεις που έχουν γίνει στις προσομοιώσεις.

4.1.2 Δίκτυα Διασποράς Παρουσία Ενός Κακόβουλου Χρήστη

Στον αντίποδα των δικτύων μη-διασποράς βρίσκονται τα δίκτυα διασποράς, στα οποία οι νόμιμοι και κακόβουλοι κόμβοι διαθέτουν τα απαραίτητα μέσα ώστε να είναι εφικτό το κακόβουλο λογισμικό που κυκλοφορεί να μεταδίδεται και μεταξύ νόμιμων κόμβων. Κατά βάση, οι μολυσμένοι νόμιμοι κόμβοι λειτουργούν ως κακόβουλοι και επομένως για να μπορέσει να μελετηθεί η διάδοση και η επίδραση

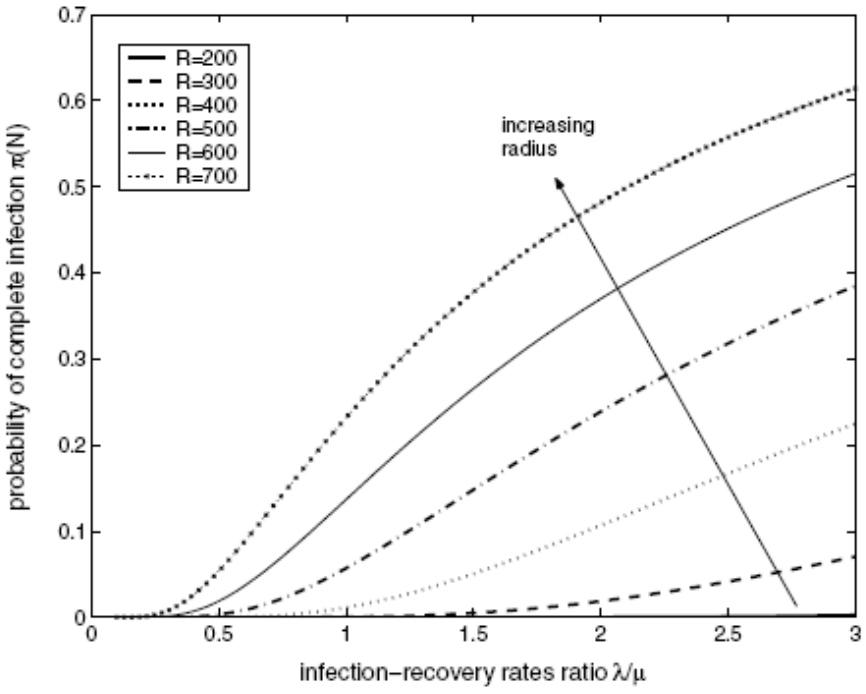
όλων των παραμέτρων σε τέτοια δίκτυα, στην αρχή της διαδικασίας θεωρείται μόνο ένας κακόβουλος χρήστης, ο οποίος επιτυγχάνει να μολύνει ένα υποσύνολο των N νόμιμων κόμβων, οι οποίοι με τη σειρά τους λειτουργούν ως κακόβουλοι. Η περιοχή δικτύου θεωρείται όπως και πριν τετραγωνική με πλευρά L.

Το Διάγραμμα 9 δείχνει τις προσεγγιστικές και ακριβείς τιμές της εργοδικής πιθανότητας απουσίας μολυσμένων κόμβων δικτύου για διάφορους συνδυασμούς παραμέτρων. Επειδή όλες οι εργοδικές πιθανότητες καταστάσεων εκφράζονται συναρτήσει της $\pi(0)$, πρέπει να σημειωθεί ότι αντίστοιχα συμπεράσματα με τα επόμενα μπορούν να εξαχθούν και για αυτές. Γίνεται φανερό ότι για τις συνήθεις τιμές των παραμέτρων το σφάλμα προσέγγισης είναι πρακτικά μηδενικό, ακόμα και για ακραίες τιμές της τάξης των 10-15 κόμβων (20 κόμβοι δικτύου είναι μια χαμηλή τιμή για συνήθη δίκτυα αισθητήρων και αυτοργανούμενα τύπου ad hoc) το σφάλμα παραμένει σε πολύ χαμηλά επίπεδα. Επιπρόσθετα, λόγω της παραπάνω παρατήρησης, αντίστοιχη μορφή θα έχουν και οι υπόλοιπες εργοδικές πιθανότητες καταστάσεων, έτσι ώστε η προσέγγιση που έγινε να είναι αποδεκτή και να μην έχει επίδραση στα συμπεράσματα που λαμβάνονται.



Διάγραμμα 9 – Επίδραση προσέγγισης στην πιθανότητα μη-μολυσμένων κόμβων $\pi(0)$ (σφάλμα προσέγγισης) συναρτήσει των κόμβων του δικτύου N

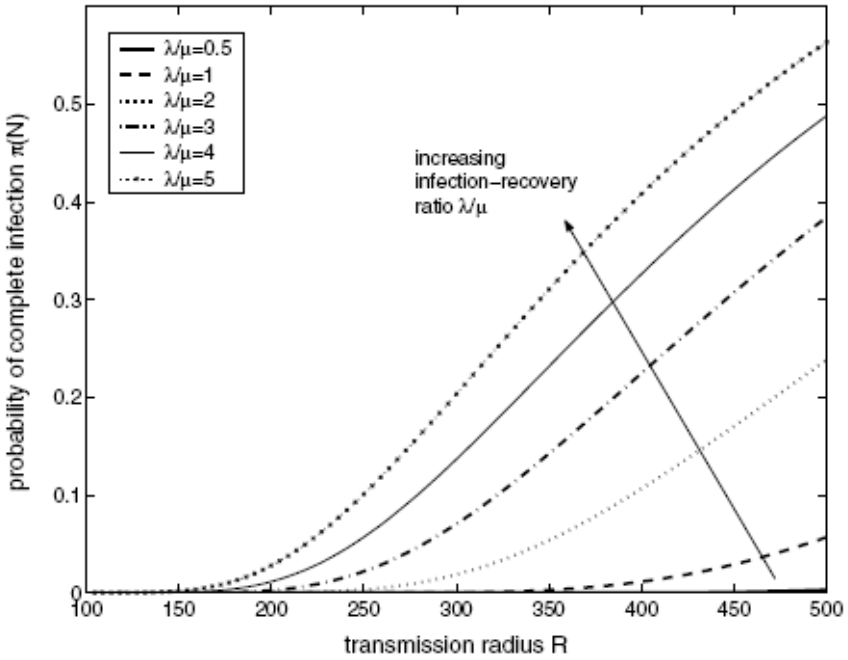
Η σημαντικότητα της πιθανότητας πανδημίας εξηγήθηκε προηγουμένως και για το λόγο αυτό στο Διάγραμμα 10 και Διάγραμμα 11 παρουσιάζεται ως συνάρτηση του λόγου λ/μ και της ακτίνας R αντίστοιχα. Στο πρώτο διάγραμμα φαίνεται η ισχυρή εξάρτηση από το λόγο του ρυθμού μόλυνσης προς το ρυθμό ανάκαμψης και από την ακτίνα μετάδοσης κόμβων. Από τη σκοπιά των κακόβουλων χρηστών η πανδημία αποτελεί τον απόλυτο στόχο, κάτι που όπως φαίνεται από τα αποτελέσματα είναι πολύ δύσκολο, αν λάβει κανείς υπόψη ότι για να πετύχει υψηλή πιθανότητα πανδημίας, πρέπει είτε να αυξήσει την ακτίνα μετάδοσης υπερβολικά (ώστε η αντίστοιχη κατανάλωση ενέργειας να είναι απαγορευτική για ρεαλιστική λειτουργία) ή να αυξήσει το λόγο του ρυθμού μόλυνσης προς το ρυθμό ανάκαμψης επίσης υπερβολικά (κάτι το οποίο συνεπάγεται σπατάλη πολλών πόρων για τη δημιουργία ιδιαίτερα επικίνδυνων απειλών λογισμικού και αντίστοιχο κόστος συντήρησης). Αντίστοιχη τάση διαφαίνεται και στο δεύτερο διάγραμμα, όπου όμως ο ρυθμός αύξησης της πιθανότητας πανδημίας ως συνάρτηση της ακτίνας μετάδοσης, εμφανίζεται λίγο χαμηλότερος σε σχέση με την αντίστοιχη περίπτωση του λόγου ρυθμού μόλυνσης προς ρυθμό ανάκαμψης κόμβων.



Διάγραμμα 10 – Πιθανότητα πανδημίας $\pi(N)$ συναρτήσει του λόγου λ/μ

Στο Διάγραμμα 12 φαίνεται η αναλυτική έκφραση του μέσου πλήθους μολυσμένων κόμβων ως συνάρτηση του λόγου του ρυθμού μόλυνσης προς το ρυθμό

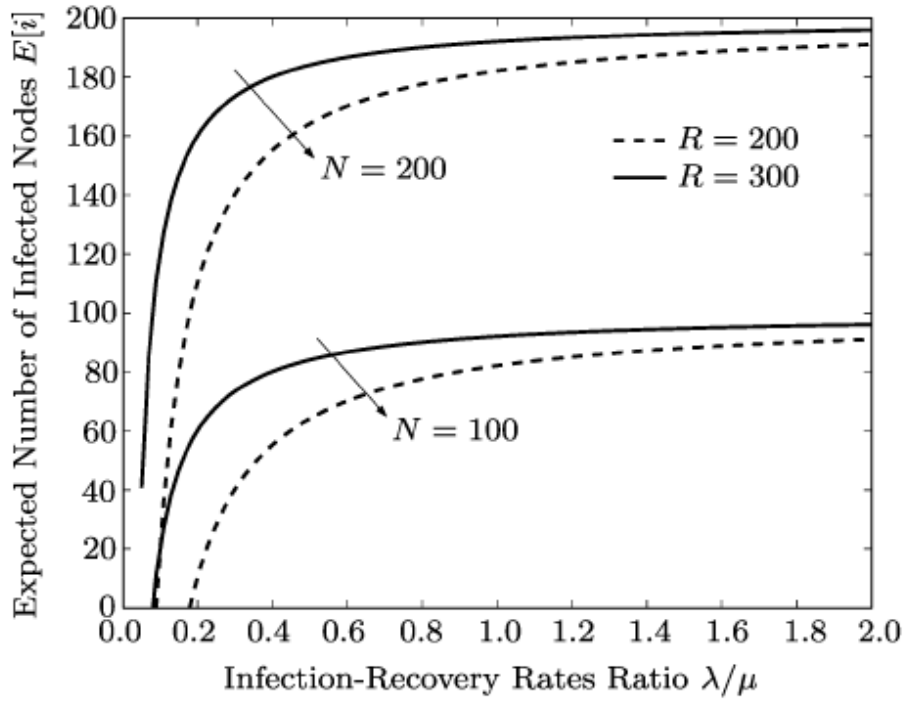
ανάκαμψης για διαφορετικές τιμές της ακτίνας μετάδοσης και δίκτυα διαφορετικού αριθμού νόμιμων κόμβων. Η συμπεριφορά είναι παρόμοια με την περίπτωση δικτύων μη-διασποράς, το οποίο επιβεβαιώνει το διαισθητικό αποτέλεσμα που προαναφέρθηκε ότι ένα δίκτυο διασποράς κατά βάση είναι μια περίπτωση δικτύου μη-διασποράς με πολλαπλούς κακόβουλους χρήστες, κατάλληλα τροποποιημένο όσον αφορά τους πληθυσμούς των διαφορετικών ομάδων κόμβων, κάνοντας τη θεώρηση ότι οι κόμβοι δικτύου που έχουν μολυνθει διαδραματίζουν το ρόλο κακόβουλων χρηστών.



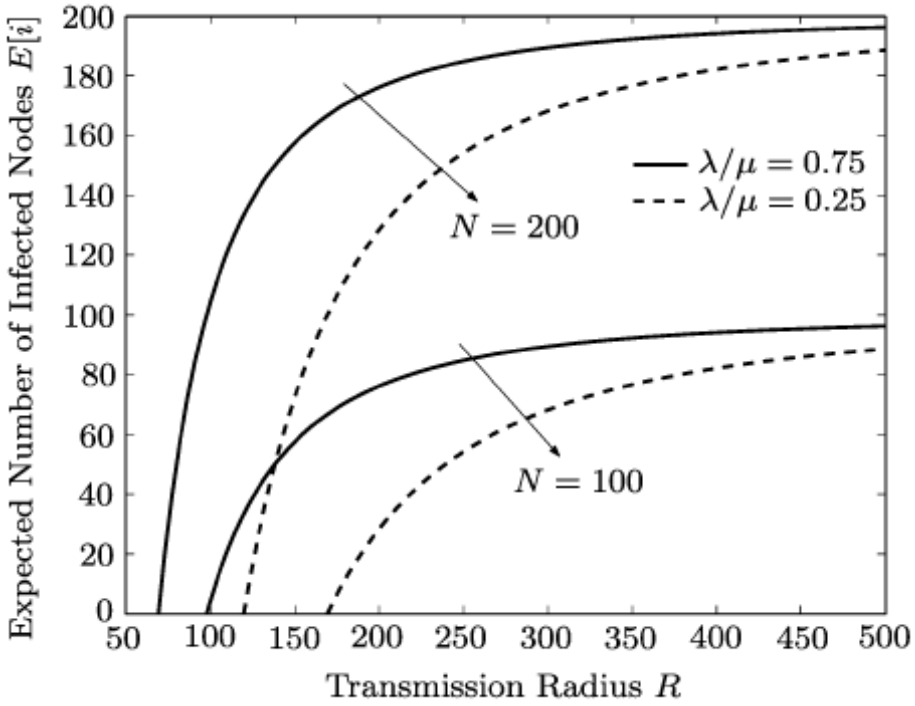
Διάγραμμα 11 – Πιθανότητα πανδημίας $\pi(N)$ συναρτήσει της ακτίνας μετάδοσης R

Στο Διάγραμμα 13 παρουσιάζεται το μέσο πλήθος μολυσμένων κόμβων συναρτήσει της ακτίνας μετάδοσης. Η μορφή της συνάρτησης είναι παρόμοια με την παραπάνω περίπτωση με διαφορά στην ευαισθησία ως προς τον αριθμό των κόμβων δικτύου, δηλαδή στο βαθμό που μια μεταβολή στο R, αλλάζει το μέσο πλήθος μολυσμένων κόμβων. Για πολύ χαμηλές τιμές του R, η επίδραση μπορεί πράγματι να είναι μεγάλη, για συνήθεις και υψηλές τιμές όμως η επίδραση ελαττώνεται σημαντικά. Επίσης σημαντική διαφορά παρατηρείται μεταξύ δύο διαφορετικών σεναρίων δικτύων, αναφορικά με τον αριθμό των κόμβων τους και επομένως την πυκνότητά τους. Στο δίκτυο με διπλάσιους νόμιμους κόμβους (διπλάσια πυκνότητα), η διαφορά στην επίδοση δεν είναι αντίστοιχα διπλάσια, αλλά ακόμα μεγαλύτερη καταδεικνύοντας το συμπέρασμα ότι πυκνότερα δίκτυα ευνοούν περισσότερο τη

διάδοση/διασπορά κακόβουλου λογισμικού. Τέτοια συμπεριφορά είναι αποτέλεσμα διαδικασιών κατωφλίων, όπως ήδη φάνηκε σε προγενέστερες μεθόδους με την εμφάνιση επιδημικών κατωφλίων.

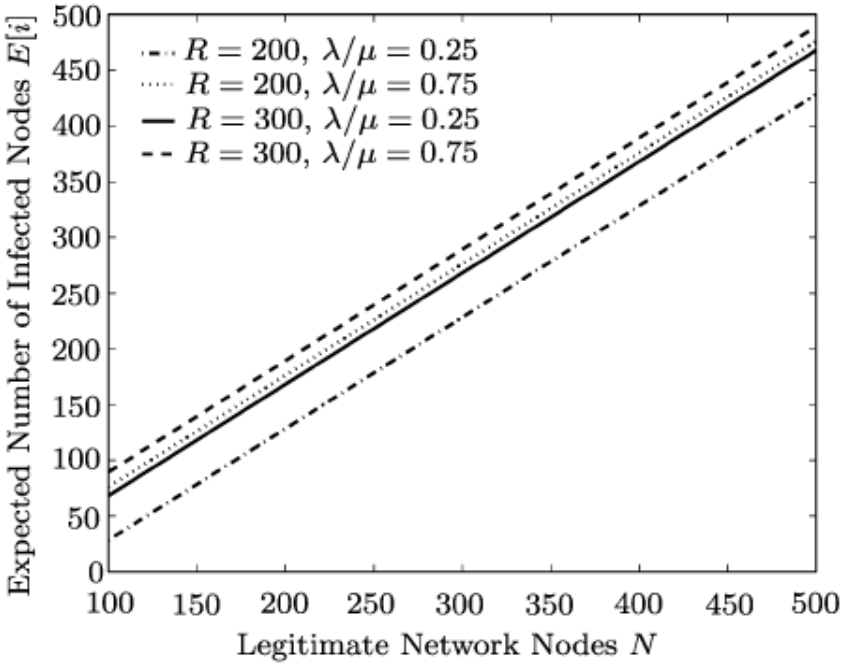


Διάγραμμα 12 – Μέσος αριθμός μολυσμένων κόμβων $E[i]$ συναρτήσει του λόγου λ / μ



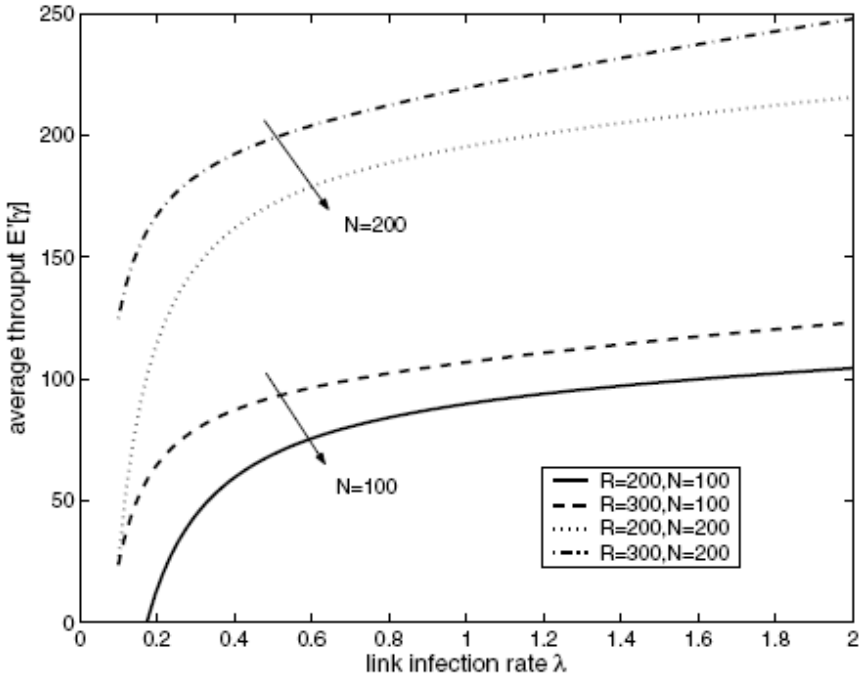
Διάγραμμα 13 – Μέσος αριθμός μολυσμένων κόμβων $E[i]$ συναρτήσει ακτίνας μετάδοσης R

Στο Διάγραμμα 14 φαίνεται η αντίστοιχη μεταβολή συναρτήσει του αριθμού των κόμβων δικτύου. Αντίθετα με τις άλλες παραμέτρους η εξάρτηση είναι πλέον γραμμική. Αύξηση της ακτίνας μετάδοσης των κακόβουλων χρηστών ή του λόγου λ/μ οδηγεί σε αντίστοιχη αύξηση του αριθμού των μολυσμένων κόμβων. Ωστόσο μεταξύ των δύο, ο λόγος λ/μ έχει μεγαλύτερη επίδραση από την ακτίνα μετάδοσης, όπως φαίνεται από τα δύο ενδιάμεσα σενάρια του διαγράμματος, όπου εκείνο με μεγαλύτερο λ/μ υπερτερεί του σεναρίου με μεγαλύτερο αριθμό κόμβων δικτύου.

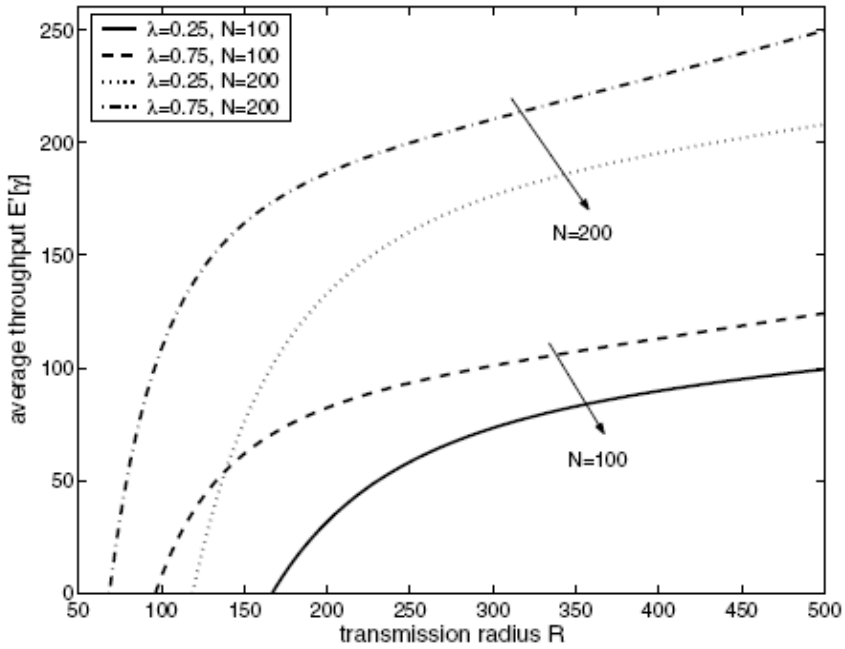


Διάγραμμα 14 – Μέσος αριθμός μολυσμένων κόμβων συναρτήσει πλήθους κόμβων δικτύου N

Στο Διάγραμμα 15 παρουσιάζεται ο μέσος συνολικός ρυθμός μόλυνσης κόμβων ως συνάρτηση του ρυθμού διάδοσης κακόβουλου λογισμικού στους κόμβους. Τα αποτελέσματα ακολουθούν την ίδια τάση με τον αναμενόμενο αριθμό μόλυνσης κόμβων με επακόλουθο να ισχύουν τα ίδια συμπεράσματα σε σχέση με την επίδραση των παραμέτρων στο αποτέλεσμα της διασποράς, καθώς και τον τρόπο που θα επηρέαζαν τη σχεδίαση στρατηγικών διάδοσης λογισμικού. Αξίζει να παρατηρηθεί και σε αυτή την περίπτωση η ύπαρξη μιας τιμής κατωφλίου του λόγου του ρυθμού μόλυνσης προς το ρυθμό ανάκαμψης, πάνω από την οποία το επιπρόσθετο κέρδος δεν είναι σημαντικό, ειδικά λαμβάνοντας υπόψη το αυξημένο κόστος που υπεισέρχεται σε τέτοιες περιπτώσεις.



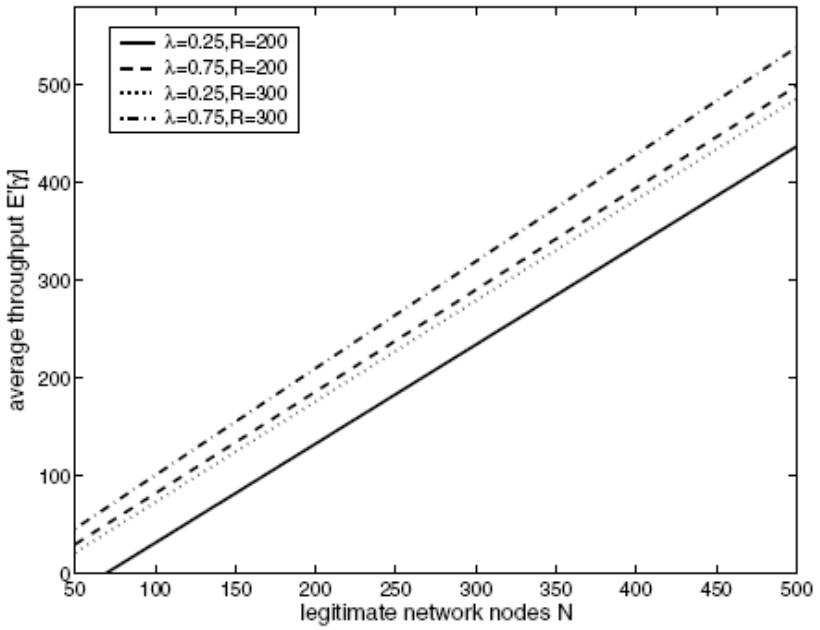
Διάγραμμα 15 – Μέσος συνολικός ρυθμός μόλυνσης κόμβων $E'[\gamma]$ συναρτήσει ρυθμού μετάδοσης λ



Διάγραμμα 16 – Μέσος συνολικός ρυθμός μόλυνσης κόμβων $E'[\gamma]$ συναρτήσει ακτίνας μετάδοσης R

Στο Διάγραμμα 16 παρουσιάζεται ο μέσος συνολικός ρυθμός μόλυνσης κόμβων ως συνάρτηση της ακτίνας μετάδοσης. Από τη μορφή του διαγράμματος γίνεται εμφανής η ομοιότητα με την περίπτωση των δικτύων μη-διασποράς, και τον

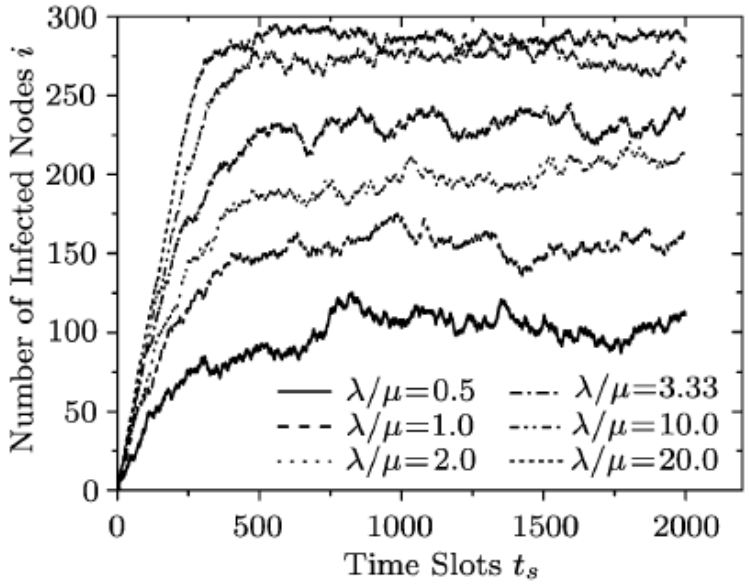
αναμενόμενο αριθμό μολυσμένων κόμβων. Επομένως, οι ίδιες παρατηρήσεις σε σχέση με την επίδραση των παραμέτρων στη διάδοση μπορούν να υιοθετηθούν και να ληφθούν υπόψη στη μελέτη τέτοιων προβλημάτων από τη σκοπιά του κακόβουλου χρήστη ή του διαχειριστή δικτύου. Στο Διάγραμμα 17 παρατίθεται ο μέσος συνολικός ρυθμός μόλυνσης κόμβων ως συνάρτηση του αριθμού των νόμιμων κόμβων του δικτύου. Σε αυτή την περίπτωση παρατηρείται γραμμική μεταβολή καθώς ο αριθμός των κόμβων αυξάνει, ωστόσο η επίδραση του ρυθμού μόλυνσης λ φαίνεται να είναι μεγαλύτερη σε σχέση με την ακτίνα μετάδοσης R. Κάτι τέτοιο μπορεί άμεσα να χρησιμοποιηθεί για τη σχεδίαση προσαρμοστικών στρατηγικών κακόβουλου λογισμικού.



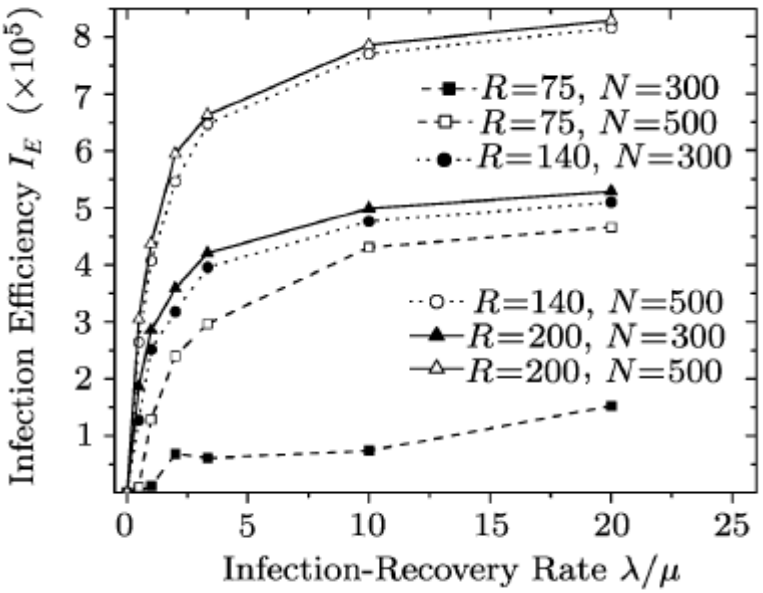
Διάγραμμα 17 – Μέσος συνολικός ρυθμός μόλυνσης κόμβων $E'[\gamma]$ συναρτήσει των νόμιμων κόμβων δικτύου N

Στο Διάγραμμα 18 παρουσιάζεται η χρονική εξέλιξη του αριθμού των μολυσμένων κόμβων δικτύου, όπως προέκυψε σε διάφορα στιγμιότυπα προσομοίωσης 2000 χρονικών στιγμών για διαφορετικές τιμές του λόγου λ/μ. Από το διάγραμμα γίνεται εμφανής η ύπαρξη ενός μεταβατικού φαινομένου στην αρχή κάθε σεναρίου, μετά το πέρας του οποίου ο αριθμός των μολυσμένων κόμβων μεταβάλλεται μεταξύ διαδοχικών χρονικών στιγμών, αλλά όχι σε σημαντικό βαθμό και γύρω από την εκάστοτε μέση τιμή που έχει για το συγκριμένο σενάριο. Το γεγονός αυτό επιβεβαιώνει το συμπέρασμα απότομης έναρξης της διάδοσης κακόβουλου λογισμικού που είχε επισημανθεί σε προηγούμενες εργασίες και είχε

μελετηθεί αναλυτικότερα σε αυτές. Αύξηση του λόγου ρυθμού μόλυνσης – ρυθμού ανάκαμψης, οδηγεί σε αύξηση του αριθμού των μολυσμένων κόμβων σε κάθε χρονική στιγμή, όσο όμως ο λόγος αυξάνει λαμβάνοντας μεγάλες τιμές, η αύξηση γίνεται μικρότερη, επειδή ήδη από μια τιμή του λόγου και πάνω οι μολύνσεις που προκύπτουν είναι πολλές σε σχέση με τις ανακάμψεις, ώστε να μην παρατηρείται τελικά σημαντική διαφορά στη συνολική συμπεριφορά της διάδοσης.



Διάγραμμα 18 – Εξέλιξη επίθεσης και αριθμού μολυσμένων κόμβων στο χρόνο (προσομοίωση)



Διάγραμμα 19 – Αποδοτικότητα Μόλυνσης για δίκτυα διασποράς (προσομοίωση)

Τέλος, στο Διάγραμμα 19 φαίνεται η Αποδοτικότητα Μόλυνσης ως συνάρτηση του λόγου ρυθμού μόλυνσης προς το ρυθμό ανάκαμψης για διαφορετικούς συνδυασμούς κόμβων δικτύου, ακτίνας μετάδοσης και κακόβουλων κόμβων. Η συμπεριφορά είναι παρόμοια με αυτή των δικτύων μη-διασποράς εκτός από παράγοντες κλιμάκωσης των τιμών που οφείλονται στις συγκεκριμένες θεωρήσεις και συνδυασμούς παραμέτρων. Όπως και πριν, αύξηση οποιασδήποτε παραμέτρου οδηγεί σε αύξηση της αποδοτικότητας μιας επίθεσης. Συγκρίνοντας μεταξύ της επίδρασης των παραμέτρων του συστήματος, γίνεται εμφανές ότι η επίδραση της ακτίνας είναι σημαντικότερη σε σχέση με τον αριθμό κόμβων δικτύου, ενώ ταυτόχρονα είναι άμεσα ελέγξιμη από την πλευρά των επιτιθέμενων, σε σχέση με τις υπόλοιπες μεταβλητές.

4.2 Βέλτιστες Στρατηγικές Επίθεσης

Έχοντας διαθέσιμες αναλυτικές εκφράσεις για τον αναμενόμενο αριθμό μολυσμένων κόμβων σε ένα δίκτυο, είναι δυνατόν να ορισθούν κατάλληλα προβλήματα βελτιστοποίησης, ώστε να καθοριστούν βέλτιστες στρατηγικές επίθεσης/άμυνας.

Στην παρούσα εργασία παρουσιάζεται η μέθοδος βελτιστοποίησης για την περίπτωση δικτύων μη-διασποράς, ακολουθώντας τη σκοπιά των κακόβουλων χρηστών και επομένως με γνώμονα την αποδοτικότητα μιας επίθεσης. Κάτι τέτοιο είναι επιτρεπτό μιας και υπάρχει διαθέσιμη η έκφραση των μεγεθών (αναμενόμενες τιμές αριθμού μολυσμένων κόμβων, συνολικού ρυθμού μόλυνσης κόμβων) συναρτήσει της ακτίνας κακόβουλων κόμβων. Ωστόσο, η διαδικασία μπορεί εύκολα να αντιστραφεί και να οδηγήσει σε βελτιστοποίηση της άμυνας του δικτύου, με βάση τη διαθεσιμότητα των αντίστοιχων εκφράσεων και συναρτήσει της ακτίνας μετάδοσης των νόμιμων κόμβων δικτύου.

Θεωρώντας τις αναμενόμενες τιμές του αριθμού των μολυσμένων κόμβων $E[i]$ και του συνολικού ρυθμού μόλυνσης κόμβων $E'[\gamma]$ ως μεταβλητές βελτιστοποίησης, ενώ οι υπόλοιπες μεταβλητές θεωρούνται ως σταθερές, μπορούν να οριστούν προβλήματα βελτιστοποίησης από την πλευρά των κακόβουλων χρηστών (μεγιστοποίησης) ή από την πλευρά του δικτύου (ελαχιστοποίησης). Ο στόχος των κακόβουλων χρηστών είναι να μεγιστοποιήσουν την επίδρασή τους, επομένως να μεγιστοποιήσουν τον αναμενόμενο αριθμό μολυσμένων κόμβων και τον αναμενόμενο

συνολικό ρυθμό μόλυνσης κόμβων του δικτύου. Και τα δύο αυτά προβλήματα μεγιστοποίησης έχουν τη μορφή:

$$\begin{aligned} \max \quad & \frac{cx_1x_2^2}{1+dx_1x_2^2} \\ s.t. \quad & 1 \le x_1 \le M_{\max} \\ & r_{\min} \le x_2 \le r_{\max} \\ & x_1, x_2 > 0 \end{aligned} \tag{56}$$

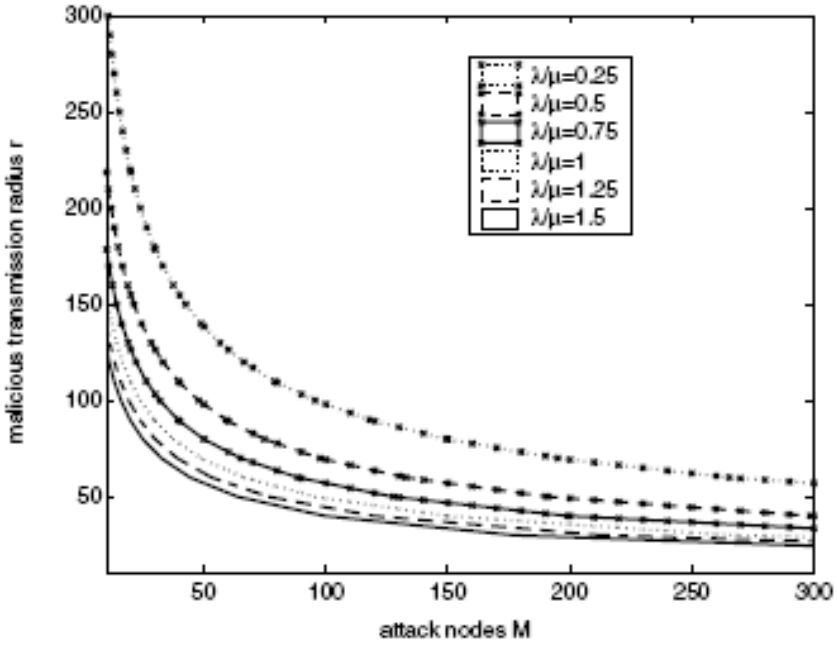
όπου η μεταβλητή x_1 αντιστοιχεί στον αριθμό των κακόβουλων κόμβων M, η x_2 αντιστοιχεί στην ακτίνα μετάδοσης των κακόβουλων κόμβων r και οι μεταβλητές $M_{\max}$, $r_{\min}$, $r_{\max}$ είναι σταθερές που υποδηλώνουν το μέγιστο αριθμό κακόβουλων κόμβων, την ελάχιστη και μέγιστη ακτίνα μετάδοσής τους αντίστοιχα. Η παράμετρος $d = \frac{\lambda\pi}{\mu L^2}$ είναι ίδια και για τα δύο προβλήματα μεγιστοποίησης, ενώ η παράμετρος c ορίζεται ως $c = \frac{\lambda\pi N}{\mu L^2}$ για το πρόβλημα βελτιστοποίησης του $E[i]$ και $c = \frac{\lambda\pi N}{L^2}$ για το πρόβλημα βελτιστοποίησης του $E'[\gamma]$. Στη γενική περίπτωση όπου οι κόμβοι είναι ενεργειακά περιορισμένοι, επιπρόσθετοι περιορισμοί μπορούν να προστεθούν στο πρόβλημα (56) και να οριστούν προβλήματα με παρόμοια μορφή.

Η αντικειμενική συνάρτηση $f(x_1, x_2) = \frac{cx_1x_2^2}{1+dx_1x_2^2}$ που έχει την ίδια μόρφή για τα δύο προβλήματα, είναι δύο φορές παραγωγίσιμη στο $\Re^2$ και επομένως ο πίνακας Hess της $f(x_1, x_2)$ μπορεί να υπολογισθεί με τυπικές μεθόδους. Ο πίνακας $H(x_1, x_2)$ της $f(x_1, x_2)$ είναι αρνητικά ορισμένος (negative definite) όταν η συνθήκη $3dx_1x_2^2 > 1$ ικανοποιείται. Σε αυτή την περίπτωση η συνάρτηση $f(x_1, x_2)$ είναι κοίλη (concave function) [70]. Επομένως, σε όρους παραμέτρων του δικτύου που μελετάται, η συνάρτηση $f(x_1, x_2)$ είναι κοίλη όταν ικανοποιείται η συνθήκη:

$$3\left(\frac{\lambda}{\mu}\right)\pi M > \left(\frac{L}{r}\right)^2 \tag{57}$$

Στο Διάγραμμα 20 παρουσιάζονται οι ισοσταθμικές καμπύλες της συνάρτησης $g(x_1, x_2) = 3\left(\frac{\lambda}{\mu}\right)\pi x_1 - \left(\frac{L}{x_2}\right)^2$ για $L = 1500m$ και διάφορες τιμές του λόγου $\frac{\lambda}{\mu}$. Οι

περιοχές του επιπέδου $[x_1, x_2]$ για τις οποίες ισχύει $g(x_1, x_2) > 0$ αντιπροσωπεύουν συνδυασμούς των παραμέτρων βελτιστοποίησης για τις οποίες η συνθήκη (57) ισχύει και επομένως η συνάρτηση $f(x_1, x_2)$ είναι κοίλη. Στο Διάγραμμα 20 αυτές οι περιοχές βρίσκονται πάνω από τις απεικονιζόμενες ισοσταθμικές καμπύλες. Επιπρόσθετα, παρατηρείται άμεσα ότι για τις συνήθεις τιμές ακτίνων μετάδοσης που χρησιμοποιούνται στην πράξη για τους κακόβουλους κόμβους ($200m \le r \le 300m$), η συνάρτηση $f(x_1, x_2)$ είναι κοίλη και επομένως μπορούν να χρησιμοποιηθούν τυπικές μέθοδοι αντιμετώπισης των προβλημάτων βελτιστοποίησης που ορίστηκαν.



Διάγραμμα 20 – Ισοσταθμικές καμπύλες στο επίπεδο $(0,0)$ **για τη συνάρτηση** $g(x_1, x_2)$

Για την αξιολόγηση του συστήματος και την παρουσίαση αποτελεσμάτων για την κατανόηση της λειτουργίας του, επιλέγεται $M_{\max} = 50$, το εύρος των ακτίνων μετάδοσης στο διάστημα $[r_{\min}, r_{\max}] = [200, 300]$ και η ακτίνα μετάδοσης των νόμιμων κόμβων $R = 200m$.

Η αντικειμενική συνάρτηση και των δύο προβλημάτων μεγιστοποίησης είναι κοίλη μέσα στο χώρο βελτιστοποίησης που καθορίζεται από τις παραπάνω τιμές των παραμέτρων. Επομένως, από τη μορφή της συνάρτησης και των περιορισμών που καθορίζει το πρόβλημα (56), η αναζήτηση βέλτιστης λύσης περιορίζεται σε ένα κλειστό χώρο που οριοθετείται από γραμμικούς περιορισμούς. Με βάση τυπικές

μεθόδους θεωρίας βελτιστοποίησης κυρτών συναρτήσεων [70], η βέλτιστη λύση βρίσκεται στις ακμές της συνοριακής επιφάνειας που οριοθετεί το χώρο αναζήτησης.

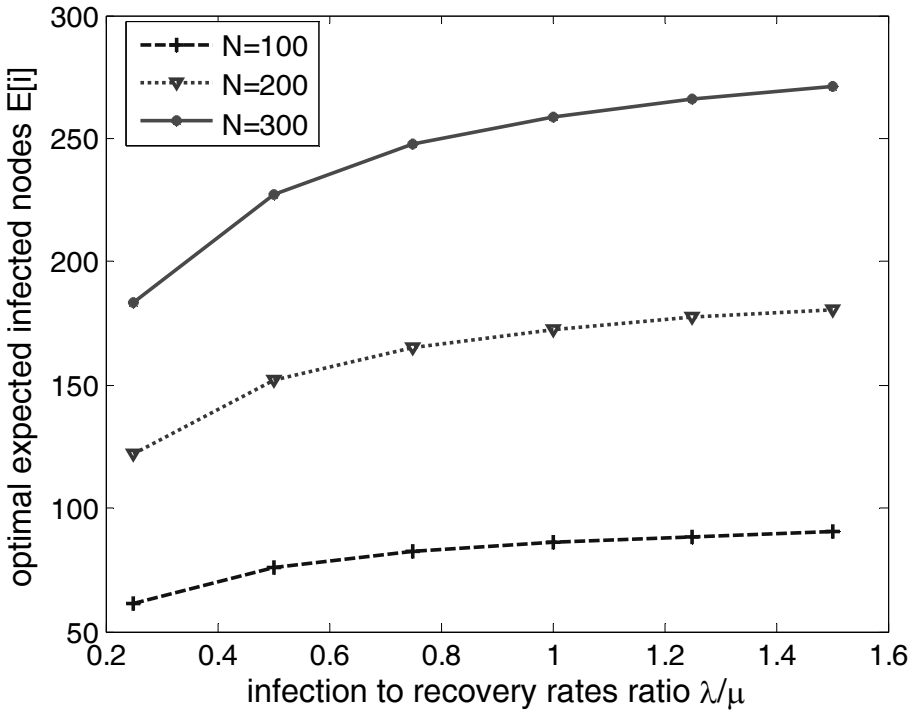
Η διαφορά ενός πολλαπλασιαστικού παράγοντα στην παράμετρο c μεταξύ των δύο αντικειμενικών συναρτήσεων επηρεάζει μόνο τη βέλτιστη τιμή της κάθε αντικειμενικής συνάρτησης στο σημείο της βέλτιστης λύσης και όχι το σημείο στο οποίο επιτυγχάνεται η λύση καθ' αυτή. Εφαρμόζοντας τη μέθοδο των πολλαπλασιαστών Lagrange [71], προκύπτει ότι η βέλτιστη λύση από τη σκοπιά των κακόβουλων χρηστών επιτυγχάνεται στο σημείο $\{x_1 = 50, x_2 = 300\}$, όπου οι μεταβλητές του προβλήματος ικανοποιούν τα πάνω όρια των περιορισμών του προβλήματος βελτιστοποίησης (56). Σε αυτή την περίπτωση η βέλτιστη στρατηγική που μεγιστοποιεί την επίδοση μιας στρατηγικής είναι $\{M = 50, r = 300\}$. Ο κάθε κακόβουλος χρήστης, εφόσον δεν έχει περιορισμούς ενέργειας, πρέπει να χρησιμοποιήσει τη μέγιστη δυνατή ακτίνα εκπομπής και όλοι οι διαθέσιμοι κακόβουλοι κόμβοι πρέπει να χρησιμοποιηθούν για τη μεγιστοποίηση της επίδρασης στο δίκτυο.

Θεωρώντας το χώρο λύσεων $\{x_1, x_2\}$ ως ένα σύστημα μεταβλητών ελέγχου η μορφή της βέλτιστης λύσης από τη σκοπιά των κακόβουλων χρηστών είναι τύπου bang-bang [72]. Αυτή η μορφή ελεγκτή καθορίζει δύο δυνατές καταστάσεις για μια μεταβλητή ελέγχου, μια κατάσταση όπου ο έλεγχος έχει την ελάχιστη τιμή και μια δεύτερη όπου ο έλεγχος λαμβάνει τη μέγιστη (συμπεριφορά ανοιχτού – κλειστού συστήματος, ON – OFF behavior). Στη συγκεκριμένη λύση ο έλεγχος (αριθμός κακόβουλων χρηστών, ακτίνα μετάδοσής τους) πρέπει να έχει τη μέγιστη κατά περίπτωση τιμή για τη μεγιστοποίηση της επίδρασης της διασποράς στο δίκτυο. Παρόλο που το αποτέλεσμα φαίνεται διαισθητικά απλό, είναι αρκετά σημαντικό μιας και αφενός οριοθετεί την επίδοση ενός μηχανισμού διάδοσης κακόβουλου λογισμικού, αφετέρου υποδηλώνει ότι σύνθετες τεχνικές ελέγχου των παραμέτρων δεν έχουν αναγκαστικά το βέλτιστο αποτέλεσμα, με την πλάστιγγα να γέρνει προς τις απλούστερες δυνατές.

Μεταξύ άλλων, τέτοια συμπεριφορά ελέγχου τύπου bang-bang είναι απόρροια της μοντελοποίησης της διάδοσης κακόβουλου λογισμικού με χρήση κλειστών δικτύων ουρών αναμονής [72]. Οι λύσεις των εργοδικών πιθανοτήτων καταστάσεων που προκύπτουν από συστήματα όπως αυτό των δύο εν σειρά ουρών με ανάδραση,

είναι τύπου γινομένου. Οι ρυθμαποδόσεις των ουρών και οι αναμενόμενες τιμές των πελατών στις ουρές είναι συναρτήσεις ανάλογες αυτών που μελετήθηκαν παραπάνω και συνήθως είναι κυρτές συναρτήσεις των μεταβλητών βελτιστοποίησης. Επομένως, οι λύσεις που επιδέχονται είναι παρόμοιες και οδηγούν σε πολιτικές ελέγχου των ουρών τύπου bang-bang [67],[72].

Παρόμοια αποτελέσματα έχουν προκύψει σε παρεμφερείς μελέτες ανίχνευσης κακόβουλου λογισμικού σε ασύρματα αυτοργανούμενα δίκτυα με έλεγχο ισχύος. [73]. Χρησιμοποιώντας ένα παρόμοιο πλαίσιο βελτιστοποίησης (δίκτυο επικοινωνιών, παράμετροι ελέγχου) σε διαφορετικό όμως μοντέλο μόλυνσης κόμβων (SIR), αποδεικνύεται ότι η βέλτιστη πολιτική ελέγχου για ανίχνευση (δυϊκό πρόβλημα επίθεσης) είναι τύπου bang-bang, καθορίζοντας μάλιστα και τρεις διαφορετικούς τύπους συγκεκριμένων ελεγκτών. Ο πρώτος από αυτούς είναι ο ίδιος με αυτόν του προβλήματος βελτιστοποίσης (56), καταδεικνύοντας ότι τα δύο προβλήματα μπορούν να ιδωθούν μέσα από το ίδιο πλαίσιο, απλά αντιστρέφοντας την οπτική γωνία κατά περίπτωση και κάνοντας τις αναγκαίες ερμηνείες των αποτελεσμάτων.

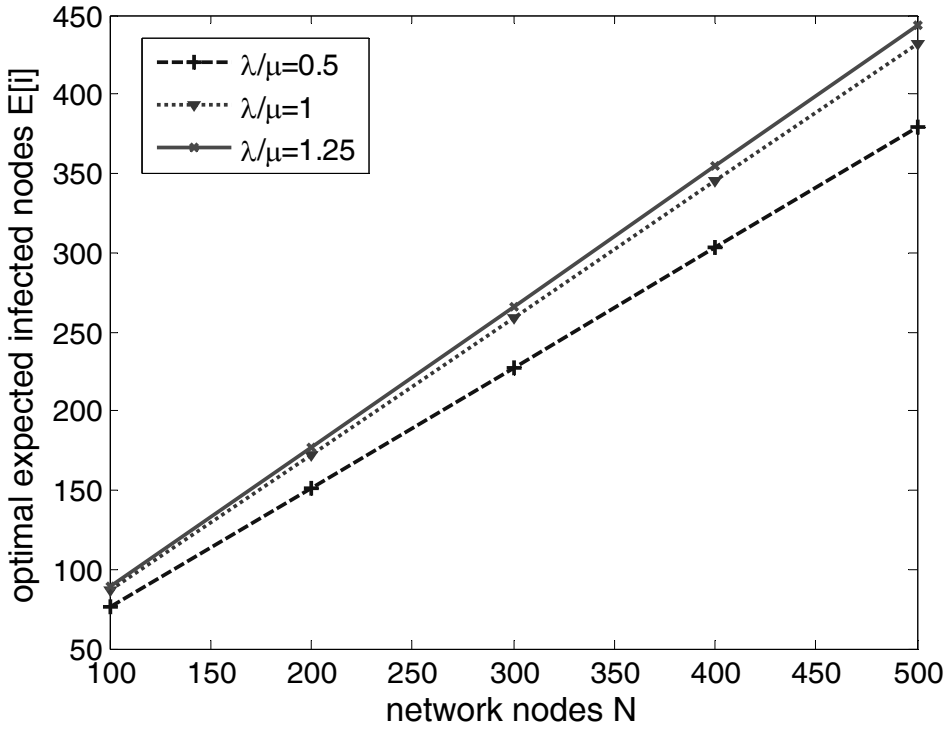


Διάγραμμα 21 – Βέλτιστες τιμές του αναμενόμενου αριθμού μολυσμένων κόμβων $E[i]$ συναρτήσει του λόγου λ / μ

Στην περίπτωση που υπήρχαν περιορισμοί ενέργειας, θα έπρεπε η αντικειμενική συνάρτηση να τροποποιηθεί, ώστε να λαμβάνει υπόψη την κατανάλωση ισχύος των κόμβων, καθώς και το κέρδος από την επίτευξη ενός συγκεκριμένου αριθμού μολυσμένων κόμβων/συνολικού ρυθμού μόλυνσης κόμβων. Κάτι τέτοιο θα άλλαζε και τη μορφή του προβλήματος, καθιστώντας τη σχεδίαση της νέας αντικειμενικής συνάρτησης (συνάρτηση χρησιμοποίησης – utility function) καθοριστική για την επίλυση του προβλήματος και την ερμηνεία/εφαρμογή των αποτελεσμάτων.

Στο Διάγραμμα 21 παρουσιάζονται οι βέλτιστες τιμές του αναμενόμενου αριθμού μολυσμένων κόμβων που θα μπορούσαν να επιτευχθούν με μια βέλτιστη στρατηγική επίθεσης για διαφορετικές περιπτώσεις δικτύων (διαφορετικό πλήθος κόμβων N) ως συνάρτηση του λόγου λ / μ.

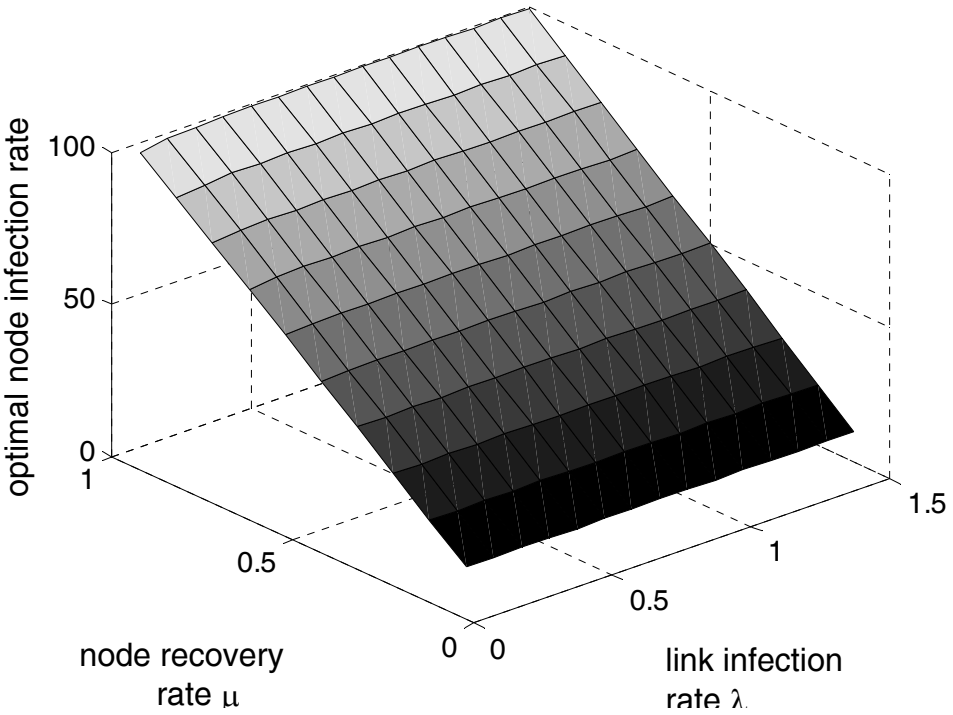
Στο Διάγραμμα 22 φαίνεται το ίδιο μέγεθος ως συνάρτηση του αριθμού των κόμβων του δικτύου N, δηλαδή ως συνάρτηση της πυκνότητας του δικτύου. Η διαφορά στην εξάρτηση μεταξύ των δύο παραμέτρων που δείχνονται στα διαγράμματα είναι εμφανής (γραμμική στη δεύτερη, ασυμπτωτικά εκθετική στην πρώτη).



Διάγραμμα 22 – Βέλτιστες τιμές του αναμενόμενου αριθμού μολυσμένων κόμβων $E[i]$ συναρτήσει του αριθμού νόμιμων κόμβων δικτύου N

Με αναφορά τα δύο διαγράμματα για τις βέλτιστες τιμές του αναμενόμενου αριθμού μολυσμένων κόμβων οριοθετούνται οι δυνατότητες μεθόδων διάδοσης κακόβουλου λογισμικού αναφορικά με τις αντίστοιχες παράμετρους. Παράλληλα τα αποτελέσματα αυτά μπορούν να χρησιμοποιηθούν για να σχεδιαστούν ευριστικοί (heuristic) αλγόριθμοι, οι οποίοι θα λειτουργούν υποβέλτιστα, αλλά με μικρότερο κόστος. Σύγκριση της επίδοσής τους με τα όρια επίδοσης που παρέχονται στα διαγράμματα είναι εφικτή και μπορεί να αποτελέσει αναφορά για την ορθή εξέταση προσεγγιστικών μεθόδων.

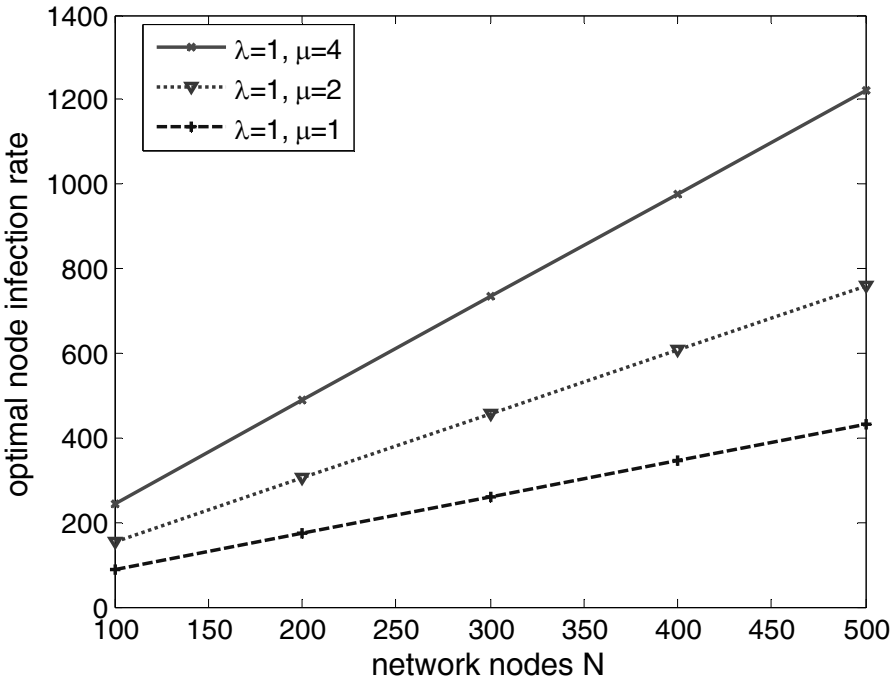
Στο Διάγραμμα 23 φαίνονται οι βέλτιστες τιμές του αναμενόμενου ρυθμού μόλυνσης κόμβων συναρτήσει του ρυθμού μόλυνσης λ και ανάκαμψης δικτύου κόμβων μ για ένα δίκτυο με $N = 100$ κόμβους. Αντίστοιχο διάγραμμα (κατάλληλα κλιμακωμένο) θα λαμβάνονταν στην περίπτωση διαφορετικών πυκνοτήτων δικτύου. Η εξάρτηση από τους ρυθμούς λ και μ είναι γραμμική, αλλά ο ρυθμός αύξησης διαφέρει μεταξύ των δύο παραμέτρων (ελαφρά μεγαλύτερος για το ρυθμό μ).



Διάγραμμα 23 – Βέλτιστες τιμές του αναμενόμενου ρυθμού μόλυνσης κόμβων $E'[\gamma]$ συναρτήσει των ρυθμών μόλυνσης λ, ανάκαμψης κόμβων μ

Τέλος, στο Διάγραμμα 24 φαίνονται τα ίδια αποτελέσματα συναρτήσει της πυκνότητας δικτύου. Παρόμοιες παρατηρήσεις ισχύουν όπως στο Διάγραμμα 23 και

σε αυτή την περίπτωση. Επιπρόσθετα, για αραιές τοπολογίες τα αποτελέσματα σχεδόν συγκλίνουν, οι διαφορές όμως μεταξύ διαφορετικών συνδυασμών παραμέτρων γίνονται περισσότερο εμφανείς καθώς η πυκνότητα αυξάνει.



Διάγραμμα 24 – Βέλτιστες τιμές του αναμενόμενου ρυθμού μόλυνσης κόμβων $E'[\gamma]$ συναρτήσει του αριθμού νόμιμων κόμβων δικτύου N

Κεφάλαιο 5

Έξυπνες Τεχνικές Διάδοσης Κακόβουλου Λογισμικού

Στο παρόν κεφάλαιο παρουσιάζονται και αναλύονται έξυπνες τεχνικές διάδοσης κακόβουλου λογισμικού που βασίζονται σε μεθόδους Ελέγχου Τοπολογίας (Topology Control – TC) και η σχεδίασή τους αποβλέπει σε επιθέσεις κυρίως σε ασύρματα αυτοργανούμενα δίκτυα και δίκτυα αισθητήρων [60]. Η παρουσίαση των προτεινόμενων τεχνικών που βασίζονται σε Έλεγχο Τοπολογίας ακολουθεί πρωτίστως το διαχωρισμό με βάση το στρώμα δικτύου στο οποίο λειτουργεί η εκάστοτε μέθοδος και κατά δεύτερον αναφορικά με την αύξηση της πολυπλοκότητας που παρουσιάζει η λειτουργία τους.

Ο Έλεγχος Τοπολογίας αποτελεί μια τεχνική έμμεσου ελέγχου των γειτόνων ενός κόμβου και κατά συνέπεια της τοπολογίας του δικτύου [74],[75],[76]. Ελέγχοντας με ηλεκτρονικό τρόπο την ισχύ εκπομπής τους οι κόμβοι μπορούν να μεταβάλλουν την ακτίνα μετάδοσής τους, και επομένως με αυτόν τον τρόπο να καθορίσουν τον αριθμό και το σύνολο των γειτόνων με τους οποίους μπορούν να ανταλλάξουν αξιόπιστα πακέτα, μεταβάλλοντας αντίστοιχα την τοπολογία του δικτύου.

Ο Έλεγχος Τοπολογίας αποτελεί ένα μηχανισμό συμβιβασμού μεταξύ της προσφερόμενης ισχυρής συνδετικότητας δικτύου που εξασφαλίζεται με μεγάλη ισχύ εκπομπής (και αντίστοιχη υψηλή κατανάλωση ενέργειας) και εξοικονόμησης ενεργειακών πόρων με χαμηλά επίπεδα παρεμβολής που συνοδεύουν τις χαμηλότερες ακτίνες μετάδοσης (Σχήμα 5). Μεταξύ άλλων, η ισχυρή συνδετικότητα επιτρέπει αντοχή του δικτύου σε σφάλματα ζεύξεων, ενώ χαμηλότερες ακτίνες μετάδοσης εξασφαλίζουν καλύτερη διαχείριση των παρεμβολών και χωρική επαναχρησιμοποίηση συχνοτήτων [76]. Ο Έλεγχος Τοπολογίας κατά βάση αποτελεί μια διαστρωματική τεχνική ελέγχου της υποκείμενης τοπολογίας δικτύου, όπου το στρώμα Ελέγχου Πρόσβασης στο Μέσο (MAC) αλληλεπιδρά με το στρώμα Δικτύου (Network) και αντίστροφα προκειμένου να εξασφαλιστεί η απρόσκοπτη λειτουργία

των υπηρεσιών που χρησιμοποιούν την εν λόγω υποδομή, χωρίς να παρατηρηθούν εμφανείς αλλαγές (όπως γίνεται με το μηχανισμό μεταγωγής στα κυψελωτά ασύρματα δίκτυα) [75]. Για αυτό το λόγο επιλέγεται η σχεδίαση μεθόδων Ελέγχου Τοπολογίας σε διαφορετικά στρώματα δικτύου και μελετώνται τα επακόλουθα και οι ιδιότητες καθεμιάς.

Σχήμα 5 – Ο Έλεγχος Τοπολογίας ως μηχανισμός συμβιβασμού μεταξύ εξοικονόμησης ενέργειας/μείωσης παρεμβολών και συνδετικότητας δικτύου

Στην παρούσα εργασία, ο Έλεγχος Τοπολογίας χρησιμοποιείται από τη σκοπιά του κακόβουλου χρήστη, προκειμένου να σχεδιαστεί και να αναγνωριστεί το εύρος της επίδρασης που μπορεί να έχει η λειτουργία ενός μεμονωμένου επιτιθέμενου ή μιας ομάδας σε ένα ασύρματο αυτοργανούμενο δίκτυο. Με βάση τα αποτελέσματα είναι δυνατόν να σχεδιαστούν αποδοτικά αντίμετρα και τα αντίστοιχα δίκτυα να προετοιμαστούν κατάλληλα για την αντιμετώπιση παρόμοιων στοχευμένων επιθέσεων. Πρόσφατες προσεγγίσεις έχουν ακολουθήσει την αντίστροφη πορεία, εφαρμόζοντας έλεγχο ισχύος (δηλαδή μια μορφή Έλέγχου Τοπολογίας) προκειμένου να ανοσοποιήσουν το δίκτυο νόμιμων κόμβων [73]. Βασιζόμενες στον ίδιο μηχανισμό του Ελέγχου Τοπολογίας, επιχειρούν να σχεδιάσουν βέλτιστες στρατηγικές ανοσοποίησης ασύρματων δικτύων

Στον παρακάτω πίνακα (Πίνακας 1) συνοψίζονται όλες οι μέθοδοι που βασίζονται σε Έλεγχο Τοπολογίας και μελετώνται στην παρούσα εργασία με βάση το στρώμα δικτύου στο οποίο λειτουργούν. Επίσης παρατίθεται το αναγνωριστικό κάθε μεθόδου, ώστε να είναι εύληπτα τα αποτελέσματα της μελέτης που παρουσιάζονται στη συνέχεια.

Από τα παραπάνω, γίνεται φανερό ότι ο Έλεγχος Τοπολογίας είναι από μόνος του ένας μηχανισμός βελτίωσης της λειτουργίας ενός δικτύου, είτε πρόκειται για το δίκτυο νόμιμων κόμβων, οπότε η βελτίωση αφορά στην παροχή ποιότητας υπηρεσίας (Quality of Service – QoS), είτε για το δίκτυο των κακόβουλων χρηστών, το οποίο

χρησιμοποιεί το δίκτυο των νόμιμων κόμβων και η βελτίωση έγκειται στη μόλυνση περισσότερων κόμβων δικτύου, για μεγαλύτερο χρονικό διάστημα.

Πίνακας 1 – Έξυπνες μέθοδοι διάδοσης κακόβουλου λογισμικού βασισμένες στο μηχανισμό του Ελέγχου Τοπολογίας

Στρώμα	Όνομα Μεθόδου	Αναγνωριστικό
Φυσικό - PHY	Ενεργειακός Έλεγχος Τοπολογίας	*NRGbased*
Ελέγχου Πρόσβασης στο Μέσο - MAC	Τυχαίου Ύπνου – ομοιόμορφη κατανομή	*RS-u*
	Τυχαίου Ύπνου – εκθετική κατανομή	*RS-e*
	Διαφορετικό Σχήμα Ύπνου – ομοιόμορφη κατανομή	*DRSS-u*
	Διαφορετικό Σχήμα Ύπνου – εκθετική κατανομή	*DRSS-e*
	Κοινό Σχήμα Ύπνου – ομοιόμορφη κατανομή	*CRSS-u*
	Κοινό Σχήμα Ύπνου – εκθετική κατανομή	*CRSS-e*
Δικτύου - NET	Τοπικής Πληφορορίας χωρίς Γνώση Τοπολογίας	*LINT*
	K – Γειτόνων	*Kneigh*

Ωστόσο, υπό το πρίσμα της ανάλυσης που παρουσιάστηκε στο προηγούμενο κεφάλαιο με το δίκτυο κλειστών ουρών, οι τεχνικές διάδοσης που βασίζονται σε Έλεγχο Τοπολογίας αποκτούν μεγαλύτερη βαρύτητα και σχεδόν φαίνονται ως άμεσο επακόλουθο της ανάλυσης που προέκυψε. Οι σημαντικοί παράγοντες που αναγνωρίστηκαν στην ανάλυση της διάδοσης κακόβουλου λογισμικού και κατά βάση καθορίζουν την έκβαση μιας επίθεσης (ακτίνα μετάδοσης, πυκνότητα κόμβων) είναι τοπολογικού χαρακτήρα και μάλιστα τοπικού. Κατά συνέπεια μέθοδοι οι οποίες βασίζουν τη λειτουργία τους στη διαθέσιμη τοπική πληροφορία τοπολογίας και τη διαθέσιμη ενέργεια (όπως είναι αυτές του Ελέγχου Τοπολογίας που ακολουθούν), αναμένεται να είναι περισσότερο αποδοτικές από άλλες που λειτουργούν υπό άλλα πλαίσια. Για αυτό το λόγο, η παρούσα διατριβή αρχικά εστιάζει σε τέτοιου είδους προσεγγίσεις.

5.1 Τεχνικές Φυσικού Στρώματος

Διάφορες παράμετροι του φυσικού στρώματος θα μπορούσαν να χρησιμοποιηθούν για την αξιολόγηση της ποιότητας των ζεύξεων μεταξύ κόμβων

δικτύου, έτσι ώστε να γίνει εφικτή η υλοποίηση αλγορίθμων Ελέγχου Τοπολογίας. Στα ασύρματα αυτοργανούμενα δίκτυα και δίκτυα αισθητήρων η διαθέσιμη υπολογιστική ισχύς είναι περιορισμένη (ειδικά στην περίπτωση δικτύων αισθητήρων), εστιάζοντας το σχεδιαστικό ενδιαφέρον στην παρακολούθηση παραμέτρων και μεθόδων που μπορούν να οδηγήσουν σε γρήγορες αποφάσεις με άμεσο επακόλουθο στην επίδοση των συστημάτων.

Η πρώτη τεχνική βασιζόμενη σε Έλεγχο Τοπολογίας, αναφέρεται ως Έλεγχος Τοπολογίας βασιζόμενος στην ενέργεια (Energy-based Topology Control – NRGbased) και χρησιμοποιεί πληροφορία του φυσικού στρώματος για την τροποποίηση της τοπολογίας του κόμβου. Για συντομία στη συνέχεια θα αναφερόμαστε σε αυτή την προσέγγιση ως Ενεργειακός Έλεγχος Τοπολογίας. Συγκεκριμένα, σε αυτό το σχήμα κάθε κόμβος έχει από κατασκευής διαθέσιμες δύο στάθμες εκομπής ισχύος, μια ονομαστική και μια μικρότερη, με αντίστοιχα καθορισμένες ακτίνες μετάδοσης (ως συνάρτηση του μοντέλου διάδοσης, κατωφλίων σηματοθορυβικού λόγου και σχημάτων κωδικοποίησης/διαμόρφωσης που χρησιμοποιούνται). Κάθε κόμβος ξεκινά με την κανονική ακτίνα μετάδοσης. Σε κάθε χρονική στιγμή μετράται το διαθέσιμο απόθεμα ενέργειας του εκάστοτε κόμβου και μόλις αυτό μειωθεί στο μισό του αρχικού, ο κόμβος αλλάζει στη μικρότερη ακτίνα μετάδοσης για το υπόλοιπο της λειτουργίας του.

Η λογική που διέπει αυτή την προσέγγιση προέρχεται από την παρατήρηση ότι η διάρκεια ζωής κάθε κακόβουλου κόμβου σε ένα δίκτυο με περιορισμένα αποθέματα ενέργειας μπορεί να αποβεί καθοριστική για την επίδοση ενός συγκεκριμένου σχήματος επίθεσης. Σε ένα δίκτυο με δομικά χαρακτηριστικά ή συμπεριφορά χρηστών που ευνοούν τη διάδοση κακόβουλου λογισμικού, ένας κακόβουλος χρήστης δεν χρειάζεται να σπαταλήσει ενέργεια για να μολύνει τοπικά και στιγμιαία πολλούς κόμβους. Με άλλα λόγια δεν έχει μεγάλο κέρδος εάν εξασφαλίσει ότι με μεγάλη πιθανότητα πολλαπλοί νόμιμοι γείτονές του θα μολυνθούν σε μια χρονική στιγμή, κάτι που θα συνέβαινε αν είχε μεγάλη ακτίνα μετάδοσης. Το αντίθετο συμβαίνει στην περίπτωση που το κακόβουλο λογισμικό δεν διαδίδεται εύκολα μέσω των κόμβων του δικτύου που έχουν ήδη μολυνθεί, λόγω τοπολογικών χαρακτηριστικών ή προβλεπόμενης προετοιμασίας των νόμιμων κόμβων. Τότε είναι περισσότερο αναγκαίο ένας κακόβουλος χρήστης να διατηρήσει (αν όχι να αυξήσει) την ακτίνα μετάδοσής του, ώστε να έχει περισσότερες πιθανότητες να διαδόσει το

λογισμικό του σε κάποιους κόμβους. Πρακτικά και στις δύο προσεγγίσεις ο κόμβος διαθέτει περίπου τον ίδιο αριθμό μολυσμένων γειτόνων, με τη διαφορά ότι στη δεύτερη περίπτωση αυτό γίνεται πολύ δυσκολότερα από την πρώτη και με περισσότερο κόστος.

Στον Ενεργειακό Έλεγχο Τοπολογίας ο κόμβος χρησιμοποιεί τις δυνατότητες που έχει (κανονική ακτίνα μετάδοσης) για να διαδόσει κακόβουλο λογισμικό σε όσο το δυνατόν περισσότερους κόμβους όσο τα αποθέματα ενέργειάς του είναι αρκετά. Αντίθετα, μόλις αυτά μειωθούν, ο κόμβος μειώνει την κατανάλωσή του και την αντίστοιχη επίδραση που μπορεί να έχει τοπικά στο δίκτυο, προκείμενου να αυξήσει περαιτέρω τη διάρκεια ζωής του. Σε αυτή την περίπτωση, η διάδοση στηρίζεται πλέον περισσότερο στους υπόλοιπους κακόβουλους χρήστες που βρίσκονται διεσπαρμένοι στο δίκτυο (αν πρόκειται για ομάδες κακόβουλων χρηστών) ή στους ήδη μολυσμένους κόμβους του δικτύου (στην περίπτωση μοναδικού κακόβουλου χρήστη και δικτύων διάδοσης). Με βάση αυτό το σκεπτικό ο Ενεργειακός Έλεγχος Τοπολογίας μπορεί άμεσα να εφαρμοστεί σε δίκτυα διασποράς κακόβουλου λογισμικού (πολλαπλών ή μοναδικού κακόβουλου χρήστη) και σε δίκτυα μη-διασποράς με πολλαπλούς κακόβουλους χρήστες, αναμένοντας εμφανή βελτίωση της αποδοτικότητας επίθεσης. Ωστόσο, στην περίπτωση στατικών δικτύων μη-διασποράς με μοναδικό κακόβουλο χρήστη, δεν είναι ξεκάθαρο αν ο Ενεργειακός Έλεγχος Τοπολογίας μπορεί να οδηγήσει σε βελτίωση, επειδή δεν υπάρχει άλλος τρόπος διάδοσης του λογισμικού στο υπόλοιπο δίκτυο. Αν και ο μοναδικός κακόβουλος χρήστης θα αυξήσει τη διάρκεια ζωής του, οι μολυσμένοι γείτονες που πλέον μένουν εκτός νέας ακτίνας μετάδοσης, έχουν τη δυνατότητα να ανακάμψουν οριστικά και επομένως συνολικά το δίκτυο θα έχει λιγότερους μολυσμένους κόμβους. Ο συνδυασμός αυξημένης διάρκειας ζωής με μειωμένη αποδοτικότητα μόλυνσης, δεν κλίνει ξεκάθαρα προς τη μια ή την άλλη κατεύθυνση με αποτελέσμα να μην είναι εκ των προτέρων ξεκάθαρο αν η μέθοδος ωφελεί τον κακόβουλο χρήστη.

Επεκτείνοντας αυτή τη λογική που αντιπροσωπεύει ο Ενεργειακός Έλεγχος Τοπολογίας θα μπορούσε κανείς να αυξήσει τις διατιθέμενες στάθμες ισχύος (και αντίστοιχες ακτίνες μετάδοσης), ώστε να ελέγχεται η τοπολογία μέσω της διαθέσιμης ενέργειας νωρίτερα από το κατώφλι μισής ενέργειας και να συνοδεύεται από αντίστοιχες κλιμακωτές αλλαγές στην ακτίνα μετάδοσης με βάση πολλαπλά κατώφλια ενέργειας. Στο όριο, θα μπορούσε κανείς να ορίσει ένα γραμμικό σχήμα

ελάττωσης της ακτίνας μετάδοσης σε σχέση με τη διατιθέμενη ενέργεια. Ένας εγγενής συμβιβασμός μεταξύ της τοπικής επίδρασης του κακόβουλου χρήστη και της επίδρασης που έχει η αυξημένη διάρκεια ζωής πρέπει να αντιμετωπιστεί από τα αντίστοιχα κλιμακωτά ή γραμμικά σχήματα και να χειριστεί κατάλληλα. Διάφορα σχήματα Ελέγχου Τοπολογίας βασιζόμενα στην ενέργεια (όπου η ακτίνα μεταβάλλεται ως συνεχής συνάρτηση της ενέργειας [77]) δοκιμάστηκαν σε σχέση με την απλή τεχνική δύο στάθμεων και διαπιστώθηκε ότι το απλό σχήμα με ένα κατώφλι έχει την υψηλότερη επίδοση αναφορικά με το μετρικό της Αποδοτικότητας Μόλυνσης. Επιπρόσθετα μια γραμμική ή κλιμακωτή μεταβολή της ισχύος εκπομπής στον κόμβο θα επέφερε επιπρόσθετο κόστος μεταγωγής μεταξύ των διατιθέμενων ακτίνων μετάδοσης, το οποίο θα λειτουργούσε ανταγωνιστικά με τη λογική της μείωσης της ακτίνας εκπομπής προκειμένου να ελαττωθεί η κατανάλωση ενέργειας και να παραμείνει ο κόμβος ενεργός για περισσότερη ώρα. Επομένως μόνο το απλό σχήμα δύο ακτίνων μετάδοσης και μοναδικού κατωφλίου ενέργειας, χρησιμοποιείται στη συνέχεια για τη σύγκριση με τα υπόλοιπα σχήματα επίθεσης Ελέγχου Τοπολογίας.

5.2 Τεχνικές Στρώματος MAC

Το στρώμα Ελέγχου Πρόσβασης στο Μέσο (Medium Access Control – MAC) σε ασύρματα 802.11 δίκτυα παρέχει εγγενώς δυνατότητες Ελέγχου Τοπολογίας στους κόμβους που το υιοθετούν. Οι καταστάσεις λειτουργίας που ορίζονται, εκτός της μετάδοσης πακέτου (transmission mode), λήψης πακέτου (receipt mode), της ακρόασης μέσου (promiscuous mode) και αδράνειας (idle mode), περιλαμβάνουν και μια κατάσταση παύσης λειτουργίας (sleep mode), όπου ο κόμβος παγώνει όλες τις λειτουργίες του και αδρανοποιείται πλήρως παραμένοντας σε αυτή την κατάσταση ένα προκαθορισμένο χρονικό διάστημα, μέχρι να επανέλθει στην κατάσταση κανονικής λειτουργίας [78]. Αυτή η δυνατότητα έχει χρησιμοποιηθεί πολλές φορές για τη σχεδίαση τεχνικών Έλέγχου Τοπολογίας στο παρελθόν [79],[80].

Στην κατάσταση παύσης λειτουργίας, ο κόμβος δεν επιτελεί καμία λειτουργία και πρακτικά είναι απών από το υπόλοιπο δίκτυο (δε συμμετέχει στην προώθηση πακέτων και τη συντήρηση της τοπολογίας του δικτύου με ανταλλαγή πακέτων ελέγχου). Η μοναδική συνιστώσα κατανάλωσης ενέργειας του κόμβου είναι αυτή των ηλεκτρονικών μονάδων που απαιτούνται για να αποφασιστεί ότι παρήλθε το χρονικό διάστημα της κατάστασης λειτουργίας παύσης και ο κόμβος πρέπει να μεταπηδήσει

στην κατάσταση κανονικής λειτουργίας. Η κατανάλωση κατάστασης παύσης λειτουργίας είναι η ελάχιστη δυνατή προκειμένου να συντηρηθεί η λειτουργία του κόμβου (διαφορετικά ο κόμβος θα έσβηνε και δεν θα μπορούσε να επανέλθει). Είναι τόσες τάξεις μεγέθους χαμηλότερη των υπόλοιπων συνιστωσών κατανάλωσης (μετάδοσης, λήψης, ακρόασης μέσου, αδράνειας), ώστε σε πολλές μελέτες (ακαδημαϊκές ή πρακτικές) να θεωρείται μηδενική, χωρίς σημαντική επίδραση στην ακρίβεια των αποτελεσμάτων [78],[81].

Χρησιμοποιώντας τη δυνατότητα κατάστασης παύσης, οι κόμβοι ενός αυτοργανούμενου δικτύου μπορούν να υλοποιήσουν μια μορφή Ελέγχου Τοπολογίας, καταλληλότερη για ασύρματα δίκτυα αισθητήρων και πολλαπλούς επιτιθέμενους κόμβους, εξαιτίας της ελάχιστης υπολογιστικής ισχύος που απαιτείται για την υλοποίησή της. Σε μια ομάδα κακόβουλων κόμβων διεσπαρμένων στην περιοχή ενός δικτύου, δεν είναι όλοι απαραίτητοι ταυτόχρονα για να επιτευχθεί υπολογίσιμη ζημιά. Μάλιστα, λόγω της τυχαίας κίνησης/κατανομής των κακόβουλων κόμβων, είναι πιθανό ορισμένοι κόμβοι να δρούν στην ίδια περιοχή, υπερκαλύπτοντας ο ένας τον άλλο και έτσι η συνδυασμένη τους λειτουργία να είναι ελάχιστα πιο αποδοτική από τη λειτουργία καθενός ξεχωριστά. Σε τέτοιες περιπτώσεις μπορούν ορισμένοι κόμβοι να τεθούν σε κατάσταση παύσης (sleep mode) προκειμένου να ελαχιστοποιήσουν την κατανάλωση ενέργειας και να χρησιμοποιηθούν αργότερα όταν αρχίσουν να μειώνονται τα αποθέματα των υπόλοιπων, όπως σε αντίστοιχα σχήματα Ελέγχου Τοπολογίας προοριζόμενα για επέκταση της διάρκειας ζωής του ασύρματου δικτύου, χωρίς σημαντική υποβάθμιση των προσφερόμενων δυνατοτήτων ποιότητας υπηρεσίας [79],[80]. Η διάδοση κακόβουλου λογισμικού στηρίζεται πλέον σε μικρότερο αριθμό κακόβουλων χρηστών, η στιγμιαία έλλειψη όμως σε πηγές κακόβουλου λογισμικού υπερκαλύπτεται από τη συνολικά μεγαλύτερη διάρκεια επίθεσης. Επειδή στην κατάσταση παύσης οι κόμβοι σβήνουν εντελώς το ασύρματο κομμάτι τους, διαγράφουν προσωρινά και όλους τους γείτονές τους, με απότελεσμα μια ακραία έκφανση του Ελέγχου Τοπολογίας στην οποία για ορισμένα χρονικά διαστήματα η τοπολογία για ένα κόμβο να είναι το κενό σύνολο.

Κατάλληλες τροποποιήσεις χρειάζονται για την εφαρμογή αυτής της ιδέας σε ασύρματα δίκτυα τύπου αισθητήρων ή αυτοργανούμενων ad hoc. Πιο συγκεκριμένα επειδή οι κόμβοι σε αυτά τα δίκτυα είναι συνήθως κινητοί, δεν είναι εφικτό να βρεθεί αποδοτικά το βέλτιστο σχήμα παύσης και επαναφοράς κόμβων, με βάση τις

επικαλύψεις που δημιουργούνται στην τοπολογία του δικτύου. Πιο αποδοτικά σχήματα για ασύρματα κινητά δικτύα, αναφορικά με την υπολογιστική πολυπλοκότητά τους και το χρόνο εκτέλεσης που απαιτούν, είναι αναγκαία σε αυτές τις περιπτώσεις. Πιο συγκεκριμένα, τα απαιτούμενα σχήματα πρέπει να είναι κατανεμημένα και να χρειάζονται την ελάχιστη δυνατή πληροφορία από το δίκτυο για να λειτουργήσουν.

Στην παρούσα εργασία προτείνονται απλά τυχαιοποιημένα σχήματα παύσης κόμβων με σκοπό την αύξηση της αποδοτικότητας επίθεσης, τα οποία μπορούν να εφαρμοστούν άμεσα σε ασύρματα δίκτυα ελλείψη κεντρικής υποδομής, κινητά ή στατικά. Η τυχαιοποίηση που ενσωματώνεται στα προτεινόμενα σχήματα γίνεται με σκοπό την καλύτερη ισορρόπηση των ρόλων που αναλαμβάνουν οι κακόβουλοι χρήστες που παραμένουν ενεργοί και την ομοιόμορφη εξάντληση των αποθεμάτων τους, ώστε η διάρκεια ζωής του δικτύου να αυξάνεται συνολικά. Στη συνέχεια, υποθέτουμε ένα SIS δίκτυο μη-διασποράς (δίκτυο αισθητήρων) με ένα σύνολο νόμιμων κόμβων $L=\{1,\ldots,N\}$ με ακτίνες R_i, $\forall i \in L$ και μια ομάδα κακόβουλων χρηστών $\mathrm{A}=\{1,\ldots,M\}$, με ακτίνες r_i, $\forall i \in A$ και δυνατότητα μεταβολής των ακτίνων τους κατά την έννοια του Ελέγχου Τοπολογίας.

5.2.1 Τεχνική Τυχαίου Ύπνου

Στην τεχνική Τυχαίου Ύπνου (Random Sleep – RS), κάθε κακόβουλος κόμβος λειτουργεί αυτόνομα και ανεξάρτητα από τους υπόλοιπους, επιλέγοντας τυχαία πότε θα μεταβεί στην κατάσταση ύπνου. Ο χρόνος συστήματος θεωρείται διαμερισμένος σε χρονο-σχισμές. Προβλήματα συγχρονισμού αναφορικά με τις θεωρούμενες σχισμές και κόμβους δεν μας απασχολούν στην παρούσα μελέτη και μια από τις πολλές σχετικές και αποδοτικές μεθόδους της βιβλιογραφίας θα μπορούσε να χρησιμοποιηθεί σε μια πρακτική υλοποίηση των σχημάτων [82],[83].

Στην αρχή κάθε χρονοσχισμής, ο κάθε κακόβουλος χρήστης επιλέγει τυχαία αν θα μεταβεί στην κατάσταση ύπνου ή θα συνεχίσει να λειτουργεί κανονικά. Η απόφαση μπορεί να λαμβάνεται με βάση οποιαδήποτε κατανομή πιθανότητας. Στην παρούσα εργασία εστιάζουμε σε δύο παραλλαγές κατανομών πιθανοτήτων.

Στην πρώτη, $RS-u(p)$, η επιλογή γίνεται με βάση την ομοιόμορφη κατανομή με πιθανότητα p. Έτσι στην αρχή κάθε χρονοσχισμής, ο κάθε κόμβος μεταβαίνει

στην κατάσταση ύπνου με πιθανότητα p και παραμένει ενεργός με πιθανότητα $1-p$.

Στη δεύτερη παραλλαγή, $RS-e\left(\frac{1}{\ell}\right)$, οι κόμβοι λαμβάνουν αποφάσεις με εκθετική πιθανότητα. Η απόφαση κάθε κόμβου για ύπνο λαμβάνεται με βάση την εκθετική κατανομή με παραμέτρο ℓ (και άρα μέσης τιμής $1/\ell$). Η εκθετική απόφαση αποβλέπει στον καθορισμό ενός διαφορετικού σχήματος ανάθεσης καταστάσεων των κόμβων που δίνει έμφαση προς μια κατεύθυνση. Για παράδειγμα, με βάση την παραμετροποίηση της εκθετικής κατανομής και το συγκεκριμένο τρόπο που χρησιμοποιείται για τη λήψη απόφασης, το τελικό σχήμα μπορεί να οδηγεί σε μεγαλύτερες διάρκειες ύπνου ή περισσότερο χρόνο κανονικής λειτουργίας. Τα αντίστοιχα σχήματα θα έχουν και διαφορετικά χαρακτηριστικά και επιδόσεις, ανάλογα με την έμφαση που προβλέπεται για κάθε κατάσταση από την αρχική παραμετροποίηση.

Για την ανάλυση των σχημάτων τυχαίου ύπνου θεωρείται ότι η διάρκεια παρακολούθησης του συστήματος είναι συνολικά S χρονικές σχισμές. Για κάθε κόμβο j, ορίζουμε την ενδεικτική συνάρτηση τυχαίας μεταβλητής (indicator function) $X_i^{(j)}$, ως εξής:

$$X_i^{(j)} = \begin{cases} 1, & \alpha\nu\ o\ \kappa\acute{o}\mu\beta o\varsigma\ j\ \kappa o\iota\mu\acute{a}\tau\alpha\iota\ \sigma\tau\eta\ \sigma\chi\iota\sigma\mu\acute{\eta}\ i \\ 0, & \alpha\nu\ o\ \kappa\acute{o}\mu\beta o\varsigma\ j\ \delta\epsilon\nu\ \kappa o\iota\mu\acute{a}\tau\alpha\iota\ \sigma\tau\eta\ \sigma\chi\iota\sigma\mu\acute{\eta}\ i \end{cases} \tag{58}$$

Επομένως για το σχήμα $RS-u(p)$, έχουμε εκ κατασκευής $\Pr\left\{X_i^{(j)}=1\right\}=p$ και $\Pr\left\{X_i^{(j)}=0\right\}=1-p$. Η μεταβλητή $X_i^{(j)}$ είναι τύπου Bernoulli με παράμετρο p και η αναμενόμενη τιμή της αντιστοιχεί στην πιθανότητα ο κόμβος j να βρίσκεται στην κατάσταση ύπνου στη χρονοσχισμή i. Επομένως:

$$E\left[X_i^{(j)}\right]=\Pr\left\{X_i^{(j)}=1\right\}\cdot 1+\Pr\left\{X_i^{(j)}=0\right\}\cdot 0=p,\quad \forall j\in A \tag{59}$$

επειδή όλοι οι κόμβοι αποφασίζουν ανεξάρτητα και οι αποφάσεις είναι ανεξάρτητα και παρόμοια κατανεμημένες.

Στη συνέχεια ορίζουμε την τυχαία μεταβλητή X_i που αναπαριστά το συνολικό αριθμό κόμβων σε κατάσταση ύπνου στη χρονοσχισμή i. Επομένως, θα έχουμε

$X_i = \sum_{j=1}^{M} X_i^{(j)}$. Χρησιμοποιώντας το τελευταίο και την (59), ο αναμενόμενος αριθμός κοιμισμένων κόμβων σε μια δεδομένη χρονοσχισμή, $E[X_i]$, είναι:

$$E[X_i] = E\left[\sum_{j=1}^{M} X_i^{(j)}\right] = \sum_{j=1}^{M} E\left[X_i^{(j)}\right] = \sum_{j=1}^{M} p = pM \tag{60}$$

Ορίζοντας την τυχαία μεταβλητή Y_j, ως το συνολικό αριθμό χρονοσχισμών στις οποίες ο κόμβος j είναι σε κατάσταση ύπνου, τότε $Y_j = \sum_{i=1}^{S} X_i^{(j)}$, $\forall j \in A$. Επομένως, η Y_j ακολουθεί τη διωνυμική κατανομή με παράμετρους S και p, και ο αναμενόμενος αριθμός χρονοσχισμών που ένας κόμβος βρίσκεται σε κατάσταση ύπνου, προκύπτει:

$$E[Y_j] = E\left[\sum_{i=1}^{S} X_i^{(j)}\right] = \sum_{i=1}^{S} E\left[X_i^{(j)}\right] = \sum_{i=1}^{S} p = pS \tag{61}$$

Λόγω της ομοιόμορφης κατανομής στη λήψη αποφάσεων, κάθε κόμβος βρίσκεται σε κατάσταση ύπνου για ένα ποσοστό p της διάρκειας ζωής του, όπως και το ποσοστό των κόμβων που βρίσκεται σε κάθε χρονοσχισμή στην κατάσταση ύπνου.

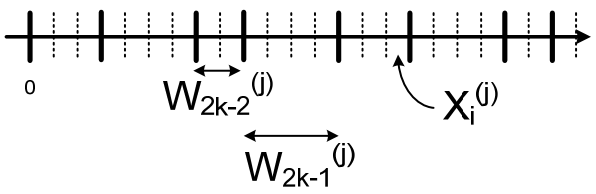
5.2.2 Τεχνική Τυχαιοποιημένων Σχημάτων Ύπνου

Στην τεχνική Τυχαιοποιημένων Σχημάτων Ύπνου (Random Sleep Schedule – RSS) ο μηχανισμός που ακολουθεί κάθε κόμβος ελέγχεται από μια κατανομή πιθανότητας. Οι κόμβοι παλινδρομούν μεταξύ κατάστασης ύπνου και κανονικής, ξεκινώντας από την τελευταία και η διάρκεια παραμονής στην κάθε κατάσταση καθορίζεται με βάση τις πιθανοτικές κατανομές κάθε σχήματος.

Δύο παραλλαγές που προκύπτουν άμεσα αναφορικά με τις χρησιμοποιούμενες κατανομές είναι οι τεχνικές Κοινού Σχήματος Ύπνου (Common Randomized Sleep Schedule – CRSS), στις οποίες ακριβώς η ίδια κατανομή, με τις ίδιες παραμέτρους χρησιμοποιείται για τον καθορισμό του χρόνου κανονικής λειτουργίας και κατάστασης ύπνου και οι τεχνικές Διαφορετικού Σχήματος Ύπνου (Different Randomized Sleep Schedule – DRSS), όπου η ίδια κατανομή με διαφορετικές παραμέτρους χρησιμοποιείται για τον καθορισμό των περιόδων κανονικής λειτουργίας και κατάστασης ύπνου.

Δύο διαφορετικές υλοποιήσεις των παραπάνω παραλλαγών, στηριζόμενες σε διαφορετικές κατανομές πυκνότητας πιθανότητας μελετώνται στην παρούσα εργασία. Όπως και στην περίπτωση του Τυχαίου Ύπνου, οι δύο κατανομές που χρησιμοποιούνται είναι η ομοιόμορφη και η εκθετική. Αμφότερες χρησιμοποιούνται για τον καθορισμό της διάρκειας διαδοχικών καταστάσεων λειτουργίας των κακόβουλων κόμβων.

Ο χρόνος για τις μεθόδους Τυχαιοποιημένων Σχημάτων Ύπνου θεωρείται συνεχής, για την απλοποίηση όμως της ανάλυσης μπορεί να διαιρεθεί σε πολύ μικρές χρονοσχισμές (mini-slots), ώστε κάθε μια να θεωρείται της τάξης μεγέθους της μονάδας μέτρησης χρόνου που υποτίθεται για τη λειτουργία του συστήματος. Η δεικτοδότηση των περιγραφόμενων μικρο-σχισμών χρόνου μπορεί να ακολουθεί αυτή της προσέγγισης Τυχαίου Ύπνου. Επομένως, η μεταβλητή $X_i^{(j)}$, χρησιμοποιείται όπως στην (58), για την αναπαράσταση της κατάστασης του κόμβου j στη χρονική μικρο-σχισμή i (Σχήμα 6).



Σχήμα 6 – Ανάλυση χρονισμού για τις μεθόδους Τυχαιοποιημένων Σχημάτων Ύπνου

Με αναφορά το Σχήμα 6, ορίζεται η τυχαία μεταβλητή $W_{2k-1}^{(j)}$ για $k=1,2,\ldots$, ως ο αριθμός των χρονικών μικρο-σχισμών κατά τις οποίες ο κόμβος j κοιμάται στο k-οστό διάστημα ύπνου. Παρόμοια ορίζεται η τυχαία μεταβλητή $W_{2k-2}^{(j)}$ για $k=1,2,\ldots$, ως ο αριθμός των χρονικών μικρο-σχισμών κατά τις οποίες ο κόμβος j βρίσκεται στην κατάσταση κανονικής λειτουργίας στο k-οστό διάστημα κανονικής λειτουργίας. Χωρίς βλάβη της γενικότητας, υποθέτοντας ότι οι κακόβουλοι κόμβοι ξεκινούν πάντα με χρονικό διάστημα κανονικής λειτουργίας, οι μεταβλητές $W_{2k-2}^{(j)}$ με άρτιους δείκτες αντιστοιχούν σε διαστήματα κανονικής λειτουργίας, ενώ οι μεταβλητές $W_{2k-1}^{(j)}$ με περιττούς δείκτες αναφέρονται σε διαστήματα λειτουργίας ύπνου των κακόβουλων χρηστών.

Αρχικά εστιάζουμε στην παραλλαγή Διαφορετικού Σχήματος Ύπνου με ομοιόμορφη κατανομή πιθανότητας ($DRSS-u(t_{\max},t'_{\max})$). Η τεχνική λειτουργεί με

δύο ομοιόμορφες κατανομές διαφορετικών παραμέτρων, $t_{\max}$ και $t'_{\max}$. Κάθε κακόβουλος χρήστης που την υλοποιεί επιλέγει με ομοιόμορφη κατανομή στο διάστημα $(0, t_{\max}]$ τη διάρκεια ενός διαστήματος κατάστασης ύπνου σε χρονικές μικρο-σχισμές και τη διάρκεια ενός διαστήματος κανονικής περιόδου με ομοιόμορφη κατανομή στο διάστημα $(0, t'_{\max}]$. Επομένως, οι μεταβλητές $W_{2k-1}^{(j)}$, $W_{2k-2}^{(j)}$ είναι κατανεμημένες ομοιόμορφα στα αντίστοιχα διαστήματα:

$$\begin{aligned} W_{2k-1}^{(j)} &\sim U\left[0, t_{\max}\right] \\ W_{2k-2}^{(j)} &\sim U\left[0, t'_{\max}\right] \end{aligned} \tag{62}$$

Οι αντίστοιχες αναμενόμενες μέσες τιμές προκύπτουν ως:

$$\begin{aligned} E\left[W_{2k-1}^{(j)}\right] &= \frac{t_{\max}}{2} \\ E\left[W_{2k-2}^{(j)}\right] &= \frac{t'_{\max}}{2} \end{aligned} \tag{63}$$

Υποθέτοντας ότι το σύστημα μελετάται για συνολικά S χρονικές μικρο-σχισμές (χρονική διάρκεια παρακολούθησης) και ότι μέσα σε ένα τέτοιο χρονικό διάστημα συνολικά λαμβάνουν χώρα $S_a^{(j)}$ αλλαγές μεταξύ καταστάσεων ύπνου/κανονικής λειτουργίας για τον κόμβο j, ο συνολικός χρόνος (αριθμός μικρο-σχισμών), στις οποίες ο κόμβος j ήταν σε κατάσταση ύπνου προκύπτει:

$$\sum_{i=1}^{S} X_i^{(j)} = \sum_{k=1}^{S_a^{(j)}} W_{2k-2}^{(j)} \tag{64}$$

Επιπρόσθετα, το άθροισμα του αριθμού των χρονικών μικρο-σχισμών στην κατάσταση ύπνου και κανονικής λειτουργίας μαζί για τον κόμβο j, δίνει το συνολικό αριθμό μικρο-σχισμών S:

$$\sum_{k=1}^{S_a^{(j)}} W_{2k-1}^{(j)} + \sum_{k=1}^{S_a^{(j)}} W_{2k-2}^{(j)} = S \tag{65}$$

Από την (64), λόγω γραμμικότητας του τελεστή αναμενόμενης τιμής μιας τυχαίας μεταβλητής, προκύπτει:

$$E\left[\sum_{i=1}^{S} X_i^{(j)}\right] = E\left[\sum_{k=1}^{S_a^{(j)}} W_{2k-1}^{(j)}\right]$$

$$\sum_{i=1}^{S} E\left[X_i^{(j)}\right] = \sum_{k=1}^{S_a^{(j)}} E\left[W_{2k-1}^{(j)}\right]$$

$$S \cdot E\left[X_i^{(j)}\right] = S_a^{(j)} \cdot E\left[W_{2k-1}^{(j)}\right]$$

$$S \cdot E\left[X_i^{(j)}\right] = S_a^{(j)} \frac{t_{\max}}{2}$$

το οποίο δίνει τελικά:

$$E\left[X_i^{(j)}\right] = S_a^{(j)} \frac{t_{\max}}{2S} \tag{66}$$

Επίσης από την (65), με εφαρμογή του γραμμικού τελεστή αναμενόμενης τιμής προκύπτει:

$$E\left[\sum_{k=1}^{S_a^{(j)}} W_{2k-1}^{(j)}\right] + E\left[\sum_{k=1}^{S_a^{(j)}} W_{2k-2}^{(j)}\right] = S$$

$$\sum_{k=1}^{S_a^{(j)}} E\left[W_{2k-1}^{(j)}\right] + \sum_{k=1}^{S_a^{(j)}} E\left[W_{2k-2}^{(j)}\right] = S$$

$$S_a^{(j)} \cdot E\left[W_{2k-1}^{(j)}\right] + S_a^{(j)} \cdot E\left[W_{2k-2}^{(j)}\right] = S$$

$$S_a^{(j)} \frac{t_{\max} + t'_{\max}}{2} = S$$

από το οποίο συνάγεται ότι:

$$S_a^{(j)} = \frac{2S}{t_{\max} + t'_{\max}} \tag{67}$$

Συνδυάζοντας τις (66), (67), η πιθανότητα ο κόμβος j να κοιμάται στη χρονική μικρο-σχισμή i, δίνεται από την αναμενόμενη τιμή της μεταβλητής $X_i^{(j)}$:

$$E\left[X_i^{(j)}\right] = \frac{t_{\max}}{t_{\max} + t'_{\max}} \tag{68}$$

Η έκφραση (68) είναι πανομοιότυπη για όλους τους κακόβουλους κόμβους $j \in A$, λόγω της ανεξαρτησίας του κάθε κόμβου στη λήψη αποφάσεων. Χρησιμοποιώντας αυτό το αποτέλεσμα, μπορούν εύκολα να προκύψουν ο αναμενόμενος αριθμός κακόβουλων χρηστών που κοιμούνται σε κάθε χρονική στιγμή i:

$$E\left[X_i\right] = E\left[\sum_{j=1}^{M} X_i^{(j)}\right] = \sum_{j=1}^{M} E\left[X_i^{(j)}\right] = M\,\frac{t_{\max}}{t_{\max} + t'_{\max}} \tag{69}$$

και ο αναμενόμενος αριθμός χρονικών μικρο-σχισμών που ο κόμβος j κοιμάται (ποσοστό χρόνου που ο κόμβος j περνά στην κατάσταση ύπνου):

$$E\left[Y_j\right] = E\left[\sum_{i=1}^{S} X_i^{(j)}\right] = \sum_{i=1}^{S} E\left[X_i^{(j)}\right] = S\,\frac{t_{\max}}{t_{\max} + t'_{\max}} \tag{70}$$

Στην τεχνική Διαφορετικού Σχήματος Ύπνου με εκθετική κατανομή πιθανότητας ($DRSS - e(\ell, \ell')$), οι τυχαίες μεταβλητές $W_{2k-1}^{(j)}$, $W_{2k-2}^{(j)}$ είναι κατανεμημένες εκθετικά με παραμέτρους ℓ και ℓ' αντίστοιχα:

$$\begin{aligned} W_{2k-1}^{(j)} &\sim \exp\left(\ell\right) \\ W_{2k-2}^{(j)} &\sim \exp\left(\ell'\right) \end{aligned} \tag{71}$$

Οι αντίστοιχες αναμενόμενες τιμές των τυχαίων μεταβλητών (71), προκύπτουν:

$$\begin{aligned} E\left[W_{2k-1}^{(j)}\right] &= \frac{1}{\ell} \\ E\left[W_{2k-2}^{(j)}\right] &= \frac{1}{\ell'} \end{aligned} \tag{72}$$

Όπως και στην περίπτωση του $DRSS - u(t_{\max}, t'_{\max})$ σχήματος, οι εξισώσεις (64) και (65), ισχύουν ως έχουν. Λαμβάνοντας υπόψη την εκθετική κατανομή των $W_{2k-1}^{(j)}$, $W_{2k-2}^{(j)}$ και ακολουθώντας την ίδια ανάλυση με βάση τη γραμμικότητα του τελεστή αναμενόμενης τιμής, όπως παραπάνω, προκύπτει:

$$E\left[X_i^{(j)}\right] = S_a^{(j)}\,\frac{1}{\ell \cdot S} \tag{73}$$

και

$$S_a^{(j)} = \frac{\ell\ell' S}{\ell + \ell'} \tag{74}$$

Συνδυάζοντας τις (73), (74), η πιθανότητα ο κόμβος j να βρίσκεται σε κατάσταση ύπνου τη χρονική μικρο-σχισμή i, δίνεται από την έκφραση:

$$E\left[X_i^{(j)}\right] = \frac{\ell}{\ell + \ell'} = \frac{1/\ell}{1/\ell + 1/\ell'} \tag{75}$$

Με βάση την τελευταία σχέση μπορεί να υπολογισθεί ο αναμενόμενος αριθμός κακόβουλων κόμβων στην κατάσταση ύπνου στη χρονική μικρο-σχισμή i:

$$E\left[X_i\right] = E\left[\sum_{j=1}^{M} X_i^{(j)}\right] = \sum_{j=1}^{M} E\left[X_i^{(j)}\right] = M\,\frac{\ell}{\ell+\ell'} \tag{76}$$

ενώ ο αναμενόμενος αριθμός χρονικών μικρο-σχισμών που ο κακόβουλος κόμβος j βρίσκεται στην κατάσταση ύπνου, δίνεται από:

$$E\left[Y_j\right] = E\left[\sum_{i=1}^{S} X_i^{(j)}\right] = \sum_{i=1}^{S} E\left[X_i^{(j)}\right] = S\,\frac{\ell}{\ell+\ell'} \tag{77}$$

Συγκρίνοντας τα ζεύγη αντίστοιχων εκφράσεων (68)-(75), (69)-(76) και (70)-(77) διαφαίνεται η στοχαστική ομοιότητα που διέπει τις δύο υλοποιήσεις της παραλλαγής Διαφορετικού Σχήματος Ύπνου (DRSS). Παρά τις διαφορετικές κατανομές που έχουν χρησιμοποιηθεί η συμπεριφορά των δύο σχημάτων διέπεται και στις δύο περιπτώσεις από τη σχέση μεταξύ των δύο παραμέτρων των κατανομών που έχουν χρησιμοποιηθεί σε κάθε υλοποίηση. Η μέση διάρκεια και ο αναμενόμενος αριθμός των κόμβων που βρίσκονται στην κατάσταση ύπνου σε κάθε χρονική στιγμή, καθορίζονται από τους σχετικούς λόγους των μέσων τιμών των κατανομών που χρησιμοποιούνται κατά περίπτωση. Υπενθυμίζεται ότι η κάθε κατανομή καθορίζει τη χρονική διάρκεια των επιμέρους διαστημάτων λειτουργίας κάθε κακόβουλου κόμβου (για την κανονική ή κατάσταση παύσης λειτουργίας). Έτσι η μέση διάρκεια κατάστασης ύπνου δίνεται από το λόγο της μέσης τιμής της κατανομής που ελέγχει τη διάρκεια κατάστασης ύπνου προς το άθροισμα των δύο μέσων τιμών των δύο κατανομών. Επομένως, διαπιστώνεται μια αναλογική σχέση στον καθορισμό της σχετικής διάρκειας κάθε κατάστασης με βάση την παράμετρο μέσης τιμής κάθε κατανομής.

Τα παραπάνω αποτελέσματα μπορούν εύκολα να επεκταθούν για τις παραλλαγές Κοινού Σχήματος Ύπνου (CRSS), τόσο για την ομοιόμορφη, όσο και για την εκθετική κατανομή. Στην πρώτη περίπτωση του $CRSS-u(t_{\max}, t_{\max})$, αρκεί να χρησιμοποιηθεί η ισότητα $t'_{\max} = t_{\max}$, ενώ στη δεύτερη περίπτωση του $CRSS-e(\ell,\ell)$, αρκεί η ανάθεση $\ell' = \ell$.

Με βάση τις παραπάνω συνθήκες για τις μεθόδους Κοινού Σχήματος Ύπνου, προκύπτει:

$$E\left[W_{2k-1}^{(j)}\right] = E\left[W_{2k-2}^{(j)}\right] = \frac{t_{\max}}{2} \tag{78}$$

για την περίπτωση του $CRSS - u(t_{\max}, t_{\max})$, και επίσης:

$$E\left[W_{2k-1}^{(j)}\right] = E\left[W_{2k-2}^{(j)}\right] = \frac{1}{\ell} \tag{79}$$

για το σχήμα $CRSS - e(\ell, \ell)$ αντίστοιχα.

Χρησιμοποιώντας τις εκφράσεις (78) και (79) για το $CRSS - u(t_{\max}, t_{\max})$ και $CRSS - e(\ell, \ell)$ αντίστοιχα, προκύπτουν εύκολα, η πιθανότητα ένας κόμβος j να βρίσκεται σε κατάσταση ύπνου στη χρονική μικρο-σχισμή i:

$$E\left[X_i^{(j)}\right]_{CRSS-u} = E\left[X_i^{(j)}\right]_{CRSS-e} = \frac{1}{2} \tag{80}$$

ο μέσος αριθμός κόμβων στην κατάσταση ύπνου σε μια τυχαία χρονική στιγμή (μικρο-σχισμή), που δίνεται από την αναμενόμενη τιμή της τυχαίας μεταβλητής X_i:

$$E\left[X_i\right]_{CRSS-u} = E\left[X_i\right]_{CRSS-e} = \frac{M}{2} \tag{81}$$

και το μέσο πλήθος χρονικών μικρο-σχισμών που ένας τυχαίος κόμβος j βρίσκεται σε κατάσταση ύπνου:

$$E\left[Y_j\right]_{CRSS-u} = E\left[Y_j\right]_{CRSS-e} = \frac{S}{2} \tag{82}$$

Επομένως, με βάση την (82), το ποσοστό χρόνου που περνά κάθε κακόβουλος χρήστης στην κατάσταση ύπνου με βάση μια παραλλαγή Κοινού Σχήματος Ύπνου (CRSS) είναι $\frac{1}{2}$.

Από τα παραπάνω, γίνεται εμφανές ότι ανεξάρτητα από τη θεωρούμενη υλοποίηση (με ομοιόμορφη ή εκθετική κατανομή) οι αναμενόμενες τιμές και ποσοστά χρόνου είναι ανεξάρτητα από τις λεπτομέρειες της υλοποίησης. Συγκεκριμένα είναι εξίσου μοιρασμένα στις δύο καταστάσεις, όπως αναμενόταν και διαισθητικά, εξαιτίας της όμοιας κατανομής που χρησιμοποείται για τον καθορισμό της χρονικής διάρκειας και των δύο καταστάσεων.

5.3 Τεχνικές Στρώματος Δικτύου

Η πλειοψηφία των μεθόδων Ελέγχου Τοπολογίας λειτουργούν κατά βάση στο στρώμα Δικτύου, εκμεταλλευόμενες διαθέσιμη πληφορορία υψηλού επιπέδου που υπάρχει διαθέσιμη, χωρίς να απαιτείται επιπρόσθετο κόστος συλλογής, με αντίστοιχη πολυπλοκότητα λειτουργίας. Οι διαθέσιμες παράμετροι, όπως είναι ο βαθμός κόμβου (αριθμός και σύνολο γειτόνων με τους οποίους μπορεί να ανταλλαχθεί πληροφορία αξιόπιστα), μπορούν να χρησιμοποιηθούν αποδοτικά για τη σχεδίαση αλγορίθμων ελέγχου ισχύος και κατ' επέκταση Ελέγχου Τοπολογίας.

Στην παρούσα εργασία χρησιμοποιούνται δύο προσεγγίσεις Ελέγχου Τοπολογίας επιπέδου στρώματος Δικτύου και συγκρίνονται με τις μεθόδους στρώματος MAC και φυσικού με βάση το μετρικό της Αποδοτικότητας Μόλυνσης, αναφορικά με τις παραμέτρους του δικτύου (ακτίνα, πυκνότητα) και του κόμβου (ακτίνα, ενέργεια).

5.3.1 Πρωτόκολλο Τοπικής Πληροφορίας Χωρίς Γνώση Τοπολογίας (LINT)

Η πρώτη από τις δύο προσεγγίσεις που χρησιμοποιούνται αναφέρεται ως Τοπική Πληροφορία Χωρίς Γνώση Τοπολογίας (Local Information No Topology – LINT) [84]. Το LINT έχει σχεδιαστεί κυρίως για κινητά αυτοργανούμενα δίκτυα. Αποτελεί ένα ευρυστικό (heuristic) αλγόριθμο με κύριο γνώμονα την αποδοτική λειτουργία, με το μικρότερο δυνατό κόστος και επίπτωση στη λειτουργία του συστήματος.

Κάθε κόμβος έχει τρεις παραμέτρους, τον επιθυμητό βαθμό κόμβου (desired node degree – d_d), το άνω κατώφλι βαθμού κόμβου (high node degree threshold – d_h) και το κάτω κατώφλι βαθμού κόμβου (low node degree threshold – d_l). Η λειτουργία του κόμβου βασίζεται στη σύγκριση του τρέχοντος βαθμού κόμβου d_c (πληροφορία που είναι ήδη διαθέσιμη στον κόμβο από το στρώμα Δικτύου) με τα δύο κατώφλια.

Αν $d_c > d_h$, σημαίνει ότι ο κόμβος έχει ήδη περισσοτέρους γείτονες από τους επιθυμητούς και επομένως υπάρχει δυνατότητα να μειώσει την ακτίνα μετάδοσης χάνοντας τους πιο απομακρυσμένους, ενώ παράλληλα θα καταναλώνει χαμηλότερη ενέργεια. Χρησιμοποιώντας κατάλληλο βήμα ελάττωσης της ισχύος και της ακτίνας

εκπομπής του, η αλλαγή στην τοπολογία μπορεί να γίνει ομαλά, με μεγάλο ενεργειακό όφελος και μικρή απώλεια γειτόνων, ώστε και πάλι ο τρέχων βαθμός κόμβου να είναι κοντά στο ανώτερο κατώφλι. Αντίθετα, αν $d_c < d_l$, ο κόμβος έχει λίγους γείτονες και επομένως πρέπει να αυξήσει την ισχύ εκπομπής, ώστε να μεγαλώσει περαιτέρω τη γειτονιά του και να αποκτήσει επιπρόσθετους γείτονες. Σε περίπτωση που $d_l < d_c < d_h$ ο κόμβος δεν πραγματοποιεί καμία ενέργεια.

Η λογική που ακολουθεί το πρωτόκολλο Τοπικής Πληροφορίας Χωρίς Γνώση Τοπολογίας, είναι η χρησιμοποίηση της μικρότερης δυνατής πληροφορίας και με τον απλούστερο δυνατό τρόπο. Με βάση τη λειτουργία του, το πρωτόκολλο επιχειρεί να κρατήσει τον αριθμό των γειτόνων του εκάστοτε κόμβου γύρω από μια επιθυμητή τιμή d_d που οριοθετείται από δύο κατώφλια, το πάνω και το κάτω. Ανάλογα με την επιλογή του άνω και κάτω κατωφλίου βαθμού κόμβου, το πρωτόκολλο μπορεί να γίνει πολύ αυστηρό, με την έννοια να απαιτεί συχνές μεταβολές της ακτίνας μετάδοσης, ή περισσότερο ομαλό, μεταβάλλοντας λιγότερο την ακτίνα, καθώς αλλάζει τοπικά η γειτονιά του κόμβου.

Η συνάρτηση μεταβολής της ισχύος μπορεί να είναι μια συνάρτηση του επιθυμητού και τρέχοντος βαθμού κόμβου, ώστε όσο περισσότερο απομακρυσμένες είναι οι δύο τιμές, τόσο μεγαλύτερο να είναι το εύρος της αλλαγής, επιτυγχάνοντας γρήγορα σύγκλιση στο ζητούμενο αποτέλεσμα. Θεωρώντας την ακτίνα εκπομπής r_c που αντιστοιχεί σε μια ισχύ μετάδοσης P_c και r_d την ακτίνα που αντιστοιχεί στην ισχύ με την οποία επιτυγχάνεται η επιθυμητή τιμή του βαθμού κόμβου d_d, τότε μπορεί να επιτευχθεί μια έκφραση για τη μεταβολή ακτίνας με βάση τον τρέχοντα και επιθυμητό βαθμό κόμβου. Υποθέτοντας a τη σταθερά διάδοσης στο μέσο (συνήθως $a \in (2,5]$, ανάλογα με το περιβάλλον διάδοσης), και p την απώλεια διάδοσης σε dB, τότε:

$$\begin{aligned} p(r) &= p(r_{th}), \alpha\nu\ r < r_{th} \\ p(r) &= p(r_{th}) + 10 \cdot a \cdot \log_{10}\left(\frac{r}{r_{th}}\right), \alpha\nu\ r \geq r_{th} \end{aligned} \tag{83}$$

όπου r_{th} είναι μια απόσταση από τον πομπό, κάτω από την οποία η απώλεια διάδοσης είναι σταθερά. Υποθέτοντας ομοιόμορφη κατανομή κόμβων στην περιοχή του

δικτύου (ξεκινώντας με ομοιόμορφη τοποθέτηση κόμβων και ένα μοντέλο κινητικότητας που τη διατηρεί όπως αυτό του τυχαίου περίπατου [43]), έχουμε:

$$\begin{aligned} d_c &= D \cdot \pi \cdot r_c^2 \\ d_d &= D \cdot \pi \cdot r_d^2 \end{aligned} \tag{84}$$

όπου D είναι η πυκνότητα του δικτύου. Αν γ είναι η ευαισθησία του πομπού, τότε:

$$\begin{aligned} p_c - \left(p(r_{th}) + 10 \cdot a \cdot \log_{10} \left(\frac{r_c}{r_{th}} \right) \right) &= \gamma \\ p_d - \left(p(r_{th}) + 10 \cdot a \cdot \log_{10} \left(\frac{r_d}{r_{th}} \right) \right) &= \gamma \end{aligned} \tag{85}$$

Εξισώνοντας τις εκφράσεις στην (85) και με αντικατάσταση των (84), προκύπτει η έκφραση μεταβολής της ισχύος εκπομπής στο πρωτόκολλο Τοπικής Πληροφορίας Χωρίς Γνώση Τοπολογίας:

$$p_d = p_c - 5 \cdot a \cdot \log_{10} \left(\frac{d_d}{d_c} \right) \tag{86}$$

5.3.2 Πρωτόκολλο K-Γειτόνων (K-Neigh)

Η δεύτερη προσέγγιση, το πρωτόκολλο K-Γειτόνων (K-*Neigh*) [85], ορίζεται για στατικές τοπολογίες, λόγω όμως του ελάχιστου κόστους που έχει για την υλοποίησή του, μπορεί να εφαρμοστεί εξίσου σε κινητά δίκτυα. Σε αυτή την περίπτωση η λειτουργία του επαναλαμβάνεται για κάθε κόμβο δικτύου με το τέλος μιας χρονικής περιόδου, ενώ μεταξύ διαδοχικών υπολογισμών του πρωτοκόλλου η τοπολογία θεωρείται ότι αλλάζει πολύ αργά ή είναι σχεδόν σταθερή. Επιλέγοντας κατάλληλα τη χρονική περίοδο μεταξύ διαδοχικών στιγμιοτύπων του πρωτοκόλλου, μπορεί το σφάλμα υπολογισμού να είναι ασήμαντο ή πρακτικά αμελητέο.

Η αρχική (μέγιστη) ακτίνα μετάδοσης υποτίθεται κοινή για όλους τους κόμβους του δικτύου και είναι κατάλληλα επιλεγμένη ώστε να εξασφαλίζει συνδεσιμότητα της υποκείμενης τοπολογίας με μεγάλη πιθανότητα (with high probability – w.h.p.). Επίσης υποτίθεται ένας μηχανισμός υπολογισμού/εκτίμησης απόστασης κόμβων με βάση την ισχύ του λαμβανόμενου σήματος [86], αλλά με μικρή ακρίβεια υπολογισμού ή με βάση τη διαφορά χρόνου μεταξύ λήψης-εκπομπής ενός πακέτου [87] και καλύτερη ακρίβεια από την περίπτωση λαμβανόμενης ισχύος. Οι δύο

παραπάνω μέθοδοι μπορούν να υλοποιηθούν αποδοτικά και γρήγορα σε ασύρματα αυτοργανούμενα δίκτυα και δίκτυα αισθητήρων, με το κόστος της αναγκαστικά μικρότερης ακρίβειας υπολογισμού. Ωστόσο, στην περίπτωση που οι κόμβοι διέθεταν συσκευή εντοπισμού (GPS) [88], η ακρίβεια θα ήταν απόλυτα ικανοποιητική, με επιπρόσθετο κόστος στην κατανάλωση ενέργειας. Συμπερασματικά, ανάλογα με το εκάστοτε δίκτυο–σύστημα και τις απαιτήσεις που καθορίζονται από τις προδιαγραφές του ή το περιβάλλον για το οποίο προορίζεται, υπάρχει δυνατότητα ενός μηχανισμού υπολογισμού αποστάσεων γειτόνων.

Στο πρωτόκολλο K-Γειτόνων, ο κάθε κόμβος ενεργοποιεί τον αλγόριθμο που υλοποιεί το πρωτόκολλο σε μια τυχαία χρονική στιγμή και ανακοινώνει στους υπόλοιπους κόμβους που βρίσκονται στη γειτονιά του την ύπαρξή του με ένα πακέτο που εκπέμπεται με μέγιστη δυνατή ισχύ. Η τυχαία στιγμή επιλέγεται με βάση μια παράμετρο μέγιστης καθυστέρησης που επιλέγεται κατάλληλα ώστε να μην δημιουργούνται ανταγωνισμοί και συγκρούσεις των αναγνωριστικών πακέτων στο μέσο. Για κάθε ένα αντίστοιχο μήνυμα που λαμβάνει, ένας κόμβος αποθηκεύει το αναγνωριστικό του κόμβου–γείτονα που το έστειλε και υπολογίζει την απόστασή του με βάση μια από τις μεθόδους που περιγράφηκαν παραπάνω. Οι αντίστοιχες εγγραφές ταξινομούνται με βάση την απόσταση, ώστε να δημιουργηθεί μια διάταξη των γειτόνων του κάθε κόμβου αυξανόμενης απόστασης. Στη συνέχεια επιλέγονται μόνο οι K πιο κοντινοί γείτονες (αν υπάρχουν τόσοι) και η ακτίνα μετάδοσης ρυθμίζεται κατάλληλα, ώστε να εξασφαλισθεί απρόσκοπτη επικοινοινωνία και με τον πιο απομακρυσμένο από τους K κοντινότερους γείτονες. Μετά την επιλογή, μεταδίδεται ένα ακόμα πακέτο με μέγιστη ισχύ με το αναγνωριστικό του κόμβου και τη λίστα των νέων K γειτόνων που έχει επιλέξει, ώστε όλοι οι γείτονες να μπορούν να δημιουργήσουν συμμετρικές ζεύξεις με βάση τα δεδομένα που προέκυψαν από το συγκεκριμένο στάδιο επιλογής.

Επιπρόσθετα, το πρωτόκολλο μπορεί να ακολουθήσει ένα στάδιο αφαίρεσης ορισμένων ζεύξεων από τον παραγόμενο γράφο, αν αυτό είναι δυνατόν και αποδοτικό. Σε αυτό το στάδιο κάθε κόμβος εξετάζει μόνο τους K πρώτους κόμβους της λίστας στην οποία έχει καταλήξει. Η λίστα αυτή (λίστα λογικών γειτόνων) είναι ήδη διατεταγμένη κατά αύξουσα σειρά χωρικής απόστασης των κόμβων που την απαρτίζουν. Η λίστα διατρέχεται σειριακά και αν βρεθεί ότι η ισχύς που απαιτείται για να μεταδοθεί απευθείας (με μία μετάδοση) ένα πακέτο από τον κόμβο i σε ένα

κόμβο n της λίστας είναι μεγαλύτερη από τη συνολική ισχύ που απαιτείται για τη μετάδοση πακέτου στον n διαμέσου ενός κόμβου m που προηγείται στη λίστα του n και άρα είναι εγγύτερος στον i (μετάδοση δύο βημάτων), τότε διαγράφεται η ζεύξη μεταξύ $i-n$ και ο n από τη λίστα λογικών γειτόνων και αναπροσαρμόζεται η ακτίνα μετάδοσης αν είναι εφικτό. Στην περίπτωση που υπάρχουν περισσότεροι από δύο ενδιάμεσοι κόμβοι m, m', διατηρείται ο κόμβος μέσω του οποίου ελαχιστοποιείται η κατανάλωση ενέργειας. Η τελική ισχύς εκπομπής και αντίστοιχη ακτίνα μετάδοσης καθορίζεται στην τιμή που εξασφαλίζει την επικοινωνία με τον πιο απομακρυσμένο από τους κόμβους που βρίσκονται τελικά στη λίστα λογικών γειτόνων του κόμβου i. Αποδεικνύεται ότι ακόμα και μετά από αυτό το στάδιο, ο παραγόμενος γράφος παραμένει ισχυρά συνδεδεμένος (αν ήταν εξαρχής) και συμμετρικός.

Ένα σημαντικό ζήτημα που εγείρει άμεσα η λειτουργία του πρωτοκόλλου K-Γειτόνων είναι η επιλογή της παραμέτρου K. Η τιμή της πρέπει να είναι τέτοια ώστε να εξασφαλίζεται στο ελάχιστο η συνδετικότητα της παραγόμενης τοπολογίας, ταυτόχρονα όμως να μην αλλοιώνονται και οι προσφερόμενες υπηρεσίες στα ανώτερα στρώματα δικτύου (π.χ. καθυστέρηση, ποσοστό απωλειών, ποιότητα υπηρεσίας). Αν και στο [85], προτείνεται η χρήση της τιμής του K που απλά εξασφαλίζει τη συνδετικότητα του παραγόμενου γράφου, με αναφορά το μοντέλο και την ανάλυση του [89], στο οποίο προτείνονται τιμές του βαθμού κόμβου (εν είδη μαγικών αριθμών – magic numbers, δηλαδή ως τιμών κατωφλίων που έχουν δειχθεί ότι οδηγούν σε αποδοτικές λύσεις), μπορεί να επιλεγχθούν καταλληλότερες τιμές του K, ώστε να εξασφαλίζεται ταυτόχρονα και μεγαλύτερη χωρητικότητα δικτύου, κάτι που αντιστοιχεί σε ευκολότερη επικοινωνία και μικρότερο ανταγωνισμό για τους κακόβουλους χρήστες. Τέτοιες τιμές αποτελούν οι $K=7$ ή $K=8$ [89].

5.4 Αποτελέσματα Προσομοιώσεων

Για τη συγκριτική αξιολόγηση της επίδοσης των σχημάτων επίθεσης βασισμένων σε Έλεγχο Τοπολογίας χρησιμοποιούνται προσομοιώσεις με τη βοήθεια του πακέτου προσομοίωσης NS2.

Αναφορικά με τους ασύρματους κόμβους, υποτίθενται τρεις καταστάσεις του μέσου ελέγχου πρόσβασης. Η πρώτη είναι η κατάσταση μετάδοσης/λήψης, η δεύτερη είναι η κατάσταση αδράνειας και τρίτη η κατάσταση παύσης (ύπνου). Η πρώτη έχει

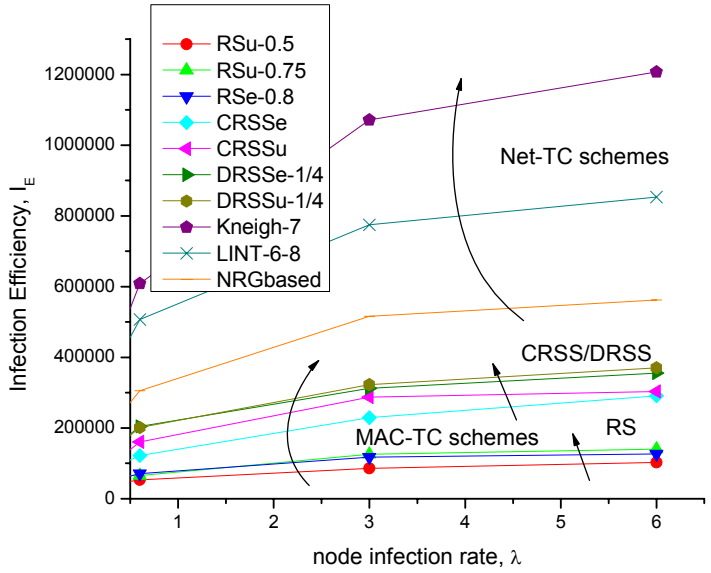
και τη μεγαλύτερη κατανάλωση ενέργειας, ενώ η δεύτερη έχει τάξεις μεγέθους χαμηλότερη. Στην τρίτη θεωρείται ότι οι κόμβοι σταματούν εντελώς τη λειτουργία τους και υποτίθεται μηδενική (αμελητέα) κατανάλωση ενέργειας, όσο παραμένουν σε αυτή.

Η ονομαστική ακτίνα μετάδοσης για τους νόμιμους κόμβους επιλέχθηκε στην τιμή $R_i = 200m$, ενώ για τους κακόβουλους το εύρος τιμών ακτίνας μετάδοσης ήταν $r \in [150m, 250m]$. Η μέγιστη ταχύτητα των επιτιθέμενων ήταν $\upsilon_{\max} = 20m/s$ και η ισχύς εκπομπής/λήψης $P_{tx/rx} = 0.6mW$.

Για την σύγκριση των μεθόδων διάδοσης κακόβουλου λογισμικού οι οποίες βασίζονται σε Έλεγχο Τοπολογίας, πιο σημαντικό ρόλο διαδραματίζει η κατανάλωση ενέργειας και το αντίστοιχο διάστημα διάρκειας ζωής του κάθε κόμβου και επομένως συνολικά του δικτύου. Κάτι τέτοιο γίνεται ιδιαίτερα εμφανές από τη βασική ιδέα στην οποία στηρίζονται οι μέθοδοι που λειτουργούν στο επίπεδο MAC και τους αντικειμενικούς στόχους που προσπαθούν να επιτύχουν/συμβιβάσουν γενικά οι μέθοδοι Ελέγχου Τοπολογίας και αποτυπώνονται στο Σχήμα 5. Επομένως το καταλληλότερο μετρικό για τη σύγκριση των μεθόδων είναι η Αποδοτικότητα Μόλυνσης. Ως επακόλουθο, η παρούσα εργασία εστιάζει σε αυτό το μετρικό για την αξιολόγηση των μεθόδων επίθεσης. Επικουρικά εξετάζεται και το χρονικά ανεξάρτητο μετρικό του αναμενόμενου αριθμού μολυσμένων κόμβων, ως ενδεικτικό των δυνατοτήτων διάδοσης κακόβουλου λογισμικού στη γειτονιά των κόμβων.

Στο Διάγραμμα 25 παρουσιάζονται τα αποτελέσματα της προσομοίωσης για τα σχήματα διάδοσης κακόβουλου λογισμικού που βασίζονται στον Έλεγχο Τοπολογίας για ένα δίκτυο με πολύ χαμηλή κατανάλωση άεργου κατάστασης, $P_{idle} = 10^{-7} mW$, ενώ στο Διάγραμμα 26 παρουσιάζονται τα αποτελέσματα για $P_{idle} = 3 \cdot 10^{-4} mW$. Πιο συγκεκριμένα φαίνεται η Αποδοτικότητα Μόλυνσης ως συνάρτηση του ρυθμού μόλυνσης κόμβου λ ή διαφορετικά ως συνάρτηση του λόγου λ/μ υποθέτοντας σταθερό ρυθμό ανάκαμψης μ. Το πρώτο δίκτυο με τη χαμηλή κατανάλωση αντιστοιχεί δυνητικά σε ένα αυτοργανούμενο ad hoc δίκτυο όπου συνήθως οι κόμβοι δεν επιτελούν κάποια λειτουργία στην άεργο κατάσταση. Αντίθετα, στα δίκτυα αισθητήρων, οι κόμβοι μπορεί να εκτελούν στην άεργο κατάσταση κάποιες λειτουργίες περιφερειακές της επικοινωνίας (όπως η συγκέντρωση ή επεξεργασία

δεδομένων – data aggregation/processing [90]) και επομένως να έχουν υψηλότερη κατανάλωση.

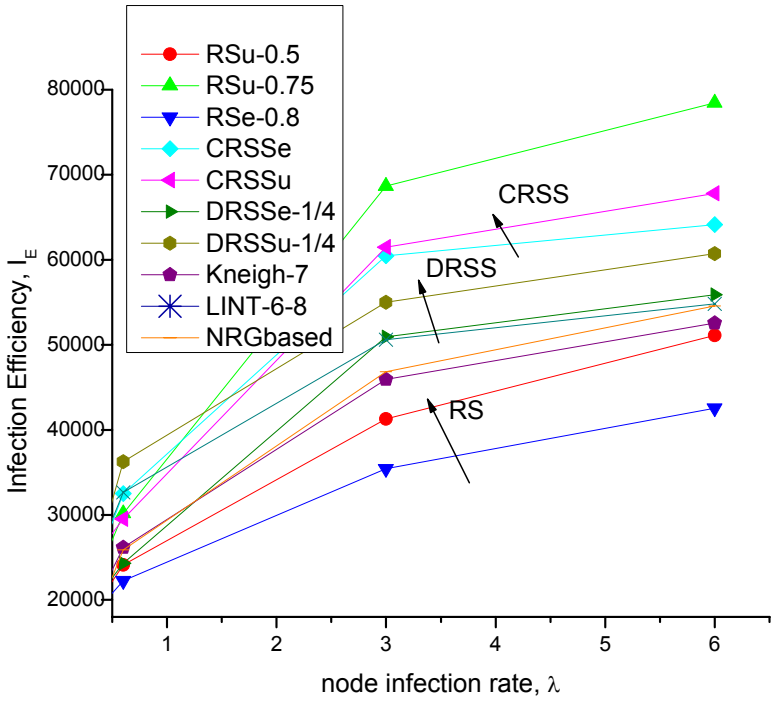


Διάγραμμα 25 – Αποδοτικότητα Μόλυνσης για τις μεθόδους διάδοσης κακόβουλου λογισμικού που βασίζονται σε Έλεγχο Τοπολογίας ($N = 200$ **,** $P_{idle} = 10^{-7} mW$ **)**

Κοιτώντας συγκριτικά τα δύο διαγράμματα φαίνεται ότι στην περίπτωση δικτύου χαμηλής κατανάλωσης άεργου κατάστασης (αυτοργανούμενα ad hoc) υπερτερούν τα σχήματα που λειτουργούν στο στρώμα δικτύου, ενώ το ανάποδο συμβαίνει στην περίπτωση δικτύων με υψηλότερη κατανάλωση άεργου καταστάσεως (δίκτυα αισθητήρων). Το γεγονός αυτό επιβεβαιώνει την ορθότητα της σχεδίασης των σχημάτων στρώματος MAC, αφού η επίδοσή τους γίνεται καλύτερη ακριβώς στις περιπτώσεις που η κατανάλωση άεργου ενέργειας είναι μεγαλύτερη. Παράλληλα, φαίνεται ότι τα σχήματα ύπνου που καθορίστηκαν είναι αποδοτικά και μπορούν να ανταπεξέλθουν στους ενεργειακούς περιορισμούς που τίθενται από τη φύση των δικτύων, παρά την τυχαιοποιημένη και απλή λειτουργία τους, όπως για παράδειγμα το σχήμα $RSu-0.75$ το οποίο είναι το πιο αποδοτικό στο μεγαλύτερο εύρος λειτουργίας του ρυθμού μόλυνσης λ που μελετάται στην περίπτωση υψηλής κατανάλωσης άεργου κατάστασης, αν και στη λειτουργία του είναι το απλούστερο δυνατό από τα σχήματα που μελετήθηκαν.

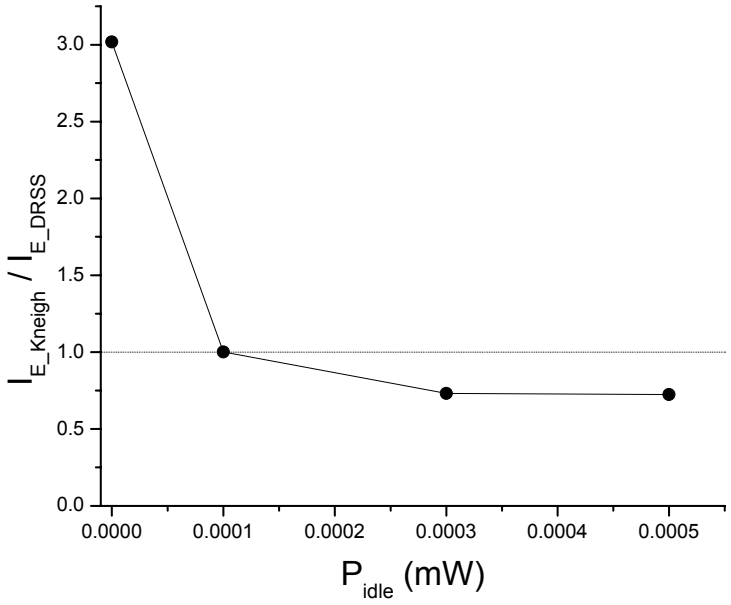
Με μια συνδυαστική θεώρηση των δύο διαγραμμάτων και τις επιδόσεις των σχημάτων για τις δύο περιπτώσεις δικτύων, μπορεί κανείς να καταλήξει στο

συμπέρασμα ότι από την οικογένεια των σχημάτων σε επίπεδο MAC το επικρατέστερο σχήμα είναι το Σχήμα Διαφορετικού Ύπνου στην παραλλαγή της ομοιόμορφης κατανομής (*DRSS-u*), ενώ από τη μεριά των σχημάτων στρώματος Δικτύου το επικρατέστερο είναι το πρωτόκολλο K-Γειτόνων (K-*Neigh*).

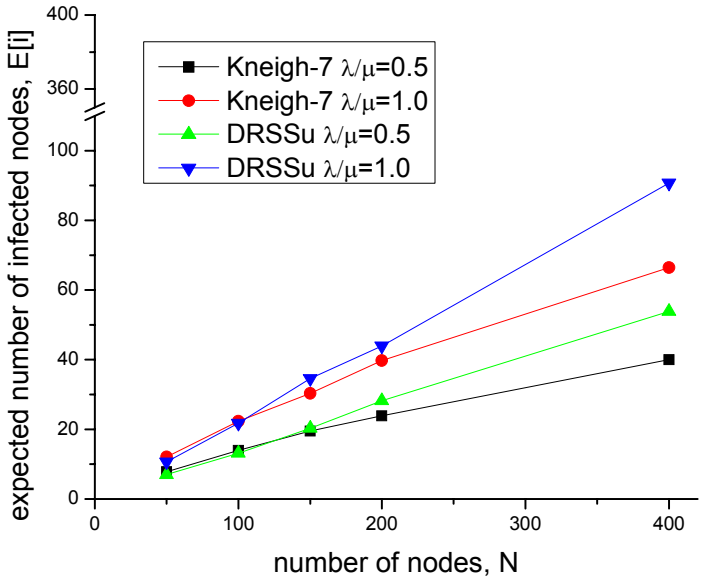


Διάγραμμα 26 – Αποδοτικότητα Μόλυνσης για τις μεθόδους διάδοσης κακόβουλου λογισμικού που βασίζονται σε Έλεγχο Τοπολογίας ($N = 200$, $P_{idle} = 3 \cdot 10^{-4} mW$)

Στο Διάγραμμα 27 συγκρίνονται οι επικρατέρεστες μέθοδοι από κάθε κατηγορία (όπως εξηγήθηκε παραπάνω) ως συνάρτηση της κατανάλωσης ισχύος άεργου κατάστασης. Από το διάγραμμα γίνεται εμφανής η περιοχή λειτουργίας κάθε σχήματος και πιο συγκεκριμένα για μικρές καταναλώσεις μέχρι περίπου την τιμή $P_{idle} = 10^{-4} mW$ το πρωτόκολλο K-Γειτόνων παρουσιάζεται αποδοτικότερο, ενώ από αυτή την τιμή και πάνω, το MAC Σχήμα Διαφορετικού Ύπνου υπερτερεί. Η διαφορά στην επίδοση αρχικά μεγαλώνει για τιμές πάνω από $P_{idle} = 10^{-4} mW$, ωστόσο για τιμές της κατανάλωσης στην άεργο κατάσταση $P_{idle} = 3 \cdot 10^{-4} mW$ και πάνω η διαφορά σταθεροποιείται, καταδεικνύοντας ότι για τόσο μεγάλες κατανάλωσεις είναι πολύ δύσκολο ακόμα και για τα ειδικά σχεδιασμένα σχήματα ύπνου να ανταπεξέλθουν και να βελτιώσουν την κατάσταση προς όφελος των κακόβουλων χρηστών.



Διάγραμμα 27 – Σύγκριση αποδοτικότητας τεχνικών Ελέγχου Τοπολογίας αναφορικά με την κατανάλωση άεργου κατάστασης κόμβων



Διάγραμμα 28 – Αναμενόμενος αριθμός μολυσμένων κόμβων $E[i]$ για τα σχήματα διάδοσης κακόβουλου λογισμικού βασισμένα στον Έλεγχο Τοπολογίας

Στο Διάγραμμα 28 παρουσιάζεται ο αναμενόμενος αριθμός μολυσμένων κόμβων ως συνάρτηση της πυκνότητας του δικτύου για διαφορετικές τιμές του ρυθμού μόλυνσης κόμβων και για τα δύο επικρατέστερα σχήματα που μελετήθηκαν

προηγουμένως. Το σχήμα επιπέδου MAC επιτυγχάνει μεγαλύτερο αναμενόμενο αριθμό μολυσμένων κόμβων σε κάθε τιμή του λόγου λ / μ.

Συνολικά και συνεκτιμώντας τις δύο αξιολογήσεις χρονικά-εξαρτημένων και χρονικά-ανεξάρτητων μετρικών, καταλήγει κανείς στο συμπέρασμα ότι το σχήμα επιπέδου MAC *DRSS-u* είναι περισσότερο αποδοτικό στη γενική περίπτωση, αφού εξασφαλίζει μεγαλύτερο αναμενόμενο αριθμό μολυσμένων κόμβων, καλύτερη διαχείριση ενέργειας και ακόμα και στην περίπτωση δικτύων χαμηλής κατανάλωσης ενέργειας άεργου κατάστασης είναι καλύτερο από τα άλλα σχήματα επιπέδου MAC. Δεδομένου ότι για δίκτυα με υψηλή κατανάλωση άεργου κατάστασης εξασφαλίζει μεγαλύτερη διάρκεια ζωής και βέλτιστη επίδοση, συνολικά φαίνεται μια καλύτερη προσέγγιση για την αποδοτική διάδοση κακόβουλου λογισμικού. Φυσικά, από τη σκοπιά του δικτύου, κάτι τέτοιο θα πρέπει να ληφθεί κατάλληλα υπόψη για την ορθή ανοσοποίηση και προστασία του, ώστε σε περίπτωση αναγνώρισης μιας επίθεσης τέτοιου τύπου, να ληφθούν τα κατάλλλα μέτρα που θα κινούνται στην αντίθετη κατεύθυνση και θα καθιστούν τους κακόβουλους κόμβους που χρησιμοποιούν αυτή την τεχνική αναποτελεσματικούς.

Κεφάλαιο 6

Στρατηγικές Διάδοσης Κακόβουλου Λογισμικού με Τυχαίους Περίπατους

Στο τρέχον κεφάλαιο παρουσιάζονται τυχαιοποιημένες τεχνικές διάδοσης κακόβουλου λογισμικού σε δίκτυα μη-διασποράς, οι οποίες αποσκοπούν στη μόλυνση όλων των κόμβων του δικτύου τουλάχιστον μια φορά. Σε μια τέτοια περίπτωση αλλάζουν τα μετρικά αποδοτικότητας της επίθεσης, δίνοντας έμφαση στο χρόνο που θα ολοκληρωθεί η διαδικασία της πλήρους μόλυνσης των νόμιμων κόμβων του δικτύου και στην ενέργεια που χρειάζεται για την επίτευξη αυτού του στόχου. Η αναμενόμενη τιμή αριθμού μολυσμένων κόμβων δεν είναι πλέον ενδεικτική, αφού τελικά όλοι οι κόμβοι πρόκειται να περάσουν στην κατάσταση μόλυνσης.

Επίσης αλλάζει το περιβάλλον εφαρμογής. Πλέον η συμπεριφορά που περιγράφεται μοντελοποιεί την περίπτωση ενός συγκεκριμένου τύπου κακόβουλου λογισμικού και μιας ειδικής υλοποίησής του, η οποία επιχειρεί να μεγιστοποιήσει την επίδρασή της στη λειτουργία του κανονικού δικτύου. Για λόγους απλότητας και για να απαλλαχθεί η ανάλυση από τεχνικές λεπτομέρειες που δεν επηρεάζουν το βασικό μηχανισμό της διάδοσης κακόβουλου λογισμικού, υποτίθεται ότι μόλις ένας κόμβος έλθει σε επαφή με τον κακόβουλο, λαμβάνει αυτόματα το κακόβουλο λογισμικό και θεωρείται ότι περνά στην κατάσταση μόλυνσης με τις αντίστοιχες συνέπειες που περιγράφηκαν σε προηγούμενο κεφάλαιο. Κατά συνέπεια η συμπεριφορά τέτοιων μεθόδων διάδοσης κακόβουλου λογισμικού μελετάται μέχρις ότου επιτευχθεί ο στόχος της μόλυνσης όλων των νόμιμων κόμβων τουλάχιστον μια φορά για καθένα από αυτούς.

Στη συνέχεια παρουσιάζονται τεχνικές που θα μπορούσαν να χρησιμοποιηθούν για την αποδοτική διάδοση κακόβουλου λογισμικού καθολικά σε ένα δίκτυο, λαμβάνοντας υπόψη τα ιδιαίτερα χαρακτηριστικά των πιο αντιπροσωπευτικών τύπων ασύρματων αυτοργανούμενων δικτύων (Πίνακας 2). Τα μεγέθη της πυκνότητας κόμβων, μεγέθους δικτύου, κινητικότητας και ενεργειακών περιορισμών που

παρατίθενται, αφορούν στη γενική συμπεριφορά που διακρίνει τον εκάστοτε τύπο δικτύου. Κατά περίπτωση μπορούν να εντοπιστούν περιπτώσεις δικτύων που αν και ανήκουν σε ένα τύπο, παρουσιάζουν και ορισμένα χαρακτηριστικά ενός άλλου, κάτι τέτοιο όμως δεν αποτελεί τον κανόνα και ειδικές επιλογές έχουν γίνει προκειμένου να λειτουργήσουν απρόσκοπτα τέτοια συστήματα. Τέτοια ειδικά σχήματα δεν ενδιαφέρουν στην παρούσα μελέτη, η οποία εστιάζει σε γενικές μεθόδους μοντελοποίησης και ανάλυσης.

Πίνακας 2 – Χαρακτηριστικά ασύρματων αυτοργανούμενων δικτύων

	Πυκνότητα κόμβων	**Μέγεθος δικτύου**	**Βαθμός κινητικότητας**	**Ενεργειακοί περιορισμοί**
Αυτοργανούμενα δίκτυα ad hoc	Χαμηλή/μέτρια	Μικρό/μέτριο	Μέτρια	Μέτριοι
Δίκτυα αισθητήρων	Υψηλή	Μέτριο	Καθόλου/χαμηλή	Υψηλοί
Δίκτυα πλέγματος	Μέτρια	Υψηλό	Καθόλου/χαμηλή	Καθόλου
Αυτοκινητιστικά δίκτυα	Μέτρια/υψηλή	Υψηλό	Υψηλή	Καθόλου

6.1 Απλός Τυχαίος Περίπατος (Simple Random Walk – SRW)

Στη θεωρία πιθανοτήτων, ο Τυχαίος Περίπατος (Random Walk – RW) [91],[92] ορίζεται ως μια στοχαστική διαδικασία τύπου Markov $\{X_i\}_{i\geq 0}$, στην οποία η τυχαία μεταβλητή X_i υποδηλώνει την κατάσταση της διαδικασίας στο βήμα i. Η επόμενη κατάσταση της διαδικασίας στο βήμα $i+1$ επιλέγεται τυχαία με ομοιόμορφη πιθανότητα μεταξύ όλων των δυνατών καταστάσεων της διαδικασίας στις οποίες μπορεί να μεταπηδήσει στο βήμα $i+1$ από την τρέχουσα κατάσταση X_i. Οι Τυχαίοι Περίπατοι που ορίζονται σε γράφους παρουσιάζουν αρκετές αναλογίες με τα ηλεκτρικά κυκλώματα (όπως παρουσιάστηκε παραπάνω με τα δίκτυα κλειστών ουρών αναμονής), μεταφέροντας πολλά στοιχεία και ιδιότητες από το ένα πεδίο στο άλλο.

Οι Τυχαίοι Περίπατοι έχουν χρησιμοποιηθεί εκτενώς σε δίκτυα υπολογιστών και επικοινωνιών, ενσύρματα δίκτυα τύπου P2P [93], στο Διαδίκτυο [94], δίκτυα αισθητήρων [95] και ασύρματα αυτοργανούμενα [96]. Εξαίτιας της Markov ιδιότητας των Τυχαίων Περίπατων, χάρις την οποία λειτουργούν ανεξάρτητα της καταστάσεως

που βρίσκονται, τα εγγενή προβλήματα που παρουσιάζουν τα ασύρματα αυτοργανούμενα δίκτυα (μεταβλητό κανάλι, κινητικότητα, έλλειψη κεντρικής δομής) δεν επηρεάζουν τη λειτουργία τους. Όλη η πληροφορία που χρειάζεται για την επόμενη μετάβαση βρίσκεται τοπικά διαθέσιμη στον τρέχοντα κόμβο που επισκέπτεται ο Περίπατος και προκύπτει από την υπάρχουσα τοπολογία.

Στην περίπτωση των επιθέσεων που στηρίζονται σε Τυχαίους Περίπατους το ζητούμενο είναι τελικά ο κάθε νόμιμος κόμβος του δικτύου να έχει επισκευτεί μία τουλάχιστον φορά από τον κακόβουλο, ή με άλλα λόγια, στο τέλος της επίθεσης, ο κάθε κόμβος του υποκείμενου γράφου $G(V,E)$ να έχει μολυνθεί μια τουλάχιστον φορά [97]. Η διαδικασία της επίσκεψης κόμβων είναι στοχαστική και μια ακριβής αναπαράστασή της είναι η κατάσταση του Τυχαίου Περίπατου να αντιστοιχεί στον τρέχοντα κόμβο που επισκέπτεται ο Περίπατος (υποθέτοντας μια τυχαία αρίθμηση κόμβων). Έτσι στο i-οστό βήμα του Περίπατου, $X_i = \upsilon$, όπου $\upsilon \in V$ είναι το αναγνωριστικό του τρέχοντος κόμβου που επισκέπτεται ο Περίπατος. Στη βασική έκδοση ενός Τυχαίου Περίπατου σε ένα γράφο επιτρέπονται μεταβάσεις μόνο μεταξύ γειτονικών κόμβων. Ο επόμενος γείτονας (δηλαδή η επόμενη κορυφή γράφου) που επισκέπτεται ο Περίπατος επιλέγεται ομοιόμορφα με την ίδια πιθανότητα. Στη συνέχεια και για να ξεχωριστεί από τις υπόλοιπες τεχνικές Τυχαίων Περίπατων που προτείνονται, η βασική έκδοση Τυχαίου Περίπατου που περιγράφηκε αναφέρεται ως Απλός Τυχαίος Περίπατος (Simple Random Walk – SRW).

Αν ο βαθμός του κόμβου u αναπαρίσταται ως d_u, τότε οι πιθανότητες μετάβασης του Απλού Τυχαίου Περίπατου μεταξύ γειτονικών καταστάσεων δίνονται από την έκφραση:

$$P_{u,v} = \begin{cases} \dfrac{1}{d_u}, & \alpha\nu\ (u,v) \in E \\ 0, & \alpha\nu\ (u,v) \notin E \end{cases} \tag{87}$$

Οι στάσιμες και εργοδικές πιθανότητες καταστάσεων του Απλού Τυχαίου Περίπατου (πιθανότητα ο Περίπατος να βρίσκεται στην κατάσταση u), δίνονται από την έκφραση:

$$\pi_u = \frac{d_u}{2|E|} = \frac{d_u}{\sum_k d_k}, \forall k \in V \tag{88}$$

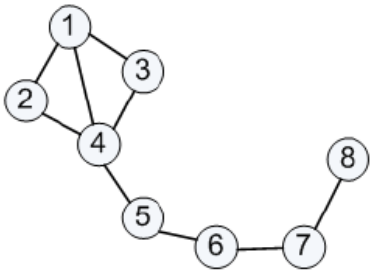
Οι Τυχαίοι Περίπατοι που ορίζονται σε πεπερασμένους γράφους, ως ειδικές περιπτώσεις αλυσίδων Markov, εμφανίζουν ορισμένες ιδιαίτερα επιθυμητές ιδιότητες, πιο χαρακτηριστικές από τις οποίες είναι η συμμετρία χρόνου (time symmetry) και η αντιστρεψιμότητα (reversibility) της αλυσίδας. Έτσι οι πιθανότητες κάλυψης ενός μονοπατιού προς τη μία ή την αντίστροφη κατεύθυνση έχουν μια συγκεκριμένη σχέση μεταξύ τους (και είναι ίσες για κανονικούς γράφους). Αυτό συνεπάγεται ότι δεν έχει σημασία στην ανάλυση η φορά των μονοπατιών που ακολουθεί ο Τυχαίος Περίπατος.

Διάφορα μεγέθη που διέπουν τη λειτουργία του Περίπατου μπορούν να οριστούν και να χρησιμοποιηθούν για τη σύγκριση διαφόρων προσεγγίσεων. Ο χρόνος κάλυψης (Cover/Coverage Time – C), ορίζεται ως ο μέσος αριθμός βημάτων της διαδικασίας που απαιτούνται για την επίσκεψη (κάλυψη) όλων των κόμβων του γράφου–δικτύου τουλάχιστον μια φορά [97]. Ο χρόνος κτυπήματος (hitting time – $H(u,v)$) μεταξύ δύο καταστάσεων u, v ορίζεται ως ο αναμενόμενος αριθμός βημάτων της διαδικασίας για να φτάσει ο Περίπατος στην κατάσταση v, ξεκινώντας από την κατάσταση u. Επίσης ο αναμενόμενος αριθμός επαναλαμβανόμενων επισκέψεων σε κάθε κόμβο και ο συνολικός μέσος αριθμός επαναλαμβανόμενων επισκέψεων είναι ενδεικτικά μεγέθη για την σπατάλη πόρων την οποία κάνει εγγενώς ένα σχήμα Τυχαίου Περίπατου αν χρησιμοποιούνταν σε μια πρακτική εφαρμογή (μπορεί να περιγράφει επαναλαμβανόμενες μεταδόσεις που έχουν ενεργειακό κόστος σε ασύρματα δίκτυα ή εισάγουν ανεπιθύμητη καθυστέρηση σε τεχνικές αναζητήσεις σε ενσύρματα δίκτυα). Στην παρούσα εργασία εστιάζουμε κυρίως στο χρόνο κάλυψης του δικτύου και την ενέργεια που καταναλίσκεται για να επιτευχθεί η κάλυψη του δικτύου.

6.2 Υβριδικοί Τυχαίοι Περίπατοι

Το βασικό σχήμα λειτουργίας του Απλού Τυχαίου Περίπατου μπορεί να επεκταθεί ώστε να γίνει πιο αποδοτικό σε σχέση με κάποια από τα υιοθετούμενα μετρικά επίδοσης. Μια δυνατή τροποίηση της βασικής έκδοσης Τυχαίων Περίπατων αποτελεί η προσθήκη της δυνατότητας εκτέλεσης μεταβάσεων πολλαπλών βημάτων (multihop jumps) στους κόμβους του δικτύου. Έτσι η συμπεριφορά του Περίπατου καθορίζεται από δύο δυνατές καταστάσεις λειτουργίας (διαφορετικές από τις καταστάσεις X_t), στη μια από τις οποίες ο Περίπατος εξελίσσεται ως ένας Απλός

Τυχαίος Περίπατος, ενώ στη δεύτερη εκτελεί την ίδια βασική λειτουργία με άλματα πολλαπλών βημάτων (αντί του ενός βήματος στην περίπτωση του Απλού Τυχαίου Περίπατου).



Σχήμα 7 – Παράδειγμα λειτουργίας υβριδικού σχήματος Τυχαίου Περίπατου

Στην πραγματικότητα κάθε άλμα πολλαπλών βημάτων υλοποιείται με ενδιάμεσα βήματα, όπως καθορίζονται από τον υποκείμενο γράφο του δικτύου. Έτσι για παράδειγμα, με αναφορά το Σχήμα 7, και για ένα Τυχαίο Περίπατο που βρίσκεται στον κόμβο 4, όταν λειτουγεί στην κατάσταση Απλού Τυχαίου Περίπατου, οι επόμενες δυνατές καταστάσεις στις οποίες μπορεί να μεταβεί είναι $\{1,2,3,5\}$. Αντίθετα στην περίπτωση που ο περίπατος εκτελεί άλματα πολλαπλών βημάτων με μήκος έστω τριών βημάτων, τότε η μόνη επόμενη μετάβαση είναι στον κόμβο $\{7\}$. Σε αυτή την περίπτωση ο Περίπατος περνά μέσω των $\{5,6\}$, η επίσκεψη όμως αυτή προσμετράται μόνο στην κατανάλωση ενέργειας και όχι στη σειρά επίσκεψης των κόμβων, ακριβώς επειδή οι ενδιάμεσες επισκέψεις δεν έχουν αποφασιστεί από τον υβριδικό Τυχαίο Περίπατο. Οι ενδιάμεσες επισκέψεις συνοδεύονται από αντίστοιχη κατανάλωση ενέργειας για την εκπομπή αναγκαίας πληροφορίας στις αντίστοιχες ζεύξεις, έτσι ώστε να υποθέσει κανείς ότι η απώλεια ενέργειας που επιφέρεται να αντιβαίνει στη λογική της αύξησης αποδοτικότητας που επιχειρούν τα σχήματα Τυχαίων Περίπατων. Στον αντίποδα, η συγκεκριμένη σειρά επίσκεψης κόμβων που αποφασίζεται από τον Τυχαίο Περίπατο, είναι πιο αποδοτική και μειώνει τον τελικό χρόνο κάλυψης σημαντικά. Επομένως, τα προτεινόμενα σχήματα καλούνται να συμβιβάσουν την αυξημένη αποδοτικότητα κάλυψης με το εγγενές αυξημένο κόστος ενέργειας που επιφέρει η υλοποίησή της. Ο βαθμός στον οποίο κάτι τέτοιο συμβαίνει διαφέρει ανάλογα με τον τύπο δικτύου, ώστε τελικά να προκύπτει η μέγιστη δυνατή επίδοση αναφορικά με το χρόνο κάλυψης και το κόστος ενέργειας που επιτρέπεται από το συγκεκριμένο τύπο δικτύου.

Ένας Τυχαίος Περίπατος σε ένα γράφο αποτελεί ουσιαστικά μια ακολουθία τυχαίων μεταβλητών με τιμές στο σύνολο των κόμβων του δικτύου $V = \{1, 2, ..., N\}$, $|V| = N$, η οποία καθορίζεται από τις δυνατές μεταβάσεις που επιτρέπει η υποκείμενη τοπολογία. Στην κατάσταση λειτουργίας με απλά άλματα μεταξύ γειτονικών κόμβων, οι μεταβάσεις καθορίζονται από τη γειτονιά του τρέχοντος κόμβου–κατάστασης. Αντίθετα στην περίπτωση μεταβάσεων αλμάτων πολλαπλών καταστάσεων, η επόμενη κατάσταση καθορίζεται από τον αριθμό των γειτόνων του τρέχοντος κόμβου που βρίσκονται τόσα βήματα μακριά του, όσα καθορίζει το μήκος του άλματος σε ενδιάμεσες ζεύξεις.

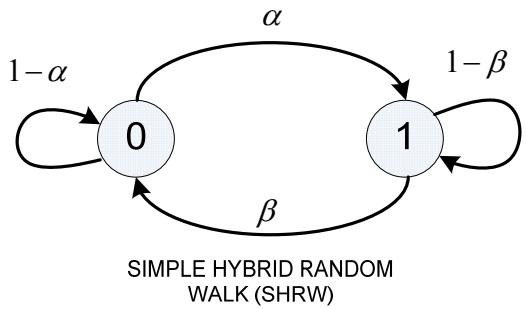
Η λογική που διέπει τα υβριδικά σχήματα Τυχαίου Περίπατου αποσκοπεί στην εκμετάλλευση των τοπολογικών ιδιαιτεροτήτων των αυτοργανούμενων δικτύων. Έτσι σε ένα πυκνό τμήμα του δικτύου, ένας Τυχαίος Περίπατος αναμένεται να πρωτο-επισκέπτεται κόμβους με γρήγορο ρυθμό, ενώ σε ένα αραιό τμήμα αναμένεται να κυκλοφορεί μεταξύ ενός περιορισμένου συνόλου γειτονικών κόμβων. Στην πρώτη περίπτωση είναι προτιμότερο να λειτουργεί όπως ο Απλός Τυχαίος Περίπατος, ενώ στη δεύτερη περίπτωση τα άλματα πολλαπλών βημάτων θα μεταφέρουν τον Περίπατο σε άλλο τμήμα του δικτύου, πιθανά πιο πυκνό, όπου ο ρυθμός επίσκεψης νέων κόμβων θα είναι μεγαλύτερος.

Στην παρούσα εργασία παρουσιάζονται τρια υβριδικά σχήματα (και παραλλαγές τους) Τυχαίων Περίπατων και αναλύεται η λειτουργία τους. Τα σχήματα αυτά μελετώνται υπό το πρίσμα των χαρακτηριστικών διαφορετικών τύπων αυτοργανούμενων δικτύων, όπως συνοψίσθηκαν παραπάνω (Πίνακας 2), με σκοπό την εύρεση του καταλληλότερου σχήματος για κάθε τύπο δικτύου και περιβάλλοντος εφαρμογής.

6.2.1 Απλός Υβριδικός Τυχαίος Περίπατος

Στην παραλλαγή Απλού Υβριδικού Τυχαίου Περίπατου με παραμέτρους α, β (Simple Hybrid Random Walk – $SHRW(\alpha, \beta)$) [98], ο Περίπατος έχει δύο καταστάσεις λειτουργίας (Σχήμα 8). Στην πρώτη κατάσταση (κατάσταση 0), εκτελείται ο τυπικός Απλός Τυχαίος Περίπατος, με μεταβάσεις μεταξύ γειτονικών κόμβων (που βρίσκονται ένα μόνο βήμα μακριά). Αντίθετα, στη δεύτερη κατάσταση λειτουργίας (κατάσταση 1), οι μεταβάσεις γίνονται με άλματα πολλαπλών βημάτων.

Το μήκος των αλμάτων σε βήματα γειτονικών κόμβων μπορεί να είναι σταθερό ή να μεταβάλλεται δυναμικά. Στη συγκεκριμένη εργασία και για να επιδειχθεί η επίδραση ενός τυχαίου μήκους αλμάτων, το μήκος επιλέγεται τυχαία με ομοιόμορφη πιθανότητα στο διάστημα $[2, \ell_{\max}]$, όπου το $\ell_{\max}$ είναι το μέγιστο επιτρεπτό μήκος άλματος. Για λόγους συμβατότητας $\ell_{\max} \le D$, όπου D είναι η διάμετρος του γράφου του δικτύου. Η κατεύθυνση εκτέλεσης των βημάτων μπορεί επίσης να επιλεχτεί με διάφορους τρόπους. Στην παρούσα εργασία η κατεύθυνση επιλέγεται τυχαία με ίση πιθανότητα μεταξύ των δυνατών κατευθύνσεων για την επόμενη μετάβαση.



Σχήμα 8 – Καταστάσεις λειτουργίας Απλού Υβριδικού Τυχαίου Περίπατου

Οι ρυθμοί μετάβασης καταστάσεων (πιθανότητες μεταβάσεων) για τον Απλό Υβριδικό Τυχαίο Περίπατο ($SHRW(\alpha, \beta)$) είναι σταθερές και μονοπαραμετρικές καθ' όλη τη διάρκεια λειτουργίας. Έτσι αν ο περίπατος λειτουργεί στην κατάσταση 0 (Απλός Τυχαίος Περίπατος), αλλάζει κατάσταση λειτουργίας με πιθανότητα α, ενώ αν βρίσκεται στην κατάσταση υβριδικής λειτουργίας (κατάσταση 1), μεταβαίνει στην κατάσταση 0 με πιθανότητα β (Σχήμα 8). οι πιθανότητες παραμονής στην εκάστοτε κατάσταση είναι συμπληρωματικές, ώστε με πιθανότητα $1-\alpha$, ο περίπατος να μένει στην κατάσταση 0 αν είναι ήδη εκεί, και με πιθανότητα $1-\beta$, ο περίπατος να συνεχίζει τη λειτουργία του στην κατάσταση 1, αν ήδη λειτουργεί σε υβριδική μορφή. Οι μεταβάσεις μεταξύ των δύο τρόπων λειτουργίας με τους αντίστοιχους ρυθμούς μεταβάσεων αποτελούν μια αλυσίδα Markov όπως φαίνεται στο Σχήμα 8. Μεταβάσεις μεταξύ των καταστάσεων λειτουργίας (αν προκύπτουν) λαμβάνουν χώρα στην αρχή κάθε βήματος του Περίπατου.

Η προσθήκη αλμάτων πολλαπλών βημάτων μέσω της κατάστασης λειτουργίας 1, αναμένεται να βελτιώσει την επίδοση του Απλού Υβριδικού Τυχαίου Περίπατου σε σχέση με αυτή του Απλού Τυχαίου Περίπατου αναφορικά με το χρόνο κάλυψης και τον αριθμό των επαναλαμβανόμενων επισκέψεων των κόμβων. Κάτι τέτοιο είναι

αναμενόμενο αν σκεφτεί κανείς ότι τα άλματα πολλαπλών βημάτων αποφεύγουν πιθανές τοπικές επαναλαμβανόμενες επισκέψεις κόμβων που μπορεί να συμβούν τοπικά σε περιοχές του δικτύου με υψηλή συγκέντρωση κόμβων. Ταυτόχρονα, διαφορετικοί και χωρικά απομακρυσμένοι κόμβοι αναμένεται να καλυφθούν γρηγορότερα στην περίπτωση αλμάτων πολλαπλών βημάτων.

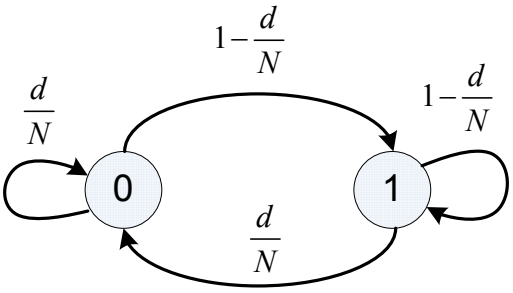
Με χρήση τυπικών μεθόδων ανάλυσης αλυσίδων Markov (εξισώσεις ισορροπίας και συνθήκη κανονικοποίησης) μπορούν εύκολα να προκύψουν οι εργοδικές πιθανότητες καταστάσεων (ποσοστά χρόνου παραμονής) στην κάθε κατάσταση λειτουργίας. Για την περίπτωση του Απλού Υβριδικού Τυχαίου Περίπατου, υπολογίζονται:

$$\pi_0 = \frac{\beta}{\alpha+\beta}, \quad \pi_1 = \frac{\alpha}{\alpha+\beta} \tag{89}$$

6.2.2 Υβριδικός Τυχαίος Περίπατος με Γνώση Τοπολογίας-Βαθμού Κόμβου

Ο Υβριδικός Τυχαίος Περίπατος με Γνώση Τοπολογίας-Βαθμού Κόμβου (Hybrid Random Walk Topology Aware-node degree – $HRWTA-n$) λειτουργεί παρόμοια με τον Απλό Υβριδικό Τυχαίο Περίπατο με παραμέτρους α, β, με τη διαφορά ότι οι μεταβάσεις καταστάσεων είναι πλέον συναρτήσεις του βαθμού κόμβου που επισκέπτεται ο Περίπατος στο τρέχον βήμα. Η επέκταση αυτή αποσκοπεί στην ενσωμάτωση πληροφορίας τοπολογίας στη λειτουργία του Τυχαίου Περίπατου, λαμβάνοντας έτσι τα ιδιαίτερα δεδομένα γειτονίας μεταξύ των κόμβων του ασύρματου δικτύου όπως προκύπτει από το ασύρματο περιβάλλον και τη λειτουργία του δικτύου.

Για τις πιθανότητες μετάβασης μεταξύ καταστάσεων λειτουργίας χρησιμοποιείται ο κανονικοποιημένος βαθμός κόμβου (βαθμός κόμβου ανηγμένος στο συνολικό αριθμό κόμβων του δικτύου, $\frac{d}{N}$) του τρέχοντος κόμβου–κατάστασης του Περίπατου. Ο ανηγμένος βαθμός κόμβου χρησιμοποιείται προκειμένου οι ρυθμοί μετάβασης που θα προκύψουν να μην είναι δραματικά υπέρ μιας κατάστασης, ώστε πρακτικά ο Περίπατος να λειτουργεί σαν να βρισκόταν μόνο στη μια από τις δύο καταστάσεις, αλλά να εξασφαλίζεται μια ομαλή και πιο ουσιαστική κατανομή του χρόνου μεταξύ των δύο καταστάσεων.



HYBRID RW TOPOLOGY AWARE – node degree
(HRWTA-n)

Σχήμα 9 – Καταστάσεις λειτουργίας Υβριδικού Τυχαίου Περίπατου με Γνώση Τοπολογίας-Βαθμού Κόμβου

Αν ο περίπατος βρίσκεται στην κατάσταση Απλού Τυχαίου Περίπατου, τότε με πιθανότητα $\left(1-\frac{d}{N}\right)$ μεταβαίνει στην κατάσταση λειτουργίας πολλαπλών βημάτων. Αντίθετα, αν βρίσκεται ήδη εκεί, επιστρέφει στην κατάσταση Απλού Τυχαίου Περίπατου με πιθανότητα $\frac{d}{N}$. Με τις συμπληρωματικές πιθανότητες, $\frac{d}{N}$ για την κατάσταση 0 και $\left(1-\frac{d}{N}\right)$ για την κατάσταση 1, ο Περίπατος παραμένει στην τρέχουσα κατάσταση λειτουργίας (Σχήμα 9).

Το σκεπτικό του Υβριδικού Τυχαίου Περίπατου με Γνώση Τοπολογίας-Βαθμού Κόμβου έγκειται στην εκμετάλλευση πληροφορίας τοπολογίας με άμεσο τρόπο. Έτσι αν ο τρέχων κόμβος που βρίσκεται ο περίπατος έχει πολλούς γείτονες (υψηλός βαθμός κόμβου, δηλαδή υψηλό $\frac{d}{N}$) , τότε είναι πιο αποδοτικό να μείνει ο περίπατος στη γειτονιά αυτού του κόμβου, ώστε να καλύψει όσο περισσότερους γείτονες γίνεται. Αντίθετα, όταν ο λόγος $\frac{d}{N}$ είναι μικρός (λίγοι γείτονες), φαίνεται περισσότερο αποδοτικό να εκτελεστούν άλματα πολλαπλών βημάτων και ο Περίπατος να μεταφερθεί σε άλλα τμήματα του δικτύου, όπου ο ρυθμός επίσκεψης νέων κόμβων θα αυξηθεί.

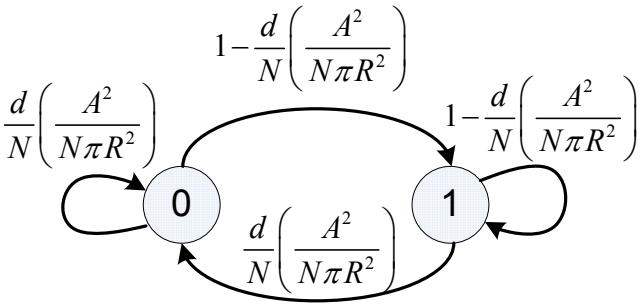
Ακολουθώντας την ίδια μέθοδο, όπως με το σχήμα Απλού Υβριδικού Ύπνου, οι εργοδικές πιθανότητες καταστάσεων λειτουργίας για τον Υβριδικό Τυχαίο Περίπατο με Γνώση Τοπολογίας-Βαθμού Κόμβου υπολογίζονται:

$$\pi_0 = \frac{d}{N}, \quad \pi_1 = 1 - \frac{d}{N} \tag{90}$$

6.2.3 Υβριδικός Τυχαίος Περίπατος με Γνώση Τοπολογίας-Πυκνότητας Δικτύου

Το σχήμα Υβριδικού Τυχαίου Περίπατου με Γνώση Τοπολογίας-Πυκνότητας Δικτύου (Hybrid Random Walk Topology Aware-density – $HRWTA-d$) είναι παρόμοιο σε λειτουργία με τον Υβριδικό Τυχαίο Περίπατο με Γνώση Τοπολογίας-Βαθμού Κόμβου. Τα δύο σχήματα διαφέρουν μόνο στους ρυθμούς μετάβασης μεταξύ καταστάσεων λειτουργίας.

Οι ρυθμοί μετάβασης στην περίπτωση του Υβριδικού Τυχαίου Περίπατου με Γνώση Τοπολογίας-Πυκνότητας Δικτύου είναι επίσης μεταβλητοί και εμπεριέχουν πληροφορία τοπολογίας που υπάρχει τοπικά στον κάθε χρήστη, σε συνδυασμό με συνολική πληροφορία του δικτύου. Ο τρέχων κόμβος που επισκέπτεται σε κάθε βήμα ο Περίπατος μπορεί να υπολογίσει την τοπική πυκνότητα δικτύου, διαιρώντας το βαθμό του με την ονομαστική περιοχή κάλυψής του $\frac{d}{\pi R^2}$, όπου R είναι η ακτίνα μετάδοσής του. Η τοπική πυκνότητα δικτύου, μπορεί να διαιρεθεί με την ολική πυκνότητα $\frac{N}{A^2}$, η οποία είναι γνωστή σε όλους τους κόμβους του δικτύου ως σχεδιαστική παράμετρος του δικτύου (αριθμός κόμβων, διαστάσεις δικτύου). Έτσι προκύπτει η τοπικά κανονικοποιημένη πυκνότητα δικτύου σε κάθε κόμβο. Απευθείας χρήση αυτής της ποσότητας οδηγούσε σε πολωμένες μεταβάσεις προς τη μια μόνο κατάσταση λειτουργίας στο μεγαλύτερο μέρος της διάρκειας μελέτης του συστήματος. Για να προκύψουν ομαλότερες μεταδόσεις και για να ισορροπηθεί κατάλληλα ο χρόνος λειτουργίας του Περίπατου μεταξύ των δύο τρόπων λειτουργίας, η κανονικοποιημένη πυκνότητα πολλαπλασιάζεται με ένα παράγοντα κλιμάκωσης που εξαρτάται από το συνολικό αριθμό κόμβων του δικτύου $K = K(N)$. Στην παρούσα μελέτη υιοθετήθηκε ο παράγοντας $K(N) = \frac{1}{N}$.



HYBRID RW TOPOLOGY AWARE - density
(HRWTA-d)

Σχήμα 10 – Καταστάσεις λειτουργίας Υβριδικού Τυχαίου Περίπατου με Γνώση Τοπολογίας-Πυκνότητας Δικτύου

Συνδυάζοντας τα παραπάνω, η πιθανότητα μετάβασης στην κατάσταση αλμάτων πολλαπλών βημάτων δίνεται από την ακόλουθη σχέση:

$$1-\frac{d}{N}\left(\frac{A^2}{N\pi R^2}\right) \tag{91}$$

ενώ η πιθανότητα παραμονής στην κατάσταση λειτουργίας Απλού Τυχαίου Περίπατου, από τη συμπληρωματική έκφραση:

$$\frac{d}{N}\left(\frac{A^2}{N\pi R^2}\right) \tag{92}$$

Αντίθετα, αν ο Περίπατος λειτουργεί στην κατάσταση αλμάτων πολλαπλών βημάτων η (92) δίνει την πιθανότητα μετάβασης στην κατάσταση 0 και η (91) αντιστοιχεί στην πιθανότητα παραμονής στην τρέχουσα κατάσταση 1 (Σχήμα 10). Οι εργοδικές πιθανότητες καταστάσεων λειτουργίας υπολογίζονται:

$$\pi_0=\frac{d}{N}\left(\frac{A^2}{N\pi R^2}\right),\ \pi_1=1-\frac{d}{N}\left(\frac{A^2}{N\pi R^2}\right) \tag{93}$$

Στο σημείο αυτό πρέπει να σημειωθεί ότι τα σχήματα Υβριδικού Τυχαίου Περίπατου με Γνώση Τοπολογίας (Πυκνότητας Δικτύου και βασιζόμενα στο Βαθμό Κόμβου) μοιράζονται την ιδέα της χρησιμοποίησης τοπικής πληροφορίας για να αποφασισθεί με ποιο τρόπο λειτουργίας θα μεταβεί ο Περίπατος στην επόμενη κατάσταση–κόμβο. Η διαφορά τους έγκειται στον χειρισμό της πληροφορίας που γίνεται διαθέσιμη και τους αντίστοιχους ρυθμούς μετάβασης μεταξύ καταστάσεων λειτουργίας.

6.3 Λειτουργία Τυχαίων Περίπατων – Αποτελέσματα Προσομοιώσεων

Οι παραλλαγές Τυχαίων Περίπατων που παρουσιάστηκαν παραπάνω εμφανίζουν διαφορετικά χαρακτηριστικά λειτουργίας και επομένως επίδοσης σε διαφορετικούς τύπους αυτοργανούμενων δικτύων. Για να βρεθεί ο καταλληλότερος τύπος μεθόδου για τους τύπους δικτύων που αναφέρθηκαν παραπάνω (Πίνακας 2), οι διαφορετικές εκδόσεις των προτεινόμενων σχημάτων (με άλματα σταθερού ή μεταβλητού μήκους) προσομοιώνονται για διαφορετικά σενάρια και συγκρίνονται με βάση το χρόνο κάλυψης και την κατανάλωση ενέργειας που απαιτείται για την επίτευξη αυτού του στόχου. Τα διαφορετικά σενάρια που λαμβάνονται υπόψη αντιστοιχούν τόσο σε διαφορετικούς τύπους δικτύων (μέσω αλλαγών στην κινητικότητα και πυκνότητά τους), όσο και σε διαφορετικά στιγμιότυπα του ίδιου τύπου δικτύου με διαφοροποιημένες συνθήκες.

Οι παράμετροι που χρησιμοποιήθηκαν για την εκτέλεση των προσομοιώσεων παρατίθενται συνοπτικά στον ακόλουθο πίνακα (Πίνακας 3). Συνολικά σε κάθε ένα σενάριο, N κόμβοι τοποθετήθηκαν στην περιοχή του δικτύου τυχαία και ομοιόμορφα, ώστε να μελετηθεί η συμπεριφορά των πρωτοκόλλων για αυξανόμενες πυκνότητες δικτύου.

Πίνακας 3 – Παράμετροι προσομοίωσης μεθόδων Τυχαίων Περίπατων

Διάσταση δικτύου	$L = 1000m$
Σταθερά απωλειών διάδοσης	$\gamma = 4$
Ισχύς μετάδοσης ενός βήματος	$P_h = 1mWatt$
Παράμετροι του *SHRW*	$\alpha = 0.3$, $\beta = 0.7$
Ακτίνα μετάδοσης	$R = 150m$
Σταθερό μήκος άλματος	*FixJump* = 3 βήματα
Μέγιστο μήκος μεταβλητού άλματος	*MaxJump* = 5 βήματα
Χαμηλή κινητικότητα	*Speed* = [0; 2 m/s], *PauseTime* = [0; 10 sec]
Μέτρια κινητικότητα	*Speed* = [0; 4 m/s], *PauseTime* = [0; 7 sec]
Υψηλή κινητικότητα	*Speed* = [0; 8 m/s], *PauseTime* = [0; 4 sec]

Στη συνέχεια παρατίθενται τα αποτελέσματα των προσομοιώσεων για τα διαφορετικά σενάρια δικτύων που μελετήθηκαν. Τα αποτελέσματα διαχωρίζονται σε δύο κατηγορίες, η πρώτη για στατικά δίκτυα και η δεύτερη για κινητά, προκειμένου

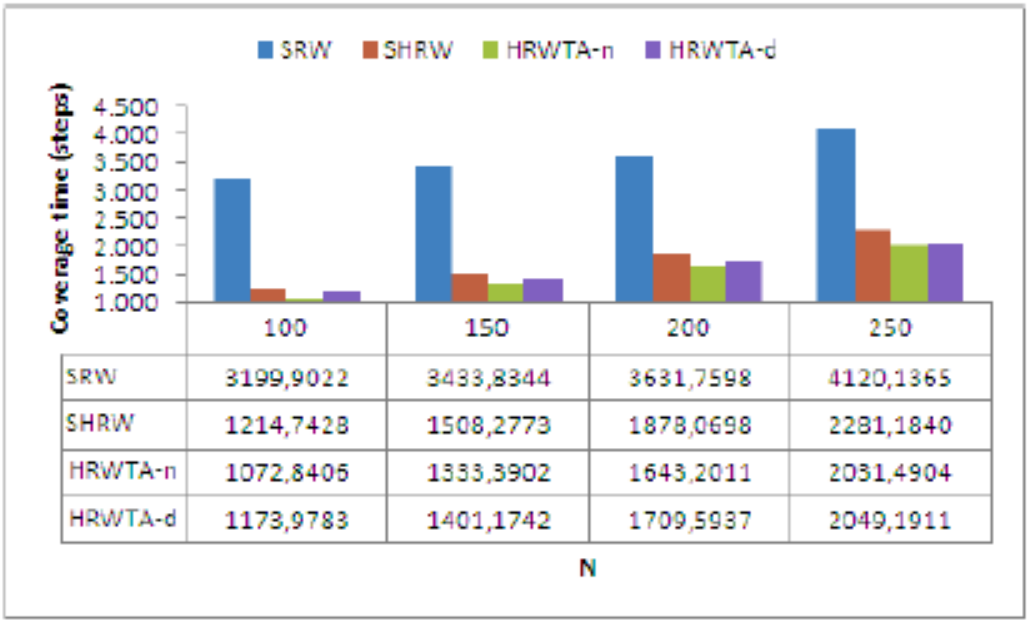
να μελετηθεί η επίδραση της κινητικότητας στη διάδοση κακόβουλου λογισμικού. Η παραλλαγή των υβριδικών σχημάτων με σταθερό μήκος άλματος αναφέρεται με το αναγνωριστικό *FixJump*. Στα αποτελέσματα που παρουσιάζονται το μήκος των αλμάτων για τις περιπτώσεις που είναι σταθερό, επιλέχθηκε *FixJump=3*. Η δεύτερη παραλλαγή με μεταβλητό μήκος άλματος τυχαία επιλεγμένου μέχρι μια μέγιστη τιμή, αναφέρεται με το αναγνωριστικό *MaxJump* και συνοδεύεται από την αντίστοιχη παράμετρο που αντιστοιχεί στο μέγιστο επιτρεπτό μήκος άλματος που μπορεί να πραγματοποιηθεί. Τα αποτελέσματα που παρουσιάζονται αποτελούν τις μέσες τιμές των αντίστοιχων μεγεθών που προέκυψαν μέσα από 10000 διαφορετικές τοπολογίες του εκάστοτε σεναρίου.

Για την αξιολόγηση της επίδοσης, η ανάλυση επικεντρώθηκε σε δύο βασικά μεγέθη, το χρόνο κάλυψης και την καταναλισκόμενη ενέργεια. Ο χρόνος κάλυψης υπολογίστηκε ως ο μέσος αριθμός βημάτων του Περίπατου για την κάλυψη του δικτύου για κάθε σενάριο. Στο απλοποιημένο μοντέλο κατανάλωσης ενέργειας κάθε απευθείας μετάδοση ενός βήματος απαιτεί μια σταθερή κατανάλωση ισχύος $P_h = 1mWatt$. Αν πρόκειται για άλμα πολλαπλών βημάτων καταναλώνεται τόση ισχύς όσο η απόσταση των κόμβων πηγής–προορισμού σε βήματα πολλαπλασιαμένη με την καταναλωση $P_h = 1mWatt$.

6.3.1 Στατικές Τοπολογίες

Αρχικά, θεωρούνται στατικές τοπολογίες δικτύων, ώστε να αναγνωριστεί η συμπεριφορά των σχημάτων και οι παράμετροι που τις επηρεάζουν, ανεξάρτητα από την επίδραση της κίνησης που θα μπορούσαν να είχαν οι κόμβοι. Στη συνέχεια προστίθεται και η παράμετρος της κινητικότητας και αναγνωρίζεται άμεσα το ποσοστό στο οποίο επηρεάζει τη λειτουργία των σχημάτων Τυχαίου Περίπατου.

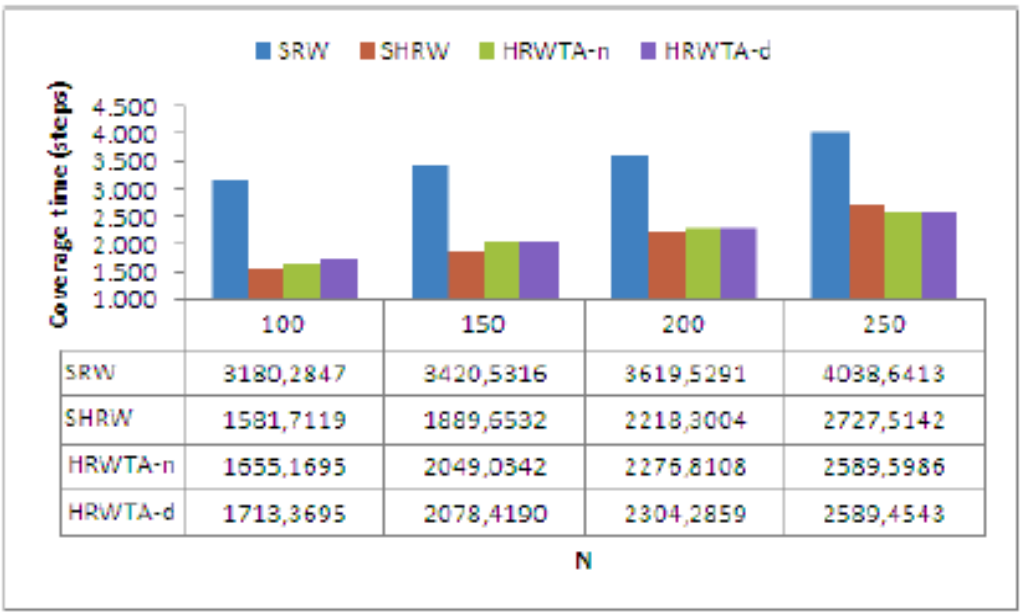
Στο Διάγραμμα 29 φαίνεται ο χρόνος κάλυψης (σε βήματα Περίπατου ή εναλλακτικά χρονικές στιγμές) για στατικά δίκτυα και μεταβλητό μήκος αλμάτων για διαφορετικές πυκνότητες δικτύων (αριθμός κόμβων δικτύου N). Τα ραβδογράμματα για κάθε τιμή αριθμού κόμβων δικτύου αντιστοιχούν κατά σειρά στο SRW, SHRW, HRWTA-n, HRWTA-d, τόσο για το Διάγραμμα 29, όσο και τα υπόλοιπα διαγραμμάτα. Στο Διάγραμμα 30 φαίνονται τα ίδια αποτελέσματα για την παραλλαγή σταθερού μήκους άλματος.



	100	150	200	250
SRW	3199,9022	3433,8344	3631,7598	4120,1365
SHRW	1214,7428	1508,2773	1878,0698	2281,1840
HRWTA-n	1072,8405	1333,3902	1643,2011	2031,4904
HRWTA-d	1173,9783	1401,1742	1709,5937	2049,1911

N

Διάγραμμα 29 – Χρόνος κάλυψης σε στατικά δίκτυα (*MaxJump*) για $N=100$, $N=150$, $N=200$ και $N=250$



	100	150	200	250
SRW	3180,2847	3420,5316	3619,5291	4038,6413
SHRW	1581,7119	1889,6532	2218,3004	2727,5142
HRWTA-n	1655,1695	2049,0342	2276,8108	2589,5986
HRWTA-d	1713,3695	2078,4190	2304,2859	2589,4543

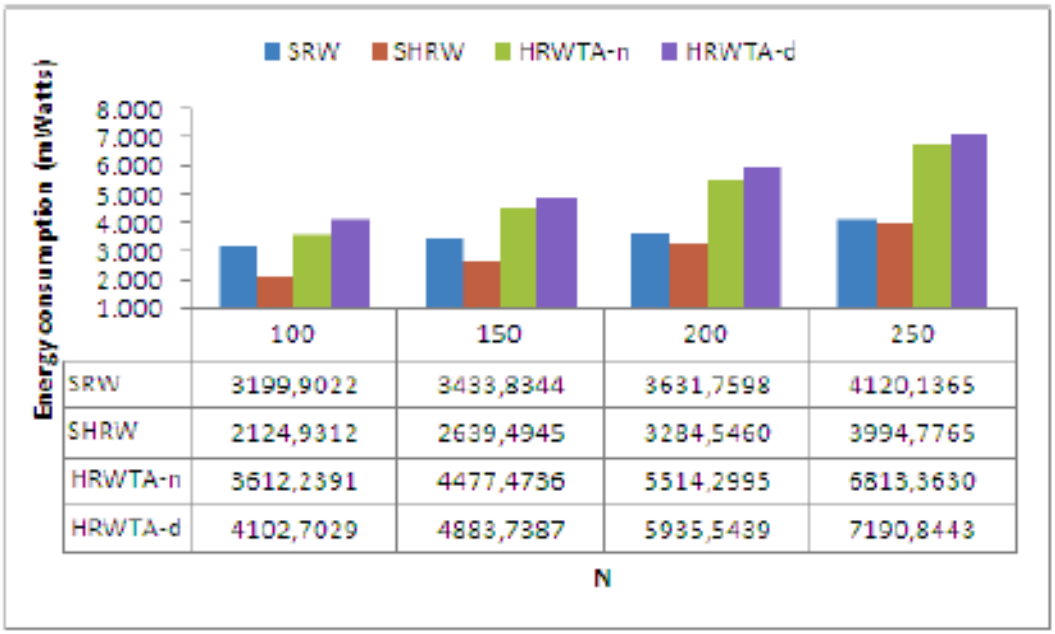
N

Διάγραμμα 30 – Χρόνος κάλυψης σε στατικά δίκτυα (*FixJump*) για $N=100$, $N=150$, $N=200$ και $N=250$

Σε όλα τα σενάρια, ο Απλός Υβριδικός Περίπατος (SRW) παρουσιάζει τη χειρότερη απόδοση, καταγράφοντας υψηλούς χρόνους κάλυψης με διαφορά σε σχέση με τα υβριδικά σχήματα, καταδεικνύοντας τη σημασία των αλμάτων πολλαπλών βημάτων. Αναφορικά με τις τοπολογίες του MaxJump το σχήμα HRWTA-n παρουσιάζει καλύτερη επίδοση από όλα τα σχήματα, ακολουθούμενο απο το

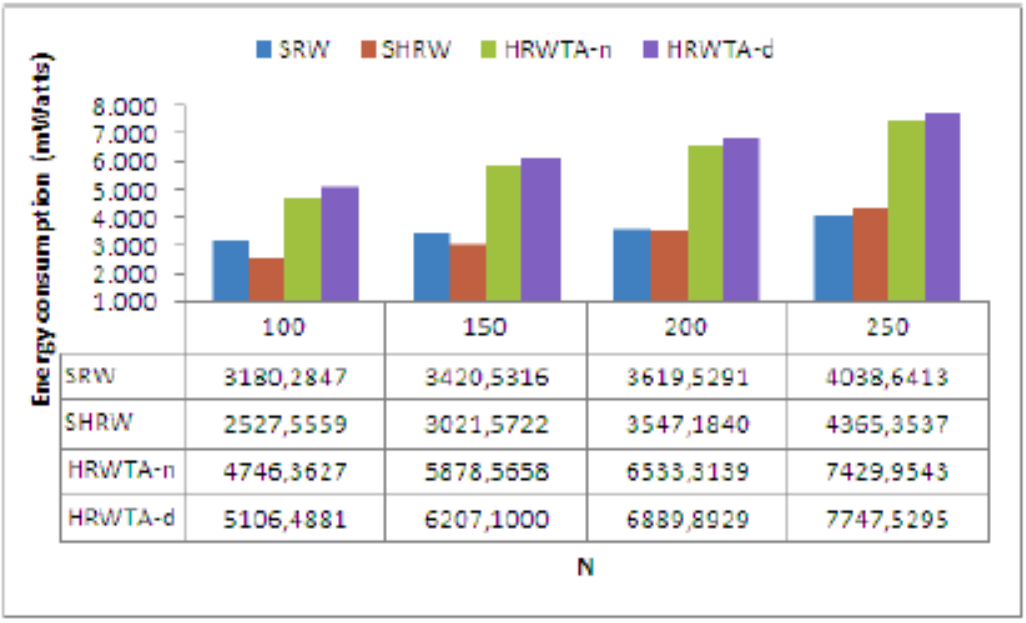
HRWTA-d και το SHRW. Ωστόσο, η διαφορά μεταξύ των υβριδικών σχημάτων είναι σχετικά μικρή, για τα πρωτόκολλα που λαμβάνουν υπόψη την υποκείμενη τοπολογία. Η διαφορά μεταξύ HRWTA-n και SHRW είναι περίπου 12% σε όλα τα σενάρια, ενώ η διαφορά μεταξύ HRWTA-n και HRWTA-d εξαρτάται από την πυκνότητα κόμβων. Πιο συγκεκριμένα, μεταβάλλεται από 8% για δίκτυα με χαμηλή πυκνότητα ($N = 100$) έως 1% για δίκτυα με υψηλή πυκνότητα ($N = 250$). Η μετάβαση από την παραλλαγή *MaxJump* στην υλοποίηση *FixJump* με άλματα σταθερού μήκους, οδηγεί σε μείωση της απόδοσης κατά περίπου 37% έως 46% για μικρή πυκνότητα κόμβων. Υπό το παραπάνω πρίσμα, το πιο αποδοτικό σχήμα είναι το SHRW όταν η πυκνότητα δικτύου είναι χαμηλή, ενώ τα HRWTA-n και HRWTA-d υπερτερούν στις άλλες περιπτώσεις.

Αναφορικά με την κατανάλωση ενέργειας, στο Διάγραμμα 31 φαίνεται η ισχύς που δαπανήθηκε (και είναι ενδεικτική της ενέργειας που καταναλώθηκε) για στατικά δίκτυα και την υλοποίηση *MaxJump* Τυχαίων Περίπατων, ενώ στο Διάγραμμα 32 φαίνεται η αντίστοιχη κατανάλωση για στατικά δίκτυα και την παραλλαγή *FixJump*.



	100	150	200	250
SRW	3199,9022	3433,8344	3631,7598	4120,1365
SHRW	2124,9312	2639,4945	3284,5460	3994,7765
HRWTA-n	3512,2391	4477,4736	5514,2995	6813,3630
HRWTA-d	4102,7029	4883,7387	5935,5439	7190,8443

Διάγραμμα 31 – Κατανάλωση ενέργειας σε στατικά δίκτυα (*MaxJump*) για $N = 100$, $N = 150$, $N = 200$ και $N = 250$



	100	150	200	250
SRW	3180,2847	3420,5316	3619,5291	4038,6413
SHRW	2527,5559	3021,5722	3547,1840	4365,3537
HRWTA-n	4746,3627	5878,5658	6533,3139	7429,9543
HRWTA-d	5106,4881	6207,1000	6889,8929	7747,5295

Διάγραμμα 32 – Κατανάλωση ενέργειας σε στατικά δίκτυα (*FixJump*) για $N=100$, $N=150$, $N=200$ **και** $N=250$

Τα αποτελέσματα των προσομοιώσεων δείχνουν ότι ο Απλός Τυχαίος Περίπατος και Απλός Υβριδικός Τυχαίος Περίπατος παρουσιάζουν την καλύτερη επίδοση αναφορικά με την κατανάλωση ενέργειας (μικρότερη συνολική απαιτούμενη ισχύς μετάδοσης). Φυσικά, η χαμηλότερη κατανάλωση ενέργειας που επιτυγχάνεται από αυτά τα σχήματα έρχεται με το αυξημένο κόστος σε χρόνο κάλυψης όπως φάνηκε παραπάνω. Τα σχήματα HRWTA-n και HRWTA-d δαπανούν περισσότερη ενέργεια λόγω των αλμάτων πολλαπλών βημάτων, τα οποία μεταφράζονται σε ενδιάμεσες απευθείας μεταδόσεις. Κάτι τέτοιο επιβεβαιώνεται και από το μέσο χρόνο που ο κάθε υβριδικός περίπατος βρίσκεται στην κατάσταση λειτουργίας αλμάτων πολλαπλών βημάτων (στάσιμη και εργοδική πιθανότητα π_1). Για την περίπτωση του SHRW αυτός ο χρόνος είναι σταθερός και ίδιος ανεξαρτήτως τρέχοντος κόμβου. Για τις παραμέτρους που χρησιμοποιήθηκαν στη συγκεκριμένη προσομοίωση (Πίνακας 3), ο μέσος χρόνος εκτέλεσης αλμάτων πολλαπλών βημάτων ανέρχεται στο 30%. Για τα υβριδικά σχήματα που λαμβάνουν υπόψη την τοπολογία, το συγκεκριμένο χρονικό ποσοστό μπορεί να ανέρχεται στο 90% (HRWTA-n) έως και 99% (HRWTA-d).

Οι επιδόσεις των απλών σχημάτων (τυπικού και υβριδικού) είναι σχεδόν παρόμοιες για πυκνά δίκτυα, ειδικά αναφορικά με την παραλλαγή *FixJump*. Το υβριδικό σχήμα (SHRW) αποδίδει καλύτερα από το τυπικό (SRW) σε δίκτυα μεγάλου μεγέθους με χαμηλή πυκνότητα κόμβων. Αντίθετα, όταν η πυκνότητα

αυξάνει οι επιδόσεις αντιστρέφονται. Μεταξύ των υβριδικών σχημάτων με γνώση τοπολογίας (HRWTA-n και HRWTA-d), το απλούστερο από αυτά που βασίζεται στο βαθμό κόμβου (HRWTA-n) εμφανίζεται καλύτερο στην κατανάλωση ενέργειας (χαμηλότερη απαιτούμενη ισχύς). Συγκριτικά με τις δύο παραλλαγές (*MaxJump* και *FixJump*), καλύτερες επιδόσεις στον τομέα κατανάλωσης ενέργειας επιτυγχάνονται με δυναμικό μήκος άλματος (*MaxJump*). Το εύρος μεταξύ των δύο υλοποιήσεων κυμαίνεται μεταξύ 10-30%.

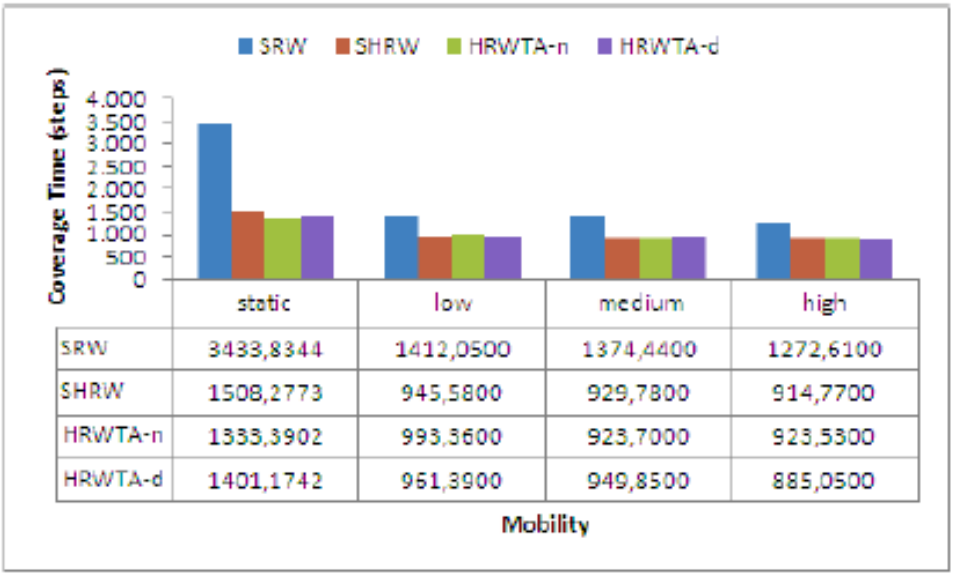
Από την ανάλυση που προηγήθηκε, γίνεται φανερό ότι τα άλματα πολλαπλών βημάτων στους Τυχαίους Περίπατους προσφέρουν σημαντικές βελτιώσεις από την οπτική γωνία των κακόβουλων χρηστών. Συγκρίνοντας το χρόνο κάλυψης για τα διάφορα πρωτόκολλα, τα υβριδικά προσφέρουν βελτιώσεις της τάξης του 60% (περίπτωση *MaxJump*) και 40% (περίπτωση FixJump) σε σχέση με τον Απλό Τυχαίο Περίπατο. Αντίθετα, η χρησιμοποίηση υβριδικών προσεγγίσεων συνοδεύεται από το κόστος της υψηλότερης κατανάλωσης ενέργειας. Επομένως, σε ένα αυτοργανούμενο δίκτυο που η κατανάλωση ενέργειας δεν είναι κρίσιμος παράγοντας, όπως είναι τα δίκτυα πλέγματος (mesh), το Υβριδικό σχήμα Τυχαίου Περίπατου με Γνώση Τοπολογίας-Βαθμού Κόμβου (HRWTA-n) μπορεί να προσφέρει τη μέγιστη αποδοτικότητα στη διάδοση ενός τμήματος κακόβουλου λογισμικού. Αντίθετα, το Απλό Υβριδικό Σχήμα (SHRW) είναι καταλληλότερο για τύπους δικτύων με περιορισμένα αποθέματα ενέργειας όπως είναι τα δίκτυα αισθητήρων.

6.3.2 Τοπολογίες Κινητών Κόμβων

Για τη μελέτη δικτύων κινητών κόμβων χρησιμοποιήθηκε το μοντέλο κινητικότητας Τυχαίων Προορισμών (Random Waypoint Model – RWP) [43]. Οι κόμβοι μετακινούνται στο δίκτυο, επιλέγοντας τυχαία και με ομοιόμορφη κατανομή τον επόμενο προορισμό εντός της περιοχής ανάπτυξης του δικτύου. Η τροχιά του κόμβου από την τρέχουσα στην επόμενη θέση είναι ευθύγραμμο τμήμα. Τρεις βαθμοί κινητικότητας έχουν χρησιμοποιηθεί (Πίνακας 3) σε σχέση με την ταχύτητα με την οποία κινούνται οι κόμβοι μεταξύ των αρχικών και τελικών θέσεων.

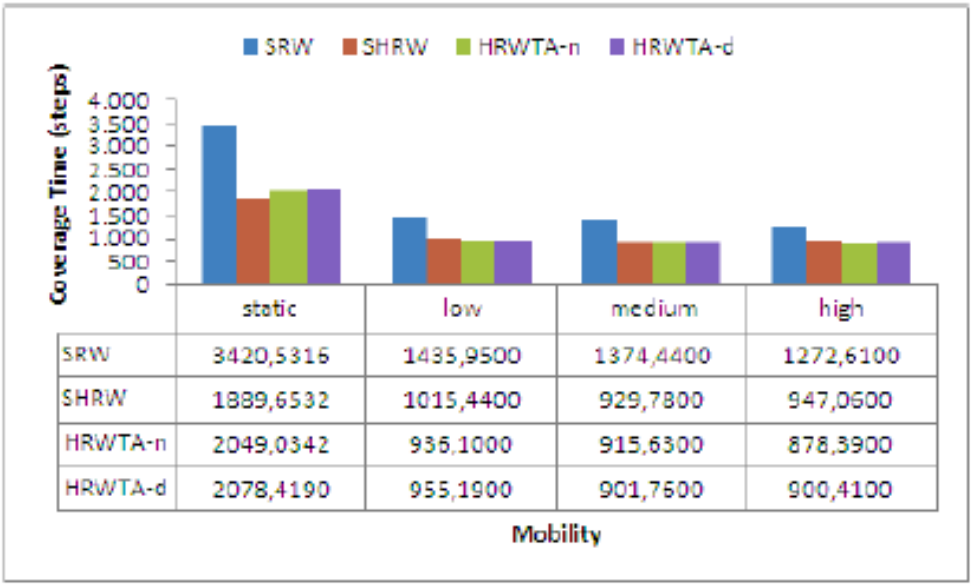
Στο Διάγραμμα 33 παρουσιάζονται τα αποτελέσματα του χρόνου κάλυψης για κινητά δίκτυα και την παραλλαγή *MaxJump*, ενώ στο Διάγραμμα 34 φαίνονται τα αντίστοιχα για την υλοποίηση *FixJump* και τα δύο για $N = 150$ κόμβους. Με μια συνολική ματιά είναι εμφάνες ότι η κινητικότητα συντελεί στη μείωση των τοπικών

επαναλαμβανόμενων επισκέψεων, οδηγώντας σε ακόμα χαμηλότερους χρόνους κάλυψης του δικτύου. Ο βαθμός της κινητικότητας δεν επηρεάζει σημαντικά τα αποτελέσματα, παρόλο που όσο αυξάνει ο βαθμός της κινητικότητας των κόμβων (μεγαλύτερες ταχύτητες), τόσο βελτιώνονται και οι χρόνοι κάλυψης των σχημάτων Τυχαίου Περίπατου.



	static	low	medium	high
SRW	3433,8344	1412,0500	1374,4400	1272,6100
SHRW	1508,2773	945,5800	929,7800	914,7700
HRWTA-n	1333,3902	993,3600	923,7000	923,5300
HRWTA-d	1401,1742	961,3900	949,8500	885,0500

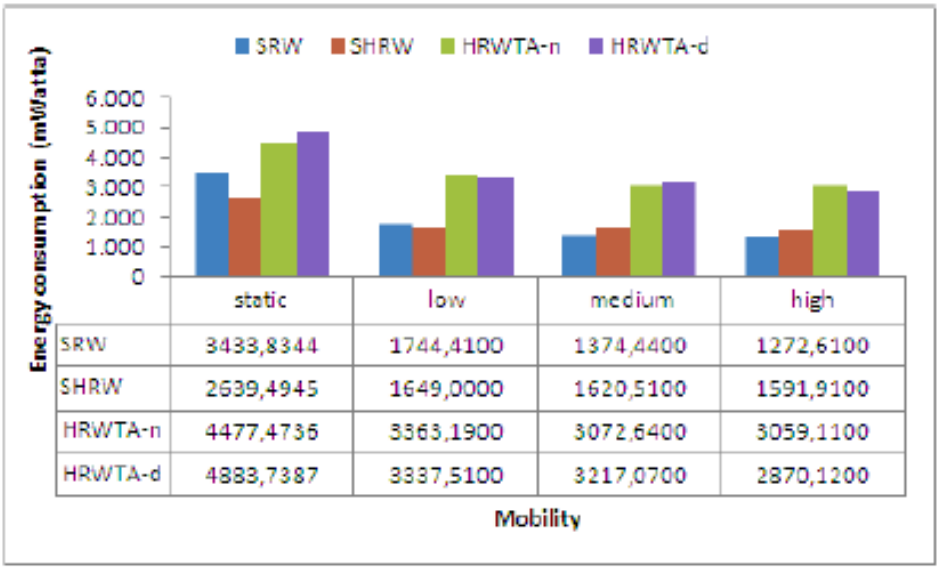
Διάγραμμα 33 – Χρόνος κάλυψης σε κινητά δίκτυα (*MaxJump*) για διαφορετικούς βαθμούς κινητικότητας {*static*, *low*, *medium*, *high*}



	static	low	medium	high
SRW	3420,5316	1435,9500	1374,4400	1272,6100
SHRW	1889,6532	1015,4400	929,7800	947,0600
HRWTA-n	2049,0342	936,1000	915,6300	878,3900
HRWTA-d	2078,4190	955,1900	901,7600	900,4100

Διάγραμμα 34 – Χρόνος κάλυψης σε κινητά δίκτυα (*FixJump*) για διαφορετικούς βαθμούς κινητικότητας {*static*, *low*, *medium*, *high*}

Με βάση το Διάγραμμα 33 και Διάγραμμα 34 φαίνεται ότι το σχήμα που ωφελείται περισσότερο από την κινητικότητα αναφορικά με το χρόνο κάλυψης των κόμβων είναι ο Απλός Τυχαίος Περίπατος (SRW). Σε αυτή την προσέγγιση δεν υπάρχει κάποιος εγγενής μηχανισμός αποφυγής επαναλαμβανόμενων επισκέψεων σε κόμβους, όπως συμβαίνει στους υβριδικούς με γνώση τοπολογικής πληροφορίας. Η κινητικότητα μπορεί να θεωρηθεί ένας έμμεσος τρόπος εκτέλεσης αλμάτων, μιας και ο κινητός κόμβος μεταφέρεται σε άλλη γειτονιά του δικτύου ακριβώς σαν να είχε εκτελέσει ένα άλμα προς εκείνη την περιοχή. Φυσικά τα υβριδικά σχήματα σε κινητό περιβάλλον μπορούν να θεωρηθούν σαν υπερθέσεις δύο μεθόδων εκτέλεσης αλμάτων. Έτσι, ο Απλός Τυχαίος Περίπατος βελτιώνεται κατά περίπου 60% σε κινητά δίκτυα. Σε σχέση με το χρόνο κάλυψης, γενικά παρατηρούνται βελτιώσεις της τάξης του 33% για την παραλλαγή *MaxJump* και 56% για την υλοποίηση *FixJump* αντίστοιχα. Συνολικά, η σχετική συμπεριφορά των πρωτοκόλλων είναι παρόμοια μεταξύ των δύο διαφορετικών εκδόσεων (*MaxJump*, *FixJump*).

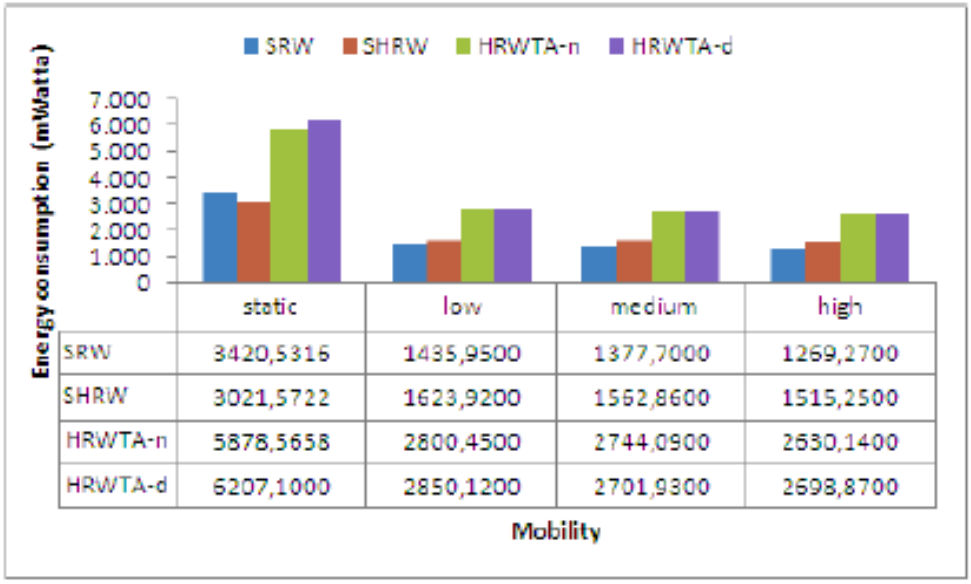


	static	low	medium	high
SRW	3433,8344	1744,4100	1374,4400	1272,6100
SHRW	2639,4945	1649,0000	1620,5100	1591,9100
HRWTA-n	4477,4736	3363,1900	3072,6400	3059,1100
HRWTA-d	4883,7387	3337,5100	3217,0700	2870,1200

Διάγραμμα 35 – Κατανάλωση ενέργειας σε κινητά δίκτυα (*MaxJump*) για διαφορετικούς βαθμούς κινητικότητας {*static*, *low*, *medium*, *high*}

Σχετικά με την απαιτούμενη ενέργεια και σχετιζόμενη ισχύ εκπομπής, τα αντίστοιχα αποτελέσματα παρουσιάζονται στο Διάγραμμα 35 (MaxJump), και το Διάγραμμα 36 (FixJump). Η βελτίωση στην κατανάλωση για τις εκδόσεις μεταβλητού μήκους άλματος είναι της τάξης του 36% και τις εκδόσεις σταθερού

μήκους της τάξης του 53%. Επομένως, η δεύτερη παραλλαγή επιτρέπει μεγαλύτερη δυνατή εκμετάλλευση της κινητικότητας που παρουσιάζει ένα δίκτυο. Ο Απλός Υβριδικός Περίπατος εμφανίζεται επικρατέστερος όλων των υπόλοιπων υβριδικών Περίπατων, ωστόσο οι διαφορές μεταξύ τους εξαφανίζονται καθώς αυξάνεται ο βαθμός κινητικότητας και επομένως το δίκτυο εμφανίζεται χωρικά πιο ομοιογενές και το ασύρματο κανάλι αλλάζει δραστικά και γρήγορα [99].



Διάγραμμα 36 – Κατανάλωση ενέργειας σε κινητά δίκτυα (*FixJump*) για διαφορετικούς βαθμούς κινητικότητας {*static*, *low*, *medium*, *high*}

6.4 Συνολική Θεώρηση Τυχαίων Περίπατων

Με βάση την ανάλυση και τα αποτελέσματα προσομοιώσεων για τα σχήματα Τυχαίων Περίπατων που δόθηκαν παραπάνω και λαμβάνοντας υπόψη τα ιδιαίτερα χαρακτηριστικά διαφόρων τύπων αυτοργανούμενων δικτύων (Πίνακας 2), επιχειρείται σε αυτό το σημείο να προσδιοριστεί το καταλληλότερο σχήμα διασποράς κακόβουλου λογισμικού σε τέτοια δίκτυα.

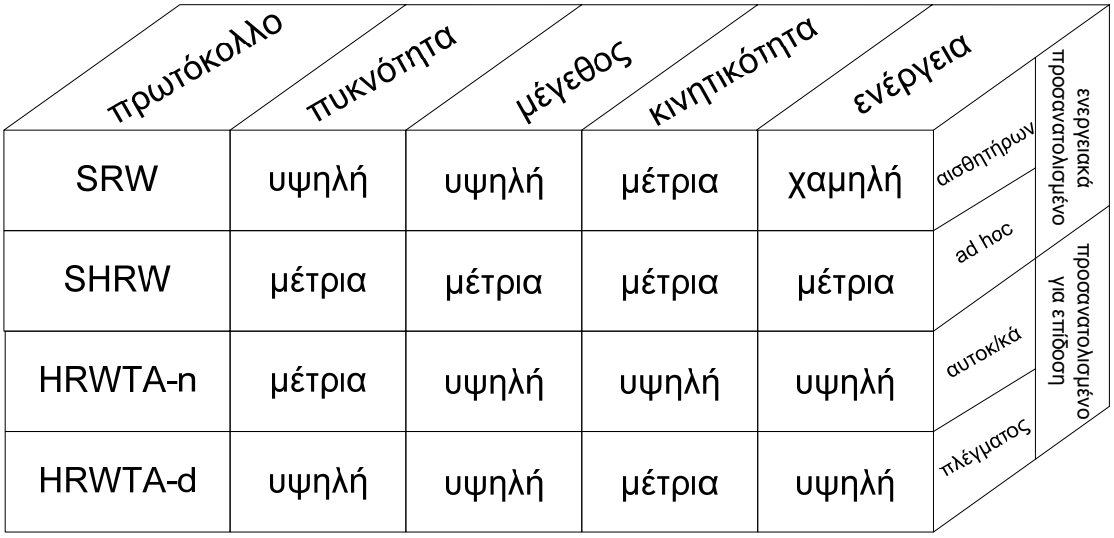
Όπως ήδη αναφέρθηκε τα υβριδικά σχήματα με γνώση τοπολογίας (HRWTA) παρουσιάζουν καλύτερες επιδόσεις με υψηλότερη κατανάλωση. Επομένως, φαίνονται καταλληλότερα για χρήση σε δίκτυα πλέγματος και αυτοκινητιστικά δίκτυα. Σε αυτά οι περιορισμοί ενέργειας δεν είναι καθόλου αυστηροί (αν υπάρχουν) και το μέγεθός τους είναι συνήθως μεγάλο με πυκνότητες μεσαίες ως ηψηλές. Επομένως, για τέτοιου είδους δίκτυα απαιτούνται υψηλές επιδόσεις για να επιτευχθεί αποδοτική διασπορά

κακόβουλου λογισμικού. Ο βαθμός της κινητικότητας μεταβάλλεται από πολύ χαμηλό (δίκτυα πλέγματος) μέχρι πολύ υψηλό (αυτοκινητιστικά δίκτυα), ωστόσο η λειτουργία των υιοθετούμενων σχημάτων παραμένει ικανοποιητική, επειδή η κινητικότητα φαίνεται να βοηθά στη διάδοση, γεγονός που έχει επιβεβαιωθεί και σε παλαιότερες μελέτες [100],[101]. Μεταξύ των δύο υβριδικών Περίπατων με γνώση τοπολογίας, ο βασιζόμενος στο βαθμό κόμβου (HRWTA-n) είναι καταλληλότερος για αυτοκινητιστικά δίκτυα και ο βασιζόμενος στην πυκνότητα δικτύου (HRWTA- d) καταλληλότερος για δίκτυα πλέγματος, μιας και ο πρώτος έχει μεν καλύτερη επίδοση, αλλά παρουσιάζει και μεγαλύτερη κατανάλωση, η οποία στην περίπτωση των αυτοκινητιστικών δικτύων δεν εγείρει ζητήματα. Επιπρόσθετα, το HRWTA-n είναι καταλληλότερο για επίθεση σε δίκτυα υψηλότερων πυκνοτήτων (αν δεν τίθεται θέμα διάρκειας ζωής), όπως συμβαίνει με τα αυτοκινητιστικά.

Αντίθετα, ο Απλός Τυχαίος Περίπατος και ο Απλός Υβριδικός Τυχαίος Περίπατος είναι καταλληλότεροι για αυτοργανούμενα ad hoc δίκτυα και δίκτυα αισθητήρων, λόγω της χαμηλότερης κατανάλωσης που εξασφαλίζουν. Η επίδοση θα είναι αναγκαστικά μειωμένη, ωστόσο το κέρδος ενέργειας είναι σημαντικά μεγαλύτερο, επιτρέποντας μακρύτερες περιόδους ζωής με ομαλότερη λειτουργία. Μεταξύ των δύο, ο Απλός Υβριδικός Τυχαίος Περίπατος είναι καταλληλότερος για δίκτυα με μέτρια προς χαμηλή πυκνότητα κόμβων, ενώ ο Απλός Τυχαίος Περίπατος αποδίδει καλύτερα σε υψηλές πυκνότητες κόμβων. Επομένως, ο Απλός Υβριδικός Τυχαίος Περίπατος διαφαίνεται κατάλληλος για αυτοργανούμενα δίκτυα και ο Απλός Υβριδικός για δίκτυα αισθητήρων. Η κατανάλωση ενέργειας είναι χαμηλή και για τα δύο σχήματα για πυκνότητες και μεγέθη δικτύου, τα οποία είναι αρκετά ρεαλιστικά, ενώ η επίδοσή τους δεν είναι σημαντικά χαμηλότερη από τις υβριδικές μεθόδους που έχουν καλύτερη απόδοση.

Επιγραμματικά, τα υβριδικά σχήματα παρουσιάζονται καταλληλότερα για τύπους δικτύων που η επίδοση είναι καίριο ζητούμενο, ενώ τα σχήματα απλών υβριδικών Περίπατων είναι αποδοτικότερα για ενεργειακά περιορισμένα δίκτυα. Ειδικότερα για τα σχήματα που προτάθηκαν και εξετάστηκαν στην παρούσα μελέτη, ο Υβριδικός Τυχαίος Περίπατος με Γνώση Τοπολογίας-Βαθμού Κόμβου (HRWTA-n) είναι καταλληλότερος για αυτοκινητιστικά δίκτυα, ο Υβριδικός Τυχαίος Περίπατος με Γνώση Τοπολογίας-Πυκνότητας Δικτύου (HRWTA-d) καταλληλότερος για δίκτυα πλέγματος, ο Απλός Υβριδικός Τυχαίος Περίπατος (SHRW) για αυτοργανούμενα

δίκτυα και ο Απλός Τυχαίος Περίπατος (SRW) για δίκτυα αισθητήρων. Στο Σχήμα 11 φαίνεται εποπτικά το κάθε σχήμα και ο τύπος δικτύου για το οποίο είναι καταλληλότερο με βάση τα ιδιαίτερα χαρακτηριστικά λειτουργίας και απαιτήσεων.



Σχήμα 11 – Καταλληλότητα σχημάτων Τυχαίων Περίπατων για διάφορους τύπους δικτύων

Κεφάλαιο 7

Συμπεράσματα και Μελλοντική Εργασία

Στην παρούσα διατριβή μελετήθηκε το πρόβλημα της διάδοσης κακόβουλου λογισμικού σε ασύρματα αυτοργανούμενα δίκτυα χωρίς κεντρική δομή, όπως είναι τα δίκτυα αισθητήρων, τα ad hoc, τα δίκτυα πλέγματος και τα αυτοκινητιστικά δίκτυα. Το συγκεκριμένο πρόβλημα είναι ιδιαίτερα επίκαιρο και με αυξανόμενο ενδιαφέρον, όσο μεγεθύνεται η διείσδυση των ασύρματων δικτύων χωρίς κεντρική υποδομή στην καθημερινή ζωή. Παρά το μέγεθος της προγενέστερης εργασίας, οι προσπάθειες μελέτης και σχεδίασης εστιάζονταν μέχρι πρότινος σε ενσύρματα δίκτυα, ενώ όσες μελέτες επικεντρώνονταν σε ασύρματα τροποποιούσαν τις υπάρχουσες, χωρίς να μπορούν να ενσωματώσουν τα ιδιαίτερα χαρακτηριστικά των αυτοργανούμενων δικτύων με εγγενή τρόπο. Αντίθετα στην παρούσα εργασία έγινε προσπάθεια για ακριβή και αναλυτική περιγραφή της διάδοσης κακόβουλου λογισμικού σε ασύρματα αυτοργανούμενα δίκτυα με γενικό και σαφή τρόπο.

Η μελέτη ξεκίνησε από την περιγραφή και μελέτη της διάδοσης μέσω ενός πρωτοποριακού μοντέλου κλειστού δικτύου ουρών αναμονής. Από την ανάλυση του προτεινόμενου μοντέλου προέκυψαν αναλυτικές εκφράσεις για τον αναμενόμενο αριθμό μολυσμένων κόμβων και τον αναμενόμενο συνολικό ρυθμό μόλυνσης κόμβων σε δίκτυα διασποράς και μη-διασποράς. Τα δύο αυτά μεγέθη χρησιμοποιήθηκαν ως χρονικά–ανεξάρτητα κριτήρια σύγκρισης επίδοσης μεταξύ διαφόρων σχημάτων διασποράς κακόβουλου λογισμικού. Επιπρόσθετα, προτάθηκε και χρησιμοποιήθηκε ένα χρονικά–εξαρτώμενο μέγεθος, η Αποδοτικότητα Μόλυνσης, με βάση την οποία καθίσταται δυνατή η μελέτη της επίδρασης και της κατανάλωσης ενέργειας σε επιθέσεις τέτοιου τύπου δικτύων.

Από τις αναλυτικές εκφράσεις που ελήφθησαν, κατέστη δυνατό να αναγνωριστούν οι παράγοντες που επηρεάζουν περισσότερο τη διασπορά του κακόβουλου λογισμικού και να χρησιμοποιηθούν για τη σχεδίαση έξυπνων τεχνικών διάδοσης κακόβουλου λογισμικού. Εκμεταλλευόμενοι την τεχνική του Ελέγχου Τοπολογίας, σχεδιάστηκαν αποδοτικότερες τεχνικές διασποράς κακόβουλου

λογισμικού και συγκρίθηκαν μεταξύ τους, ώστε να αναγνωριστεί η κατά περίπτωση ιδανικότερη, ανάλογα με τα ιδιαίτερα χαρακτηριστικά του δικτύου για το οποίο επιλέγεται. Επιπρόσθετα, μελετήθηκαν τεχνικές διάδοσης κακόβουλου λογισμικού που βασίζονται σε Τυχαίους Περίπατους με σκοπό τη διασπορά ενός κακόβουλου τμήματος λογισμικού σε όλο το δίκτυο, όσο το δυνατόν πιο αποδοτικά και με το μικρότερο δυνατό κόστος. Προτάθηκαν υβριδικές μέθοδοι Τυχαίων Περίπατων και συγκρίθηκαν με τον απλό Τυχαίο Περίπατο, ώστε να αναγνωριστούν οι καταλληλότερες για διαφορετικά σενάρια και τύπους αυτοργανούμενων δικτύων.

7.1 Συμπεράσματα

Μέσα από την εργασία που συνοψίσθηκε παραπάνω, προέκυψαν αρκετά συμπεράσματα, αρχικά θεωρητικού χαρακτήρα που θα μπορούσαν να χρησιμοποιηθούν για την επέκταση των αναλυτικών αποτελεσμάτων, αλλά και πιο πρακτικά που θα μπορούσαν να χρησιμοποιηθούν για τη σχεδίαση αποδοτικών αντίμετρων για την προστασία των δικτύων και των υπηρεσιών χρηστών.

Αναφορικά με το προτεινόμενο αναλυτικό μοντέλο περιγραφής της διάδοσης κακόβουλου λογισμικού προέκυψαν τα ακόλουθα συμπεράσματα:

- Το σχήμα του δικτύου κλειστών ουρών και πιο συγκεκριμένα το ισοδύναμο Norton των δύο εν σειρά ουρών με ανάδραση μπορεί να περιγράψει γενικότερα τη διάδοση κακόβουλου λογισμικού σε οποιοδήποτε τύπο δικτύου, αρκεί να ενσωματωθούν κατάλληλα οι λεπτομέρειες των μεταβάσεων καταστάσεων που εξαρτώνται από το συγκεκριμένο τύπο δικτύου και περιβάλλοντος λειτουργίας.
- Η συγκεκριμενοποίηση του μοντέλου για την περίπτωση αυτοργανούμενων δικτυών τύπου ad hoc και αισθητήρων είναι εφικτή και οδήγησε για πρώτη φορά σε απλές αναλυτικές εκφράσεις που μπορούν να χρησιμοποιηθούν άμεσα, τόσο από τη σκοπιά των κακόβουλων χρηστών για την αύξηση της αποδοτικότητας μιας επίθεσης, όσο και από τη σκοπιά του δικτύου για την καλύτερη προστασία του απέναντι σε διάφορες επιθέσεις. Τα αποτελέσματα προσφέρονται για τον ορισμό προβλημάτων βελτιστοποίησης και την εξέταση των ορίων στα οποία μπορεί να κινηθεί μια στρατηγική επίθεσης ή αντίστοιχα ένα σύνολο αντίμετρων.
- Τα αποτελέσματα της εργασίας προέκυψαν μελετώντας τα υποκείμενα συστήματα από τη σκοπιά των κακόβουλων χρηστών. Ωστόσο, με απλή αντιστροφή των συμπερασμάτων που κατέληξε η μελέτη, μπορούν να προκύψουν ιδιαίτερα

χρήσιμα συμπεράσματα, τα οποία μπορούν να χρησιμοποιηθούν για τη θωράκιση των δικτύων από μελλοντικές και έξυπνα σχεδιασμένες απειλές. Η παρούσα εργασία αποτελεί το πρώτο βήμα, ώστε να γίνει κατανοητή η έκταση της επίδρασης που μπορεί να έχουν διάφορες αποδοτικές στρατηγικές διάδοσης κακόβουλου λογισμικού και με βάση το γενικό πλαίσιο μοντελοποίησης και ανάλυσης τέτοιων επιθέσεων να ακολουθήσει σχεδίαση και αξιολόγηση κατάλληλων μέτρων προστασίας.

- Από τη μελέτη και τις προσομοιώσεις για την εξέταση της συμπεριφοράς της διάδοσης κακόβουλου λογισμικού σε αυτοργανούμενα δίκτυα διασποράς και μη-διασποράς, έγινε φανερή η επίδραση της τοπολογίας στην εξέλιξη του φαινομένου. Πιο συγκεκριμένα διαφάνηκε ο καθοριστικός ρόλος που έχουν οι τοπικές αλληλεπιδράσεις μεταξύ των δύο ομάδων κόμβων (κακόβουλων – νόμιμων), δηλαδή η τοπολογία του δικτύου στη γειτονιά ενός κόμβου και ο τρόπος που ελέγχονται οι αλληλεπιδράσεις αυτές από την ακτίνα μετάδοσης και την πυκνότητα του δικτύου.

- Η χρήση Ελέγχου Τοπολογίας και γενικότερα ελέγχου ισχύος αποδεικνύεται ιδιαίτερα αποδοτική τόσο από τη σκοπιά των επιτιθέμενων, όσο και από την οπτική των κόμβων του δικτύου. Πρόκειται για ένα μηχανισμό ο οποίος παρέχει τα μέσα για γρήγορη προσαρμογή στις μεταβολές που επιφέρουν οι τοπικές επιδράσεις και το συμβιβασμό μεταξύ των απαιτήσεων και κόστους λειτουργίας. Η τρέχουσα μελέτη έδωσε το έναυσμα για περαιτέρω εργασίες στην περιοχή και διαφορετικές οπτικές γωνίες από τις οποίες μπορεί να προσεγγιστεί το πρόβλημα [73] .

- Μεταξύ των τεχνικών διάδοσης κακόβουλου λογισμικού που εξετάστηκαν, στη γενική περίπτωση, οι τεχνικές που βασίζονταν σε σχήματα τοποθέτησης υποσυνόλων κόμβων σε κατάσταση παύσης λειτουργίας ήταν καταλληλότερες για τις περιπτώσεις δικτύων που εμφανίζουν εγγενώς υψηλή κατανάλωση ενέργειας στην άεργο κατάσταση. Αντίθετα, οι τεχνικές που βασίζονταν σε Έλεγχο Τοπολογίας στο στρώμα Δικτύου, παρουσιάστηκαν επικρατέστερες για δίκτυα με χαμηλή κατανάλωση ενέργειας στην άεργο κατάσταση. Αναφορικά με τις μεθόδους διάδοσης ενός τύπου κακόβουλου λογισμικού σε όλους τους κόμβους δικτύου, τα υβριδικά σχήματα Τυχαίων Περίπατων παρουσιάζονται καταλληλότερα για τύπους δικτύων που η επίδοση είναι καίριο ζητούμενο, ενώ τα

σχήματα απλών υβριδικών Περίπατων είναι αποδοτικότερα για ενεργειακά περιορισμένα δίκτυα. Ειδικότερα, ο Υβριδικός Τυχαίος Περίπατος με Γνώση Τοπολογίας–Βαθμού Κόμβου (HRWTA-n) είναι καταλληλότερος για αυτοκινητιστικά δίκτυα, ο Υβριδικός Τυχαίος Περίπατος με Γνώση Τοπολογίας–Πυκνότητας Δικτύου (HRWTA-d) καταλληλότερος για δίκτυα πλέγματος, ο Απλός Υβριδικός Τυχαίος Περίπατος (SHRW) για αυτοργανούμενα δίκτυα και ο Απλός Τυχαίος Περίπατος (SRW) για δίκτυα αισθητήρων.

7.2 Μελλοντική Εργασία

Το πρόβλημα της διάδοσης κακόβουλου λογισμικού αναμένεται να αυξηθεί σημαντικά στα επόμενα χρόνια. Δεδομένης της οικονομικής και κοινωνικής σημασίας που αποκτούν τα ασύρματα αυτοργανούμενα δίκτυα, εκτιμάται ένταση των επιθέσεων και μεγαλύτερη ποικιλία στο κακόβουλο λογισμικό που ανιχνεύεται. Επομένως, η μελέτη διάδοσης κακόβουλου λογισμικού στη βάση του γενικού πλαισίου που περιγράφηκε στην παρούσα εργασία αποκτά μεγαλύτερο ενδιαφέρον και αποτελεί έναυσμα για ευρύτερες προσεγγίσεις. Τρεις κατευθύνσεις που θα μπορούσε να ακολουθήσει κανείς για να επεκτείνει την ανάλυση ή να προσεγγίσει το πρόβλημα υπό διαφορετική αλλά συμβατή οπτική με το προτεινόμενο μοντέλο της παρούσας εργασίας έχουν άμεσα αναγνωριστεί και βρίσκονται υπό ανάπτυξη ή θα τεθούν σύντομα υπό μελέτη.

Σημαντικό βήμα στην περαιτέρω γενίκευση του μοντέλου θα μπορούσε να αποτελέσει η επέκταση των διαδικασιών άφιξης–αναχώρησης στο κλειστό δίκτυο ουρών, στην ευρύτερη δυνατή περίπτωση όπου δύο G/G/1 ουρές συνδέονται σε κλειστό βρόχο. Απευθείας αντιμετώπιση αυτού του προβλήματος φαίνεται να είναι αρκετά δύσκολη (ίσως ανέφικτη), και επομένως η ανάλυση ενός τέτοιου συστήματος φαίνεται προτιμότερη μέσω προσεγγιστικών αναλυτικών μεθόδων. Μια υποσχόμενη προσέγγιση διαφαίνεται η θεώρηση κάθε μιας από τις δύο γενικές (και εν γένη διαφορετικές και ανεξάρτητες) διαδικασίες, ως στοχαστικές διαδικασίες που αποτελούνται από πολλαπλά εκθετικά στάδια. Η μέθοδος έχει χρησιμοποιηθεί στο παρελθόν [102] σε αυτοργανούμενα δίκτυα για τον υπολογισμό της ρυθμαπόδοσης (όπου και εκεί η επίδοση-συμπεριφορά εξαρτάται από τοπικές αλληλεπιδράσεις μεταξύ γειτονικών κόμβων), ενώ το θεωρούμενο σύστημα διάδοσης κακόβουλου λογισμικού είναι κατάλληλο για την εφαρμογή της προσεγγιστικής μεθόδου πολλαπλών εκθετικών σταδίων.

Ουσιαστικά η θεώρηση γενικότερων διαδικασιών αφίξεων/αναχωρήσεων καταργεί την υπόθεση της πραγματοποίησης ενός μοναδικού συμβάντος ανα χρονική στιγμή (για άφιξη μόλυνσης, ανάκαμψη κόμβου ή και τα δύο), επιτρέποντας εν δυνάμει την ταυτόχρονη μόλυνση δύο ή περισσότερων κόμβων, την ταυτόχρονη μόλυνση ενός κόμβου από περισσότερες από μια κακόβουλες απειλές, την αντίστοιχη ταυτόχρονη ανάκαμψη δύο ή περισσότερων κόμβων και την ταυτόχρονη πραγματοποίηση μολύνσεων και ανακάμψεων. Επιπρόσθετα, καθίσταται δυνατή η συμπερίληψη πολλών διαφορετικών στρατηγικών επίθεσης κόμβων και αντίστοιχων διαδικασιών ανάκαμψης, μέσω των γενικότερων στοχαστικών διαδικασιών άφιξης/αναχώρησης των ουρών.

Το προτεινόμενο πλαίσιο μοντελοποίησης αφορούσε στη διάδοση κακόβουλου λογισμικού και παρόλο που αναλύθηκε με λεπτομέρεια στην περίπτωση ασύρματων δικτύων, θα μπορούσε παρόμοια να συγκεκριμενοποιηθεί στην περίπτωση ενσύρματων δικτυών διαφόρων τύπων (power-law, scale-free, small-world, P2P). Ακολουθώντας παρόμοια μεθοδολογία με αυτή που παρουσιάστηκε παραπάνω, αναλυτικά αποτελέσματα μπορούν να προκύψουν για την περίπτωση ενσύρματων δικτύων.

Η δεύτερη κατεύθυνση αφορά στη μοντελοποίηση της διάδοσης με χρήση Τυχαίων Πεδίων Markov (Markov Random Fields – MRF) [103]. Τα Τυχαία Πεδία Markov προέκυψαν από τη μελέτη ιδιοτήτων που εξαρτώνται από αλληλεπιδράσεις μεταξύ μορίων ή σωματιδίων στη στατιστική φυσική. Αποτελούν ειδικές στοχαστικές διαδικασίες που ορίζονται σε συστήματα που αναπαριστώνται με γράφους δικτύων και χαρακτηρίζονται από την ιδιότητα Markov. Βασικό χαρακτηριστικό τους είναι η γενίκευση της ιδιότητας Markov ανεξαρτήτως τύπου του θεωρούμενου υποκείμενου γράφου. Επομένως τα Τυχαία Πεδία Markov μπορούν να χρησιμοποιηθούν για την επέκταση του μοντέλου διάδοσης κακόβουλου λογισμικού τόσο αναφορικά με τη διαδικασίες μόλυνσης και/ή ανάκαμψης, όσο και τον τύπο του δικτύου στον οποίο η διάδοση λαμβάνει χώρα. Η ουσιαστική θεώρηση που γίνεται είναι ότι μόνο γειτονικές καταστάσεις μπορούν να επηρεάσουν μια συγκεκριμένη κατάσταση ενός κόμβου του δικτύου. Με βάση τις γειτονικές αλληλεπιδράσεις, υπολογίζεται ένα πιθανοτικό μέτρο του συνόλου των δυνατών καταστάσεων του συστήματος («ενέργεια»). Σε κάθε κατάσταση-διαμόρφωση του συστήματος αντιστοιχίζεται μια πιθανότητα που είναι εκθετική συνάρτηση της ενέργειας, με βάση την οποία μπορεί να υπολογιστεί

μια σταθερά κανονικοποίησης για το συνολικό μέτρο πιθανότητας που ονομάζεται συνάρτηση διαμερισμού (partition function). Η σχετική πιθανότητα ενός υποσυνόλου καταστάσεων του συστήματος υπολογίζεται ως το γινόμενο των ενεργειών κάθε σημείου που περιλαμβάνεται σε αυτές τις καταστάσεις. Τα Τυχαία Πεδία Markov είναι κατάλληλα για τη μελέτη της διάδοσης κακόβουλου λογισμικού γενικού τύπου όπως έγινε με τα κλειστά δίκτυα ουρών αναμονής, γιατί περιλαμβάνουν αλληλεπιδράσεις μεταξύ κόμβων που βρίσκονται σε μία απο δύο δυνατές καταστάσεις και οι μεταβάσεις μεταξύ καταστάσεων για ένα κόμβο εξαρτώνται μόνο από τις καταστάσεις των γειτονικών κόμβων του δικτύου.

Μια εναλλακτική προσέγγιση κατάλληλη για συστήματα όπως αυτό που περιγράφηκε για τη διάδοση γενικού τύπου κακόβουλου λογισμικού είναι το πλαίσιο της Θεωρίας Παιγνίων [104]. Υποθέτοντας ότι οι δύο ομάδες κόμβων (επιτιθέμενοι – νόμιμοι) είναι ανταγωνιστικές, αρκεί να οριστούν κατάλληλες συναρτήσεις (συναρτήσεις χρησιμοποίησης – utility functions) για να περιγραφούν και να ποσοτικοποιηθούν οι αντικειμενικοί στόχοι της κάθε ομάδας, χρησιμοποιώντας τη θεωρία των ανταγωνιστικών παιγνίων μεταξύ των παικτών–κόμβων. Καθορίζοντας παίγνια αυτού του τύπου, μπορεί να μοντελοποιηθεί η εξέλιξη του συστήματος των παικτών και να μελετηθεί το σύστημα στην κατάσταση ισορροπίας (σημείο ισορροπίας Nash – Nash equilibrium point), όπου ο κάθε κόμβος δεν μπορεί να αλλάξει τις ελεγχόμενες παραμέτρους περαιτέρω χωρίς να προκαλέσει μείωση στη συνάρτηση χρησιμοποίησης των υπόλοιπων παικτών. Στο σημείο αυτό να σημειωθεί ότι ανάλογα με τη σκοπιά από την οποία αντιμετωπίζεται το πρόβλημα (κακόβουλου ή νόμιμου χρήστη) οι συναρτήσεις χρησιμοποίησης μπορούν να αντιστοιχούν στην επιθυμητή ζημιά που προκαλούν οι επιτιθέμενοι ή στο μέτρο προστασίας που επιτυγχάνουν οι αμυνόμενοι νόμιμοι κόμβοι του δικτύου. Με αυτόν τον τρόπο και τις ιδιότητες που εξασφαλίζει το σημείο ισορροπίας Nash μπορούν να σχεδιαστούν αποδοτικές τεχνικές επίθεσης ή άμυνας για τις επιμέρους ομάδες. Ένα σημαντικό ζήτημα που ανακύπτει σε αυτές τις προσεγγίσεις, είναι το ποσοστό στο οποίο οι σχεδιαζόμενες, κεντροποιημένες κατά κανόνα, τεχνικές μπορούν να μετατραπούν σε κατανεμημένες (με τα ίδια εχέγγυα για τις ιδιότητες που προκύπτουν αναλυτικά) και επομένως να μπορέσουν να πραγματοποιηθούν σε επιχειρησιακά συστήματα.

Αναφορικά με τα υβριδικά μοντέλα Τυχαίων Περίπατων, μια άμεση επέκταση θα ήταν η ενσωμάτωση πληροφορίας ποιότητας ασύρματου καναλιού στην ήδη

υπάρχουσα τοπολογική πληροφορία, ώστε ο κακόβουλος χρήστης να βελτιώσει περαιτέρω τη διαχείριση ενέργειας που κάνει. Παρακολουθώντας την ποιότητα των εκάστοτε ζεύξεων, μπορεί να βελτιωθεί η κατανάλωση ενέργειας απαλείφοντας περιττές επαναμεταδόσεις και συγκρούσεις πακέτων που θα καθυστερούσαν τη διάδοση στα ασύρματα δίκτυα.

Παράλληλα με τη μελέτη της διάδοσης κακόβουλου λογισμικού, το προτεινόμενο μοντέλο και οι επεκτάσεις που σκιαγραφήθηκαν παραπάνω μπορούν να επεκταθούν στη μελέτη παρόμοιων προβλημάτων με αναλυτικές μεθόδους. Μια τέτοια επέκταση αποτελεί η διανομή διαφημιστικών μηνυμάτων σε διάφορους τύπους πληθυσμών. Οι συσχετίσεις/επικοινωνίες μεταξύ των διαφόρων μελών του πληθυσμού αναπαριστώνται από το υποκείμενο δίκτυο, ενώ οι πηγές των διαφημιστικών μηνυμάτων αντιστοιχίζονται στους κακόβουλους χρήστες. Οι αντικειμενικοί στόχοι που μπορεί κανείς να εντοπίσει είναι η αύξηση της αποδοτικότητας διάδοσης των μηνυμάτων από τη μεριά των διαφημιζόμενων ή η καλύτερη προστασία των μελών ενός πληθυσμού από ανεπιθύμητα διαφημιστικά. Ανάλογα με τις λεπτομέρειες του θεωρούμενου τρόπου διακίνησης διαφημιστικού υλικού (ηλεκτρονικό/απλό ταχυδρομείο, φυλλάδια, μέσα μαζικής ενημέρωσης), μπορεί να γίνει απευθείας εφαρμογή ή κατάλληλα τροποποιημένη χρήση των περιγραφόμενων μοντέλων της παρούσας εργασίας.

Βιβλιογραφία

[1] J. Peeters and P. Dyson, "Cost-Effective Security", *IEEE Security and Privacy Mag.*, Vol. 5, No. 3, pp. 85–87, May-June 2007.

[2] S. Staniford, V. Paxson and N. Weaver, "How to Own the Internet in Your Spare Time", *Proc. of the 11th USENIX Security Symposium*, pp. 149–167, August 2002.

[3] X. Sun, Y. Wang, J. Ren, Y. Zhu and S. Liu, "Collecting Internet Malware Based on Client-Side Honeypot", *Proc. of 9th IEEE International Conference for Young Computer Scientists (ICYCS)*, pp. 1493–1498, November 2008.

[4] X. Bangnan, S. Hischke and B. Walke, "The Role of Ad Hoc Networking in Future Wireless Communications", *Proc. of International Conference on Communication Technology (ICCT)*, Vol. 2, pp. 1353–1358, April 2003.

[5] M. Conti and S. Giordano, "Multihop Ad Hoc Networking: The Reality", *IEEE Commun. Mag.*, Vol. 45, No. 4, pp. 88–95, April 2007.

[6] L. Lilien, "A Taxonomy of Specialized Ad Hoc Networks and Systems for Emergency Applications", *Proc. of 4th Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services (MobiQuitous)*, pp. 1–8, August 2007.

[7] M. Hefeeda and M. Bagheri, "Wireless Sensor Networks for Early Detection of Forest Fires", *Proc. of IEEE Internatonal Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, pp 1–6, October 2007.

[8] S. Drude, "Requirements and Application Scenarios for Body Area Networks", *Proc. of 16th IST Mobile and Wireless Communications Summit*, pp. 1–5, July 2007.

[9] D. Cypher, N. Chevrollier, N. Montavont and N. Golmie, "Prevailing over Wires in Healthcare Environments: Benefits and Challenges", *IEEE Commun. Mag.*, Vol. 44, No. 4, pp. 56–63, April 2006.

[10] S. Furnell, "Handheld Hazards: The Rise of Malware on Mobile Devices", *Computer Fraud & Security*, Vol. 2005, No. 5, pp. 4–8, May 2005.

[11] M. Hypponen, "Malware Goes Mobile", *Scientific American*, Vol. 295, No. 5, pp. 70–77, November 2006.

[12] B. Stone-Gross, C. Wilson, K. Almeroth, E. Belding, H. Zheng and K. Papagiannaki, "Malware in IEEE 802.11 Wireless Networks", *Lecture Notes in Computer Science (LNCS)*, Vol. 4979, pp. 222–231, April 2008.

[13] W. Xu, K. Ma, W. Trappe and Y. Zhang, "Jamming Sensor Networks: Attack and Defense Strategies", *IEEE Network Mag.*, Vol. 20, No. 3, pp. 41–47, May-June 2006.

[14] Y. Wang, G. Attebury and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks", *IEEE Commun. Surveys & Tutorials*, Vol. 8, No.2, pp. 2–22, 2nd Quarter 2006.

[15] M. G. Rubinstein, I. M. Moraes, M. E. Campista, L. H. M. K. Costa and O. C. M. B. Duarte, "A Survey on Wireless Ad Hoc Networks", *Book Chapter in Mobile and Wireless Communications Networks*, Springer-Verlag, Vol. 211, pp. 1–34, August 2006.

[16] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A Survey on Sensor Networks", *IEEE Commun. Mag.*, Vol. 40, No. 8, pp.102–114, August 2002.

[17] F. Cohen, "Computer Viruses Theory and Experiments", *Computers and Security*, Vol. 6, No. 1, pp. 22–35, February 1987.

[18] P. Szor, "The Art of Computer Virus Research and Defense", *Addison Wesley Professional*, February 2005.

[19] D. Kienzle and M. Elder, "Recent Worms: A Survey and Trends", *Proc. of 1st ACM Workshop on Rapid Malcode (WORM),* pp. 1–10, October 2003.

[20] H. Zhou, Y. Wen and H. Zhao, "Modeling and Analysis of Active Benign Worms and Hybrid Benign Worms Containing the Spread of Worms", *Proc. of 6th IEEE International Conference on Networking (ICN)*, pp. 65–65, April 2007.

[21] A. Moser, C. Kruegel and E. Kirda, "Exploring Multiple Execution Paths for Malware Analysis", *Proc. of IEEE Symposium on Security and Privacy (SP)*, pp. 231–245, May 2007.

[22] J. Kephart, S. White, I. Center and Y. Heights, "Measuring and Modeling Computer Virus Prevalence", *Proc. of IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 2–15, May 1993.

[23] G. Serazzi and S. Zanero, "Computer Virus Propagation Models", *Lecture Notes in Computer Science (LNCS)*, pp. 26–50, April 2004.

[24] A. Wagner, T. Dubendorfer, B. Plattner, and R. Hiestand, “Experiences with Worm Propagation Simulations”, *Proc. of the ACM workshop on Rapid Malcode (WORM)*, pp. 34–41, October 2003.

[25] S. Sellke, N. Shroff and S. Bagchi, “Modeling and Automated Containment of Worms”, *IEEE Transactions on Dependable and Secure Computing*, Vol. 5, No. 2, pp. 71–86, April 2008.

[26] C. Wong, C. Wang, D. Song, S. Bielski and G. Ganger, “Dynamic Quarantine of Internet Worms”, *Proc. of the International Conference on Dependable Systems and Networks (DSN)*, pp. 62–71, June-July 2004.

[27] E. Anderson, K. Eustice, S. Markstrum, M. Hansen and P. Reiher, “Mobile Contagion: Simulation of Infection and Defense”, *Proc. of 19th Workshop on Principles of Advanced and Distributed Simulation (PADS)*, pp. 80–87, June 2005.

[28] M. Williamson, “Throttling Viruses: Restricting Propagation to Defeat Malicious Mobile Code”, *Proc. of 18th Annual Conference on Computer Security Applications (ACSAC)*, pp. 61–68, December 2002.

[29] C. Wang, J. C. Knight and M. E. Elder, “On Computer Viral Infection and the Effect of Immunization”, *Proc. of 16th Annual Conference Computer Security Applications (ACSAC)*, pp. 246–256, December 2000.

[30] J. Kephart, S. White, D. Chess, I. Center and N. Hawthorne, “Computers and Epidemiology”, *IEEE Spectrum Mag.*, Vol. 30, No. 5, pp. 20–26, May 1993.

[31] F. Liljeros, C. R. Edling and L. A. N Amaral, “Sexual Networks: Implications for the Transmission of Sexually Transmitted Infections”, *Microbes and Infection 5*, pp. 189–196, June 2003.

[32] R. Pastor-Satorras and A. Vespignani, “Epidemics and Immunization in Scale-Free Networks”, *in Handbook of Graphs and Networks: From the Genome to the Internet*, S. Bornholdt, H. Schuster (Eds.), pp. 113–132, Wiley-VCH, Berlin, May 2002.

[33] R. Albert and A.-L. Barabasi, “Statistical Mechanics of Complex Networks”, *Review of Modern Physics*, The American Physical Society, Vol. 74, No. 1, pp. 47–97, January 2002.

[34] M. E. J. Newman, “The Structure and Function of Complex Networks”, *Society for Industrial and Applied Mathematics (SIAM) Review*, Vol. 45, No. 2, pp. 167–256, 2003.

[35] A.-L. Barabási and E. Bonabeau, “Scale-Free Networks”, *Scientific American*, pp. 50–59, May 2003.

[36] C. C. Zou, W. Gong and D. Towsley, “Code Red Worm Propagation Modeling and Analysis”, *Proc. of the 9th ACM conference on Computer and communications Security (CCS)*, pp. 138–147, November 2002.

[37] D. J. Daley and J. Gani, “Epidemic Modelling: An Introduction”, *Cambridge University Press*, 1999.

[38] G. Kesidis, I. Hamadeh, and S. Jiwasurat, “Coupled Kermack-McKendrick Models for Randomly Scanning and Bandwidth Saturating Internet Worms”, *Proc. of 3rd International Workshop on QoS in Multiservice IP Networks (QoS-IP)*, pp. 101–109, February 2005.

[39] C. C. Zou, W. Gong and D. Towsley, “Worm Propagation Modeling and Analysis under Dynamic Quarantine Defense”, P*roc. of 1st ACM Workshop on Rapid Malcode (WORM)*, pp. 51–60, October 2003.

[40] X. Yan and Y. Zou, “Optimal Internet Worm Treatment Strategy Based on the Two-Factor Model”, *ETRI Journal*, Vol. 30, No. 1, p. 81–88, February 2008.

[41] J. Kephart, S. White, I. Center and Y. Heights, “Directed-graph Epidemiological Models of Computer Viruses”, *Proc. of IEEE Computer Society Symposium on Research in Security and Privacy (RISP)*, pp. 343–359, May 1991.

[42] R. G. Cole, N. Phamdo, M. A. Rajab and A. Terzis, “Requirements on Worm Mitigation Technologies in MANETS”, *Proc. of Workshop on Principles of Advanced and Distributed Simulation (PADS)*, pp. 207–214, June 2005.

[43] J.-Y. Le Boudec and M. Vojnovic, “Perfect Simulation and Stationarity of a Class of Mobility Models”, *Proc. of 24th IEEE Conference on Computer Communications (INFOCOM)*, Vol. 4, pp. 2743–2754, March 2005.

[44] E. M. Royer and C.-K. Toh, “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks”, *IEEE Pers. Commun. Mag.*, Vol. 6, No. 2, pp. 46–55, April 1999.

[45] G. Bianchi, “Performance Analysis of the IEEE 802.11 Distributed Coordination Function”, *IEEE Journal of Selected Areas in Communications (JSAC)*, Vol. 18, No. 3, pp. 535–547, March 2000.

[46] M. Nekovee, “Worm Epidemics in Wireless Ad Hoc Networks”, *New Journal of Physics*, Vol. 9, pp. 189–200, 2007.

[47] G. Grimmett and D. Stirzaker, “Probability and Random Processes”, *Oxford University Press*, 3rd edition, New York, NY, USA, 2001.

[48] Z. Chen, L. Gao and K. Kwiat, “Modeling the Spread of Active Worms”, *Proc. of the 22nd IEEE Conference on Computer Communications (INFOCOM)*, Vol. 3, pp. 1890–1900, April 2003.

[49] K. R. Rohloff and T. Basar, “The Detection of RCS Worm Epidemics”, *Proc. of 3rd ACM Workshop on Rapid Malcode (WORM)*, pp. 81–86, October 2005.

[50] A. Baddeley, I. Barany, R. Schneider and W. Weil, “Stochastic Geometry”, *Lecture Notes in Mathematics*, Ed. W. Weil, Springer-Verlag, Berlin-Heidelberg, August 2005.

[51] A. Wald, “Sequential Tests of Statistical Hypotheses”, *Annals of Mathematical Statistics*, Vol. 16, No. 2, pp. 117–186, June 1945.

[52] C.-D. Fuh, “SPRT and CUSUM in Hidden Markov Models”, *The Annals of Statistics*, Vol. 31, No. 3, pp. 942–977, 2003.

[53] C. C. Zou, W. Gong, D. Towsley and L. Gao, “The Monitoring and Early Detection of Internet Worms”, *IEEE/ACM Trans. on Netw.*, Vol. 12, No. 5, pp. 961–974, October 2005.

[54] M. S. Grewal and A. P. Andrews, “Kalman Filtering Theory and Practice” *Prentice Hall*, Englewood Cliffs, NJ, USA, 2003.

[55] K. R. Rohloff and T. Basar, “Stochastic Behavior of Random Constant Scanning Worms”, *Proc. of 14th International Conference on Computer Communications and Networks (ICCCN)*, pp. 339–344, October 2005.

[56] M. Garetto, W. Gong and D. Towsley, “Modeling Malware Spreading Dynamics”, *Proc. of 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, Vol. 3, pp. 1869–1879, March-April 2003.

[57] A. Ganesh, L. Massoulie and D. Towsley, “The Effect of Network Topology on the Spread of Epidemics, *Proc. of 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, Vol. 2, pp. 1455–1466, March 2005.

[58] P. Van Mieghem, J. Omic and R. Kooij, “Virus Spread in Networks”, *IEEE/ACM Trans. on Netw.*, Vol. 17, No. 1, pp. 1–14, February 2009.

[59] J. S. Omic, R. E. Kooij and P. Van Mieghem, "Virus Spread in Complete Bi-partite Graphs", *Proc. of 2nd Conference on Bio-Inspired Models of Network, Information and Computing Systems (BIONETICS)*, pp. 49–56, December 2007.

[60] V. Karyotis, A. Kakalis and S. Papavassiliou, "On the Tradeoff between MAC-layer and Network-layer Topology-Controlled Malware Spreading Schemes in Ad Hoc and Sensor Networks", *Proc. of 3rd International Conference on Emerging Security Information, Systems and Technologies* (*SECURWARE)*, June 2009.

[61] C. Bettstetter, "On the Connectivity of Ad Hoc Networks", *The Computer Journal*, Oxford Journals – Oxford University Press, Vol. 47, No. 4, pp. 432–447, 2004.

[62] C. Bettstetter and C. Hartmann, "Connectivity of Wireless Multihop Networks in a Shadow Fading Environment", *ACM/Springer Wireless Networks (WINET)*, Vol. 11, No. 5, pp. 571–579, September 2005.

[63] M. Penrose, "Random Geometric Graphs", *Oxford University Press*, NY, USA, 2003.

[64] B. Bollobas, "Random Graphs", *Cambridge University Press*, Cambridge, U.K., 2001.

[65] N. T. J. Bailey, "The Mathematical Theory of Infectious Diseases", *Oxford University Press*, NY, USA, 1975.

[66] M. Schwartz, "Telecommunication Networks: Protocols, Modeling and Analysis", *Addison Wesley*, Reading, MA, USA, 1987.

[67] A. A. Lazar, "The Throughput Time Delay Function of an M/M/1 Queue", *IEEE Trans. on Inform. Theory*, Vol. 29, No. 6, pp. 914–918, November 1983.

[68] D. Betsekas and R. Gallager, "Data Networks", *Prentice Hall*, 2nd ed., Upper Saddle River, NJ, USA, 1992.

[69] B. Hajek, "Optimal Control of Two Interacting Service Stations", *IEEE Trans. Autom. Control*, Vol. 29, No. 6, pp. 491–499, June 1984.

[70] S. Boyd and L. Vandenberghe, "Convex Optimization", *Oxford University Press*, New York, USA, 2004.

[71] R. L. Rardin, "Optimization in Operations Research", *Prentice Hall*, Upper Saddle River, NJ, USA, 1998.

[72] A. A. Lazar, "Optimal Flow Control of an M/M/m Queue", *Journal of the ACM (JACM)*, Vol. 31, No. 1, pp. 86–98, January 1984.

[73] M. H. R. Khouzani, E. Altman and S. Sarkar, "Optimal Quarantining of Wireless Malware Through Power Control", *Proc. of the 4th Symposium on Information Theory and Applications*, University of California, San Diego, February 2009.

[74] P. Santi, "Topology Control in Wireless Ad Hoc and Sensor Networks", *ACM Computing Surveys (CSUR)*, Vol.37, No.2, pp. 164–194, June 2005.

[75] P. Santi, "Topology Control in Wireless Ad Hoc and Sensor Networks", *John Wiley & Sons*, West Sussex, U.K., 2005.

[76] V. Karyotis and S. Papavassiliou, "Topology Control in Cooperative Ad Hoc Networks", *Book Chapter in Cooperative Wireless Communications*, CRC Press, Taylor & Francis Group, Editors: Y. Zhang, H.-H. Chen and M. Guizani, pp. 167–189, March 2009.

[77] V. Karyotis, S. Papavassiliou and M. Grammatikou, "On the Risk-based Operation of Mobile Attacks in Wireless Ad Hoc Networks", *Proc. of the IEEE International Conference on Communications (ICC)*, pp. 1130–1135, June 2007.

[78] L.-M. Feeney and M. Nilsson, "Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment", *Proc. of 20th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, Vol. 3, pp. 1548–1557, April 2001.

[79] Y. Xu, J. Heidemann and D. Estrin, "Geographically-Informed Energy Conservation for Ad Hoc Routing", *Proc. of the 7th ACM Conference on Mobile Computing and Networking (MobiCom)*, pp. 70–84, July 2001.

[80] B. Chen, K. Jamieson, H. Balakrishnan and R.Morris, "Span: An Energy – Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks", *Proc. of the 7th ACM Conference on Mobile Computing and Networking (MobiCom)*, pp. 85–96, July 2001.

[81] K. Sakakibara, H. Nakagawa and J. Yamakita, "Analysis of Energy Consumption of IEEE 802.11 DCF under Non-Saturation Conditions", *Proc. of 1st International Symposium on Wireless Pervasive Computing (ISWPC)*", January 2006.

[82] S. Ganeriwal, R. Kumar and M. B. Srivastava, "Timing-sync Protocol for Sensor Networks", *Proc. of the 1st ACM Conference on Embedded Networked Sensor Systems (SenSys)*, pp. 138–149, November 2003.

[83] K. Romer, “Time Synchronization in Ad Hoc Networks”, *Proc. of the 2nd ACM international Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc)*, pp. 173–182, October 2001.

[84] R. Ramanathan and R. Rosales-Hain, “Topology Control of Multihop Wireless Networks using Transmit Power Adjustment”, *Proc. of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, Vol. 2, pp. 404–413, March 2000.

[85] D. M. Blough, M. Leoncini, G. Resta and P. Santi, “The K-Neigh Protocol for Symmetric Topology Control in Ad Hoc Networks”, *Proc. of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc*), pp. 141–152, June 2003.

[86] A. Savvides, C. Han and M. Srivastava, “Dynamic Fine-Grained Localization in Ad Hoc Networks of Sensors”, *Proc. of the 7th Annual International Conference on Mobile Computing and Networking (Mobicom)*, pp. 166–179, July 2001.

[87] J. Ayadi, Z. Hai and J. Farserotu, “Maximum Likelihood Time of Arrival Estimation for Ultrawideband Signals”, *Proc. of 9th International Symposium on Signal Processing and Its Applications (ISSPA)*, pp. 1–4, February 2007.

[88] V. Rodoplu and T. H. Meng, “Minimum Energy Mobile Wireless Networks”, *IEEE Journal Selected Areas in Comm. (JSAC)*, Vol. 17, No. 8, pp. 1333–1344, August 1999.

[89] H. Takagi and L. Kleinrock, “Optimal Transmission Ranges for Randomly Distributed Packet Radio Networks”, *IEEE Trans. Commun.*, Vol. 32, No. 3, pp. 246–257, March 1984.

[90] J. Zhu, S. Papavassiliou and J. Yang, “Adaptive Localized QoS-constrained Data Aggregation and Processing in Distibuted Sensor Networks”, *IEEE Trans. on Parallel and Distributed Systems*, Vol. 17, No. 9, pp. 923–933, September 2006.

[91] R. W. Wolff, “Stochastic Modeling and the Theory of Queues”, *Prentice Hall*, Upper Saddle River, NJ, USA, 1989.

[92] R. Durrett, “Probability: Theory and Examples”, *Wadsworth Pub. Co., Pacific Grove, CA, Second Edition, Duxbury Press*, 1995.

[93] C. Gkantsidis, M. Mihail and A. Saberi, “Random Walks in Peer-to-Peer Networks”, *Proc. of the Twenty-third Annual Joint Conference of the IEEE*

Computer and Communications Societies (INFOCOM), pp. 120–130, Vol. 1, March 2004.

[94] M. Mihail, A. Saberi and P. Tetali, "Random Walks with Lookahead in Power Law Random Graphs", *Internet Math.*, pp. 147–152, Vol. 3, No. 2, 2006.

[95] L. Lima and J. Barros, "Random Walks on Sensor Networks", *Proc. of the 5th International Syposium on Modeling and Optimization in Mobile, Ad hoc, and Wireless Networks (WiOpt)*, pp. 1–5, Limassol, Cyprus, April 2007.

[96] S. S. Dhillon and P. Van Mieghem, "Comparison of Random Walk Strategies for Ad Hoc Networks", *Proc. of the Sixth IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2007)*, pp. 196–203, Corfu island, Greece, June 2007.

[97] D. Aldous, "An Introduction to Covering Problems for Random Walks on Graphs", *Journal of Theoretical Probability*, pp. 87–89, Vol. 2, No. 1, 1989.

[98] L. Tzevelekas and I. Stavrakakis, "Random Walks with Jumps in Wireless Sensor Networks", *poster session of the Sixth IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2007)*, Corfu island, Greece, June 2007.

[99] S.-A. Jafar, "Too Much Mobility Limits the Capacity of Wireless Ad Hoc Networks", *IEEE Trans. Inf. Theory*, Vol. 51, No. 11, pp. 3954–3965, November 2005.

[100] S. Capcun, J.-P. Hubaux and L. Buttyan, "Mobility Helps Security in Ad Hoc Networks", *Proc. of the 4th ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc)*, pp. 46–56, June 2003.

[101] S. Sarat and A. Terzis, "On Using Mobility to Propagate Malware", *Proc. of 5th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks and Workshops (WiOpt)*, pp. 1–8, April 2007.

[102] R. Boorstyn, A. Kershenbaum, B. Maglaris, and V. Sahin, "Throughput Analysis in Multihop CSMA Packet Radio Networks", *IEEE Trans. on Communications*, Vol. 35, No. 3, pp. 267–274, March 1987.

[103] R. Kindermann and J. L. Snell, "Markov Random Fields and Their Applications", *American Mathematical Society*, Providence, RI, USA, 1950.

[104] D. Fudenberg and J. Tirole, "Game Theory", *The MIT Press*, Cambridge, MA, USA, 1991.

Κατάλογος Δημοσιευμένων Εργασιών

Δημοσιεύσεις σε Περιοδικά

[1] **V. Karyotis**, A. Kakalis and S. Papavassiliou, "Malware-Propagative Mobile Ad Hoc Networks: Asymptotic Behavior Analysis", *Journal of Computer Science and Technology (JCST)*, Springer, Vol. 23, No. 3, pp. 389-399, May 2008.

[2] **V. Karyotis** and S. Papavassiliou, "Risk-Based Attack Strategies for Mobile Ad Hoc Networks under Probabilistic Attack Modeling Framework", *Computer Networks Journal (COMNETS)*, Elsevier, Vol. 51, No. 9, pp. 2397-2410, June 2007.

[3] **V. Karyotis**, S. Papavassiliou, M. Grammatikou and V. Maglaris, "A Novel Framework for Mobile Attack Strategy Modeling and Vulnerability Analysis in Wireless Ad-hoc Networks", *International Journal of Security and Networks (IJSN)*, Vol. 1, No. 3/4, pp. 255-265, 4th Quarter 2006.

[4] **V. A**. **Karyotis** and C. A. Valagiannopoulos, "An Analytic Stochastic Propagation Model for Urban Streets", *IET Microwaves, Antennas and Propagation*. To appear in 2009.

[5] C. A. Valagiannopoulos and **V. A. Karyotis**, "Stochastic Ray Propagation for Two Parallel Urban Streets: Exact and Approximate Results", *IEEE Antennas Wireless Propag. Lett.* , Vol. 7, pp. 381-384, 2008.

Δημοσιεύσεις σε Κεφάλαια Βιβλίων

[1] **V. Karyotis** and S. Papavassiliou, "Mobility-induced Capacity-Delay Tradeoff in Wireless Multihop Networks", *Nova Publishers*. To appear in 2009.

[2] **V. Karyotis** and S. Papavassiliou, "Topology Control in Cooperative Ad Hoc Networks", *Book Chapter in Cooperative Wireless Communications*, CRC Press, Taylor & Francis Group, Editors: Y. Zhang, H.-H. Chen and M. Guizani, pp. 167-189, March 2009.

Δημοσιεύσεις σε Διεθνή Συνέδρια με Σύστημα Κριτών

[1] **V. Karyotis**, F. Pittala, M. Fazio, S. Papavassiliou and A. Puliafito, "Topology-Aware Hybrid Random Walk Protocols in Wireless Multihop Networks",

accepted for publication in Proc. of *1st International ICST Conference on Mobile Networks and Management (MONAMI)*, October 2009.

[2] V. **Karyotis**, A. Kakalis and S. Papavassiliou, "On the Tradeoff between MAC-layer and Network-layer Topology-Controlled Malware Spreading Schemes in Ad Hoc and Sensor Networks", Proc. of *3rd International Conference on Emerging Security Information, Systems and Technologies* (*SECURWARE)*, Athens, Greece, June 2009.

[3] T. Kastrinogiannis, **V. Karyotis** and S. Papavassiliou, "An Opportunistic Combined Power and Rate Allocation Approach in CDMA Ad Hoc Networks", Proc. of *IEEE Sarnoff Symposium*, Princeton, NJ, USA, April 2008.

[4] T. Kastrinogiannis, **V. Karyotis** and S. Papavassiliou, "Power and Rate Control in CDMA Ad Hoc Networks", Proc. of *3rd IEEE International Symposium on Wireless Pervasive Computing (ISWPC*), Santorini island, Greece, May 2008.

[5] **V. Karyotis** and S. Papavassiliou, "On the Malware Spreading over Non-Propagative Wireless Ad Hoc Networks: The Attacker's Perspective", Proc. of *3rd ACM International Workshop on QoS and Security for Wireless and Mobile Networks (Q2SWinet)*, Chania, Crete, Greece, October 2007.

[6] **V. Karyotis**, M. Grammatikou and S. Papavassiliou, "On the Asymptotic Behavior of Malware-Propagative Mobile Ad Hoc Networks", Proc. of *4th IEEE International Conference on Mobile Ad Hoc and Sensor Networks (MASS)*, Pisa, Italy, October 2007.

[7] **V. Karyotis**, M. Grammatikou and S. Papavassiliou, "A Closed Queueing Network Model for Malware Spreading over Non-Propagative Ad Hoc Networks", Proc. of *Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net)*, pp. 129-136, Corfu, Greece, June 2007.

[8] **V. Karyotis**, S. Papavassiliou and M. Grammatikou, "On the Risk-based Operation of Mobile Attacks in Wireless Ad Hoc Networks", Proc. of the *IEEE International Conference on Communications (ICC)*, pp. 1130-1135, Glasgow, U.K., June 2007.

[9] **V. Karyotis**, S. Papavassiliou, M. Grammatikou and B. Maglaris, "On the Characterization and Evaluation of Mobile Attack Strategies in Wireless Ad-Hoc Networks", Proc. of the *11th IEEE Symposium on Computers and Communications (ISCC)*, Pula-Cagliari, Sardinia, Italy, June 2006.

[10] **V. Karyotis**, S. Papavassiliou and B. Maglaris, "Modeling Framework for the Study and Analysis of Mobile Attack Propagation in Wireless Ad-Hoc Networks", Proc. of the *12th European Wireless conference (EW2006)*, Athens, Greece, April 2006.