ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Κατηγοριοποίηση και Σύγκριση Μοντέλων Εμπιστοσύνης και Φήμης σε P2P Δίκτυα

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΧΑΔΟΥΜΕΛΛΗ ΑΝΔΡΕΑ

Επιβλέπουσα : Θεοδώρα Βαρβαρίγου
Καθηγήτρια Ε.Μ.Π.

Αθήνα, 31/10/ 2023

Η σελίδα αυτή είναι σκοπίμως κενή.

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Κατηγοριοποίηση και σύγκριση μοντέλων Εμπιστοσύνης και Φήμης σε P2P δίκτυα

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΧΑΔΟΥΜΕΛΛΗ ΑΝΔΡΕΑ

Επιβλέπουσα: Θεοδώρα Βαρβαρίγου
Καθηγήτρια Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 31η Οκτωβρίου 2023.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Θεοδώρα Βαρβαρίγου Καθηγήτρια Ε.Μ.Π.	Συμεών Παπαβασιλείου Καθηγητής Ε.Μ.Π.	Εμμανουήλ Βαρβαρίγος Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2023

Η σελίδα αυτή είναι σκοπίμως κενή.

(Υπογραφή)

.....

ΧΑΔΟΥΜΕΛΛΗΣ ΑΝΔΡΕΑΣ

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Η ραγδαία εξάπλωση των Δικτύων Peer-To-Peer (P2P), και των ανοιχτών δυναμικών συστημάτων γενικότερα, έχει οδηγήσει στην ανάγκη για εδραίωση ενός μηχανισμού ο οποίος θα διασφαλίζει την ασφάλεια των συναλλαγών μεταξύ των χρηστών στα συστήματα αυτά. Για την επίτευξη του στόχου αυτού έχουν προταθεί μοντέλα Εμπιστοσύνης και Φήμης (Trust & Reputation Models) τα οποία έχουν ως βασικό σκοπό να παρακολουθούν τη συμπεριφορά των χρηστών του συστήματος και να περιορίζουν όσους παρουσιάζουν κακόβουλη συμπεριφορά.

Το αντικείμενο της παρούσας διπλωματικής εργασίας είναι η μελέτη και η σύγκριση διαφορετικών μοντέλων Εμπιστοσύνης και Φήμης σε P2P δίκτυα, τα οποία έχουν προταθεί κατά καιρούς στη βιβλιογραφία. Συγκεκριμένα, επιλέχθηκαν έξι μοντέλα από τη βιβλιογραφία τα οποία παρουσίαζαν διαφορετικά χαρακτηριστικά μεταξύ τους, μελετήθηκαν και στη συνέχεια έγινε μία κατηγοριοποίησή τους. Τέλος, τα μοντέλα αυτά υλοποιήθηκαν και εφαρμόστηκαν σε P2P δίκτυα χρησιμοποιώντας τον προσομοιωτή TRMSim-WSN με στόχο τη σύγκριση της απόδοσής τους.

Λέξεις - Κλειδιά: Φήμη, Εμπιστοσύνη, e-commerce, P2P

Η σελίδα αυτή είναι σκοπίμως κενή.

Ευχαριστίες

Με την περάτωση αυτής της διπλωματικής η φοίτησή μου στη Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του ΕΜΠ φτάνει στο τέλος της. Θα ήθελα αρχικά να ευχαριστήσω την καθηγήτριά μου, κυρία Βαρβαρίγου, που μου έδωσε την ευκαιρία να καταπιαστώ με ένα τόσο ενδιαφέρον θέμα. Επίσης, θα ήθελα να ευχαριστήσω τους Ορφέα Βουτυρά, Αντώνη Λίτκε και Αλέξανδρο Ψυχά για την συνεχή στήριξη και καθοδήγησή τους, καθώς και για τη διάθεση εργαστηριακών πόρων. Τέλος, ένα μεγάλο ευχαριστώ από καρδιάς σε όλους όσοι στάθηκαν δίπλα μου κατά τη διάρκεια των σπουδών μου.

Ανδρέας Χαδουμέλλης

Αθήνα, 31/10/2023

Πίνακας περιεχομένων

1

Εισαγωγή

Τα τελευταία χρόνια, η ανάπτυξη του διαδικτύου έχει επιφέρει ραγδαία αύξηση στα συστήματα Peer-To-Peer (P2P), με κυριότερα παραδείγματα το Διαδίκτυο των Πραγμάτων (Internet of Things - IoT), συστήματα που χρησιμοποιούν Κρυπτονομίσματα, καθώς και πλήθος συστημάτων ηλεκτρονικών συναλλαγών, στα οποία οι χρήστες - άνθρωποι ή υπολογιστές – πραγματοποιούν δοσοληψίες μεταξύ τους.

Τα συστήματα αυτά χαρακτηρίζονται από το γεγονός ότι είναι ανοιχτά, δηλαδή οι χρήστες μπορούν ανά πάσα στιγμή να σταματήσουν να αποτελούν μέρος του συστήματος, ενώ νέοι χρήστες μπορεί να εισέλθουν στο σύστημα στην πορεία. Άλλο ένα χαρακτηριστικό των εν λόγω συστημάτων είναι η έλλειψη πληροφορίας ως προς την αξιοπιστία των νεοεισελθέντων χρηστών, ενώ σε αρκετές περιπτώσεις η πληροφορία αυτή είναι ελλιπής ακόμη και για χρήστες που αποτελούν μέρος του συστήματος για μεγαλύτερο χρονικό διάστημα.

Λόγω των παραπάνω χαρακτηριστικών, εγείρονται προκλήσεις όσον αφορά την προστασία των συστημάτων αυτών από κακόβουλους χρήστες/συσκευές οι οποίοι δρουν ιδιοτελώς με σκοπό είτε το προσωπικό κέρδος, είτε την δολιοφθορά του συστήματος. Για τον παραπάνω λόγο, υλοποιούνται τα συστήματα Εμπιστοσύνης και Φήμης (Trust and Reputation – T&R) μέσω των οποίων πραγματοποιείται η αξιολόγηση της αξιοπιστίας και φερεγγυότητας των χρηστών του εκάστοτε συστήματος.

Στην παρούσα διπλωματική εργασία γίνεται μία μελέτη ορισμένων μοντέλων Εμπιστοσύνης και Φήμης τα οποία έχουν προταθεί κατά καιρούς στη βιβλιογραφία και στη συνέχεια πραγματοποιείται μία σύγκριση μεταξύ τους.

1.1 Αντικείμενο διπλωματικής

Τα P2P συστήματα κατέχουν κυρίαρχη θέση στην ανθρώπινη καθημερινότητα και χρησιμοποιούνται σε πληθώρα περιπτώσεων. Τα συστήματα διαμοιρασμού αρχείων, το IoT και τα Κρυπτονομίσματα αποτελούν μερικά μόνο παραδείγματα τέτοιων περιπτώσεων. Προκειμένου να εξασφαλιστεί η ασφάλεια των συστημάτων αυτών και να μην κινδυνεύουν οι χρήστες τους να πέσουν θύματα εξαπάτησης από κακόβουλους παρόχους, υιοθετούνται μηχανισμοί οι οποίοι παρακολουθούν και διαχειρίζονται τη Φήμη των παρόχων, και την Εμπιστοσύνη των χρηστών προς αυτούς. Οι μηχανισμοί αυτοί, τα μοντέλα Εμπιστοσύνης και Φήμης όπως ονομάζονται, έχουν ως στόχο να προστατεύουν τους χρήστες του συστήματος από κακόβουλους παρόχους, ενώ ταυτόχρονα τους βοηθούν να επιλέξουν κάποιον αξιόπιστο πάροχο.

Στην παρούσα διπλωματική έχουν επιλεγεί έξι τέτοια μοντέλα, με βασικό κριτήριο επιλογής να παρουσιάζουν σημαντικές διαφορές ως προς τα χαρακτηριστικά τους, προκειμένου να εξασφαλιστεί μεγαλύτερη ποικιλία στα αποτελέσματα. Συγκεκριμένα, έχουν επιλεγεί τα εξής: EigenTrust, PowerTrust, PeerTrust, TRAVOS, RDTM, TRM-SIoT. Στα επόμενα κεφάλαια πραγματοποιείται εκτενής παρουσίαση των μοντέλων αυτών ως προς τα χαρακτηριστικά και τον τρόπο λειτουργίας τους καθώς και σύγκριση μεταξύ τους, τόσο σε ποιοτικό επίπεδο, με βάση τα διάφορα χαρακτηριστικά τους, όσο και σε ποσοτικό επίπεδο χρησιμοποιώντας τον προσομοιωτή TRMSiM-WSN, με τον οποίο αξιολογήθηκαν οι επιδόσεις των μοντέλων σε προσομοιώσεις P2P δικτύων. Η σύγκριση αυτή έχει σκοπό να αναδείξει το καταλληλότερο μοντέλο Εμπιστοσύνης και Φήμης ανά περίπτωση.

1.2 Οργάνωση κειμένου

Το περιεχόμενο της παρούσας διπλωματικής έχει διαρθρωθεί ως εξής:

- Στο Κεφάλαιο 2 πραγματοποιείται μία σύντομη ανασκόπηση σχετικών εργασιών στην ακαδημαϊκή βιβλιογραφία.
- Στο Κεφάλαιο 3 παρουσιάζονται κάποιες εισαγωγικές έννοιες με τις οποίες είναι απαραίτητη η εξοικείωση προτού κανείς διαβάσει ολόκληρη την παρούσα διπλωματική εργασία.

- Στο Κεφάλαιο 4 παρουσιάζονται αναλυτικά η σχεδίαση και ο τρόπος λειτουργίας των μοντέλων Εμπιστοσύνης και Φήμης τα οποία μελετήθηκαν στα πλαίσια της διπλωματικής εργασίας.
- Το Κεφάλαιο 5 αφορά την ποιοτική σύγκριση και κατηγοριοποίηση των μοντέλων αυτών με βάση τα διάφορα χαρακτηριστικά τους.
- Στο Κεφάλαιο 6 γίνεται μία παρουσίαση του προσομοιωτή TRMSim-WSN, ο οποίος χρησιμοποιήθηκε στο πειραματικό σκέλος της εργασίας.
- Το Κεφάλαιο 7 αφορά το πειραματικό σκέλος της εργασίας. Εκεί αρχικά περιγράφεται η πειραματική μέθοδος που ακολουθήθηκε για την αξιολόγηση των μοντέλων, ενώ στη συνέχεια παρουσιάζονται τα πειραματικά αποτελέσματα και η ανάλυσή τους.
- Το Κεφάλαιο 8 αποτελεί μία σύνοψη της εργασίας και απαριθμεί ορισμένες μελλοντικές επεκτάσεις που θα μπορούσαν να πραγματοποιηθούν ως συνέχεια της εργασίας.
- Τέλος, στο Κεφάλαιο 9 παρατίθενται οι βιβλιογραφικές αναφορές που χρησιμοποιήθηκαν στα πλαίσια της εργασίας.

2

Σχετικές εργασίες

2.1 Συστήματα Εμπιστοσύνης και Φήμης

Η διαχείριση της Εμπιστοσύνης και της Φήμης είναι ευρέως αποδεκτή ως μία αποτελεσματική λύση σε διάφορα συστήματα συναλλαγών, στα οποία δεν υπάρχει προηγούμενη πληροφορία για τις οντότητες οι οποίες απαρτίζουν τα συστήματα αυτά. Κατά καιρούς έχουν γίνει διάφορες προσπάθειες για την κατανόηση και τον σαφή ορισμό των όρων της Εμπιστοσύνης και της Φήμης, καθώς και για την ανάλυση των συστημάτων Εμπιστοσύνης και Φήμης, ενώ προτείνονται συνεχώς νέα μοντέλα Εμπιστοσύνης και Φήμης [1].

2.2 Σύγκριση Μοντέλων Εμπιστοσύνης και Φήμης

Κατά καιρούς έχουν γίνει αρκετές προσπάθειες σύγκρισης διαφόρων μοντέλων Εμπιστοσύνης και Φήμης [2], [3]. Ωστόσο, οι περισσότερες περιορίζονται σε μία καθαρά ποιοτική σύγκριση και κατηγοριοποίηση των μοντέλων με βάση τα χαρακτηριστικά τους, το είδος των συστημάτων για τα οποία προορίζονται, καθώς και τις επιθέσεις ενάντια στις οποίες αυτά είναι αποτελεσματικά. Δεν παρουσιάζεται δηλαδή κάποια ποσοτική σύγκριση των μοντέλων με βάση κάποια μετρική.

Από την άλλη, τις τελευταίες δεκαετίες, οι περισσότερες δημοσιεύσεις που αφορούν τον τομέα της Εμπιστοσύνης και Φήμης έχουν ως θέμα την πρόταση νέων μοντέλων και επικεντρώνονται στην περιγραφή της προσέγγισής τους. Οι δημοσιεύσεις αυτές, συνήθως περιλαμβάνουν και ένα πειραματικό σκέλος, με σκοπό την επίδειξη της αποτελεσματικότητας του προτεινόμενου μοντέλου, ενώ ορισμένες παρέχουν και μία σύγκριση με κάποιο υπάρχον μοντέλο. Ωστόσο, δεν υπάρχει κάποια δημοσίευση η οποία να έχει ως κύριο θέμα τη σύγκριση, συγχρόνως ποιοτική και ποσοτική, περισσότερων μοντέλων Εμπιστοσύνης και Φήμης.

Μοναδική εξαίρεση αποτελεί η [4], όπου γίνεται σύγκριση τεσσάρων μοντέλων Εμπιστοσύνης και Φήμης σε ποσοτικό επίπεδο. Η παρούσα διπλωματική αντλεί έμπνευση από τη συγκεκριμένη δημοσίευση και έχει ως στόχο να συμβάλει στο υπάρχον αυτό κενό. Χρησιμοποιεί ως βάση τη συγκεκριμένη δημοσίευση, συμπεριλαμβάνοντας τα τρία εκ των τεσσάρων μοντέλων που περιγράφονται σε αυτήν (EigenTrust, PowerTrust, PeerTrust), και προσθέτει επιπλέον τρία νέα μοντέλα (TRAVOS, RDTM, TRM-SIoT), προκειμένου να οδηγηθεί σε όσο το δυνατόν πληρέστερα και εγκυρότερα αποτελέσματα.

3

Θεωρητικό υπόβαθρο

3.1 Δίκτυα Ομότιμων Κόμβων – P2P

Η αρχιτεκτονική Ομότιμων Κόμβων (Peer-To-Peer, P2P) είναι μία αποκεντρωμένη αρχιτεκτονική δικτύου που χρησιμοποιείται για τη δημιουργία κατανεμημένων συστημάτων και εφαρμογών, στα οποία οι κόμβοι εντός του δικτύου διαμοιράζονται και χρησιμοποιούν τους πόρους (πχ. υπολογιστική ισχύς, εύρος ζώνης, αποθηκευτικός χώρος κτλ.) ώστε να εξυπηρετήσουν άλλους κόμβους παρέχοντας (ή αντίστοιχα λαμβάνοντας) μία υπηρεσία. Αρκετές φορές μάλιστα, το σύνολο των κόμβων του συστήματος συντελούν στην προσφορά μίας ενιαίας υπηρεσίας.

Σε αντίθεση με τα συστήματα πελάτη-εξυπηρετητή, τα συστήματα ομότιμων κόμβων δεν διαθέτουν κάποιον ενεργό υπολογιστή – εξυπηρετητή ο οποίος λαμβάνει αιτήσεις, τις επεξεργάζεται και απαντά σε αυτές με κάποιον τρόπο. Αντιθέτως, οι κόμβοι έχουν άμεση επικοινωνία μεταξύ τους και πραγματοποιούν διάφορες δοσοληψίες μεταξύ τους χωρίς την ανάγκη ενός σταθερού εξυπηρετητή, καθώς κάθε κόμβος μπορεί να δρα και ως χρήστης (client) και ως εξυπηρετητής (server). Τα Peer-To-Peer δίκτυα βρίσκουν εφαρμογή σε διάφορες εφαρμογές διαμοιρασμού αρχείων ή/και πολυμέσων, όπως το Gnutella [5] και το BitTorrent [6], σε κρυπτονομίσματα όπως το Bitcoin [7], ή άλλες εφαρμογές που χρησιμοποιούν την τεχνολογία blockchain, καθώς και σε διάφορα αποκεντρωμένα υπολογιστικά συστήματα.

3.2 Ορισμοί Εμπιστοσύνης και Φήμης

3.2.1 Εμπιστοσύνη

Όσον αφορά την Εμπιστοσύνη, πρόκειται για μία αρκετά αφηρημένη και περίπλοκη έννοια. Κατά καιρούς έχουν προταθεί διάφοροι ορισμοί, χωρίς όμως να έχει καθιερωθεί κάποιος συγκεκριμένος [8]. Στον ακόλουθο Πίνακα (Πίνακας 1) παρατίθενται ενδεικτικά παραδείγματα.

Deutsch (1958)	Εμπιστοσύνη είναι η μη ορθολογική επιλογή ενός ανθρώπου που έρχεται αντιμέτωπος με ένα αβέβαιο γεγονός, στην οποία η προσδοκώμενη ζημία ήταν μεγαλύτερη από το προσδοκώμενο όφελος.
Wrightsman (1964)	Εμπιστοσύνη είναι μια προσδοκία για το πώς συμπεριφέρονται οι άνθρωποι. Η αξιοπιστία αντιπροσωπεύει το πόσο κάποιος πιστεύει ότι οι άνθρωποι είναι κατά βάση ειλικρινείς, και όχι ανήθικοι και ανεύθυνοι.
Rotter (1967)	Μια γενικευμένη προσδοκία που έχει ένα άτομο ότι μπορεί να βασιστεί στα λόγια, τις υποσχέσεις, και τις προφορικές ή γραπτές δηλώσεις ενός άλλου ατόμου.
Zand (1972)	Η Εμπιστοσύνη είναι μια ατομική απόφαση που βασίζεται σε αισιόδοξες προσδοκίες ή στην αυτοπεποίθηση σχετικά με την έκβαση ενός αβέβαιου γεγονότος, παρά την προσωπική τρωτότητα και την αδυναμία ελέγχου πάνω στις πράξεις των άλλων.
Schlenker (1973)	Εμπιστοσύνη είναι η εξάρτηση από πληροφορίες τρίτου ατόμου σχετικά με αβέβαιες περιβαλλοντικές συνθήκες και τον αντίκτυπό τους σε μια ριψοκίνδυνη κατάσταση.
Arrow (1974)	Η Εμπιστοσύνη μπορεί να διευκολύνει τη σύναψη μιας σχέσης.
Frost (1976)	Η Εμπιστοσύνη είναι η προσδοκία ενός ατόμου ότι η συμπεριφορά ενός άλλου ατόμου ή ενός συνόλου θα είναι αλτρουιστική και προσωπικά ωφέλιμη.
Luhmann (1979)	Η Εμπιστοσύνη είναι μια ριψοκίνδυνη δέσμευση.
Matthews, Shimoff (1979)	Η εμπιστοσύνη είναι μια αντίδραση με την οποία οι άνθρωποι δεσμεύονται στην ενδεχόμενη ζημία που προκύπτει από τη συμπεριφορά άλλων ανθρώπων.
Larzelere, Huston (1980)	Εμπιστοσύνη είναι να βασίζεσαι στην καλοσύνη στο προσδοκώμενο μέλλον.
Cook, Wall (1980)	Ο βαθμός στον οποίο κάποιος είναι διατεθειμένος να αποδίδει καλές προθέσεις και να έχει πίστη στις λέξεις και τις πράξεις των άλλων.
Schurr, Ozanne (1985)	Η πεποίθηση ότι τα λόγια ή οι υποσχέσεις ενός μέρους είναι αξιόπιστες και ότι το εν λόγω μέρος θα εκπληρώσει τις υποχρεώσεις του σε μια ανταλλακτική σχέση.

Zucker (1986)	Η Εμπιστοσύνη είναι ένα σύνολο κοινωνικών προσδοκιών κοινό σε όλους όσοι εμπλέκονται σε μια οικονομική ανταλλαγή το οποίο είναι βασισμένο στους ανθρώπους, τη διαδικασία και τους θεσμούς.
Swan, Trawick (1987)	Ο πελάτης πιστεύει ότι αυτό που λέει ή υπόσχεται να κάνει ο πωλητής είναι αξιόπιστο σε μια κατάσταση όπου η αποτυχία του πωλητή να φανεί αξιόπιστος μπορεί να προκαλέσει προβλήματα στον πελάτη.
Jarillo (1988)	Η Εμπιστοσύνη μπορεί να λειτουργήσει ως συνδετικό υλικό στις σχέσεις.
Gambetta (1988)	Η Εμπιστοσύνη είναι ένα συγκεκριμένο επίπεδο υποκειμενικής βεβαιότητας με το οποίο ένα άτομο εκτιμά πως ένα άλλο άτομο ή σύνολο ατόμων θα εκτελέσει μια συγκεκριμένη πράξη, τόσο πριν μπορέσει να παρακολουθήσει την εν λόγω πράξη (ή ανεξάρτητα από την ικανότητά του να την παρακολουθήσει εν γένει) όσο και σε ένα πλαίσιο στο οποίο επηρεάζει τη δική του πράξη.
Hawes (1989)	Εμπιστοσύνη είναι η εξάρτηση από πληροφορίες τρίτου ατόμου σχετικά με αβέβαιες συνθήκες του περιβάλλοντος και αποτελέσματα σε μια ριψοκίνδυνη κατάσταση.
Michalos (1990)	Η Εμπιστοσύνη είναι μια σχετικά συνειδητή διάθεση ή τάση να επιτρέπει κανείς στον εαυτό του και ενδεχομένως σε άλλους να υπόκεινται σε ζημία για χάρη ενός εκτιμώμενου κοινού καλού.
Boon, Holmes (1991)	Η Εμπιστοσύνη είναι μια κατάσταση που περιλαμβάνει βέβαιες προσδοκίες σχετικά με τα κίνητρα του άλλου, σε σχέση με τον εαυτό του, σε καταστάσεις που εμπεριέχουν ρίσκο.
Lagace, Gassenheimer (1991)	Η Εμπιστοσύνη είναι μια διάθεση που οδηγεί κάποιον να δεσμευτεί σε μια ενδεχόμενη ζημία η οποία εξαρτάται από την μελλοντική συμπεριφοράς ενός άλλου ατόμου.
Moorman (1993)	Εμπιστοσύνη είναι η προθυμία να βασίζεται κανείς στην αλληλεπίδραση με έναν συνεργάτη στον οποίο πιστεύει.
Lagace, Marshall (1994)	Εμπιστοσύνη είναι ένα άτομο να δεσμεύεται σε μια πιθανή ζημία η οποία έρχεται ως επακόλουθο της μετέπειτα συμπεριφοράς ενός συγκεκριμένου άλλου ατόμου.
Barney, Hansen (1994)	Εμπιστοσύνη είναι η αμοιβαία πίστη ότι κανένα μέρος σε μια συναλλαγή δεν θα εκμεταλλευτεί τις αδυναμίες του άλλου.
Ganesan (1994)	Η προθυμία να βασίζεται κανείς σε έναν συνεργάτη στον οποίο πιστεύει. Δυο διαφορετικά στοιχεία: η αντικειμενική αξιοπιστία, η πεποίθηση ότι ο άλλος έχει την ειδημοσύνη να εκτελέσει το έργο, και η καλοπιστία, η πεποίθηση ότι ο άλλος έχει κίνητρα ωφέλιμα για τον στόχο όταν προκύπτουν νέες συνθήκες για τις οποίες δεν έχει υπάρξει προηγούμενη δέσμευση.
Lewicki, Bunker (1995)	Η Εμπιστοσύνη είναι μια κατάσταση που εμπεριέχει θετικές προσδοκίες για τα κίνητρα του άλλου σε σχέση με τον ίδιο σε καταστάσεις που εμπεριέχουν ρίσκο.
Mayer (1995)	Η Εμπιστοσύνη είναι η προθυμία ενός μέρους που βασίζεται στην προσδοκία ότι το άλλο μέρος θα τελέσει μια συγκεκριμένη πράξη που

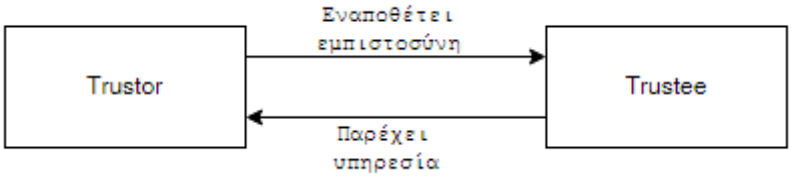
	είναι σημαντική για τον καταπιστευματοδόχο, ανεξάρτητα από την ικανότητά του να ελέγξει ή να επιβλέψει το εν λόγω μέρος.
Hosmer (1995)	Εμπιστοσύνη είναι η αξιοπιστία ενός ατόμου, μιας ομάδας ή μιας επιχείρησης σε ένα εθελοντικά αποδεκτό καθήκον εκ μέρους άλλου ατόμου, ομάδας ή εταιρείας να αναγνωρίζει και να προστατεύει τα δικαιώματα και τα συμφέροντα όλων των άλλων που συμμετέχουν σε μια κοινή προσπάθεια ή οικονομική ανταλλαγή.
Bhattacharya (1998)	Εμπιστοσύνη είναι η προσδοκία θετικών (μη αρνητικών) εκβάσεων που μπορεί κανείς να λάβει βάσει των προσδοκώμενων δράσεων ενός άλλου μέρους σε μια αλληλεπίδραση που χαρακτηρίζεται από αβεβαιότητα.
Strutton (1996)	Η προθυμία να βασίζεται κανείς σε έναν συνεργάτη τον οποίο ο πελάτης εμπιστεύεται.
Bidault, Jarillo (1997)	Εμπιστοσύνη είναι η πίστη ότι το άλλο μέρος θα συμπεριφερθεί υπηρετώντας το συμφέρον μας.
Rousseau (1998)	Η Εμπιστοσύνη είναι μια ψυχολογική κατάσταση που συνίσταται στην πρόθεση να αποδεχτεί κανείς την τρωτότητα που βασίζεται στις θετικές προσδοκίες όσον αφορά στις προθέσεις και τις συμπεριφορές των άλλων.
Lippert (2001)	Η Τεχνολογική εμπιστοσύνη είναι η προθυμία ενός ατόμου να είναι ευάλωτο ως προς την τεχνολογία η οποία βασίζεται στις προσδοκίες προβλεψιμότητας, αξιοπιστίας και ωφελιμότητας και επηρεάζεται από την προδιάθεση του ατόμου να εμπιστεύεται την τεχνολογία.
Medlin (2002)	Η Εμπιστοσύνη μπορεί να θεωρηθεί ψυχολογική κατασκευή, η οποία γεννάται μέσα σε κοινωνικές δομές (για παράδειγμα εταιρίες ή σχέσεις) από την ατομική ή συλλογική ερμηνεία τετελεσμένων πράξεων.
Halliday (2003)	Η Εμπιστοσύνη μπορεί να γίνει αντιληπτή ως μια θεματική η οποία προσφέρει μια προσέγγιση σχετικά με την εξέλιξη σε συνθήκες αβεβαιότητας καθώς και ως μια πλούσια και περίπλοκη έννοια.
Riegelsberger (2003)	Η Εμπιστοσύνη είναι ένας μηχανισμός για την μείωση της περιπλοκότητας, ένας σύντομος δρόμος για την αποφυγή μιας περίπλοκης διαδικασίας λήψεως αποφάσεων όταν έρχεται κανείς αντιμέτωπος με αποφάσεις που εμπεριέχουν ρίσκο.
Svensson (2004)	Η Εμπιστοσύνη αποτελεί σημαντικό παράγοντα στις εταιρικές σχέσεις δεδομένου ότι οι εταιρικές δραστηριότητες διευθύνονται από ανθρώπους.
Michael, Rowe (2006)	Η Εμπιστοσύνη δεν είναι κατά βάση ατομικό χαρακτηριστικό ή χαρακτηριστικό διάθεσης, ούτε ψυχολογική κατάσταση. Είναι κατασκευασμένη από ένα σύνολο διαπροσωπικών συμπεριφορών ή από μια κοινή ταυτότητα. Αυτές οι συμπεριφορές ενισχύονται από θεσμικούς κανόνες, νόμους και έθιμα.
Chen, Barnes (2007)	Η Εμπιστοσύνη είναι η αντιλαμβανόμενη χρησιμότητα, η αντιλαμβανόμενη ασφάλεια, η αντιλαμβανόμενη ιδιωτικότητα, και η αντιλαμβανόμενη καλή φήμη, ενώ η προθυμία να προσαρμόζεται

	κανείς αποτελεί τον πιο σημαντικό σημείο αναφοράς στην αρχική διαμόρφωση της εμπιστοσύνης στο διαδίκτυο.
Kim (2009)	Η Εμπιστοσύνη είναι μια περίπλοκη και πολυδιάστατη κατασκευή.

Πίνακας 1: Διάφοροι ορισμοί της Εμπιστοσύνης

Παρότι δεν υπάρχει ενιαίος ορισμός της έννοιας της Εμπιστοσύνης, παρατηρείται πως σχεδόν όλοι οι ορισμοί κινούνται γύρω από κάποιους βασικούς άξονες.

Ένας από τους βασικούς άξονες είναι πως η Εμπιστοσύνη μπορεί να μοντελοποιηθεί ως μία σχέση ανάμεσα σε δύο οντότητες: τον Trustee, στον οποίο εναποτίθεται η εμπιστοσύνη, και ο οποίος παρέχει κάποια υπηρεσία, και στον Trustor, ο οποίος λαμβάνει την υπηρεσία αυτή.



Εικόνα 1: Σχέση μεταξύ Trustor και Trustee

Ένας δεύτερος άξονας είναι η αποδοχή πως η Εμπιστοσύνη δεν είναι απόλυτη, αλλά εξαρτάται από την εκάστοτε περίσταση και υπηρεσία. Για παράδειγμα, ο καθένας θα εμπιστευόταν έναν γιατρό εάν χρειαζόταν ιατρική περίθαλψη, ωστόσο αν χρειαζόταν σύσταση ως προς τα χαρακτηριστικά του αυτοκινήτου που επιθυμεί να αγοράσει, η εμπιστοσύνη σε αυτόν θα ήταν τελείως διαφορετική.

Άλλο ένα κοινό γνώρισμα που αποδίδουν οι περισσότεροι ορισμοί στην έννοια της Εμπιστοσύνης είναι πως εμπεριέχει αβεβαιότητα και ρίσκο, λόγω της ελλιπούς πληροφορίας από πλευράς Trustor.

Τέλος, αρκετοί ορισμοί υποστηρίζουν πως η έννοια της Εμπιστοσύνης είναι μία πολυδιάστατη έννοια η οποία συνίσταται από επιμέρους χαρακτηριστικά. Αυτό ακριβώς το χαρακτηριστικό της είναι που καθιστά δύσκολο τον σαφή και καθολικά αποδεκτό ορισμό της. Παρότι οι διαφορετικές διαστάσεις της έννοιας δεν μπορούν να αποδοθούν με πληρότητα και ακρίβεια, συσχετίζονται συχνά με τις έννοιες της απόδοσης, της αξιοπιστίας και της προβλεψιμότητας της συμπεριφοράς.

Συνοπτικά, ένας ορισμός που θα μπορούσε να δοθεί, είναι πως ***η Εμπιστοσύνη μίας οντότητας Α προς μία οντότητα Β για μία υπηρεσία Υ, είναι ο βαθμός πίστης της Α ως προς το αν η οντότητα Β θα της παρέχει την υπηρεσία Υ σε κάποιον αποδεκτό βαθμό***. Το τελευταίο κομμάτι του ορισμού ("σε ποιο βαθμό") είναι αρκετά υποκειμενικό και μπορεί να ποικίλλει ανάλογα με την εκάστοτε εφαρμογή.

3.2.2 Φήμη

Η έννοια της Φήμης αντιμετωπίζει το ίδιο πρόβλημα με την έννοια της Εμπιστοσύνης: την έλλειψη ενός καθιερωμένου και καθολικού ορισμού. Και σε αυτήν την περίπτωση ωστόσο, οι περισσότεροι ορισμοί έχουν αρκετά κοινά στοιχεία.

Το πρώτο εντοπίζεται σε έναν αρκετά αφηρημένο ορισμό της έννοιας, σύμφωνα με τον οποίο η Φήμη είναι η εκτίμηση ενός μέρους ή ολόκληρου του συνόλου ως προς μία άλλη οντότητα, η οποία χρησιμοποιείται για να επιλεγεί τελικά κάποιος συνεργάτης/πάροχος υπηρεσίας. Πιο συγκεκριμένα, συνίσταται στην απομνημόνευση και χρήση των τετελεσμένων πράξεων ενός χρήστη προκειμένου να προβλεφθεί η μελλοντική συμπεριφορά του. Η Φήμη, λοιπόν, γίνεται ένα εργαλείο για τη διαχείριση του ρίσκου, με απώτερο σκοπό να περιορίσει την υπάρχουσα ασυμμετρία πληροφοριών.

Το δεύτερο στοιχείο έχει να κάνει με την κοινωνική διάσταση της Φήμης. Η Φήμη αντιμετωπίζεται συχνά ως έννοια κοινωνική, ενώ έχει χαρακτηριστεί ακόμα και μηχανισμός κοινωνικού ελέγχου, ο οποίος αναπτύχθηκε μέσω της κοινωνικής αλληλεπίδρασης ενός συνόλου με κοινά συμφέροντα. Οι ρίζες της στο αρχαίο κοινωνικό πλαίσιο είναι εμφανείς και στα ακόλουθα χαρακτηριστικά. Αρχικά, το γεγονός ότι η έννοια της κλίμακας αποτελεί απαραίτητο στοιχείο προκειμένου να λειτουργήσει η έννοια της φήμης. Δεύτερον, η αντίληψη ότι η φήμη πρέπει να διαδίδεται και να μοιράζεται προκειμένου να είναι ωφέλιμη. Τέλος, το γεγονός ότι η φήμη ενός χρήστη δεν είναι απόλυτη, αλλά η τιμή της μπορεί να ποικίλει ανάλογα με τον χρήστη που τον αξιολογεί.

Πρέπει επίσης να επισημανθεί ότι ο η κατεύθυνση της Φήμης μπορεί να είναι είτε μονόδρομη είτε αμφίδρομη. Με άλλα λόγια, σε μια τυχαία συναλλαγή μπορεί είτε μόνο το ένα μέρος να αξιολογήσει το άλλο, είτε και τα δύο να αξιολογήσουν το ένα το άλλο.

Το τελευταίο στοιχείο έχει να κάνει με την κοινή αντίληψη ότι η Φήμη πρόκειται για μία έννοια η οποία για να αποκτήσει νόημα χρειάζεται ένα πλήθος διαφορετικών πηγών πληροφορίας. Αν και υπάρχει η δυνατότητα ένα σύστημα να περιοριστεί σε μία μόνο δυνητική πηγή πληροφοριών, συνήθως θεωρείται καλύτερη η χρήση περισσοτέρων πηγών.

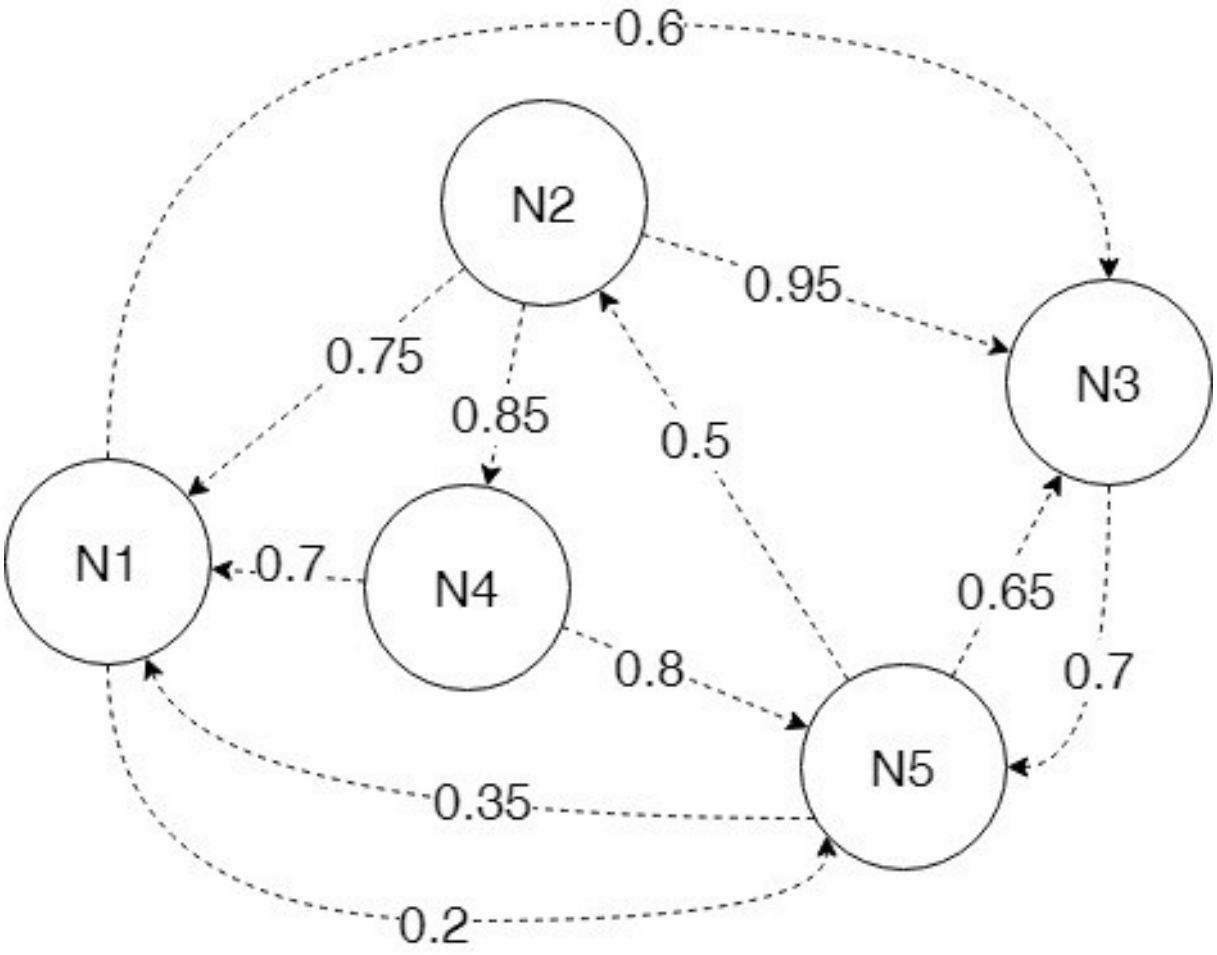
Η Φήμη, λοιπόν, όπως και η Εμπιστοσύνη, δεν είναι σταθερή και μπορεί να μεταβάλλεται ανάλογα την περίσταση. Προκειμένου να φωτιστούν περισσότερο τα παραπάνω κρίνεται σκόπιμο να αναφερθεί ένα παράδειγμα. Θα χρησιμοποιηθεί, λοιπόν, το παράδειγμα ενός γιατρού. Ο γιατρός έχει υψηλή Φήμη εάν η ζητούμενη υπηρεσία είναι η ιατρική περίθαλψη, εάν όμως η ζητούμενη η ζητούμενη υπηρεσία είναι συμβουλές για τα χαρακτηριστικά ενός αυτοκινήτου η Φήμη του είναι χαμηλή. Επίσης, η Φήμη ενός χρήστη μπορεί να μεταβάλλεται και ανάλογα με το σύνολο το οποίο τον αξιολογεί. Για παράδειγμα, ο ίδιος γιατρός μπορεί να έχει υψηλή Φήμη ως προς την ιατρική περίθαλψη που προσφέρει μεταξύ των ασθενών του, ωστόσο αν το σύνολο το οποίο τον αξιολογεί αποτελείται από συναδέλφους του οι οποίοι δεν τον έχουν σε εκτίμηση, η Φήμη του στο συγκεκριμένο σύνολο είναι χαμηλή.

3.2.3 Υπερκείμενο Δίκτυο Εμπιστοσύνης (Trust Overlay Network)

Ένας πολύ βοηθητικός τρόπος να μοντελοποιηθεί η Εμπιστοσύνη και η Φήμη εντός ενός δικτύου είναι η χρήση ενός Υπερκείμενου Δικτύου Εμπιστοσύνης (Trust Overlay Network – TON) [9]. Το Υπερκείμενο Δίκτυο Εμπιστοσύνης αντιπροσωπεύεται από έναν κατευθυνόμενο γράφο με βάρη στις ακμές του.

Οι κόμβοι του γράφου αντιστοιχούν στους χρήστες του συστήματος, ενώ οι ακμές αντιπροσωπεύουν την Εμπιστοσύνη του ενός χρήστη προς τον άλλο, όπως φαίνεται στην Εικόνα 2. Συγκεκριμένα, κάθε ακμή αντιπροσωπεύει την Εμπιστοσύνη του κόμβου από τον οποίο εξέρχεται για τον κόμβο στον οποίο εισέρχεται, με το βάρος της ακμής να καθορίζει την τιμή της Εμπιστοσύνης. Έτσι, για παράδειγμα, στο δίκτυο της Εικόνας 2, ο κόμβος N_2 έχει Εμπιστοσύνη προς τους κόμβους N_1, N_3 και N_4 με 0.75, 0.95 και 0.85 αντίστοιχα, ενώ η τιμή της Εμπιστοσύνης του κόμβου N_5 προς αυτόν είναι 0.5. Έπειτα από την πραγματοποίηση μίας συναλλαγής, ο κόμβος ο οποίος έλαβε την υπηρεσία ανανεώνει την τιμή της Εμπιστοσύνης του προς τον κόμβο που του παρείχε την υπηρεσία, με αποτέλεσμα η τιμή της ακμής που εξέρχεται από τον πρώτο και εισέρχεται στον δεύτερο να αλλάζει.

Σε επόμενο βήμα, η Φήμη κάποιου κόμβου θα μπορούσε πολύ απλά να υπολογιστεί ως ο μέσος όρος των τιμών των εισερχόμενων σε αυτόν τον κόμβο ακμών. Έτσι, η Φήμη του κόμβου N_1 θα μπορούσε



Εικόνα 2: Δίκτυο εμπιστοσύνης 5 κόμβων

να υπολογιστεί ως $\frac{0.75+0.7+0.35}{3} = 0.583$. Ωστόσο, αξίζει να σημειωθεί πως συνήθως ο υπολογισμός της Φήμης είναι πιο περίπλοκος και λαμβάνει υπόψιν και άλλες παραμέτρους, όπως ο χρόνος, η αξιοπιστία των κόμβων οι οποίοι παρέχουν τις αξιολογήσεις αυτές, κ.ά. Οι παράμετροι αυτές μπορεί να ποικίλουν ανάλογα το μοντέλο Εμπιστοσύνης και Φήμης που ακολουθείται σε κάθε περίπτωση.

4

Παρουσίαση των Μοντέλων

4.1 Μοντέλο EigenTrust

4.1.1 Εισαγωγή και Γενικές Ιδέες

Το μοντέλο EigenTrust [10] χρησιμοποιεί μία κατανεμημένη μέθοδο υπολογισμού για την καθολική Φήμη του κάθε κόμβου του δικτύου. Έστω ότι η τιμή $\boldsymbol{s_{ij}}$ αντιπροσωπεύει την ***ατομική εμπιστοσύνη*** ενός κόμβου $\boldsymbol{i}$ προς έναν κόμβο $\boldsymbol{j}$. Για να υπολογιστεί η καθολική Φήμη κάθε κόμβου, λαμβάνονται υπ' όψη οι τιμές της ατομικής εμπιστοσύνης των υπολοίπων κόμβων του δικτύου προς αυτόν.

Αρχικά, πραγματοποιείται μία κανονικοποίηση των τιμών ατομικής εμπιστοσύνης. Έτσι, ορίζεται η ***κανονικοποιημένη ατομική εμπιστοσύνη*** ως εξής:

$$c_{ij} = \frac{max(s_{ij}, 0)}{\sum_k max(s_{ik}, 0)} \quad (4.1.a)$$

Με αυτόν τον τρόπο εξασφαλίζεται πως οι τιμές θα βρίσκονται μεταξύ 0 και 1. Ένα μειονέκτημα της συγκεκριμένης μεθόδου είναι πως οι τιμές αυτές δίνουν παρά μόνο μία σχετική εικόνα. Δηλαδή, στην περίπτωση που $c_{ij} = c_{ik}$, γνωρίζουμε πως οι κόμβοι j και k έχουν την ίδια Φήμη με βάση τον κόμβο i, ωστόσο δεν είναι δυνατό να γνωρίζουμε την ποιότητα της συμπεριφοράς τους.

Στη συνέχεια, οι τιμές της κανονικοποιημένης ατομικής εμπιστοσύνης αθροίζονται έτσι ώστε να προκύψει τελικά η τιμή της καθολικής Φήμης για κάθε κόμβο. Σε ένα κατανεμημένο περιβάλλον, κάτι τέτοιο μπορεί να γίνει για τον κόμβο i ζητώντας πληροφορίες από τους γειτονικούς του κόμβους. Οι

πληροφορίες που λαμβάνει αθροίζονται με συντελεστή την ατομική εμπιστοσύνη του i προς κάθε γείτονά του. Έτσι, προκύπτει η ακόλουθη τιμή:

$$t_{ik} = \sum_{j} c_{ij} c_{jk} \quad (4.1.b)$$

Η τιμή αυτή αντιπροσωπεύει την εμπιστοσύνη του κόμβου i προς τον κόμβο k με βάση τις πληροφορίες των γειτόνων του.

Η παραπάνω σχέση μπορεί να γραφτεί χρησιμοποιώντας τη σημειογραφία πινάκων. Εάν ορίσουμε τον πίνακα $C = [c_{ij}]$ και $\vec{t_i}$ το διάνυσμα με τις τιμές t_{ik} τότε $\vec{t_i} = C^T \vec{c_i}$. Έτσι, έχουμε έναν τρόπο για τους κόμβους να αποκτήσουν μία εικόνα του δικτύου η οποία εκτείνεται έξω από τις δικές τους εμπειρίες/αλληλεπιδράσεις.

Ωστόσο, οι τιμές αυτές δεν δείχνουν παρά μόνο την εμπειρία του κόμβου i και των γειτόνων του. Θα μπορούσαμε να λάβουμε μία ακόμα ευρύτερη εικόνα του δικτύου εάν λαμβάναμε πληροφορία και από τους γείτονες των γειτόνων του i, σύμφωνα με τη σχέση $\vec{t_i} = (C^T)^2 \vec{c_i}$. Εάν συνεχίσουμε με τον ίδιο τρόπο ($\vec{t_i} = (C^T)^n \vec{c_i}$), θα έχουμε μία πλήρη εικόνα του δικτύου έπειτα από n επαναλήψεις. Αποδεικνύεται πως για μεγάλες τιμές του n, το διάνυσμα $\vec{t_i}$ συγκλίνει στην ίδια τιμή **για κάθε κόμβο i** του δικτύου. Συγκεκριμένα, συγκλίνει στο αριστερό ιδιοδιάνυσμα του C. Με άλλα λόγια, το διάνυσμα $\vec{t}$ είναι το διάνυσμα καθολικής Φήμης.

4.1.2 Βασικός Αλγόριθμος EigenTrust

Ο στόχος του συγκεκριμένου μοντέλου είναι ο υπολογισμός του

$$\vec{t} = (C^T)^n \vec{c_i} \quad (4.1.c)$$

όπου $\vec{c_i}$ το διάνυσμα που περιέχει τις κανονικοποιημένες τιμές ατομικής εμπιστοσύνης ενός κόμβου i. Αντί αυτού, μπορεί να χρησιμοποιηθεί το διάνυσμα $\vec{e}$, το οποίο αντιπροσωπεύει μία ομοιόμορφη κατανομή εμπιστοσύνης στους κόμβους του δικτύου, δηλαδή $e_i = 1/m$, όπου m το πλήθος των κόμβων του δικτύου.

Μέχρι στιγμής υπάρχουν ορισμένα ζητήματα τα οποία δεν έχουν ληφθεί υπ' όψη:

1. **Εξ ορισμού έμπιστοι κόμβοι:** Είναι συχνό φαινόμενο σε ορισμένα δίκτυα να υπάρχουν εξ ορισμού έμπιστοι κόμβοι (πχ. οι σχεδιαστές και αρχικοί χρήστες ενός P2P δικτύου). Για αυτόν το λόγο ορίζεται μία κατανομή εμπιστοσύνης $\vec{p}$ στο σύνολο των κόμβων του δικτύου, όπου

$$p_i = \begin{cases} \frac{1}{|P|} \ \alpha\nu \ i \in \ P, \text{όπου } P \text{ το σύνολο των εξ ορισμού έμπιστων κόμβων} \\ 0, \alpha\lambda\lambda\iota\acute{\omega}\varsigma \end{cases}$$

2. **Περίπτωση μη-αλληλεπίδρασης:** Είναι εμφανές πως εάν ένας κόμβος δεν έχει λάβει κάποια υπηρεσία από κανέναν άλλο κόμβο, τότε στην Εξίσωση $4.1.a$ ο παρονομαστής μηδενίζεται. Για αυτόν το λόγο ορίζεται εκ νέου ως εξής:

$$c_{ij} = \begin{cases} \frac{max(s_{ij}, 0)}{\sum_k max(s_{ik}, 0)}, \alpha\nu \sum_k max(s_{ik}, 0) \neq 0 \\ p_j, \alpha\lambda\lambda\iota\acute{\omega}\varsigma \end{cases}$$

Με αυτόν τον τρόπο, αν ο κόμβος i δεν έχει προηγούμενη πληροφορία, είναι πιθανότερο να εμπιστευθεί τους εξ ορισμού έμπιστους κόμβους.

3. **Κακόβουλες Συλλογικότητες:** Οι κακόβουλες συλλογικότητες είναι ομάδες κόμβων οι οποίες αποδίδουν υψηλές τιμές Εμπιστοσύνης μεταξύ τους και χαμηλές τιμές στους υπόλοιπους κόμβους του δικτύου, με σκοπό να αποκτήσουν τελικά υψηλή καθολική Φήμη. Για να αντιμετωπιστούν τέτοιου είδους συλλογικότητες, η Εξίσωση $(4.1.c)$ τροποποιείται ως ακολούθως:

$$\vec{t}^{(k+1)} = (1-a)(C^T)^n \ \vec{t}^{(k)} + a\vec{p} \quad (4.1.d)$$

όπου $0 < a < 1$. Με αυτόν τον τρόπο εξασφαλίζεται πως τουλάχιστον κατά κάποιον βαθμό θα αποδίδεται Εμπιστοσύνη στους εξ ορισμού έμπιστους κόμβους, οι οποίοι δεν ανήκουν σε κάποια κακόβουλη συλλογικότητα.

4.1.3 Κατανεμημένος Αλγόριθμος EigenTrust

Σε ένα κατανεμημένο σύστημα οι κόμβοι συνεργάζονται έτσι ώστε να υπολογίσουν όλοι μαζί το διάνυσμα καθολικής φήμης. Έστω πως κάθε κόμβος, εκτός από το διάνυσμα με τις ατομικές τιμές εμπιστοσύνης του, διατηρεί στη μνήμη του και το διάνυσμα καθολικής Φήμης του εαυτού του ($\vec{t_i}$). Τότε, κάθε κόμβος μπορεί να υπολογίσει το δικό του διάνυσμα καθολικής Φήμης ως εξής:

$$t_i^{(k+1)} = (1-a)\left(c_{1i}t_1^{(k)} + \cdots + c_{ni}t_n^{(k)}\right) + ap_i \quad (4.1.e)$$

Ο υπολογισμός αυτός μπορεί να γίνει εύκολα σύμφωνα με τον Αλγόριθμο 1:

Ορισμοί:

- $\boldsymbol{A_i}$**:** Το σύνολο των κόμβων που έχουν λάβει υπηρεσία από τον κόμβο i
- $\boldsymbol{B_i}$**:** Το σύνολο των κόμβων από τους οποίους έχει λάβει υπηρεσία ο κόμβος i

Αλγόριθμος:

Για κάθε κόμβο i:

Πραγματοποίηση αιτήματος προς όλους τους κόμβους $j \in A_i$ για την τιμή $t_j^{(0)} = p_j$;

Επανάλαβε:

Υπολογισμός του $\mathrm{t_i^{(k+1)}} = (1 - \mathrm{a})(\mathrm{c_{1i}t_1^{(k)}} + \mathrm{c_{2i}t_2^{(k)}} + \ldots + \mathrm{c_{ni}t_n^{(k)}}) + ap_\mathrm{i}$;

Αποστολή του $c_{ij}t_i^{(k+1)}$ σε όλους τους κόμβους $j \in B_i$;

Υπολογισμός σφάλματος $\delta = |\,\mathrm{t_i^{(k+1)}} - \mathrm{t_i^{(k)}}|$;

Αναμονή για λήψη των τιμών $c_{ji}t_j^{(k+1)}$;

Έως ότου $\delta < \varepsilon$;

Τέλος Επανάληψης

Αλγόριθμος 1: Κατανεμημένος Αλγόριθμος EigenTrust

4.1.4 Ζητήματα Ασφάλειας στο EigenTrust

Στον κατανεμημένο αλγόριθμο EigenTrust που περιεγράφηκε στην Ενότητα 4.1.3 κάθε κόμβος i υπολογίζει και αποστέλλει την δική του τιμή καθολικής φήμης t_i. Γίνεται εύκολα αντιληπτό πως τυχόν κακόβουλοι κόμβοι μπορούν να εκμεταλλευτούν το γεγονός αυτό έτσι ώστε να αποστέλλουν ψευδείς τιμές προς όφελός τους και εις βάρος του συστήματος.

Το ζήτημα αυτό αντιμετωπίζεται με κύριο άξονα τις ακόλουθες ιδέες. Για αρχή, η τιμή της καθολικής φήμης ενός κόμβου i δεν πρέπει να υπολογίζεται και να αποθηκεύεται στον ίδιο, αλλά σε κάποιον άλλο κόμβο του συστήματος. Δεύτερον, επειδή οι κακόβουλοι κόμβοι μπορούν να αποστείλουν ψευδείς τιμές όσον αφορά τον υπολογισμό της καθολικής Φήμης ενός άλλου κόμβου, πρέπει να συμμετέχουν περισσότεροι από ένας κόμβοι στον υπολογισμό αυτό.

Έτσι, για κάθε κόμβο i, υπάρχουν M κόμβοι του συστήματος οι οποίοι είναι υπεύθυνοι για τον υπολογισμό του t_i. Οι κόμβοι αυτοί ονομάζονται *διαχειριστές βαθμολογίας (score managers)* του κόμβου i. Οι διαχειριστές βαθμολογίας επιλέγονται συνήθως χρησιμοποιώντας έναν Κατανεμημένο Πίνακα Κατακερματισμού. Εάν ένας κόμβος χρειάζεται να μάθει την τιμή του t_i, αποστέλλει αίτημα στους διαχειριστές βαθμολογίας του κόμβου i και κατά τον υπολογισμό πραγματοποιείται ο κατάλληλος έλεγχος για τον εντοπισμό τυχόν κακόβουλων κόμβων ανάμεσα στους διαχειριστές βαθμολογίας με βάση τα αποτελέσματα που έχουν αποστείλει.

Με βάση τα παραπάνω, παρουσιάζεται ο Αλγόριθμος 2, ο οποίος λαμβάνει υπ’ όψη όσα ζητήματα παρουσιάστηκαν στην Ενότητα 4.1.4.

Ορισμοί:

- $\boldsymbol{A_i}$**:** Το σύνολο των κόμβων που έχουν λάβει υπηρεσία από τον κόμβο i
- $\boldsymbol{B_i}$**:** Το σύνολο των κόμβων από τους οποίους έχει λάβει υπηρεσία ο κόμβος i
- $\boldsymbol{D_i}$**:** Το σύνολο των κόμβων για τους οποίους ο κόμβος i είναι διαχειριστής βαθμολογίας
- $\boldsymbol{c_d^i}$**:** Το διάνυσμα κανονικοποιημένων τιμών εμπιστοσύνης για τον κόμβο $d \in D_i$
- $\boldsymbol{A_d^i}$**:** Το σύνολο των κόμβων που έχουν λάβει υπηρεσία από τον κόμβο $d \in D_i$
- $\boldsymbol{B_d^i}$**:** Το σύνολο των κόμβων από τους οποίους έχει λάβει υπηρεσία ο κόμβος $d \in D_i$

Αλγόριθμος:

Για κάθε κόμβο i **επανάλαβε:**

Αποστολή του διανύσματος εμπιστοσύνης $\overrightarrow{c_i}$ στους διαχειριστές βαθμολογίας του i;

Συλλογή των διανυσμάτων εμπιστοσύνης $\overrightarrow{c_d}$ και συνόλων B_d^i από τους κόμβους $d \in D_i$;

Αποστολή των τιμών c_{dj} στους διαχειριστές βαθμολογίας των κόμβων $d \in D_i, \forall j \in B_d^i$;

Συλλογή των A_d^i για τους κόμβους $d \in D_i$**;**

Για κάθε κόμβο $d \in D_i$**:**

Συλλογή των τιμών $c_{jd}p_j$ από τους κόμβους $j \in A_d^i$;

Επανάλαβε:

Υπολογισμός του $\mathrm{t_d^{(k+1)}} = (1 - \mathrm{a})(\mathrm{c_{1d}t_1^{(k)}} + \mathrm{c_{2d}t_2^{(k)}} + \ldots + \mathrm{c_{nd}t_n^{(k)}}) + ap_d$;

Αποστολή του $c_{dj}t_i^{(k+1)}$ σε όλους τους κόμβους $j \in B_d^i$;

Αναμονή για λήψη των τιμών $c_{jd}t_j^{(k+1)}$από τους κόμβους $j \in A_d^i$

Έως ότου $= |\mathrm{t_d^{(k+1)}} - \mathrm{t_d^{(k)}}| < \varepsilon$;

Τέλος επανάληψης

Τέλος επανάληψης

Αλγόριθμος 2: Ασφαλής Αλγόριθμος EigenTrust

4.2 Μοντέλο PowerTrust

4.2.1 Εισαγωγή και Γενικές Ιδέες

Το μοντέλο PowerTrust [11] λειτουργεί με τρόπο παρόμοιο με το EigenTrust, δηλαδή πραγματοποιεί έναν κατανεμημένο υπολογισμό της Εξίσωσης 4.1.c. Κάθε κόμβος i, έχει επίσης έναν ή περισσότερους *διαχειριστές βαθμολογίας*, οι οποίοι είναι υπεύθυνοι για τον υπολογισμό του διανύσματος καθολικής φήμης $\vec{t_i}$. Για κάθε κόμβο i οι διαχειριστές βαθμολογίας του επιλέγονται με βάση μία συνάρτηση κατακερματισμού.

Ο σχεδιασμός του PowerTrust βασίζεται στην υπόθεση πως ο αριθμός αξιολογήσεων για κάθε κόμβο, δηλαδή ο έσω-βαθμός του στο Υπερκείμενο Δίκτυο Εμπιστοσύνης, ακολουθεί την Κατανομή Νόμου Δύναμης (Power-Law Distribution), δηλαδή πως υπάρχουν λίγοι κόμβοι του συστήματος οι οποίοι λαμβάνουν έναν πολύ υψηλό αριθμό αξιολογήσεων, ενώ οι περισσότεροι κόμβοι του δικτύου έχουν μικρό αριθμό αξιολογήσεων. Κάτι τέτοιο επιβεβαιώνεται και εμπειρικά. Οι κόμβοι αυτοί οι οποίοι συγκεντρώνουν μεγάλο αριθμό αξιολογήσεων τείνουν επίσης να έχουν υψηλή απόδοση και σωστή συμπεριφορά στο σύστημα. Το PowerTrust εκμεταλλεύεται αυτά τα χαρακτηριστικά και επιλέγει ανά διαστήματα τους m πιο αξιόπιστους κόμβους του συστήματος με βάση τη φήμη τους.

4.2.2 Εύρεση Αξιόπιστων Κόμβων – Power Nodes

Όπως αναλύθηκε στην Ενότητα 4.1, στο EigenTrust υπάρχουν ορισμένοι κόμβοι οι οποίοι θεωρούνται εξ' ορισμού έμπιστοι. Ένα από τα κρίσιμα σημεία του EigenTrust είναι πως εάν αυτοί οι κόμβοι φύγουν από το σύστημα, ή για κάποιο λόγο αποκτήσουν κακόβουλη συμπεριφορά, η αποτυχία του συστήματος είναι βέβαιη. Για αυτόν το λόγο, στο PowerTrust η αντίστοιχη ιδιότητα είναι δυναμική. Έτσι, με βάση τον μηχανισμό που περιγράφεται στον Αλγόριθμο 3, επιλέγονται οι m πιο έμπιστοι κόμβοι του συστήματος μία δεδομένη χρονική στιγμή, οι λεγόμενοι Power Nodes. Για την επιλογή αυτή χρησιμοποιείται και μία συνάρτηση κατακερματισμού διατήρησης τοπικότητας (locality preserving hashing function - LPH).

Ορισμοί:

- $\boldsymbol{m}$**:** Το πλήθος των πιο αξιόπιστων κόμβων που επιθυμούμε να βρούμε

Αλγόριθμος:

Για κάθε κόμβο j, ο οποίος είναι διαχειριστής βαθμολογίας του κόμβου i:

Υπολογισμός της τιμής $H(v_i)$ χρησιμοποιώντας μία συνάρτηση κατακερματισμού LPH

Αποθήκευση της τριπλέτας (v_i, i, j) στον κόμβο με το αμέσως μεγαλύτερο αναγνωριστικό σε σχέση με την $H(v_i)$.

Τέλος επανάληψης

$Κόμβος\ x =$ Ο κόμβος με αναγνωριστικό αμέσως επόμενο από τη μέγιστη τιμή της συνάρτησης κατακερματισμού

$p =$ Ο αριθμός των τριπλετών με τις μέγιστες τιμές φήμης που είναι αποθηκευμένες στον x

Επανάλαβε:

Αν $p > m$ **:**

Τέλος

Αλλιώς:

Ο κόμβος x στέλνει μήνυμα στον κόμβο y με το αμέσως μικρότερο αναγνωριστικό για να βρει τις επόμενες $m - p$ τριπλέτες

$Κόμβος\ x = y$

$m = m - p$

$p =$ Ο αριθμός των τριπλετών αποθηκευμένες στον y

Τέλος επανάληψης

Αλγόριθμος 3: Εύρεση των m πιο αξιόπιστων κόμβων (Power Nodes)

Μία συνάρτηση κατακερματισμού είναι LPH εάν έχει τις ακόλουθες ιδιότητες:

1. $H(v_i) < H(v_j), \alpha\nu\ \kappa\alpha\iota\ \mu\acute{o}\nu o\ \alpha\nu\ v_i < v_j$
2. $A\nu\ \tau o\ \delta\iota\acute{a}\sigma\tau\eta\mu\alpha\ [v_i, v_j]\ \chi\omega\rho\iota\sigma\tau\epsilon\acute{\iota}\ \sigma\tau\alpha\ \upsilon\pi o\delta\iota\alpha\sigma\tau\acute{\eta}\mu\alpha\tau\alpha\ [v_i, v_k]\ \kappa\alpha\iota\ [v_k, v_j]$,
   $\tau\acute{o}\tau\epsilon\ \tau o\ \alpha\nu\tau\acute{\iota}\sigma\tau o\iota\chi o\ \delta\iota\acute{a}\sigma\tau\eta\mu\alpha\ [H(v_i), H(v_j)]\ \pi\rho\acute{\epsilon}\pi\epsilon\iota\ \nu\alpha\ \chi\omega\rho\acute{\iota}\zeta\epsilon\tau\alpha\iota\ \sigma\tau\alpha\ [H(v_i), H(v_k)]$,
   $[H(v_k), H(v_j)]$.

Αποδεικνύεται πως σε μία τοπολογία όπου η κωδικοποίηση του αναγνωριστικού των κόμβων χρησιμοποιεί b-bits, χρησιμοποιώντας μία συνάρτηση κατακερματισμού LPH, ο Αλγόριθμος 3 βρίσκει τους m πιο αξιόπιστους κόμβους σε h βήματα, όπου h είναι ο αριθμός των κόμβων μεταξύ του $Succ(H(v_k))$ και $Succ(2^b - 1)$, όπου $Succ(x)$ ο κόμβος με αναγνωριστικό αμέσως μεγαλύτερο από την τιμή x και v_k η m-οστή υψηλότερη τιμή φήμης.

4.2.3 Αρχικός Υπολογισμός Διανύσματος Φήμης

Έστω ο πίνακας εμπιστοσύνης R στο Δίκτυο Εμπιστοσύνης του συστήματος. Κατά τον αρχικό υπολογισμό του Διανύσματος φήμης, κάθε κόμβος i στέλνει τις τιμές εμπιστοσύνης του στους διαχειριστές βαθμολογίας των έξω-γειτόνων του.

Αποδεικνύεται πως για μικρό περιθώριο σφάλματος ε, ο Αλγόριθμος 4 είναι άνω φραγμένος από τον αριθμό $k = \lceil \log_b \varepsilon \rceil$, όπου $b = \lambda_2/\lambda_1$ και λ_1, λ_2 είναι οι δύο μεγαλύτερες ιδιοτιμές του πίνακα R.

Αλγόριθμος:

Για κάθε κόμβο i **επανάλαβε:**

Για κάθε κόμβο j, ο οποίος είναι έξω-γείτονας του i **επανάλαβε:**

Αποστολή της βαθμολογίας (r_{ij}, i) στον διαχειριστή βαθμολογίας του j

Τέλος επανάληψης

Αν ο i είναι διαχειριστής βαθμολογίας κάποιου κόμβου k**:**

Για κάθε κόμβο m, ο οποίος είναι έσω-γείτονας του k**:**

Λήψη της βαθμολογίας (r_{mk}, m) από τον m

Εντοπισμός του διαχειριστή βαθμολογίας του m

Τέλος επανάληψης

Αρχικοποίηση μεταβλητής $pre = 0$

Αρχικοποίηση κατωφλίου σφάλματος ε

Επανάλαβε:

$pre = v_k$

$v_k = 0$

Για κάθε βαθμολογία (r_{jk}, j) που λήφθηκε από τους έσω γείτονες του k**:**

Λήψη της τιμής v_j από τον διαχειριστή βαθμολογίας του j

$v_k = v_k + v_j r_{jk}$

Τέλος Επανάληψης

$\delta = |v_k - pre|$

Έως ότου $\delta < \varepsilon$

Τέλος αν

Τέλος Επανάληψης

Αλγόριθμος 4: Αρχικός Υπολογισμός Διανύσματος Φήμης

4.2.4 Ενημέρωση του Διανύσματος Φήμης

Έπειτα από τον αρχικό υπολογισμό του διανύσματος φήμης, οι διαχειριστές βαθμολογίας συνεργάζονται μεταξύ τους ώστε να βρουν τους Power Nodes χρησιμοποιώντας τον Αλγόριθμο 5.

Αλγόριθμος:
Για κάθε κόμβο i **επανάλαβε:**
Για κάθε κόμβο j, ο οποίος είναι έξω-γείτονας του i **επανάλαβε:**
Αποστολή της βαθμολογίας (r_{ij}, i) στον διαχειριστή βαθμολογίας του j
Τέλος επανάληψης
Αν ο i είναι διαχειριστής βαθμολογίας κάποιου κόμβου k**:**
Για κάθε κόμβο m, ο οποίος είναι έσω-γείτονας του k**:**
Λήψη της βαθμολογίας (r_{mk}, m) από τον m
Εντοπισμός του διαχειριστή βαθμολογίας του m
Τέλος επανάληψης
Αρχικοποίηση μεταβλητής $pre = 0$
Αρχικοποίηση κατωφλίου σφάλματος ε
Επανάλαβε:
$pre = v_k$
$v_k = 0$
Για κάθε βαθμολογία (r_{jk}, j) που λήφθηκε από τους έσω γείτονες του k**:**
Λήψη της τιμής v_j από τον διαχειριστή βαθμολογίας του j
Τέλος Επανάληψης
Αν ο k είναι Power Node**:**
$$v_k = (1 - a) \sum (v_j r_{jk}) + a/m$$
Αλλιώς:
$$v_k = (1 - a) \sum (v_j r_{jk})$$
Τέλος αν
$\delta = |v_k - pre|$
Έως ότου $\delta < \varepsilon$
Τέλος αν
Τέλος Επανάληψης

Αλγόριθμος 5: Ενημέρωση Διανύσματος Φήμης

4.3 Μοντέλο PeerTrust

4.3.1 Εισαγωγή και Γενικές Ιδέες

Το μοντέλο PeerTrust[12] σχεδιάστηκε για την αντιμετώπιση των κακόβουλων χρηστών σε P2P συστήματα e-commerce. Στο συγκεκριμένο μοντέλο η Εμπιστοσύνη υπολογίζεται λαμβάνοντας υπ' όψη τους εξής σημαντικούς παράγοντες:

1. Αξιολογήσεις από τρίτους,
2. Αριθμός συναλλαγών,
3. Αξιοπιστία αξιολόγησης,
4. Είδος συναλλαγής,
5. Κοινωνικοί παράγοντες (community context).

Με βάση τους παράγοντες αυτούς, έστω $I(Y,X)$ ο συνολικός αριθμός συναλλαγών που έχουν πραγματοποιηθεί μεταξύ του παρόχου Y και του πελάτη X, $I(Y)$ ο συνολικός αριθμός συναλλαγών που έχει πραγματοποιήσει ο Y με οποιονδήποτε κόμβο, $p(Y,i)$ ο κόμβος με τον οποίο ο Y πραγματοποίησε την i-οστή συναλλαγή, $S(Y,i)$ η αξιολόγηση που έλαβε ο Y από τον $p(Y,i)$ για τη συγκεκριμένη συναλλαγή. Η $Cr(u)$ δηλώνει την αξιοπιστία της αξιολόγησης του κόμβου u, η $TF(Y,i)$ είναι ο συντελεστής είδους συναλλαγής για την i-οστή συναλλαγή του Y και η $CF(Y)$ είναι ο συντελεστής κοινωνικού παράγοντα του Y. Έτσι, η Εμπιστοσύνη για έναν κόμβο Y δίνεται από τον τύπο:

$$T(Y) = a \cdot \sum_{i=1}^{I(Y)} S(Y,i) \cdot Cr\big(p(Y,i)\big) \cdot TF(Y,i) + \beta \cdot CF(Y)$$

όπου α, β οι συντελεστές για τη συλλογική αξιολόγηση και για τους κοινωνικούς παράγοντες, οι οποίοι λαμβάνουν τιμές ανάλογα με τις ανάγκες και τα χαρακτηριστικά του συστήματος.

Η Εμπιστοσύνη, λοιπόν, αποτελείται από δύο μέρη. Το πρώτο και κύριο μέρος είναι ένας μέσος όρος σταθμισμένος ανάλογα με την αξιοπιστία των αξιολογήσεων που λαμβάνονται και το είδος των συναλλαγών στις οποίες αναφέρονται οι αξιολογήσεις αυτές. Το δεύτερο μέρος μπορεί να συμβάλει θετικά ή αρνητικά στην Εμπιστοσύνη ανάλογα με τα κοινωνικά χαρακτηριστικά του χρήστη. Για παράδειγμα, εάν ο χρήστης αυτός άνηκε στους αρχικούς κόμβους του δικτύου και είχε εγκατασταθεί από τους δημιουργούς του, οι πιθανότητες να είναι κακόβουλος είναι μηδαμινές, επομένως η τιμή CF θα είναι υψηλή.

4.3.2 Υπολογισμός Αξιοπιστίας Αξιολογήσεων

Μία πιο απλοποιημένη μορφή του υπολογισμού της Εμπιστοσύνης προκύπτει αν αγνοηθεί ο συντελεστής είδους συναλλαγής (δηλαδή αν τεθεί $TF(u,i)=1$), και ο κοινωνικός συντελεστής (δηλαδή αν τεθεί $\beta=0$). Σε αυτήν την περίπτωση, προκύπτει

$$T(Y)=\sum_{i=1}^{I(Y)} S(Y,i)\cdot Cr(p(Y,i))$$

Η Ικανοποίηση $S(Y,i)$ είναι μία ποσότητα η οποία μπορεί να αναπαρασταθεί σε μία κλίμακα από 0 έως 1 και να υπολογιστεί εύκολα με βάση τη ληφθείσα αξιολόγηση. Εγείρεται όμως το ζήτημα του υπολογισμού της αξιοπιστίας της αξιολόγησης ενός χρήστη, δηλαδή της ποσότητας $Cr(u)$.

Μία αρχική προσέγγιση θα ήταν η τιμή της αξιοπιστίας της αξιολόγησης ενός χρήστη να είναι ίση με την τιμή της Εμπιστοσύνης του, δηλαδή $Cr(u)=T(u)$. Η σύμβαση αυτή βασίζεται στις ακόλουθες υποθέσεις. Αρχικά, στο ότι οι χρήστες που επιδεικνύουν αναξιόπιστη συμπεριφορά στις συναλλαγές τους είναι σύνηθες να παρέχουν και αναξιόπιστες αξιολογήσεις. Κατά δεύτερον, στο ότι οι χρήστες που επιδεικνύουν αξιόπιστη συμπεριφορά στις συναλλαγές τους παρέχουν και αξιόπιστες αξιολογήσεις. Ενώ η πρώτη υπόθεση είναι γενικά ορθή, η δεύτερη μπορεί να μην ισχύει πάντα. Για παράδειγμα, μπορεί κάποιος χρήστης να διατηρεί υψηλή τη Φήμη του επιδεικνύοντας σωστή συμπεριφορά στις συναλλαγές του και στη συνέχεια να διαδίδει λανθασμένες αξιολογήσεις για να μειώσει τη φήμη άλλων χρηστών.

Ως αποτέλεσμα, χρησιμοποιείται μία διαφορετική μέθοδος υπολογισμού της, η οποία είναι η ομοιότητα του χρήστη που ζητάει την αξιολόγηση με εκείνον που την παρέχει. Αν $IS(X)$ το σύνολο των χρηστών που έχουν πραγματοποιήσει συναλλαγές με τον χρήστη X, τότε το σύνολο των χρηστών που έχουν πραγματοποιήσει συναλλαγές τόσο με τον X όσο και με έναν άλλο χρήστη w είναι το σύνολο $IJS(X,w)=IS(X)\cap IS(w)$. Για να υπολογίσει ο Χ την αξιοπιστία της αξιολόγησης του w, λαμβάνει υπ' όψη την ομοιότητα των αξιολογήσεων των χρηστών στο $IJS(X,w)$ τόσο ως προς τον ίδιο όσο και ως προς τον w. Συγκεκριμένα, χρησιμοποιεί την τυπική απόκλιση των δύο διανυσμάτων που προκύπτουν για να υπολογίσει την ομοιότητά του με τον w, δηλαδή:

$$Sim(x,w)=1-\sqrt{\frac{\sum_{u\in IJS(X,w)}\left(\frac{\sum_{i=1}^{I(u,X)}S(u,i)}{I(u,X)}-\frac{\sum_{i=1}^{I(u,w)}S(u,i)}{I(u,w)}\right)^2}{|IJS(X,w)|}}$$

και η συνολική Εμπιστοσύνη υπολογίζεται ως:

$$T(X,Y) = \sum_{i=1}^{I(Y)} S(Y,i) \cdot \frac{Sim(p(Y,i),X)}{\sum_{i=1}^{I(Y)} Sim(p(Y,i),X)}$$

4.4 Μοντέλο TRAVOS

4.4.1 Εισαγωγή και Γενικές Ιδέες

Το μοντέλο TRAVOS [13] προσεγγίζει το πρόβλημα του υπολογισμού της Εμπιστοσύνης μοντελοποιώντας την χρησιμοποιώντας την κατανομή β [14]. Συγκεκριμένα, με βάση τις προηγούμενες συναλλαγές ενός χρήστη X με έναν πάροχο Y, θέτονται οι τιμές $\boldsymbol{a}, \boldsymbol{b}$ της κατανομής β ως εξής:

- $\boldsymbol{a}$: Το πλήθος των συναλλαγών οι οποίες ήταν ικανοποιητικές για τον χρήστη X.
- $\boldsymbol{b}$**:** Το πλήθος των συναλλαγών οι οποίες δεν ήταν ικανοποιητικές για τον χρήστη X.

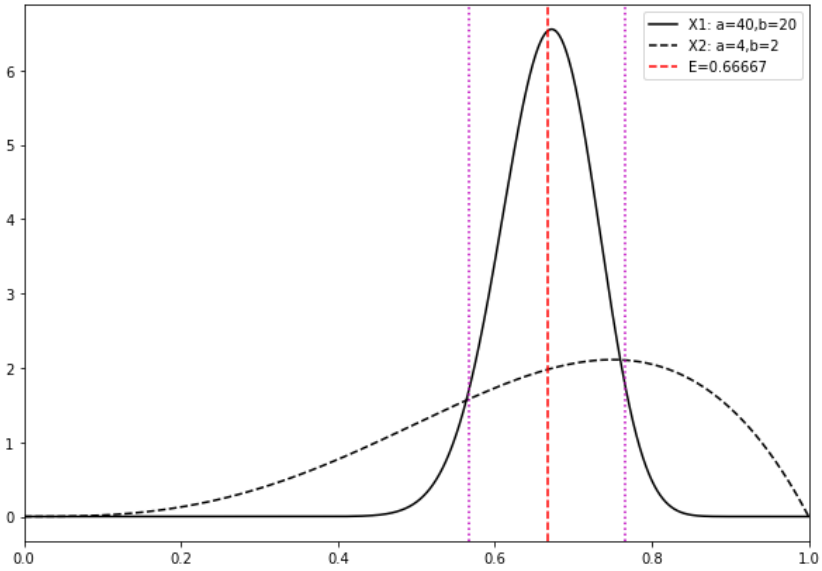
Με βάση τις τιμές αυτές μπορεί να οριστεί μία κατανομή β, της οποίας η μέση τιμή ορίζεται ως

$$E = \frac{a}{a+b}$$

Αυτή είναι και η τιμή της Εμπιστοσύνης $\boldsymbol{T_{XY}}$ του X προς τον Y.

Εκτός από την Εμπιστοσύνη $\boldsymbol{T_{XY}} = E = \frac{a}{a+b}$, ορίζεται και η αυτοπεποίθηση $\boldsymbol{\gamma}$, η οποία αντιπροσωπεύει το κατά πόσο ο υπολογισμός της $\boldsymbol{T_{XY}}$ είναι αξιόπιστος. Για τον υπολογισμό της αυτοπεποίθησης $\boldsymbol{\gamma}$, το μοντέλο εμμέσως λαμβάνει υπ' όψη το πλήθος των συναλλαγών του χρήστη με τον πάροχο. Συγκεκριμένα, επειδή όσο μεγαλύτερες τιμές λαμβάνουν οι παράμετροι $\boldsymbol{a}, \boldsymbol{b}$, τόσο περισσότερο «συγκεντρώνεται» η κατανομή β γύρω από τη μέση τιμή της, η τιμή της αυτοπεποίθησης $\boldsymbol{\gamma}$ υπολογίζεται ως το ολοκλήρωμα της κατανομής β γύρω από τη μέση τιμή της σε διάστημα $\pm\boldsymbol{\varepsilon}$, όπου $\boldsymbol{\varepsilon}$ ορίζεται ως το μέγιστο αποδεκτό σφάλμα. Δηλαδή

$$\boldsymbol{\gamma} = \int_{\boldsymbol{T_{X,Y}-\varepsilon}}^{\boldsymbol{T_{X,Y}+\varepsilon}} \boldsymbol{X^{\alpha-1}(1-X)^{b-1}dX}$$



Εικόνα 3: Σύγκριση αυτοπεποίθησης γ για δύο διαφορετικές κατανομές β

Έστω, για παράδειγμα, οι χρήστες X_1 και X_2 οι οποίοι υπολογίζουν την τιμή Εμπιστοσύνης για τον κόμβο Y. Ο X_1 είχε 40 επιτυχημένες και 20 αποτυχημένες συναλλαγές με τον Y, ενώ ο X_2 είχε 4 επιτυχημένες και 2 αποτυημένες συναλλαγές με τον Y. Έτσι, η εμπιστοσύνη του καθενός μοντελοποιείται από τις κατανομές β που φαίνονται στην Εικόνα 3. Έστω επίσης πως θέτουμε αποδεκτό σφάλμα $\varepsilon = 0.1$. Παρατηρούμε πως και στις δύο περιπτώσεις η Εμπιστοσύνη που υπολογίζουν οι X_1 και X_2 είναι ίση με $T_{X_1,Y} = T_{X_2Y} = 0.66667$ καθώς οι δύο κατανομές β έχουν ίδια μέση τιμή. Ωστόσο, η αυτοπεποίθηση γ_1 του X_1 είναι μεγαλύτερη από την αυτοπεποίθηση γ_2 του X_2 αφού μεγαλύτερο μέρος της κατανομής β του X_1 βρίσκεται εντός του διαστήματος $(E - \varepsilon, E + \varepsilon)$, το οποίο βρίσκεται εντός των μωβ διακεκομμένων γραμμών.

4.4.1.1 Συστάσεις από γειτονικούς κόμβους

Για τον υπολογισμό της εμπιστοσύνης ως προς έναν πάροχο Y, ένας χρήστης X εκτός από τις συναλλαγές που ο ίδιος έχει πραγματοποιήσει μέχρι στιγμής, μπορεί να ζητήσει πληροφορίες και από γειτονικούς του κόμβους, έτσι ώστε να ενισχύσει την αυτοπεποίθησή του. Συγκεκριμένα, αν με βάση τις προσωπικές του εμπειρίες, η αυτοπεποίθηση $\boldsymbol{\gamma}$ είναι μικρότερη από ένα κατώφλι $\boldsymbol{\theta_\gamma}$, τότε αναζητά επιπλέον πληροφορίες από τρίτους. Έτσι, η νέα τιμή της Εμπιστοσύνης για τον Y υπολογίζεται ως

$T_{XY}{}' = E' = \frac{a+a'}{a+a'+b+b'}$ όπου:

- $\boldsymbol{\alpha'}$: Το πλήθος των ικανοποιητικών συναλλαγών από τους κόμβους στους οποίους ζητήθηκε η πληροφορία.
- $\boldsymbol{b'}$: Το πλήθος των μη-ικανοποιητικών συναλλαγών από τους κόμβους στους οποίους ζητήθηκε η πληροφορία.

Με βάση το προηγούμενο παράδειγμα, ο X_1 όντας πιο βέβαιος για την αξιοπιστία της Εμπιστοσύνης που έχει υπολογίσει, ενδεχομένως να μη αναζητήσει επιπλέον πληροφορίες από τρίτους, ενώ ο X_2 είναι αρκετά αβέβαιος και πιθανότατα θα πρέπει να καταφύγει στην αναζήτηση επιπλέον πληροφοριών για τον Y από άλλους χρήστες, ανάλογα με το κατώφλι $\boldsymbol{\theta_\gamma}$ που έχει οριστεί.

4.4.2 Διαχείριση κακόβουλων κόμβων και ανακριβών αξιολογήσεων

Η προσέγγιση του μοντέλου TRAVOS έχει ως στόχο η τελική τιμή της Εμπιστοσύνης που υπολογίζεται από έναν χρήστη, δοσμένων και των επιπλέον παρατηρήσεων που έχει λάβει από τρίτους, να είναι η ίδια με την τιμή που θα προέκυπτε στην περίπτωση που όλες οι παρατηρήσεις είχαν πραγματοποιηθεί από τον ίδιο. Αυτό, ωστόσο, προϋποθέτει την αληθή αναφορά παρατηρήσεων από όλους τους κόμβους.

Κάτι τέτοιο δεν είναι αναμενόμενο σε πραγματικές συνθήκες, όπου διάφοροι χρήστες δρουν για προσωπικό τους όφελος, παρέχοντας ψευδείς παρατηρήσεις σε άλλους χρήστες. Για τους παραπάνω λόγους, το TRAVOS υιοθετεί έναν μηχανισμό ο οποίος φιλτράρει τις ψευδείς παρατηρήσεις τρίτων μειώνοντας τον αντίκτυπο που έχουν στη διαμόρφωση της ολικής Εμπιστοσύνης που διαμορφώνεται τελικά.

Συγκεκριμένα, κάθε χρήστης διατηρεί ιστορικό για κάθε άλλο χρήστη ο οποίος του παρείχε πληροφορίες/παρατηρήσεις και αποθηκεύει, έπειτα από την ολοκλήρωση της εκάστοτε συναλλαγής, κατά πόσο οι πληροφορίες που έλαβε ήταν έγκυρες ή όχι. Αυτό επιτυγχάνεται αρχικά διαχωρίζοντας το διάστημα $[0,1]$ σε $\boldsymbol{N}$ υποδιαστήματα (bins). Ανάλογα με τις πληροφορίες που λαμβάνονται από έναν τρίτο χρήστη, οι οποίες είναι της μορφής (a_k, b_k), ορίζεται μία κατανομή β με μέση τιμή E_k. Η μέση τιμή αυτή βρίσκεται σε κάποιο από τα $\boldsymbol{N}$ διαστήματα που ορίστηκαν προηγουμένως. Για κάθε υποδιάστημα τίθενται δύο τιμές $\boldsymbol{m}, \boldsymbol{n}$ οι οποίες αντιπροσωπεύουν το πλήθος των συναλλαγών που ήταν αποτυχημένες και επιτυχημένες αντίστοιχα. Έπειτα από την ολοκλήρωση της συναλλαγής με τον πάροχο για τον οποίο ζητήθηκαν οι πληροφορίες, γίνεται αποτίμηση του αποτελέσματος και αυξάνεται κατά 1 η τιμή του $\boldsymbol{m}$ ή του $\boldsymbol{n}$ του αντίστοιχου bin ανάλογα με το αποτέλεσμα. Για παράδειγμα, αν $N = 5$ και ένας χρήστης X_1 λάβει πληροφορίες από έναν χρήστη X_2 για έναν πάροχο Y, από τις οποίες προκύψει Εμπιστοσύνη $T_{X_2Y} = 0.15$, τότε το αποτέλεσμα της συναλλαγής θα αποθηκευτεί στο διάστημα $0 < T_{X_2Y} <= 0.2$. Με βάση τις τιμές m_i, n_i του bin_i μπορεί επίσης να οριστεί μία κατανομή β D_i. Με βάση αυτήν την κατανομή D_i υπολογίζεται η ποσότητα ρ_{X_2Y} η οποία αντιπροσωπεύει την ακρίβεια των πληροφοριών του X_2 για τον Y. Για τον υπολογισμό του ρ_{X_2Y}, ολοκληρώνουμε την κατανομή D_i στο διάστημα του bin_i, δηλαδή:

$$\rho_{X_2Y} = \int_{\min(bin_i)}^{\max(bin_i)} X^{n_i-1}(1-X)^{m_i-1}dX$$

Έτσι, όσο περισσότερο μέρος της κατανομής D_i βρίσκεται στο διάστημα του bin_i, τόσο υψηλότερη τιμή λαμβάνει το ρ_{X_2Y}. Με βάση το ρ_{X_2Y} υπολογίζονται οι νέες σταθμισμένες ποσότητες

$$\bar{E} = E_{uniform} + \rho_{X_2Y} \cdot \left(E - E_{uniform}\right)$$

$$\bar{\sigma} = \sigma_{uniform} + \rho_{X_2Y} \cdot \left(\sigma - \sigma_{uniform}\right)$$

$$\bar{a} = \frac{\bar{E}^2 - \bar{E}^3}{\bar{\sigma}^2} - \bar{E}$$

$$\bar{b} = \frac{(1-\bar{E})^2 - (1-\bar{E})^3}{\bar{\sigma}^2} - (1-\bar{E})$$

$$\bar{m}_{X_2Y} = \bar{a} - 1, \bar{n}_{X_2Y} = \bar{b} - 1$$

Όπου $E_{uniform}$, $\sigma_{uniform}$ η μέση τιμή και η τυπική απόκλιση της κατανομής β με $a = b = 1$.

Έτσι, η νέα τιμή Εμπιστοσύνης έπειτα και από τη στάθμιση των λαμβανόμενων πληροφοριών υπολογίζεται ως η μέση τιμή της κατανομής β που προκύπτει με τιμές a, b τα αθροίσματα των $\bar{m}_{X_iY}$ και $\bar{n}_{X_iY}$ αντίστοιχα.

4.5 Μοντέλο RDTM

4.5.1 Εισαγωγή και Γενικές Ιδέες

Το μοντέλο RDTM (Reputation-based Dynamic Trust Model) [15] σχεδιάστηκε για συστήματα ηλεκτρονικών συναλλαγών. Πρόκειται για ένα καθαρά υπολογιστικό μοντέλο στο οποίο η λήψη πληροφοριών γίνεται μέσω ορισμένων υπέρ-κόμβων (supernodes). Πρόκειται είτε για κόμβους εγκατεστημένους εξ αρχής στο σύστημα, οι οποίοι θεωρούνται εξ' ορισμού έμπιστοι, είτε για κόμβους που επιδεικνύουν σωστή συμπεριφορά και υψηλές επιδόσεις κατά τη διάρκεια λειτουργίας τους στο σύστημα. Στους κόμβους αυτούς αναφέρονται τα αποτελέσματα κάθε συναλλαγής μετά την ολοκλήρωσή της από τους απλούς κόμβους του συστήματος και είναι υπεύθυνοι για τη διατήρηση και τη διαμοίραση της πληροφορίας αυτής.

Το μοντέλο αυτό λαμβάνει ποικίλους παράγοντες στον υπολογισμό της Εμπιστοσύνης. Τέτοιοι παράγοντες είναι τα χρονικά διαστήματα στα οποία έγιναν οι συναλλαγές, το κόστος της εκάστοτε συναλλαγής, η ομοιότητα των χρηστών ανάλογα με τη συμπεριφορά τους, καθώς και η αυτοπεποίθηση ενός κόμβου για την προσωπική του Εμπιστοσύνη.

4.5.2 Υπολογισμός Ιδιωτικής Εμπιστοσύνης (Private Trust – PTR)

Η Ιδιωτική Εμπιστοσύνη $PTR_{X,Y}$ αντιπροσωπεύει τον βαθμό εμπιστοσύνης ενός κόμβου X προς έναν κόμβο Y με βάση τις προσωπικές του εμπειρίες από προηγούμενες συναλλαγές με αυτόν. Εάν $\boldsymbol{t_0}$ είναι η στιγμή που ο X έγινε μέλος του δικτύου, και τα $\boldsymbol{t_k}, \boldsymbol{m_k}, \boldsymbol{U_k}$ $(\boldsymbol{0 \leq U_k \leq 1})$ αντιπροσωπεύουν τη χρονική στιγμή, το ποσό και την αποτίμηση της συναλλαγής αντίστοιχα, τότε για μία χρονική στιγμή $\boldsymbol{t_n}$, η Ιδιωτική Εμπιστοσύνη του X ως προς τον Y ορίζεται ως:

$$PTR_{XY}(t_n) = \begin{cases} C_n \sum_{k=1}^{n} \varphi_k U_k \,, \alpha\nu\ \upsilon\pi\acute{\alpha}\rho\chi\epsilon\iota\ \iota\sigma\tau o\rho\iota\kappa\acute{o}\ \sigma\upsilon\nu\alpha\lambda\lambda\alpha\gamma\acute{\omega}\nu \\ 0.5, \alpha\nu\ \delta\epsilon\nu\ \upsilon\pi\acute{\alpha}\rho\chi\epsilon\iota\ \iota\sigma\tau o\rho\iota\kappa\acute{o}\ \sigma\upsilon\nu\alpha\lambda\lambda\alpha\gamma\acute{\omega}\nu \end{cases}$$

όπου:

i) $\boldsymbol{\varphi_k}$ είναι ο συντελεστής της αποτίμησης $\boldsymbol{U_k}$, ο οποίος υπολογίζεται ως εξής:

$$\varphi_k = \frac{(t_k - t_0)m_k}{\sum_{k=1}^{n}(t_k - t_0)m_k}$$

Πρόκειται για έναν συντελεστή βάρους, ο οποίος όσο πιο πρόσφατη ήταν η εκάστοτε συναλλαγή και όσο μεγαλύτερο ήταν το κόστος της συναλλαγής, τόσο μεγαλύτερη τιμή λαμβάνει.

ii) $\boldsymbol{C_n}$ είναι μία συνάρτηση ελέγχου, η οποία σκοπό έχει να εμποδίσει κακόβουλους κόμβους από το να αποκτήσουν υψηλή Εμπιστοσύνη με το να συμπεριφέρονται ορθά σε συναλλαγές χαμηλού κόστους (με σκοπό να εξαπατήσουν στη συνέχεια σε μία συναλλαγή υψηλού κόστους για δικό τους όφελος). Ορίζεται ως:

$$C_n = e^{-\frac{1}{\sum m_k}}$$

Παρατηρούμε πως όσο μεγαλύτερο είναι το κόστος όλων των συναλλαγών, τόσο το C_n συγκλίνει προς το 1, ενώ όσο μικρότερο είναι, τόσο συγκλίνει προς το 0.

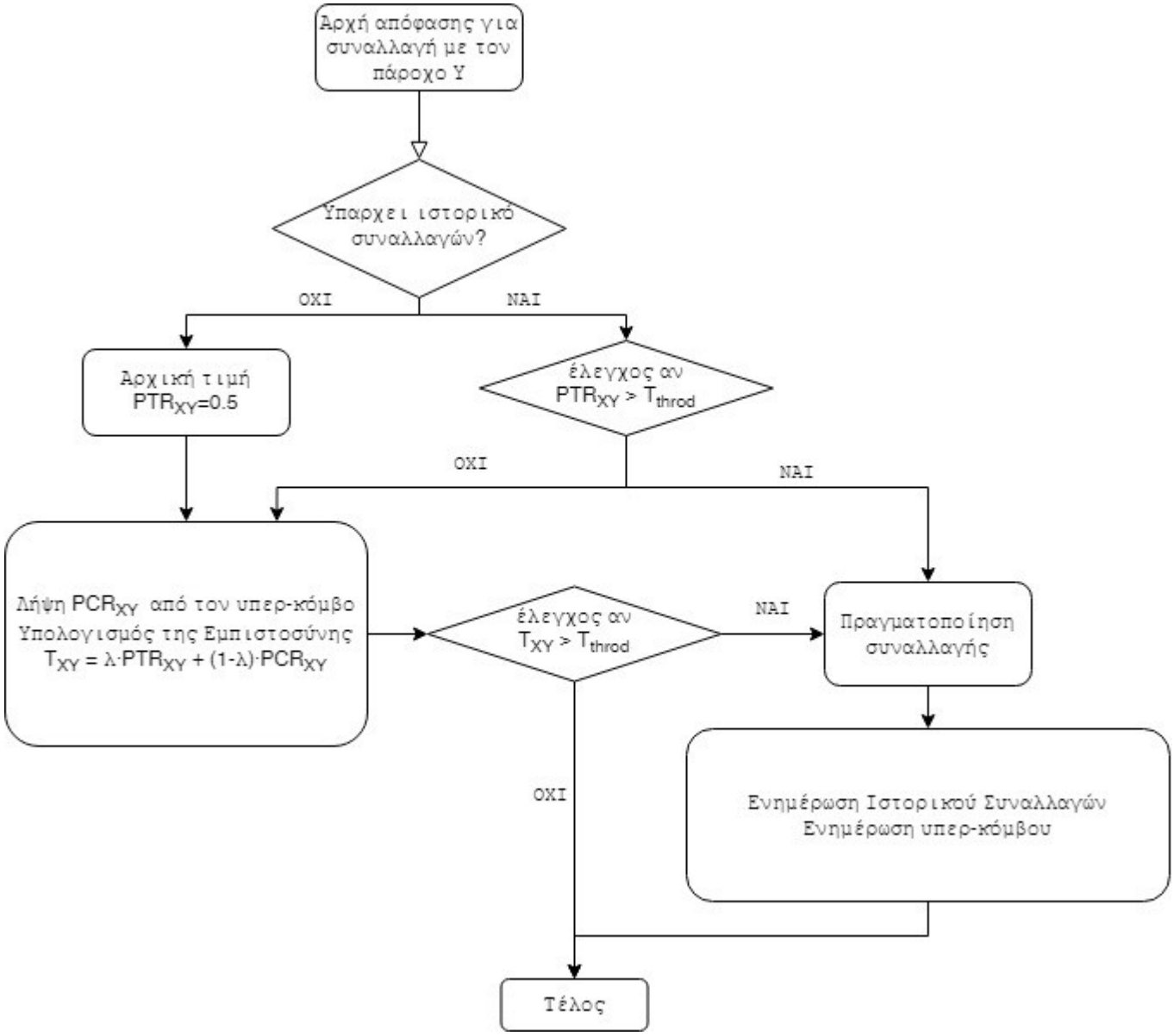
4.5.3 Δημόσια Φήμη (Public Cognitive Reputation – PCR)

Έπειτα από τον υπολογισμό της Ιδιωτικής Εμπιστοσύνης $\boldsymbol{PTR_{XY}}$, ο κόμβος X χρειάζεται να αποφανθεί αν οι πληροφορίες που έχει είναι αρκετά αντιπροσωπευτικές έτσι ώστε να αποφασίσει μόνος του αν θα προβεί ή όχι σε συναλλαγή με τον πάροχο Y. Αυτό καθορίζεται με τον δείκτη αυτοπεποίθησης $\boldsymbol{\lambda}$:

$$\lambda = \begin{cases} \sin\left(\frac{\pi n_{XY} s_{XY}}{2\, N_{min} S_{min}}\right), n_{XY} \in [0, N_{min}] \cap s_{XY} \in [0, S_{min}] \\ 1, \alpha\lambda\lambda\iota\acute{\omega}\varsigma \end{cases}$$

Όπου $\boldsymbol{n_{XY}, s_{XY}}$ ο συνολικός αριθμός συναλλαγών και το συνολικό ποσό όλων των συναλλαγών μεταξύ των X, Y αντίστοιχα και $\boldsymbol{N_{min}, S_{min}}$ παράμετροι που καθορίζονται ανάλογα με τις ανάγκες του συστήματος.

Στην περίπτωση που η τιμή του $\boldsymbol{\lambda}$ δεν είναι 1, ή που η τιμή $\boldsymbol{PTR_{XY}}$ είναι χαμηλότερη από ένα κατώτατο όριο $\boldsymbol{T_{throd}}$, ο X θα πρέπει να αναζητήσει επιπλέον πληροφορίες από τον υπέρ-κόμβο με τον οποίο επικοινωνεί.



Εικόνα 4: Διάγραμμα ροής RDTM

Ο υπέρ-κόμβος, έχοντας πληροφορίες από όλους τους κόμβους X_i που έχουν πραγματοποιήσει συναλλαγές με τον Y, επιστρέφει την Δημόσια Φήμη $\boldsymbol{PCR_Y(t)}$, όπου t είναι η χρονική στιγμή την οποία υπολογίζεται η τιμή αυτή:

$$PCR_Y(t) = e^{-\frac{1}{m \cdot S_b}} \sum_{k=1}^{m} \mu_k \cdot PTR_{X_k Y}(t)$$

Όπου:

i) $\boldsymbol{m, S_b}$ το πλήθος των κόμβων X_i και το συνολικό ποσό των συναλλαγών αντίστοιχα.

ii) $\boldsymbol{\mu_k}$ ο συντελεστής της Εμπιστοσύνης $PTR_{X_i Y}(t)$ του κόμβου X_i ως προς τον κόμβο Y όπως εκείνος την έχει αναφέρει στον υπερ-κόμβο
Υπολογίζεται ως εξής:

$$\mu_k = \frac{sim(X_k, Y) \cdot AM_{X_k} \cdot S_{X_k Y}}{\sum_{i=1}^{m} sim(X_k, Y) \cdot AM_{X_i} \cdot S_{X_i Y}}$$

όπου:

a) $\boldsymbol{AM_X} = \frac{\sum_{k=1}^{N(AM_X)} 1 - |U_k - E_k|}{|N(AM_X)|}$, αντιπροσωπεύει το κατά πόσο η πληροφορία που προήλθε από τον κόμβο X είναι κακόβουλη ή όχι και αντιστοιχεί στο κατά πόσο η τιμή της πληροφορίας που προήλθε από τον X αποκλίνει από την αναμενόμενη τιμή E_k. Η τιμή αυτή διατηρείται στο ιστορικό των υπέρ-κόμβων για κάθε συναλλαγή.

b) $\boldsymbol{E_k} = \frac{\sum_{X \in U_k} AM_X \cdot U_k}{\sum_{X \in U_k} AM_X}$, αντιπροσωπεύει την αναμενόμενη τιμή της πληροφορίας που προέρχεται από τον κόμβο X με βάση τις προηγούμενες αξιολογήσεις που έχει δώσει. Αν δεν υπάρχει ιστορικό για τον συγκεκριμένο κόμβο, λαμβάνει τιμή 0.5.

c) $\boldsymbol{sim(X, Y)}$ η ομοιότητα των κόμβων X, Y. Έστω ότι $\beta_Y = (\beta_1, \beta_2, \dots, \beta_n)$, ο αριθμός της κάθε μίας από τις n υπηρεσίες που προσφέρονται στο σύστημα, που έχει προσφέρει ο Y, και $a_X = (a_1, a_2, \dots, a_n)$, ο αριθμός κάθε μίας από τις n υπηρεσίες που έχει λάβει ο X. Η ομοιότητα μεταξύ των X, Y ορίζεται ως η ομοιότητα συνημίτονου των διανυσμάτων a_X, β_Y:

$$sim(X, Y) = \frac{\beta_Y \cdot a_X}{|\beta_Y| \cdot |a_X|}$$

4.5.4 Συνολική Εμπιστοσύνη

Με βάση τις τιμές PCR_{XY} και PTR_Y, καθώς και της τιμής λ, η συνολική Εμπιστοσύνη ενός κόμβου X ως προς έναν κόμβο Y δίνεται από τον τύπο:

$$T_{XY} = [\lambda \quad 1-\lambda] \begin{bmatrix} PTR_{XY} \\ PCR_Y \end{bmatrix}$$

Με άλλα λόγια, όσο πιο κοντά είναι η τιμή της βεβαιότητας λ στο 1, τόσο περισσότερο βάρος έχει η προσωπική Εμπιστοσύνη του X προς τον Y, ενώ όσο πιο χαμηλή είναι η τιμή του λ, τόσο περισσότερο λαμβάνεται υπ' όψη η Δημόσια Φήμη του Y.

4.6 Μοντέλο TRM-SIoT

4.6.1 Εισαγωγή και Γενικές Ιδέες

Το TRM-SIoT [16] είναι ένα μοντέλο το οποίο προτάθηκε για εφαρμογή σε συστήματα στο Διαδίκτυο των Πραγμάτων (Internet of Things – IoT). Το μοντέλο αυτό αξιοποιεί τα χαρακτηριστικά των κοινωνικών δικτύων και της γενικότερης ιδέας του Social Internet of Things [17] ώστε να περιγράψει τις σχέσεις μεταξύ των κόμβων του δικτύου.

Έτσι, οι κόμβοι του δικτύου δημιουργούν μεταξύ τους σχέσεις Follower-Followee ανάλογα με τα αποτελέσματα των μεταξύ τους δοσοληψιών. Συγκεκριμένα, οι Followers ενός κόμβου είναι οι κόμβοι εκείνοι στους οποίους έχει προσφέρει κάποια υπηρεσία, ενώ Followees είναι οι κόμβοι από τους οποίους λαμβάνει υπηρεσίες.

Επειδή στα συστήματα IoT οι κόμβοι έχουν περιορισμένη υπολογιστική ισχύ και μνήμη, κάθε κόμβος διατηρεί το δικό του πρόσφατο ιστορικό, ενώ υπάρχει και μία κεντρική βάση δεδομένων η οποία ενημερώνεται ανά τακτά χρονικά διαστήματα και διατηρεί ολόκληρο το ιστορικό του συστήματος.

4.6.2 Εμπιστοσύνη

Η Εμπιστοσύνη θεωρείται αυστηρά υποκειμενική έννοια στο συγκεκριμένο μοντέλο και υπολογίζεται χρησιμοποιώντας το ιστορικό που διατηρεί στη μνήμη του ο κάθε κόμβος. Συγκεκριμένα, κάθε κόμβος διατηρεί αρχεία εγγραφών, κάθε ένα από τα οποία αντιστοιχεί σε μία υπηρεσία την οποία έλαβε. Για να επιτευχθεί όσο το δυνατόν μεγαλύτερη αποτελεσματικότητα, η Εμπιστοσύνη στο συγκεκριμένο μοντέλο χωρίζεται σε διαφορετικά επίπεδα.

Αρχικά, για να περιοριστούν συμπεριφορές κόμβων οι οποίοι για ορισμένα είδη υπηρεσιών επιδεικνύουν σωστή συμπεριφορά, αλλά για άλλα η συμπεριφορά τους είναι κακόβουλη, η εμπιστοσύνη διαχωρίζεται ανάλογα με το είδος της υπηρεσίας. Έτσι, ένας κόμβος X μπορεί να αποθέτει εμπιστοσύνη $T_{XY,A}$ σε έναν κόμβο Y όσον αφορά την υπηρεσία A, αλλά στον ίδιο κόμβο Y να εναποθέτει εμπιστοσύνη $T_{XY,B} \neq T_{XY,A}$ όσον αφορά την υπηρεσία B.

Άλλος ένας διαχωρισμός που γίνεται στο μοντέλο αυτό είναι μεταξύ της Εμπιστοσύνης για παροχή υπηρεσίας και της Εμπιστοσύνης για παροχή συστάσεων. Ένα κοινό είδος επίθεσης στα P2P και IoT συστήματα είναι κάποιοι κόμβοι να συμπεριφέρονται σωστά όταν παρέχουν υπηρεσίες, αλλά να μην παρέχουν ειλικρινείς αξιολογήσεις. Με αυτόν τον διαχωρισμό, τέτοιες συμπεριφορές είναι ευκολότερο να ανιχνευθούν και να περιοριστούν.

Η τιμή της Εμπιστοσύνης υπολογίζεται χρησιμοποιώντας ορισμένα μεγέθη τα οποία αποθηκεύονται στις εγγραφές ιστορικού έπειτα από κάθε συναλλαγή. Τα μεγέθη αυτά παρουσιάζονται παρακάτω:

- **Ικανοποίηση (s):** Πρόκειται για έναν δείκτη ποιότητας υπηρεσίας. Η τιμή της Ικανοποίησης υπολογίζεται με βάση την ορθότητα της υπηρεσίας που έλαβε ο κόμβος και λαμβάνει υψηλότερη τιμή όσο καλύτερη ήταν και η ποιότητα της υπηρεσίας. Παράγοντες που μπορεί να επηρεάζουν την τιμή της Ικανοποίησης είναι επίσης ο χρόνος ο οποίος χρειάστηκε για να παρασχεθεί η υπηρεσία, το κόστος της υπηρεσίας, καθώς και το αποτέλεσμά της.
- **Συντελεστής Βαρύτητας (w):** Ο Συντελεστής Βαρύτητας αντιπροσωπεύει το πόσο σημαντική είναι η υπηρεσία που έλαβε ο κόμβος. Όσο πιο μείζονος σημασίας είναι για τον κόμβο η υπηρεσία, τόσο μεγαλύτερη τιμή λαμβάνει και ο Συντελεστής Βαρύτητας. Με αυτόν τον τρόπο οι κακόβουλοι χρήστες είναι πιο δύσκολο να αυξήσουν την Εμπιστοσύνη τους σε μεγάλο βαθμό παρέχοντας μικρής σημασίας υπηρεσίες, ενώ αν παρέχουν μία κακής ποιότητας υπηρεσία μεγάλης σημασίας, η Εμπιστοσύνη προς αυτούς θα μειωθεί ραγδαία.
- **Συντελεστής Εξασθένησης (f):** Καθώς πραγματοποιούνται καινούργιες συναλλαγές μεταξύ των κόμβων, οι παλιότερες συναλλαγές θα έπρεπε να λαμβάνονται υπ' όψη σε μικρότερο βαθμό κατά τον υπολογισμό της εμπιστοσύνης. Ο Συντελεστής Εξασθένησης συντελεί σε αυτόν το σκοπό. Οι παλιότερες εγγραφές ιστορικού θα πρέπει να έχουν μικρό Συντελεστή Εξασθένησης, ενώ όσο πιο πρόσφατες είναι, ο Συντελεστής Εξασθένησης πρέπει να αυξάνεται. Με αυτόν τον τρόπο ένας κακόβουλος κόμβος δε μπορεί να εξαπατά συνεχώς βασιζόμενος στην εμπιστοσύνη την οποία έχει χτίσει με την προηγουμένως σωστή συμπεριφορά του. Επιπλέον, η χρήση του Συντελεστή Εξασθένησης βοηθά στην επεκτασιμότητα του συστήματος. Κάθε φορά που μία νέα εγγραφή ιστορικού αποθηκεύεται, ο Συντελεστής Εξασθένησής της λαμβάνει τιμή 1. Ταυτόχρονα, ο Συντελεστής Εξασθένησης όλων των προηγούμενων μειώνεται κατά μία τιμή $f_s < 1$. Οι εγγραφές ιστορικού των οποίων ο Συντελεσής Εξασθένησης μηδενίζεται διαγράφονται και δε λαμβάνονται πλέον υπ' όψη.

Όταν ένας κόμβος επιθυμεί να υπολογίσει την τιμή της Εμπιστοσύνης για έναν άλλο κόμβο, πραγματοποιεί μία αναζήτηση στις εγγραφές ιστορικού που είναι αποθηκευμένες στη μνήμη του και υπολογίζει τον σταθμισμένο μέσο όρο:

$$\mu_t^k = \frac{\sum_{i=1}^{n}(s_i \cdot w_i \cdot f_i)}{W} \quad (4.6.a)$$

Όπου W είναι ο συντελεστής κανονικοποίησης, ο οποίος εξασφαλίζει πως η τιμή αυτή θα βρίσκεται στο διάστημα [0,1]:

$$W = \sum_{i=1}^{n}(w_i \cdot f_i)$$

Ο μέσος όρος είναι μία μετρική που αντικατοπτρίζει τη συμπεριφορά του κόμβου-παρόχου με βάση την εμπειρία του κόμβου-πελάτη και αντιπροσωπεύει την αναμενόμενη συμπεριφορά του στο μέλλον. Χρειάζεται ωστόσο και μία μετρική για τη βεβαιότητα αυτής της πρόβλεψης. Για το λόγο αυτό υπολογίζεται επίσης η τυπική απόκλιση της συμπεριφοράς αυτής:

$$\sigma_t^k = \frac{\sqrt{\sum_{i=1}^{n}(s_i^2 \cdot w_i \cdot f_i) \cdot W - \left(\sum_{i=1}^{n} s_i \cdot w_i \cdot f_i\right)^2}}{W} \quad (4.6.b)$$

και η Εμπιστοσύνη ορίζεται τελικά ως εξής:

$$T^k = \mu_t^k - \sigma_t^k$$

4.6.3 Φήμη

Στο TRM-SIoT, για τον υπολογισμό της Φήμης κάθε κόμβου δεν συμβάλλουν όλοι οι υπόλοιποι κόμβοι του συστήματος. Συγκεκριμένα, ο υπολογισμός αυτός δεν πραγματοποιείται καν σε καθολικό επίπεδο, αλλά σε επίπεδο κόμβου. Με άλλα λόγια, αν δύο κόμβοι X, Y υπολογίσουν μία τιμή Φήμης για έναν κόμβο Z, κατά πάσα πιθανότητα αυτή να διαφέρει μεταξύ τους. Για τον υπολογισμό της Φήμης υποστηρίζονται δύο ανεξάρτητες μεταξύ τους μέθοδοι:

- **Μέθοδος Γειτονιάς:** Πρόκειται για την κύρια μέθοδο υπολογισμού Φήμης, κατά την οποία κάθε κόμβος ζητά πληροφορίες από τον κοινωνικό του περίγυρο (Followees).
- **Μέθοδος Πλατφόρμας:** Η μέθοδος αυτή χρησιμοποιείται όταν ο κοινωνικός περίγυρος του κόμβου δεν καταφέρνει να παρέχει πληροφορίες για έναν τρίτο κόμβο. Σε αυτήν την περίπτωση, η πλατφόρμα, ένας κεντρικός μηχανισμός διαχείρισης της Φήμης, η οποία έχει μία ευρύτερη εικόνα του συστήματος, καλείται να παρέχει αξιολογήσεις.

4.6.3.1 Υπολογισμός Φήμης – Μέθοδος Γειτονιάς

Για τον υπολογισμό της Φήμης ενός κόμβου k, ο κόμβος X ακολουθεί την ακόλουθη διαδικασία:

1. Ο κόμβος X εντοπίζει τους N_F Followees τους οποίους εμπιστεύεται περισσότερο ως παρόχους αξιολογήσεων και τους ζητά την τιμή Εμπιστοσύνης τους για τον κόμβο k. Έπειτα, υπολογίζει τον σταθμισμένο μέσο όρο και την τυπική απόκλιση ως εξής:

$$\mu_r^k = \frac{\sum_{i=1}^{N_F}(T_i^k \cdot T_{rec}^i)}{W'} \quad (4.6.c)$$

$$\sigma_r^k = \frac{\sqrt{\sum_{i=1}^{N_F}((T_i^k)^2 \cdot T_{rec}^i) \cdot W' - \left(\sum_{i=1}^{N_F} T_i^k \cdot T_{rec}^i\right)^2}}{W'} \quad (4.6.d)$$

όπου T_{rec}^i είναι η τιμή της εμπιστοσύνης στον κόμβο i όσον αφορά την παροχή αξιολογήσεων και

$$W' = \sum_{i=1}^{N_F} T_{rec}^i$$

Η αρχική τιμή της Φήμης ορίζεται ως:

$$R^k = \mu_r^k - \sigma_r^k$$

2. Έπειτα από τον αρχικό υπολογισμό της Φήμης, ο κόμβος X ζητάει και από τους υπόλοιπους Followees του την τιμή της Εμπιστοσύνης τους για τον X. Στην προκειμένη περίπτωση δεν λαμβάνονται υπ' όψη όλες οι αξιολογήσεις που λαμβάνονται, αλλά μόνο εκείνες που βρίσκονται στο διάστημα $[\boldsymbol{\mu_r - 0.7\sigma_r, \mu_r + 0.7\sigma_r}]$. Οι τιμές που λαμβάνονται εν τέλει υπ' όψη ενσωματώνονται στις εξισώσεις (4.6.c) και (4.6.d) και έτσι υπολογίζεται η τελική τιμή Φήμης.

4.6.3.2 Υπολογισμός Φήμης – Μέθοδος Πλατφόρμας

Η Πλατφόρμα είναι ένας κεντρικός μηχανισμός διαχείρισης του συστήματος και είναι υπεύθυνη για την παροχή αξιολογήσεων όταν ένας κόμβος δε λάβει αποτελέσματα μέσω της Μεθόδου Γειτονιάς λόγω έλλειψης αξιολογήσεων από τον κοινωνικό του περίγυρο. Η Πλατφόρμα, για να καταφέρει να έχει μία πιο πλήρη εικόνα του συστήματος, πραγματοποιεί αιτήματα σε τυχαίους κόμβους ανά χρονικά διαστήματα. Οι κόμβοι που έλαβαν αίτημα αποστέλλουν σε αυτή μέρος από τις εγγραφές ιστορικού τους.

4.6.4 Πραγματοποίηση Συναλλαγών στο TRM-SIoT

Όταν ένας κόμβος θέλει να λάβει μία υπηρεσία, ο ίδιος γνωρίζει την κρισιμότητα της υπηρεσίας αυτής για εκείνον. Η κρισιμότητα αυτή είναι και το κατώφλι Εμπιστοσύνης που θέτει για τους πιθανούς παρόχους του. Δηλαδή, εάν θέλει να λάβει μία υπηρεσία με κρισιμότητα 80%, θα επιλέξει παρόχους με τιμή Εμπιστοσύνης τουλάχιστον 0.8.

Αλγόριθμος:

Αρχικοποίηση κατωφλίου thr με βάση την κρισιμότητα της υπηρεσίας

$Best = 0$

$Trust_{best} = 0$

Για κάθε followee $i \in Service$**:**

$log\_file = get\_log\_file(Service, i)$

Αν το log_file έχει μέγεθος πάνω από $N_{T_{short}}/2$**:**

$T_{short} = calculate\_trust(i, size(log\_file)/N_{T_{short}})$

Αλλιώς:

$T_{short} = 1.0$

Τέλος Αν

$T_{long} = calculate\_trust(i, size(log\_file))$

$T = min(T_{short}, T_{long})$

Αν $T > Trust_{best}$**:**

$Best = i$

$Trust_{best} = T$

Τέλος Αν

Τέλος Επανάληψης

Αν $Trust_{best} > thr$**:**

Πραγματοποίηση αιτήματος λήψης υπηρεσίας από τον $Best$

Αλλιώς αν η υπηρεσία είναι χαμηλής κρισιμότητας **ΚΑΙ** $math.random() \leq 0.1$**:**

Πραγματοποίηση αιτήματος λήψης υπηρεσίας από έναν κόμβο με μηδενική Εμπιστοσύνη

Τέλος Αν

Αλγόριθμος 6: Διαδικασία πραγματοποίησης συναλλαγής

Μόλις καθοριστεί το κατώφλι εμπιστοσύνης, ο κόμβος υπολογίζει για όλους τους Followees του δύο τιμές Εμπιστοσύνης, την Βραχυχρόνια Εμπιστοσύνη - T_{short} - και τη Μακροχρόνια Εμπιστοσύνη - T_{long} χρησιμοποιώντας τις εξισώσεις (4.1.a) και (4.1.b). Η πρώτη λαμβάνει υπ' όψη μόνο τις $N_{T_{short}}$ πιο πρόσφατες εγγραφές ιστορικού και υπολογίζεται μόνο εάν το σύνολο των εγγραφών ιστορικού είναι μεγαλύτερο από $N_{T_{short}}/2$. Η δεύτερη λαμβάνει υπ' όψη όλες τις εγγραφές και υπολογίζεται πάντα. Η Εμπιστοσύνη σε αυτό το στάδιο προκύπτει ως $T = \min(T_{long}, T_{short})$. Με αυτόν τον τρόπο μπορούν να εντοπιστούν διαφορές στις συμπεριφορές των παρόχων.

Έπειτα από τον υπολογισμό της Εμπιστοσύνης για τους Followees, ο κόμβος αποστέλλει αίτημα σε εκείνον με την υψηλότερη τιμή Εμπιστοσύνης η οποία είναι μεγαλύτερη από το ορισμένο κατώφλι. Εάν η υπηρεσία έχει μικρό συντελεστή κρισιμότητας, ο κόμβος μπορεί να επιλέξει και έναν πάροχο με μικρό ή μηδενικό δείκτη Εμπιστοσύνης.

Έτσι, οι νεοεισαχθέντες κόμβοι μπορούν να ενταχθούν στο σύστημα παρέχοντας υπηρεσίες, ενώ κόμβοι οι οποίοι έχασαν την Εμπιστοσύνη τους λόγω κάποιας εσφαλμένης παροχής υπηρεσίας έχουν την ευκαιρία να επανενταχθούν στο σύστημα. Η διαδικασία αυτή περιγράφεται αναλυτικά στον Αλγόριθμο 6.

Εάν η μέθοδος αυτή δεν οδηγήσει στην εύρεση κάποιου αξιόπιστου παρόχου υπηρεσίας, ο κόμβος μπορεί να καταφύγει είτε στη μέθοδο Γειτονιάς, είτε στη μέθοδο Πλατφόρμας οι οποίες αναλύθηκαν παραπάνω, έτσι ώστε να βρει έναν πάροχο. Σε περίπτωση που το αποτέλεσμα της συναλλαγής από τον πάροχο που προτάθηκε είναι ικανοποιητικό, τότε ο πάροχος προστίθεται στους Followees του κόμβου που έλαβε την υπηρεσία.

Συγκεκριμένα όσον αφορά τη μέθοδο της Πλατφόρμας, επιλέγεται τυχαία ένας από τους $N_{best_{platform}}$ πιο αξιόπιστους κόμβους, ώστε να κατανεμηθεί το φορτίο μεταξύ των πιο αξιόπιστων κόμβων. Ωστόσο, στην περίπτωση που υπάρχουν κόμβοι που αναφέρουν ψευδή στοιχεία στην Πλατφόρμα, ενδέχεται οι $N_{best_{platform}}$ πιο αξιόπιστοι κόμβοι να είναι κακόβουλοι και να έχουν αποκτήσει υψηλή Φήμη μέσω ψευδών αξιολογήσεων από άλλους κακόβουλους κόμβους. Για αυτόν το λόγο, ορίζεται πιθανότητα 80% η Πλατφόρμα να προτείνει έναν από τους $N_{best_{platform}}$ κόμβους και 20% να προτείνει κάποιον με χαμηλότερη Φήμη.

5

Κατηγοριοποίηση Μοντέλων

5.1 Παρουσίαση Μεθοδολογίας Κατηγοριοποίησης

Η [2] παρουσιάζει ένα πλαίσιο ταξινόμησης για μοντέλα Εμπιστοσύνης και Φήμης, το οποίο λαμβάνει υπ' όψη ποικίλα χαρακτηριστικά. Χρησιμοποιώντας το ίδιο πλαίσιο θα γίνει και η ταξινόμηση των μοντέλων που παρουσιάστηκαν στο Κεφάλαιο 4.1. Στη συνέχεια παρουσιάζονται τα χαρακτηριστικά τα οποία λαμβάνει υπ' όψη το συγκεκριμένο πλαίσιο.

5.1.1 Τρόπος Αξιολόγησης (K1)

Α) Αξιολόγηση με ένα κριτήριο: Στον συγκεκριμένο τρόπο αξιολόγησης υπάρχει ένα και μόνο κριτήριο βάσει του οποίου γίνεται η αξιολόγηση (πχ. η γενική απόδοση ενός παρόχου κατά τη συναλλαγή).

Β) Αξιολόγηση με πολλαπλά κριτήρια: Σε αυτόν τον τρόπο αξιολόγησης οι χρήστες αξιολογούν και αξιολογούνται με βάση διάφορα κριτήρια και την επιμέρους απόδοσή τους σε καθένα από αυτά, ανάλογα με το βάρος του κάθε κριτηρίου για την εκάστοτε συναλλαγή (πχ. ποιότητα υπηρεσίας, χρόνος κτλ.).

5.1.2 Μέθοδος Αναζήτησης Αξιολογήσεων (K2)

Α) Κεντρική: Στα συστήματα αυτά όλες οι αξιολογήσεις και οι πληροφορίες για την ποιότητα υπηρεσιών ενός κόμβου αποθηκεύονται σε μία κεντρική βάση δεδομένων. Οι χρήστες αναφέρουν τα αποτελέσματα των συναλλαγών τους στη βάση και ο υπολογισμός της Φήμης του κάθε κόμβου υπολογίζεται εκεί.

Β) Αποκεντρωμένη: Σε αυτά τα συστήματα δεν υπάρχει κάποια κεντρική αποθήκευση της πληροφορίας και όλοι οι κόμβοι διατηρούν ιστορικό των συναλλαγών τους. Επίσης, ο υπολογισμός της Φήμης των κόμβων πραγματοποιείται στους ίδιους τους κόμβους.

Γ) Υβριδική: Η υβριδική μέθοδος συνδυάζει στοιχεία από τις δύο παραπάνω μεθόδους. Συνήθως σε τέτοιου είδους συστήματα υπάρχουν ορισμένοι κόμβοι οι οποίοι είναι υπεύθυνοι για τον υπολογισμό της Φήμης των κόμβων και τον διαμοιρασμό της πληροφορίας αυτής εφόσον τους ζητηθεί.

5.1.3 Μέθοδος Υπολογισμού Φήμης (K3)

Α) Ντετερμινιστική: Με αυτήν τη μέθοδο ο υπολογισμός της Φήμης προκύπτει από κάποιους δοσμένους μαθηματικούς τύπους, στους οποίους εφαρμόζονται τα δεδομένα εισόδου, δηλαδή οι πληροφορίες που διατηρεί ο κόμβος ή/και που λαμβάνει από άλλους κόμβους σε συνδυασμό με προκαθορισμένες παραμέτρους του εκάστοτε συστήματος.

Β) Ασαφές μοντέλο: Χρησιμοποιώντας τη θεωρία των Ασαφών Συστημάτων, οι βασικές παράμετροι ενός μοντέλου μπορούν να εκφραστούν με τη χρήση Ασαφών Συνόλων. Για παράδειγμα, η ποιότητα μίας υπηρεσίας μπορεί να εκφραστεί από το σύνολο [***κακή, μέτρια, καλή***]. Σε συνδυασμό με τις Συναρτήσεις Μέλους, οι οποίες δείχνουν κατά ποιον βαθμό θεωρείται η ποιότητα αυτή κακή, μέτρια ή καλή, και την εφαρμογή Ασαφών Κανόνων, μπορούν να υπολογιστούν η Φήμη και η Εμπιστοσύνη για τους κόμβους του Συστήματος.

Γ) Μπεϋζιανό μοντέλο: Η προσέγγιση αυτή χρησιμοποιεί τη θεωρία πιθανοτήτων για να μοντελοποιήσει τη Φήμη και την Εμπιστοσύνη. Συνήθως χρησιμοποιείται η Συνάρτηση Πυκνότητας Πιθανότητας (PDF) κάποιας κατανομής για την έκφραση και τον υπολογισμό τους, με επικρατέστερη την κατανομή β.

5.1.4 Πηγές Πληροφοριών (K4)

Ένα βασικό χαρακτηριστικό ενός μοντέλου Εμπιστοσύνης και Φήμης είναι από πού λαμβάνονται οι πληροφορίες για τον υπολογισμό της Εμπιστοσύνης προς έναν άλλο κόμβο. Στο συγκεκριμένο πλαίσιο ταξινόμησης διακρίνονται οι ακόλουθες πηγές πληροφοριών:

Α) Προσωπικές εμπειρίες: Πρόκειται για την πιο βασική πηγή πληροφοριών στα συστήματα Εμπιστοσύνης και Φήμης. Προτού ένας κόμβος πραγματοποιήσει μία συναλλαγή με κάποιον πάροχο,

ανατρέχει στο ιστορικό των προηγούμενων συναλλαγών του με εκείνον τον πάροχο ώστε να αποφανθεί εάν είναι αξιόπιστος ή όχι.

Β) Εμπειρίες τρίτων: Σε περίπτωση που δεν υπάρχουν αρκετές προσωπικές εμπειρίες για έναν συγκεκριμένο πάροχο, η επόμενη πιο δημοφιλής μέθοδος είναι η αναζήτηση πληροφοριών από τρίτους. Έτσι, σε αυτήν την περίπτωση ο κόμβος ζητά από τους γείτονές του πληροφορίες για τον πάροχο αυτό και εκείνοι αποκρίνονται ανάλογα με την πληροφορία που έχουν για εκείνον.

Γ) Πιστοποιημένη φήμη: Η συγκεκριμένη μέθοδος αφορά περιπτώσεις κατά τις οποίες ένας κόμβος δεν έχει προσωπικές εμπειρίες, ούτε έχει καταφέρει να βρει πληροφορίες από τρίτους κόμβους. Σε αυτήν την περίπτωση, ο κόμβος από τον οποίο ζητείται η υπηρεσία μπορεί να δώσει πληροφορίες για τις συναλλαγές που έχει πραγματοποιήσει. Ωστόσο, η συγκεκριμένη μέθοδος δεν είναι ιδιαίτερα αξιόπιστη, διότι ο κόμβος αυτός μπορεί είτε να δώσει ψευδείς πληροφορίες, είτε να αποκρύψει τις πληροφορίες που αφορούν συναλλαγές κατά τις οποίες παρείχε κακή υπηρεσία και να εμφανίσει μόνο ικανοποιητικά αποτελέσματα.

Δ) Εμπιστοσύνη ρόλων: Σε ορισμένα συστήματα υπάρχει η δυνατότητα οι κόμβοι να έχουν διαφορετικούς ρόλους ή ταυτότητες, βάσει των οποίων μπορούν να αντληθούν πληροφορίες για την αξιοπιστία τους. Για παράδειγμα, εάν ένας χρήστης είναι πιστοποιημένος από μία καθολικά αξιόπιστη αρχή, τότε οι άλλοι χρήστες είναι πιο πιθανό να τον θεωρήσουν αξιόπιστο και να λάβουν μία υπηρεσία από εκείνον.

5.1.5 Πλαίσιο Συναλλαγής (K5)

Εκτός από την αξιοπιστία των αξιολογήσεων που παρέχονται σε έναν κόμβο, είναι σημαντικό να ελέγχεται και το πλαίσιο στο οποίο πραγματοποιείται μία συναλλαγή. Με άλλα λόγια, να πραγματοποιείται κάποιος έλεγχος πως η αξιολόγηση η οποία λήφθηκε από κάποιον κόμβο για έναν πάροχο Χ αφορά υπηρεσία η οποία παρουσιάζει παρόμοια χαρακτηριστικά με την επιθυμητή. Παρουσιάζονται τα ακόλουθα βασικά κριτήρια για τον παραπάνω έλεγχο:

Α) Ομοιότητα πλαισίου συναλλαγής: Κατά τον υπολογισμό της φήμης των διάφορων παρόχων υπηρεσιών, είναι σημαντικό να ορίζεται και ποιο πλαίσιο αφορά. Έστω ότι ένας χρήστης X επιθυμεί να λάβει μία υπηρεσία S_1.Ο χρήστης αυτός λαμβάνει μία αξιολόγηση από έναν αξιόπιστο χρήστη Y, η οποία όμως αφορά την αξιοπιστία του παρόχου P_1 για την υπηρεσία S_2, η οποία διαφέρει από την S_1. Ο χρήστης X λαμβάνει επίσης και μία αξιολόγηση από έναν λιγότερο αξιόπιστο χρήστη W, η οποία

αφορά τον πάροχο P_2 για την υπηρεσία S_1. Η αξιολόγηση του W θα πρέπει να ληφθεί υπ' όψη με μεγαλύτερη βαρύτητα απ' ότι του Y.

Β) Ομοιότητα επιμέρους κριτηρίων υπηρεσίας: Κατά την πραγματοποίηση μίας συναλλαγής, ένας χρήστης ορίζει τη βαρύτητα των επιμέρους χαρακτηριστικών που αποτελούν την υπηρεσία που επιθυμεί να λάβει (πχ. για την υπηρεσία λήψης δεδομένων, τέτοια χαρακτηριστικά θα μπορούσαν να είναι η ακεραιότητα των δεδομένων και ο χρόνος αποστολής). Κρίνεται σημαντικό, κατά την ερώτηση στους υπόλοιπους κόμβους για να προτείνουν κάποιον πάροχο, να γνωστοποιείται το βάρος που θέτει ο χρήστης στα επιμέρους χαρακτηριστικά της υπηρεσίας.

Έστω οι χρήστες Y, W οι οποίοι έλαβαν τις υπηρεσίες λήψης δεδομένων από τον πάροχο P, καθώς και ο χρήστης X, ο οποίος επιθυμεί να λάβει την υπηρεσία λήψης δεδομένων. Κάθε ένας από τους κόμβους αυτούς θέτει τους δικούς του συντελεστές βάρους για τα κριτήρια 'Ακεραιότητα Δεδομένων' και 'Χρόνος Αποστολής', όπως φαίνεται στους Πίνακες 3-5. Γίνεται αμέσως αντιληπτό πως παρ'όλο που οι χρήστες Y,W έμειναν ικανοποιημένοι σε μεγάλο βαθμό από την υπηρεσία του P, εάν ο X λάμβανε την ακριβώς ίδια υπηρεσία δεν θα έμενε το ίδιο ικανοποιημένος. Συνεπώς, κρίνεται σημαντικό κατά την αποστολή αξιολογήσεων να λαμβάνεται υπ' όψη και η σημασία των επιμέρους χαρακτηριστικών της υπηρεσίας για τον χρήστη που ζητά τις αξιολογήσεις.

Χρήστης *Y*			
Κριτήριο	**Συντελεστής Βαρύτητας (/10)**	**Ποιότητα Υπηρεσίας(/10)**	**Εκτιμώμενη Ποιότητα Υπηρεσίας**
Ακεραιότητα Δεδομένων	9	10	10
Χρόνος Αποστολής	1	3	10
		93	100
		93%	

Πίνακας 2: *Ο χρήστης **Y** έχει βαθμολογήσει τον πάροχο P με 93/100 βάσει της υπηρεσίας που έλαβε και των συντελεστών βαρύτητας που έθεσε.*

Χρήστης W			
Κριτήριο	**Συντελεστής Βαρύτητας (/10)**	**Ποιότητα Υπηρεσίας(/10)**	**Εκτιμώμενη Ποιότητα Υπηρεσίας**
Ακεραιότητα Δεδομένων	8	10	10
Χρόνος Αποστολής	2	3	10
		86	100
		86%	

Πίνακας 3: *Ο χρήστης **W**έχει βαθμολογήσει τον πάροχο P με 86/100 βάσει της ίδιας υπηρεσίας που έλαβε και των δικών του συντελεστών βαρύτητας.*

Χρήστης Χ			
Κριτήριο	**Συντελεστής Βαρύτητας (/10)**	**Ποιότητα Υπηρεσίας(/10)**	**Εκτιμώμενη Ποιότητα Υπηρεσίας**
Ακεραιότητα Δεδομένων	5	10	10
Χρόνος Αποστολής	5	3	10
		65	100
		65%	

Πίνακας 4: *Ο χρήστης* ***Χ*** *θα αξιολογούσε τον πάροχο* ***Ρ*** *με βαθμολογία 65/100 για την ίδια υπηρεσία με τους δικούς του συντελεστές βαρύτητας.*

5.1.6 Προσαρμοστικότητα (Κ6)

Ένα χαρακτηριστικό των συστημάτων στα οποία εφαρμόζονται τα μοντέλα Εμπιστοσύνης και Φήμης είναι η δυναμικότητά τους, δηλαδή το γεγονός ότι μεταβάλλονται συνεχώς. Ένα πολύ σημαντικό χαρακτηριστικό ενός αποδοτικού μοντέλου Εμπιστοσύνης και Φήμης είναι να παρέχει μηχανισμούς συνεχούς αναπροσαρμογής στις μεταβολές αυτές.

Α) Ενσωμάτωση νέων κόμβων: Κατά την είσοδό τους στο σύστημα οι νέοι κόμβοι δυσκολεύονται να συνάψουν σχέσεις με άλλους κόμβους ως πάροχοι υπηρεσιών. Αυτό συμβαίνει διότι δεν υπάρχει προηγούμενο ιστορικό για τους νεοεισελθέντες κόμβους, με αποτέλεσμα να επιλέγονται ως πάροχοι κόμβοι οι οποίοι έχουν ήδη υψηλή Φήμη. Είναι επομένως αναγκαία η ύπαρξη ενός μηχανισμού ενσωμάτωσης των νεοεισελθέντων κόμβων ώστε να αποφευχθεί ο αποκλεισμός τους από το σύστημα.

Β) Προσαρμογή στις αλλαγές του συστήματος: Σε ένα δυναμικό περιβάλλον είναι αδύνατο να προβλεφθούν επιτυχώς οι διάφορες αλλαγές στο σύστημα. Ωστόσο, κρίνεται σημαντικό να υπάρχει ένας μηχανισμός αναπροσαρμογής στις αλλαγές αυτές, όπως για παράδειγμα σε πιθανές αλλαγές συμπεριφοράς των κόμβων.

5.1.7 Αξιοπιστία και Ειλικρίνεια(Κ7)

Σε αυτό το κομμάτι εξετάζονται ορισμένοι παράγοντες που κρίνονται απαραίτητοι για την ενίσχυση της αξιοπιστίας και της ακρίβειας στον υπολογισμό της τιμής της Εμπιστοσύνης. Συγκεκριμένα, με τη βοήθεια αυτών των παραγόντων καθίσταται δυνατή η ελάττωση της επίδρασης των κακόβουλων παρόχων πληροφοριών και των ψευδών αξιολογήσεων.

Α) Εντοπισμός τάσεων και αστάθειας στη συμπεριφορά παρόχων υπηρεσιών: Κατά τον υπολογισμό της Φήμης ενός παρόχου είναι σημαντικό να λαμβάνεται υπ' όψη η συμπεριφορά του όχι μόνο την παρούσα χρονική στιγμή, αλλά και γενικότερα σε κάποια χρονικά διαστήματα. Με αυτόν τον τρόπο είναι δυνατό να εντοπιστούν κακόβουλες συμπεριφορές. Τέτοιο παράδειγμα είναι η ικανοποιητική υπηρεσία για συναλλαγές στις οποίες ο πάροχος λαμβάνει μικρό όφελος, ενώ αντιθέτως παρέχει χαμηλής ποιότητας υπηρεσία σε κάποια συναλλαγή στην οποία το κέρδος για εκείνον είναι μεγάλο.

Β) Ικανότητα των παρόχων αξιολογήσεων να παρέχουν σωστές αξιολογήσεις: Το κριτήριο αυτό αφορά την ικανότητα ενός κόμβου να έχει την απαραίτητη κριτική ικανότητα ώστε να παρέχει σωστή αξιολόγηση για έναν πάροχο. Για παράδειγμα, ένας κόμβος ο οποίος έχει μικρό αριθμό αλληλεπιδράσεων με έναν πάροχο, ακόμη και αν δεν συμπεριφέρεται κακοβούλως, δεν έχει την ικανότητα να παρέχει μία πραγματικά αξιόπιστη αξιολόγηση για τον πάροχο αυτό.

Γ) Καταπολέμηση κακόβουλων συλλογικοτήτων: Ένα χαρακτηριστικό των συστημάτων στα οποία εφαρμόζονται τα μοντέλα Εμπιστοσύνης και Φήμης είναι πως μπορούν να λάβουν μέρος σε αυτά χρήστες οποιουδήποτε είδους. Ως αποτέλεσμα, δίνεται η δυνατότητα σε ομάδες κακόβουλων χρηστών να δημιουργούν συλλογικότητες, παρέχοντας υψηλές αξιολογήσεις για τα μέλη της συλλογικότητας και χαμηλές για άλλους παρόχους εκτός αυτής. Τα μοντέλα Εμπιστοσύνης και Φήμης πρέπει να αναπτύσσουν μηχανισμούς καταπολέμησης και περιορισμού τέτοιων συλλογικοτήτων.

Δ) Αξιοπιστία των παρόχων αξιολογήσεων: Είναι συχνό φαινόμενο, ορισμένοι χρήστες του συστήματος, ενώ μπορεί να παρέχουν αξιόπιστες υπηρεσίες, να μην παρέχουν αξιόπιστες αξιολογήσεις, κυρίως προσπαθώντας να μειώσουν τους υπόλοιπους παρόχους. Τέτοιες συμπεριφορές πρέπει να εντοπίζονται από τα μοντέλα Εμπιστοσύνης και Φήμης.

Ε) Εντοπισμός διακρίσεων: Επίσης συχνό φαινόμενο αποτελεί ένας κόμβος ή μία ομάδα κόμβων να επιδεικνύουν γενικά αξιόπιστη συμπεριφορά ως προς την πλειοψηφία του συστήματος, αλλά να παρέχουν χαμηλού επιπέδου υπηρεσίες ή αξιολογήσεις προς κάποια συγκεκριμένη ομάδα κόμβων αδικαιολόγητα. Οι συμπεριφορές αυτές είναι καλό να εντοπίζονται από το μοντέλο ώστε να διασφαλίζεται η ακεραιότητα των αξιολογήσεων στο σύστημα.

5.1.8 Επιπλέον Παράγοντες στον Υπολογισμό της Φήμης (K8)

Α) Συντελεστής Μεταβατικότητας: Προκειμένου να υπολογιστεί με ακρίβεια η προσδοκώμενη Εμπιστοσύνη προς έναν συγκεκριμένο πάροχο, είναι απαραίτητο να ταξινομηθούν οι εισερχόμενες συστάσεις από τα διάφορα μέλη. Διακρίνονται, λοιπόν, τρεις κατηγορίες αξιολογήσεων («από πρώτο χέρι», «από δεύτερο χέρι», «από τρίτο χέρι») ανάλογα με τον βαθμό μεταβατικότητας.

Αρχικά, κάθε Σύστημα Εμπιστοσύνης και Φήμης θα πρέπει να επιτρέπει στον χρήστη να θεωρεί πιο αξιόπιστες και με μεγαλύτερη βαρύτητα τις συστάσεις που προέρχονται από γνωστά μέλη, δηλαδή μέλη με τα οποία έχει ήδη αλληλεπιδράσει. Οι συστάσεις αυτές πρέπει λοιπόν να θεωρούνται αξιολόγηση «από πρώτο χέρι» (με βαθμό μεταβατικότητας ένα), η οποία κατ' επέκταση ασκεί σημαντική επιρροή στη λήψη αποφάσεων του εξαρτώμενου χρήστη.

Παρομοίως, όταν ο εξαρτώμενος χρήστης θέτει ένα ερώτημα Φήμης σχετικά με έναν συγκεκριμένο πάροχο, ενδέχεται να απαντήσουν πολλοί συμμετέχοντες των οποίων τα επίπεδα εμπιστοσύνης δεν είναι γνωστά στον εξαρτώμενο χρήστη. Σε αυτήν την περίπτωση οι συστάσεις τους θεωρούνται αξιολόγηση «από τρίτο χέρι» (με βαθμό μεταβατικότητας τρία) και ασκούν ελάχιστη επιρροή στην αξιολόγηση της εμπιστοσύνης.

Τέλος, είναι αρκετά πιθανό οι γνωστοί χρήστες να μην έχουν αλληλεπιδράσει οι ίδιοι με τον εν λόγω πάροχο, παρ' όλα αυτά να απαντούν παραθέτοντας μια λίστα από χρήστες που έχουν εμπειρία με τον εν λόγω πάροχο. Οι συστάσεις τους, λοιπόν, σε αυτήν την περίπτωση ασκούν μια μεσαίου επιπέδου επίδραση στον καθορισμό της προσδοκώμενης τιμής της φήμης (ανάλογα με το επίπεδο εμπιστοσύνης των μελών που προτείνουν) και θεωρούνται αξιολόγηση «από δεύτερο χέρι» (με βαθμό μεταβατικότητας δύο).

Αξίζει να αναφερθεί ότι αν ο εξαρτώμενος χρήστης είχε άμεση αλληλεπίδραση με κάποιον πάροχο, αυτή η πληροφορία θεωρείται ως η πιο σημαντική. Συνεπώς, η τιμή της Εμπιστοσύνης που υπολογίζεται με αυτόν τον τρόπο ασκεί ιδιαίτερα σημαντική επιρροή στη φάση λήψεων αποφάσεων, σε σημείο που είναι ικανή ακόμα και να ασκήσει βέτο στην τιμή της φήμης που έχει ληφθεί από άλλες πηγές πληροφοριών.

Β) Χρονικός Παράγοντας: Ο χρόνος είναι ένας σημαντικός παράγοντας που πρέπει να λαμβάνεται υπ' όψη κατά τον υπολογισμό της Φήμης των κόμβων. Θεωρείται καλή πρακτική να δίνεται περισσότερη βαρύτητα σε περισσότερο πρόσφατες αξιολογήσεις – που αφορούν δηλαδή πιο πρόσφατες συναλλαγές – ενώ μικρότερη βαρύτητα σε λιγότερο πρόσφατες. Όσο πιο παλιές είναι οι αξιολογήσεις, τόσο μικρότερη επιρροή ασκούν στον υπολογισμό της Φήμης και της Εμπιστοσύνης.

Ένας από τους λόγους που ο χρονικός παράγοντας έχει τέτοια βαρύτητα είναι οι πιθανές αλλαγές που μπορούν να προκύψουν στη συμπεριφορά ενός παρόχου με την πάροδο του χρόνου. Για παράδειγμα,

αλλαγές στην ιδιοκτησία ή στη διοίκηση ενός παρόχου μπορεί να έχουν ως αποτέλεσμα την εφαρμογή διαφορετικών εσωτερικών πολιτικών ως προς την παροχή υπηρεσιών.

Για τον λόγο αυτό, οι αξιολογήσεις που έχουν πραγματοποιηθεί πριν από ένα καθορισμένο χρονικό διάστημα, δεν θα πρέπει να λαμβάνονται υπ' όψιν.

5.2 Κατηγοριοποίηση

Με βάση τα χαρακτηριστικά του κάθε μοντέλου, καθώς και τους παράγοντες που αναλύθηκαν στην Ενότητα 5.1, παρατίθεται ο Πίνακας 4, στον οποίο πραγματοποιείται κατηγοριοποίηση των μοντέλων που μελετήθηκαν.

		PeerTrust	PowerTrust	EigenTrust	TRAVOS	RDTM	TRM-SioT
Τρόπος Αξιολόγησης (K1)	A	✅	✅	✅	✅		
	B					✅	✅
Μέθοδος Αναζήτησης Αξιολογήσεων (K2)	A						
	B	✅	✅	✅	✅		
	Γ					✅	✅
Μέθοδος Υπολογισμού Φήμης (K3)	A	✅	✅	✅		✅	✅
	B						
	Γ				✅		
Πηγές Πληροφοριών (K4)	A	✅	✅	✅	✅	✅	✅
	B	✅	✅	✅	✅	✅	✅
	Γ	✅					
	Δ	✅					
Πλαίσιο Συναλλαγής (K5)	A					✅	✅
	B					✅	
Προσαρμοστικότητα (K6)	A	✅				✅	✅
	B	✅				✅	✅

Αξιοπιστία και Ειλικρίνεια (K7)	A					✅	✅
	B						
	Γ		✅	✅	✅	✅	✅
	Δ				✅	✅	✅
	E						
Επιπλέον Παράγοντες στον Υπολογισμό της Φήμης (K8)	A	✅	✅	✅	✅	✅	✅
	B					✅	✅

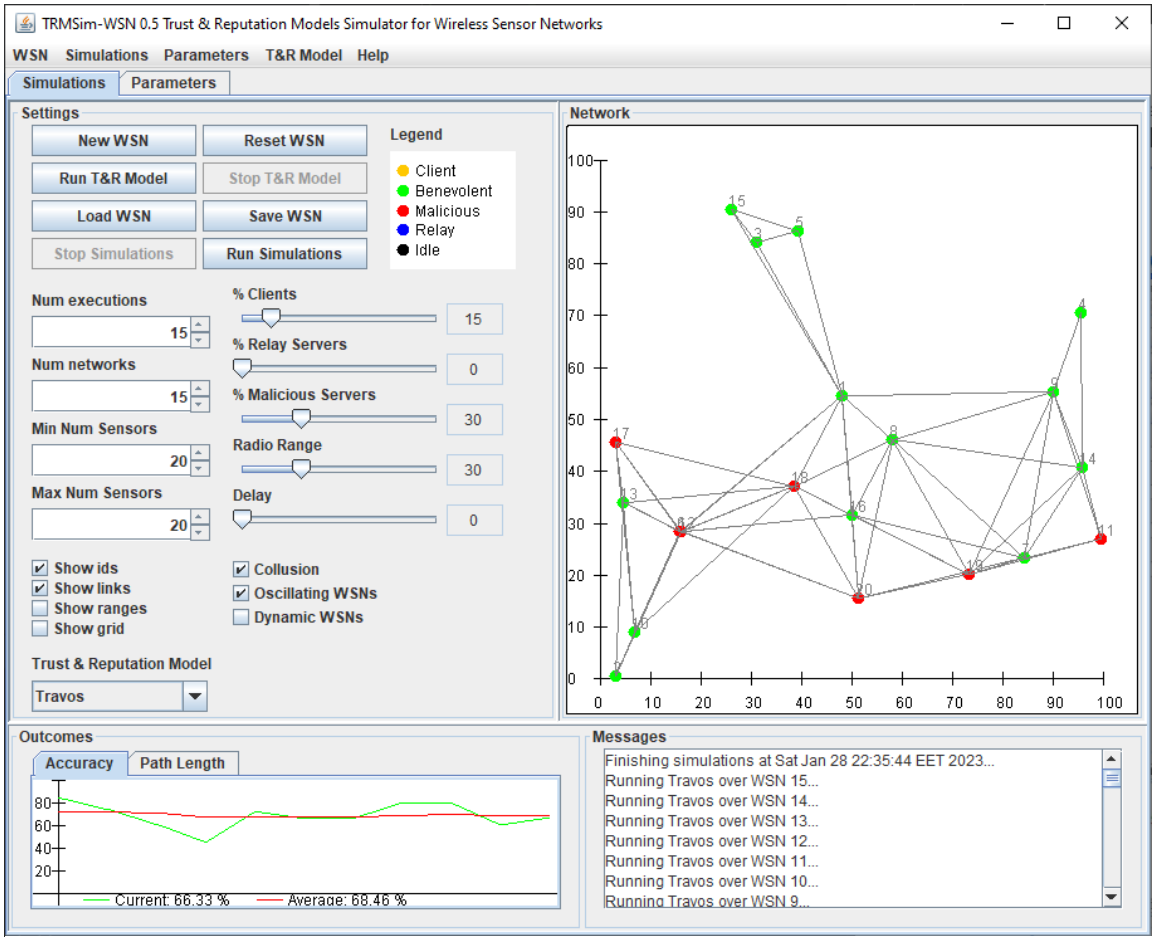
Πίνακας 5: *Κατηγοριοποίηση των μοντέλων*

6

Ο Προσομοιωτής TRMSim-WSN

6.1 Εισαγωγή

Ο προσομοιωτής TRMSim-WSN [18] είναι μία εφαρμογή προσομοίωσης και σύγκρισης μοντέλων Εμπιστοσύνης και Φήμης σε Ασύρματα Δίκτυα Αισθητήρων (Wireless Sensor Networks – WSN). Είναι υλοποιημένος με τη γλώσσα προγραμματισμού Java και αποτελεί εφαρμογή ανοιχτού κώδικα.



Εικόνα 5: Κεντρική οθόνη του προσομοιωτή TRMSim-WSN

Ο εν λόγω προσομοιωτής προσφέρει διάφορες διεπαφές στον χρήστη με τις οποίες μπορεί να υλοποιήσει τα δικά του μοντέλα Εμπιστοσύνης και Φήμης, καθώς και μία γραφική διεπαφή μέσω της οποίας μπορούν να εκτελεστούν προσομοιώσεις και να εμφανιστούν τα αντίστοιχα αποτελέσματα.

Ο συγκεκριμένος προσομοιωτής, τη στιγμή συγγραφής της εργασίας, προσφέρει επίσης υλοποιημένα τα μοντέλα EigenTrust [10], PowerTrust [11], PeerTrust [12], BTRM-WSN [19], LFTM [20] και TRIP [21].

6.2 Διεπαφή Μοντέλου Εμπιστοσύνης και Φήμης

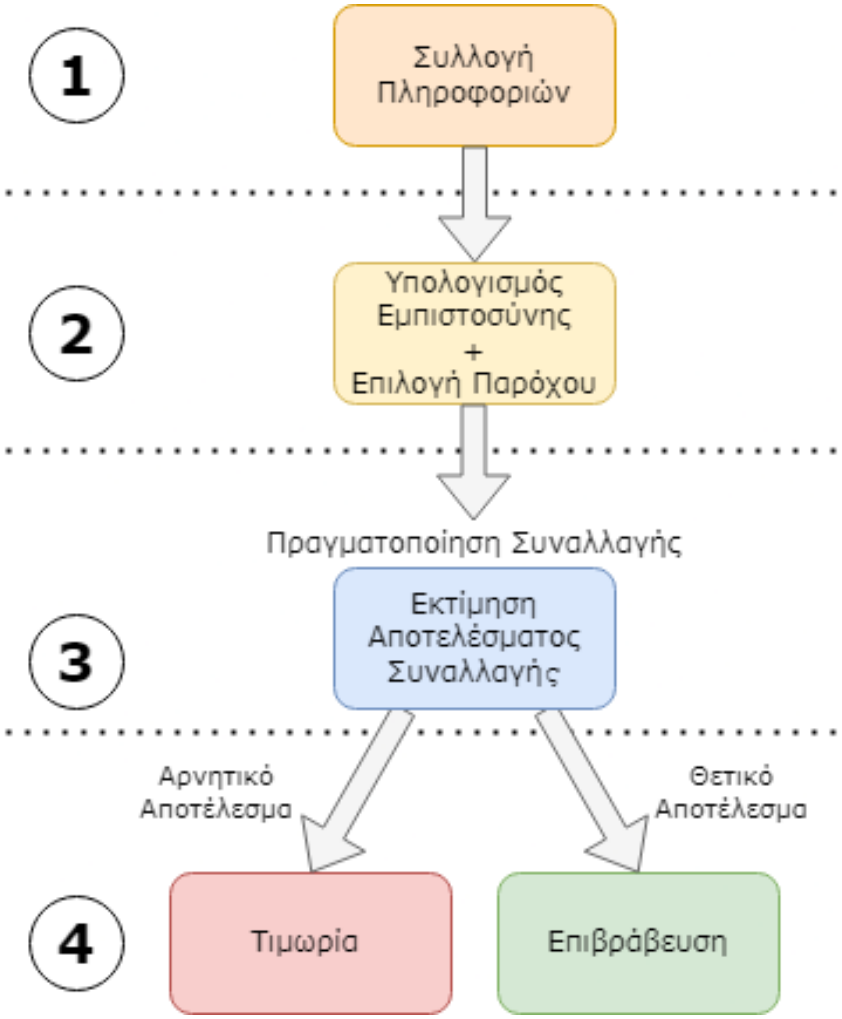
Η Διεπαφή που προσφέρει ο προσομοιωτής για την υλοποίηση μοντέλων Εμπιστοσύνης και Φήμης από τον χρήστη βασίζεται στην ιδέα πως, κατά κανόνα, τα μοντέλα αυτά λειτουργούν με βάση βήματα που παρουσιάζονται στην Εικόνα 6:

1. **Συλλογή Πληροφοριών:** Σε αυτό το βήμα ο κόμβος που επιθυμεί να λάβει μία υπηρεσία συγκεντρώνει πληροφορίες για τους διαθέσιμους παρόχους. Αυτό συνήθως περιλαμβάνει την αναζήτηση στο ιστορικό των δικών του συναλλαγών και, σε ορισμένες περιπτώσεις, την αναζήτηση πληροφοριών από άλλες πηγές για τον εκάστοτε πάροχο (πχ. γειτονικούς κόμβους ή μία κεντρική βάση δεδομένων).

2. **Υπολογισμός Εμπιστοσύνης και Επιλογή Παρόχου:** Με βάση τις πληροφορίες που συγκεντρώθηκαν στο προηγούμενο βήμα, ο κόμβος πραγματοποιεί τους ανάλογους υπολογισμούς ώστε να υπολογίσει την Εμπιστοσύνη του προς τους παρόχους. Στο τέλος επιλέγει έναν με τον οποίο πρόκειται να πραγματοποιήσει τη συναλλαγή.

3. **Πραγματοποίηση Συναλλαγής και Εκτίμηση Αποτελέσματος:** Αφού επιλεγεί ο πάροχος, πραγματοποιείται η συναλλαγή. Με βάση την υπηρεσία που έλαβε τελικά ο αρχικός κόμβος, αποτιμάται και το αποτέλεσμα της συναλλαγής. Αν για παράδειγμα η ποιότητα της υπηρεσίας είναι πάνω από ένα κατώφλι, η συναλλαγή θεωρείται επιτυχημένη, αλλιώς θεωρείται ανεπιτυχής.

4. **Επιβράβευση και Τιμωρία:** Ορισμένα μοντέλα Εμπιστοσύνης και Φήμης υλοποιούνται με τέτοιον τρόπο ώστε να υπάρχει η αντίστοιχη επιβράβευση στον πάροχο έπειτα από μία επιτυχημένη συναλλαγή ή αντίστοιχα μία τιμωρία έπειτα από μία ανεπιτυχή συναλλαγή.



Εικόνα 6: Λογικό Διάγραμμα ενός αφηρημένου μοντέλου Εμπιστοσύνης και Φήμης

Με βάση τα βήματα αυτά, ο προσομοιωτής TRMSim-WSN παρέχει την αφηρημένη κλάση `TRModel_WSN`, η οποία αντιπροσωπεύει ένα αφηρημένο μοντέλο Εμπιστοσύνης και Φήμης. Στην κλάση αυτή υπάρχουν οι αφηρημένες μέθοδοι `gatherInformation`, `scoreAndRanking`, `performTransaction`, `reward` και `punish`, οι οποίες έρχονται σε αντιστοιχία με τα βήματα που περιεγράφηκαν παραπάνω.

Έτσι, κατά την υλοποίηση ενός νέου μοντέλου, ο χρήστης χρειάζεται αρχικά να υλοποιήσει αυτές τις μεθόδους ανάλογα με τις ανάγκες του μοντέλου του σε μία κλάση η οποία να κληρονομεί από την `TRModel_WSN`. Επιπρόσθετα, χρειάζεται να υλοποιήσει και μία κλάση η οποία να κληρονομεί από την αφηρημένη κλάση `TRMParameters`, η οποία είναι υπεύθυνη για τις παραμέτρους του εκάστοτε μοντέλου.

Εκτός των δύο παραπάνω αφηρημένων κλάσεων, ορίζονται και διάφορες άλλες κλάσεις, οι σημαντικότερες εκ των οποίων είναι οι `Network`, `Sensor`, `Service` και `Transaction`. Οι κλάσεις αυτές συνήθως χρειάζεται να τροποποιηθούν ανάλογα με το εκάστοτε μοντέλο, έτσι ώστε να υποστηρίζουν τις διάφορες λειτουργικότητές του ανά περίπτωση.

6.3 Ρυθμίσεις προσομοίωσης και προσαρμογή για P2P δίκτυα

Στην Εικόνα 5 φαίνεται η κεντρική οθόνη του προσομοιωτή TRMSim-WSN, μέσω της οποίας μπορούν να εκτελεστούν οι προσομοιώσεις για τα μοντέλα που είτε έχουν υλοποιηθεί από τον χρήστη, είτε υπάρχουν ήδη έτοιμα στον προσομοιωτή. Μέσω αυτής μπορούν επίσης να ρυθμιστούν οι διάφορες παράμετροι της προσομοίωσης. Βασικά μεγέθη μιας προσομοίωσης είναι ο αριθμός των διαφορετικών τυχαίων δικτύων στα οποία θα πραγματοποιηθεί η προσομοίωση, ο αριθμός των κόμβων που θα υπάρχουν σε κάθε δίκτυο (ελάχιστη και μέγιστη τιμή), καθώς και ο αριθμός των εκτελέσεων που θα πραγματοποιηθούν σε κάθε δίκτυο, δηλαδή ο αριθμός των συναλλαγών που θα πραγματοποιήσει κάθε κόμβος κατά την προσομοίωση.

Εκτός αυτών, σημαντικό ρόλο σε μία προσομοίωση παίζουν και οι αναλογίες των ειδών των κόμβων, δηλαδή σε τι ποσοστό θα είναι κακόβουλοι ή όχι, κτλ. Στο υπόμνημα στην Εικόνα 5 φαίνονται τα είδη κόμβων που υποστηρίζει ο προσομοιωτής. Συγκεκριμένα:

- *Client*: Κόμβος ο οποίος λαμβάνει υπηρεσίες
- *Benevolent*: Κόμβος ο οποίος προσφέρει υπηρεσίες όντας καλοπροαίρετος
- *Malicious*: Κόμβος ο οποίος προσφέρει υπηρεσίες κακοβούλως
- *Relay*: Κόμβος ο οποίος λειτουργεί ως αναμεταδότης πληροφορίας, χωρίς να προσφέρει ή να λαμβάνει υπηρεσίες
- *Idle*: Ανενεργός κόμβος

Όπως αναφέρθηκε παραπάνω, ο συγκεκριμένος προσομοιωτής υλοποιήθηκε με σκοπό τη δοκιμή μοντέλων Εμπιστοσύνης και Φήμης σε ασύρματα δίκτυα αισθητήρων, τα οποία εμφανίζουν ορισμένες διαφορές σε σχέση με ένα γενικευμένο P2P δίκτυο. Για παράδειγμα, στα P2P δίκτυα συνήθως δεν υπάρχει διαχωρισμός μεταξύ server και client, σε αντίθεση με τη σύμβαση την οποία ακολουθεί ο προσομοιωτής. Επίσης, στα P2P δίκτυα δεν υπάρχουν αναμεταδότες πληροφορίας. Τέλος, σε ένα P2P δίκτυο κάθε κόμβος μπορεί – δυνητικά – να συνδεθεί με οποιονδήποτε άλλο κόμβο του δικτύου.

Συνεπώς, στα P2P δίκτυα η έννοια του Radio Range δεν έχει νόημα, σε αντίθεση με τα ασύρματα δίκτυα αισθητήρων, στα οποία οι κόμβοι έχουν περιορισμένη εμβέλεια και μπορούν να συνδεθούν μόνο με κόμβους οι οποίοι βρίσκονται εντός αυτής.

Για να αντιμετωπιστούν οι παραπάνω διαφορές, πραγματοποιήθηκαν οι ακόλουθες ενέργειες:

1. Υλοποιήθηκε η κλάση `Network_P2P`, στην οποία όλοι οι κόμβοι λειτουργούν και ως servers και ως clients, σε αντίθεση με την υπάρχουσα κλάση `Network`, στην οποία υπάρχει σαφής διαχωρισμός μεταξύ των δύο. Έτσι, το ποσοστό των client κόμβων στις ρυθμίσεις του προσομοιωτή δεν επηρεάζει την προσομοίωση για τα δίκτυα που κληρονομούν από την κλάση `Network_P2P`.
2. Σε όλες τις προσομοιώσεις η τιμή του Radio Range τέθηκε στο μέγιστο.
3. Το ποσοστό των Relay κόμβων τέθηκε στο μηδέν.

6.4 Υποστηριζόμενα είδη επιθέσεων

6.4.1 Συντονισμένη Επίθεση - Collusion Attack

Κατά το συγκεκριμένο είδος επίθεσης θεωρούμε πως υπάρχει μία "συνεννόηση" μεταξύ των κακόβουλων κόμβων, οι οποίοι προσπαθούν συλλογικά να σαμποτάρουν το σύστημα. Για να το πετύχουν αυτό, υιοθετούν την ακόλουθη συμπεριφορά:

Όταν πραγματοποιούν συναλλαγές με μη-κακόβουλους χρήστες, παρέχουν τη χειρότερη δυνατή υπηρεσία και όταν τους ζητούνται πληροφορίες για έναν μη-κακόβουλο κόμβο, παρέχουν τη χαμηλότερη δυνατή αξιολόγηση - η οποία σαφώς δεν ανταποκρίνεται στην υπηρεσία που ενδεχομένως να έλαβαν από εκείνον.

Αντιθέτως, όταν πραγματοποιούν συναλλαγές με άλλους κακόβουλους κόμβους, η παρεχόμενη υπηρεσία είναι εκείνη η οποία ζητήθηκε, και όταν τους ζητείται να παρέχουν πληροφορίες για έναν μη-κακόβουλο κόμβο, ανταποκρίνονται με μία υψηλή αξιολόγηση.

Με αυτόν τον τρόπο προσπαθούν να υποβαθμίσουν τη φήμη των κόμβων που έχουν σωστή συμπεριφορά στο σύστημα, ενισχύοντας ταυτόχρονα τη Φήμη των κόμβων που ανήκουν στην κακόβουλη ομάδα. Το συγκεκριμένο είδος επίθεσης χρειάζεται να υλοποιηθεί ξεχωριστά σε κάθε μοντέλο από τον χρήστη.

Στα μοντέλα που υλοποιήθηκαν, οι κακόβουλοι κόμβοι παρείχαν υψηλές αξιολογήσεις για άλλους κακόβουλους χρήστες (που αντιστοιχούν σε ποσοστό ευχαρίστησης 80%-100%) και χαμηλές αξιολογήσεις για μη-κακόβουλους χρήστες (0%-20%).

6.4.2 Εναλλασσόμενη Συμπεριφορά - Oscillating behavior

Σε αυτό το είδος επίθεσης, η συμπεριφορά των κακόβουλων κόμβων παρουσιάζει μία περιοδικότητα. Οι κόμβοι αρχικά συμπεριφέρονται σωστά, παρέχοντας ειλικρινείς αξιολογήσεις και υπηρεσίες, ενώ στη συνέχεια, αφού έχουν εδραιώσει τη Φήμη τους λόγω της ορθής συμπεριφοράς τους, ξεκινούν να

συμπεριφέρονται κακοβούλως. Έπειτα από ένα διάστημα αρχίζουν ξανά να συμπεριφέρονται σωστά μέχρι να ξαναχτίσουν τη χαμένη τους Φήμη, με το μοτίβο αυτό να επαναλαμβάνεται.

Το συγκεκριμένο είδος επίθεσης προσομοιώνεται στον TRMSim-WSN ως εξής: Έπειτα από κάθε 20 κύκλους συναλλαγών, όλοι οι κακόβουλοι κόμβοι γίνονται μη-κακόβουλοι. Στη συνέχεια, ένα ποσοστό κόμβων ίσο με το ποσοστό κακόβουλων κόμβων που έχει οριστεί, αλλάζει από μη-κακόβουλο σε κακόβουλο. Αυτό φυσικά σημαίνει πως ένας κόμβος που ήταν κακόβουλος στον προηγούμενο κύκλο των 20 συναλλαγών μπορεί να παραμείνει κακόβουλος και στον επόμενο.

7

Αξιολόγηση Μοντέλων

7.1 Κριτήρια αξιολόγησης

Τα βασικά κριτήρια που χρησιμοποιήθηκαν για την αξιολόγηση των μοντέλων ήταν η μέση ικανοποίηση σε αυξανόμενο ποσοστό κακόβουλων κόμβων, η επεκτασιμότητα, δηλαδή η ικανότητά του μοντέλου να είναι αξιόπιστο καθώς ο αριθμός των κόμβων αυξάνεται, καθώς και η υπολογιστική πολυπλοκότητα, η οποία μετρήθηκε εμμέσως από τον χρόνο εκτέλεσης των προσομοιώσεων του κάθε μοντέλου.

7.2 Οργάνωση πειραμάτων

Οι προσομοιώσεις πραγματοποιήθηκαν σε δίκτυα με N=50 έως 400 κόμβους, με ποσοστό κακόβουλων κόμβων από 20%-80. Πραγματοποιήθηκαν προσομοιώσεις σε κανονικές συνθήκες, καθώς και στις δύο επιθέσεις που υποστηρίζει ο προσομοιωτής, το Collusion Attack και την Επίθεση Εναλλασσόμενης Συμπεριφοράς, καθώς και σε συνδυασμό τους. Η κάθε προσομοίωση πραγματοποιήθηκε για 20 τυχαία δίκτυα και είχε διάρκεια 100 κύκλους συναλλαγών. Παρακάτω παρουσιάζονται οι παράμετροι που επιλέχθηκαν για κάθε μοντέλο κατά την προσομοίωση:

- EigenTrust:
  - $\boldsymbol{p = 10\%}$
  - $\boldsymbol{\varepsilon = 0.05}$
  - $\boldsymbol{a = 0.2}$

- PowerTrust
  - $\boldsymbol{p = 10\%}$
  - $\boldsymbol{\varepsilon = 0.05}$
  - $\boldsymbol{a = 0.2}$

- PeerTrust
  - $\boldsymbol{a = 1}$
  - $\boldsymbol{b = 0}$

- TRAVOS:
  - $\boldsymbol{N_{bins} = 5}$
  - $\boldsymbol{E = 0.2}$
  - $\boldsymbol{\theta_{\gamma} = 0.85}$

- RDTM:
  - $\boldsymbol{T_{throd} = 0.75}$
  - $\boldsymbol{N_{supernodes} = 10}$
  - $\boldsymbol{N_{tr_{min}} = 20}$
  - $\boldsymbol{S_{tr_{min}} = 500}$
  - $\boldsymbol{T_0 = 15}$

- TRM-SIoT:
  - $\boldsymbol{f_s = 0.05}$
  - $\boldsymbol{N_f = 4}$
  - $\boldsymbol{N_{best_{platform}} = 5}$

Όλες οι προσομοιώσεις πραγματοποιήθηκαν σε μηχάνημα με τα ακόλουθα χαρακτηριστικά:

OS: Ubuntu 20.04.3 LTS, 64-bit

CPU: Intel(R) Core(TM) i7-3820 CPU @ 3.60GHz

RAM: DDR3, 32Gb

GPU: GeForce GTX 560 Ti/PCIe/SSE2

Hard Drive: 4,3 TB HDD

7.3 Αποτελέσματα

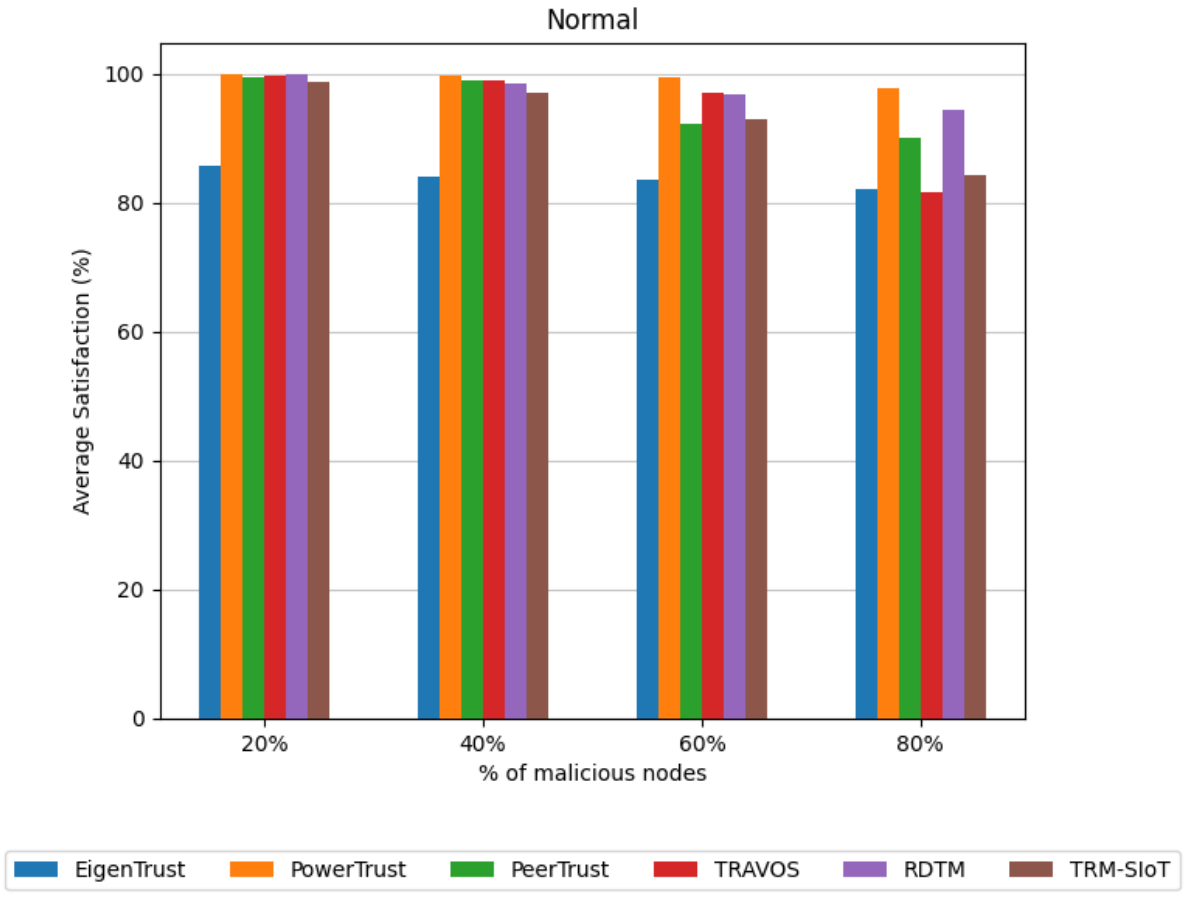
7.3.1 Μέση Ικανοποίηση

Η πρώτη και κυριότερη μετρική που πρέπει να λαμβάνεται υπ' όψη κατά την αξιολόγηση ενός μοντέλου Εμπιστοσύνης και Φήμης είναι η Ικανοποίηση των κόμβων του συστήματος, δηλαδή το κατά πόσο είναι οι κόμβοι ευχαριστημένοι από τις συναλλαγές που πραγματοποίησαν στο σύστημα. Είναι εμφανές, συνεπώς, πως αυτό συνδέεται άμεσα με το αν επιλέχθηκε ο σωστός πάροχος, και, επομένως, με το κατά πόσο είναι αξιόπιστο το μοντέλο Εμπιστοσύνης και Φήμης που εφαρμόζεται στο παρόν σύστημα.

Παρακάτω παρουσιάζονται τα αποτελέσματα των προσομοιώσεων σε δίκτυα με 50 κόμβους.

7.3.1.1 Κανονική Συμπεριφορά

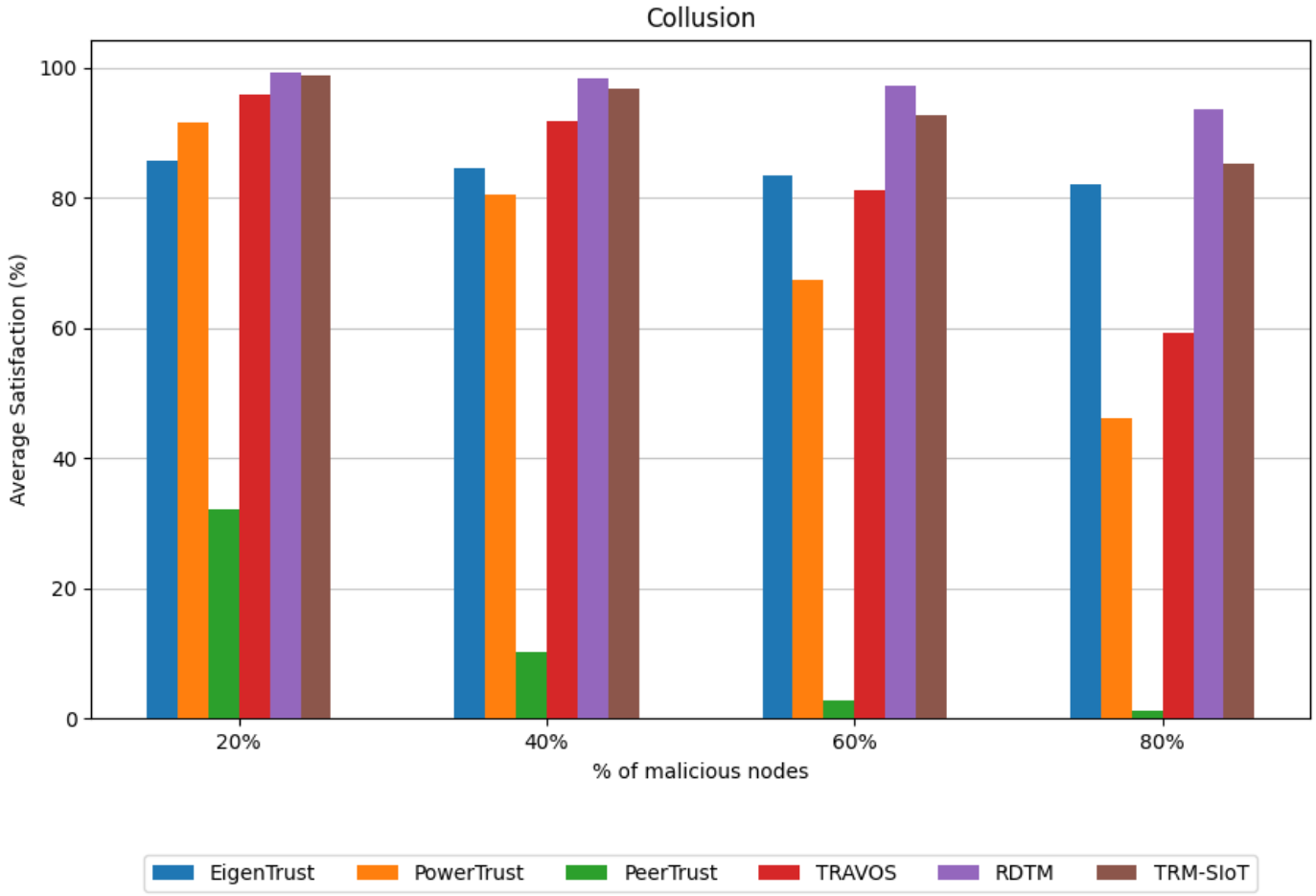
Το πρώτο πείραμα που πραγματοποιήθηκε ήταν η προσομοίωση των μοντέλων υπό κανονική συμπεριφορά κόμβων, χωρίς δηλαδή κάποιο συγκεκριμένο είδος επίθεσης.



Στη συγκεκριμένη περίπτωση όλα τα μοντέλα παρέχουν αρκετά ικανοποιητικά αποτελέσματα, με τα PowerTrust και RDTM να επιτυγχάνουν μέση ικανοποίηση πάνω από 90% ακόμα και σε δίκτυα με ποσοστό κακόβουλων κόμβων 80%.

7.3.1.2 Collusion Attack

Στη συνέχεια πραγματοποιήθηκαν προσομοιώσεις του collusion attack, κατά το οποίο οι κακόβουλοι κόμβοι είναι "συνεννοημένοι" μεταξύ τους ώστε να αλληλοπροωθούνται παρέχοντας θετικές αξιολογήσεις ό ένας στον άλλο, ενώ ταυτόχρονα παρέχουν ψευδείς χαμηλές αξιολογήσεις για τους μη-κακόβουλους κόμβους

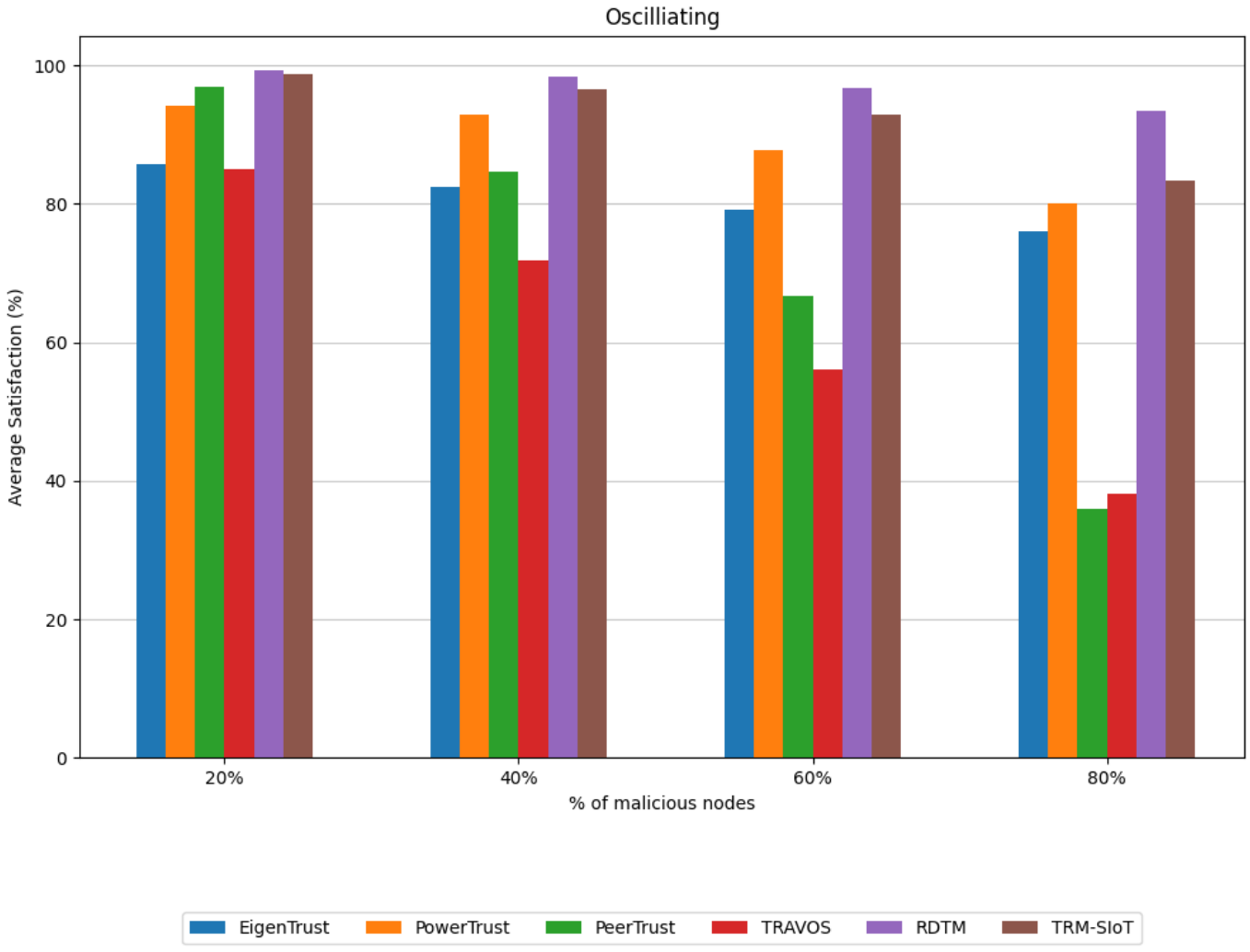


Γίνεται εύκολα αντιληπτή η αδυναμία ορισμένων μοντέλων ενάντια στο συγκεκριμένο είδος επίθεσης, με κύριο το PeerTrust, το οποίο φαίνεται να αποτυγχάνει πλήρως, ακόμη και σε δίκτυα με χαμηλό ποσοστό κακόβουλων κόμβων. Πιθανότατα αυτό οφείλεται στην έλλειψη κάποιου μηχανισμού τιμωρίας σε περίπτωση ψευδούς αξιολόγησης από έναν εν δυνάμει κακόβουλο κόμβο. Τα μοντέλα PowerTrust και TRAVOS ενώ για ποσοστό κακόβουλων κόμβων έως 40% παρέχουν αξιοπρεπή

αποτελέσματα, εάν το ποσοστό αυτό αυξηθεί, η απόδοσή τους πέφτει. Από την άλλη, τα μοντέλα EigenTrust, RDTM και TRM-SIoT φαίνεται να αντιστέκονται καλά στο συγκεκριμένο είδος επίθεσης.

7.3.1.3 Εναλλασσόμενη Συμπεριφορά

Έπειτα, προσομοιώθηκε η επίθεση της εναλλασσόμενης συμπεριφοράς, κατά την οποία, ανά ορισμένο αριθμό κύκλων συναλλαγών, οι κακόβουλοι κόμβοι συμπεριφέρονται σωστά ώστε να αυξήσουν τη Φήμη τους, ενώ στη συνέχεια επανέρχονται στην κανονική τους συμπεριφορά.

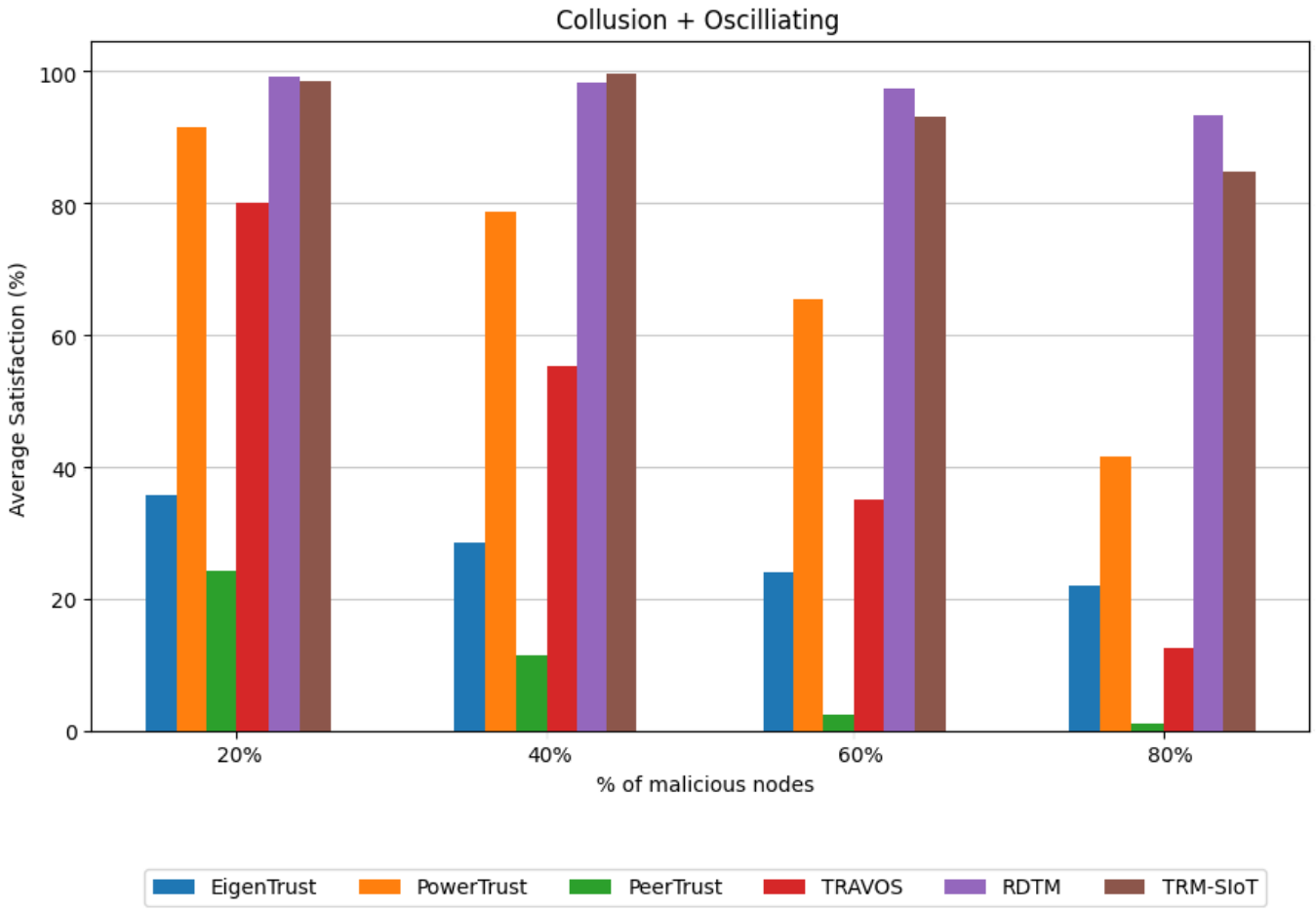


Ενάντια στο συγκεκριμένο είδος επίθεσης, γίνεται εύκολα αντιληπτό πως τα μοντέλα PeerTrust και TRAVOS βρίσκονται σε μειονεκτική θέση. Ειδικότερα όσον αφορά το TRAVOS, η αδυναμία του ενάντια στο συγκεκριμένο είδος επίθεσης είναι αναμενόμενη λόγω της έλλειψης κάποιου συντελεστή ο οποίος να λαμβάνει υπ' όψη του το χρόνο κατά τον υπολογισμό της εμπιστοσύνης. Με άλλα λόγια, δεν υπάρχει διαχωρισμός ανάμεσα σε παλιότερες και νεότερες αξιολογήσεις προς κάποιον κόμβο. Έτσι,

ένας κακόβουλος κόμβος που αρχικά συμπεριφέρεται ορθώς μπορεί να αυξήσει τη Φήμη του και στη συνέχεια να εξαπατά τους υπόλοιπους κόμβους χωρίς αυτό να επηρεάζει αρνητικά τη Φήμη του σε μεγάλο βαθμό. Τα υπόλοιπα μοντέλα φαίνεται να αντιστέκονται σε αξιοπρεπή βαθμό στο συγκεκριμένο είδος επίθεσης.

7.3.1.4 Συνδυασμός Επιθέσεων

Τέλος, πραγματοποιήθηκαν προσομοιώσεις κατά τις οποίες οι δύο επιθέσεις πραγματοποιούνταν ταυτόχρονα.



Στο συγκεκριμένο πείραμα φαίνεται πως μόνο τα δύο νεότερα μοντέλα, RDTM και TRM-SIoT είναι ικανά να αντισταθούν στον συνδυασμό των δύο επιθέσεων, ενώ τα υπόλοιπα μοντέλα παρέχουν όλο και χαμηλότερα αποτελέσματα όσο το ποσοστό των κακόβουλων κόμβων αυξάνεται. Εξάγεται επομένως το συμπέρασμα πως σε συστήματα τα οποία είναι πιθανό να δεχτούν τέτοιου είδους επιθέσεις, τα μοντέλα RDTM και TRAVOS αποτελούν αξιόπιστες λύσεις.

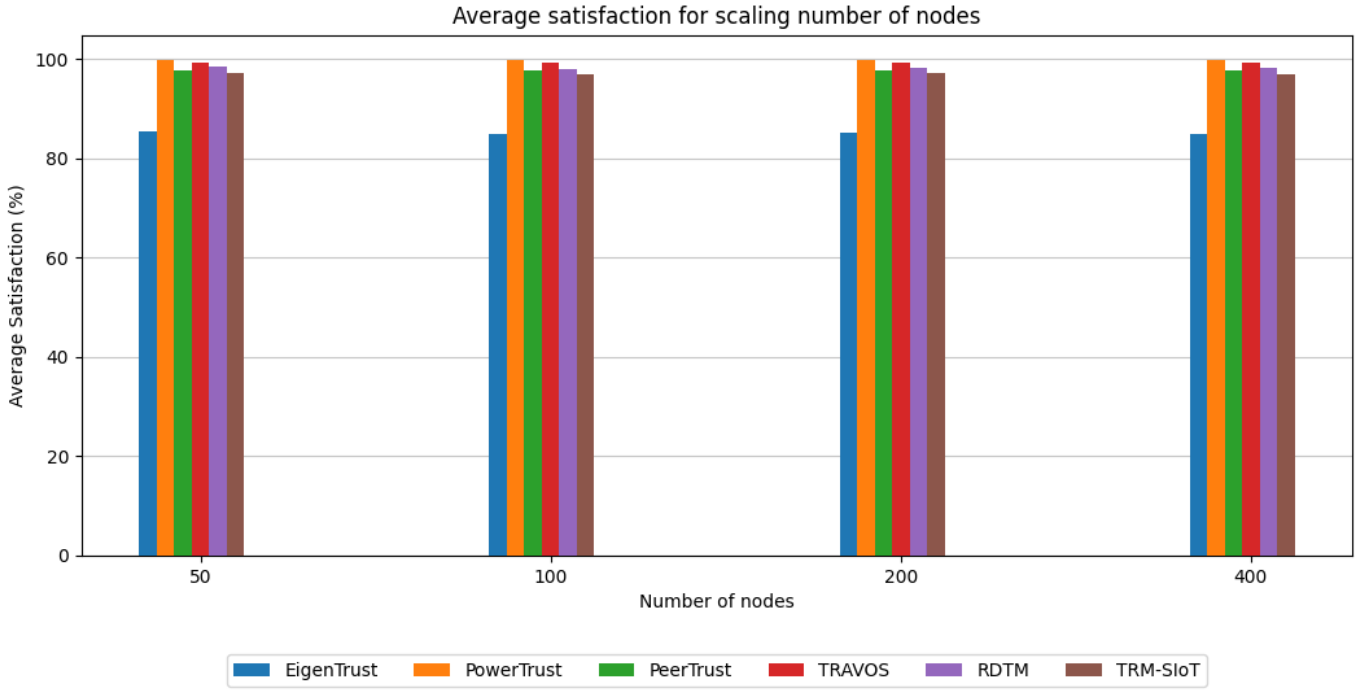
7.3.2 Επεκτασιμότητα

Άλλο ένα βασικό κριτήριο που πρέπει να λαμβάνεται υπ' όψη είναι η επεκτασιμότητα των μοντέλων, δηλαδή το κατά πόσο εξακολουθούν να είναι αποδοτικά καθώς ο αριθμός των κόμβων αυξάνεται. Εκτός αυτού, είναι σημαντικό να εξεταστεί και η πολυπλοκότητα του αλγορίθμου που χρησιμοποιείται στο εκάστοτε μοντέλο.

Για την εξέταση της επεκτασιμότητας των μοντέλων πραγματοποιήθηκαν προσομοιώσεις με αυξανόμενο αριθμό κόμβων δικτύου και μετρήθηκε η Μέση Ικανοποίηση των κόμβων, καθώς και ο χρόνος ολοκλήρωσης των προσομοιώσεων, ο οποίος παρέχει μία εικόνα για την πολυπλοκότητα του κάθε μοντέλου. Συγκεκριμένα, οι προσομοιώσεις που αφορούσαν την αξιολόγηση της επεκτασιμότητας των μοντέλων, πραγματοποιήθηκαν σε δίκτυα με N=50, 100, 200, 400 κόμβους με ποσοστό κακόβουλων κόμβων 40% χωρίς να πραγματοποιείται κάποια επίθεση.

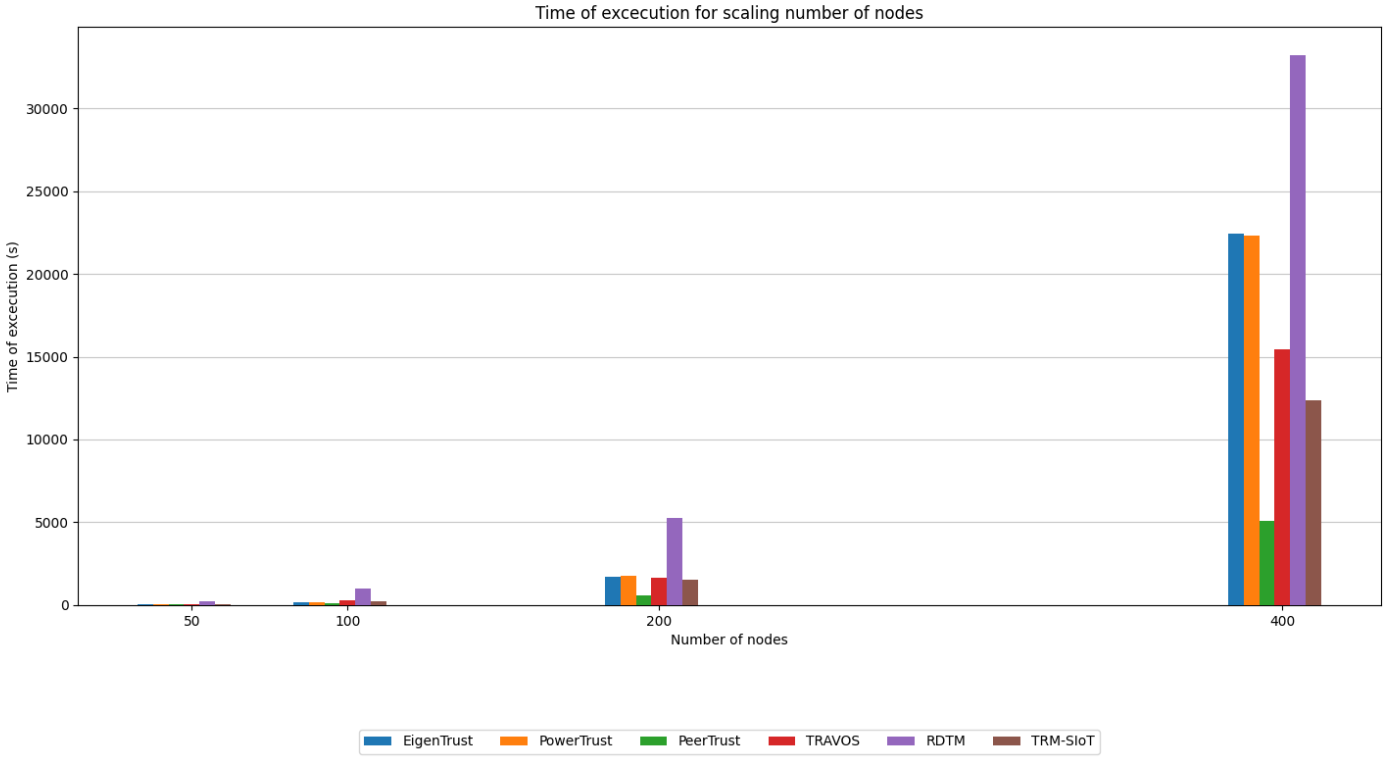
7.3.2.1 Μέση Ικανοποίηση

Όσον αφορά το κομμάτι της Μέσης Ικανοποίησης των χρηστών, δεν παρατηρήθηκε κάποια αδυναμία στα μοντέλα. Καθώς ο αριθμός των κόμβων αυξάνεται, τα μοντέλα εξακολουθούν να παρέχουν πολύ κοντινά αποτελέσματα.



7.3.2.2 Χρόνος Εκτέλεσης

Όσον αφορά τον χρόνο εκτέλεσης, παρατηρήθηκε πως όλα τα μοντέλα τείνουν προς την εκθετική πολυπλοκότητα με τα PeerTrust και TRM-SIoT να είναι τα γρηγορότερα.



Αυτό μπορεί εύκολα να δικαιολογηθεί. Το PeerTrust δεν υλοποιεί κάποιον πολύπλοκο μηχανισμό για τον υπολογισμό της Εμπιστοσύνης και της Φήμης, επομένως είναι αναμενόμενο και ο χρόνος που απαιτείται ώστε να ολοκληρωθούν οι προσομοιώσεις να είναι χαμηλός. Το TRM-SIoT, αν και χρησιμοποιεί έναν αρκετά πιο σύνθετο μηχανισμό, βάζει όρια ως προς το πόσες αξιολογήσεις θα λαμβάνονται υπ'όψη και πόσοι γείτονες θα προτείνονται, κάτι που μειώνει σε μεγάλο βαθμό την πολυπλοκότητα.

Στην άλλη πλευρά, τα μοντέλα EigenTrust, PowerTrust και RDTM φαίνεται πως δεν είναι τόσο αποδοτικά από πλευράς χρόνου όσο το μέγεθος δικτύου αυξάνεται. Για τα EigenTrust και PowerTrust, αυτό είναι αναμενόμενο, καθώς εκ φύσεως του ο αλγόριθμος υπολογισμού του διανύσματος $\overrightarrow{t_i} = (C^T)^n \overrightarrow{c_i}$, έχει εκθετική πολυπλοκότητα. Όσον αφορά το μοντέλο RDTM, ένα κύριο πρόβλημα που εντοπίζεται είναι πως δεν υπάρχει κάποιος κανόνας βάσει του οποίου δε λαμβάνονται καθόλου υπ' όψη οι παλιές αξιολογήσεις. Ως αποτέλεσμα, όσο μεγαλύτερο ιστορικό υπάρχει, τόσο περισσότερους όρους έχει το άθροισμα κατά τον υπολογισμό της εμπιστοσύνης. Αυτό επιβεβαιώθηκε και κατά το πειραματικό στάδιο, όπου παρατηρήθηκε πως όσο προχωρούσαν οι κύκλοι συναλλαγών, τόσο περισσότερο αργούσαν να ολοκληρωθούν.

Επιπροσθέτως, σε συστήματα όπως το RDTM, όπου ο περισσότερος υπολογιστικός φόρτος συγκεντρώνεται σε λίγους μονάχα κόμβους – τους Power-Nodes εν προκειμένω – είναι απαραίτητο οι κόμβοι αυτοί να έχουν αυξημένη υπολογιστική ισχύ ώστε να ανταποκρίνονται στον φόρτο αυτό χωρίς να προκαλούν bottlenecks στο σύστημα. Στην προσομοίωση δεν ήταν δυνατός ο διαχωρισμός της υπολογιστικής ισχύος ανάμεσα στους απλούς κόμβους και στους Power-Nodes, επομένως τα αποτελέσματα ενδέχεται να διέφεραν σε άλλη περίπτωση.

7.4 Σύνοψη συμπερασμάτων αξιολόγησης

Εξετάζοντας τα πειραματικά αποτελέσματα που παρουσιάστηκαν παραπάνω, διαπιστώνεται πως αν και όλα τα μοντέλα έχουν καλή απόδοση σε ένα κανονικό σύστημα, εάν αυτό δεχτεί επίθεση, τότε θα είναι ευάλωτο σε αρκετές περιπτώσεις.

Το μοντέλο EigenTrust, φαίνεται να αντιστέκεται καλά στο Collusion Attack και υποχωρεί ελαφρώς όταν δέχεται επίθεση Εναλλασσόμενης Συμπεριφοράς, διατηρώντας ωστόσο σε υψηλά ποσοστά τη Μέση Ικανοποίηση. Ωστόσο, όταν οι δύο επιθέσεις συμβαίνουν ταυτόχρονα, το μοντέλο αποτυγχάνει. Εκτός αυτού, παρατηρείται πως σε όλες τις περιπτώσεις υπάρχει κάποιο άλλο μοντέλο το οποίο αποδίδει καλύτερα.

Το PowerTrust, ενώ παρουσιάζει πολλές ομοιότητες στην υλοποίησή του με το EigenTrust, φαίνεται να αποδίδει καλύτερα υπό κανονικές συνθήκες. Ωστόσο, φαίνεται να είναι πιο ευάλωτο στο Collusion Attack. Σε ένα σύστημα μικρής κλίμακας, το οποίο δεν δέχεται επιθέσεις θα αποτελούσε μία αξιόπιστη λύση.

Το PeerTrust, αν και παρέχει ενδιαφέρουσες ιδέες ως προς τη διαχείριση της Εμπιστοσύνης και της Φήμης και λειτουργεί καλά όταν δεν δέχεται επίθεση, σε διαφορετική περίπτωση αποτυγχάνει. Γίνεται ξεκάθαρο πως χρειάζονται επιπλέον παράγοντες στον υπολογισμό και τη διαχείριση της Εμπιστοσύνης και της Φήμης ώστε να γίνει περισσότερο αποδοτικό.

Το μοντέλο TRAVOS προσεγγίζει τη μοντελοποίηση της Εμπιστοσύνης με έναν ενδιαφέροντα και διαφορετικό από τα υπόλοιπα συστήματα τρόπο. Η αδυναμία του, κυρίως στην επίθεση Εναλλασσόμενης Συμπεριφοράς, θα μπορούσε να καταπολεμηθεί εισάγοντας έναν παράγοντα που να δίνει περισσότερο βάρος στις πιο πρόσφατες συναλλαγές και χαμηλότερο βάρος στις λιγότερο πρόσφατες.

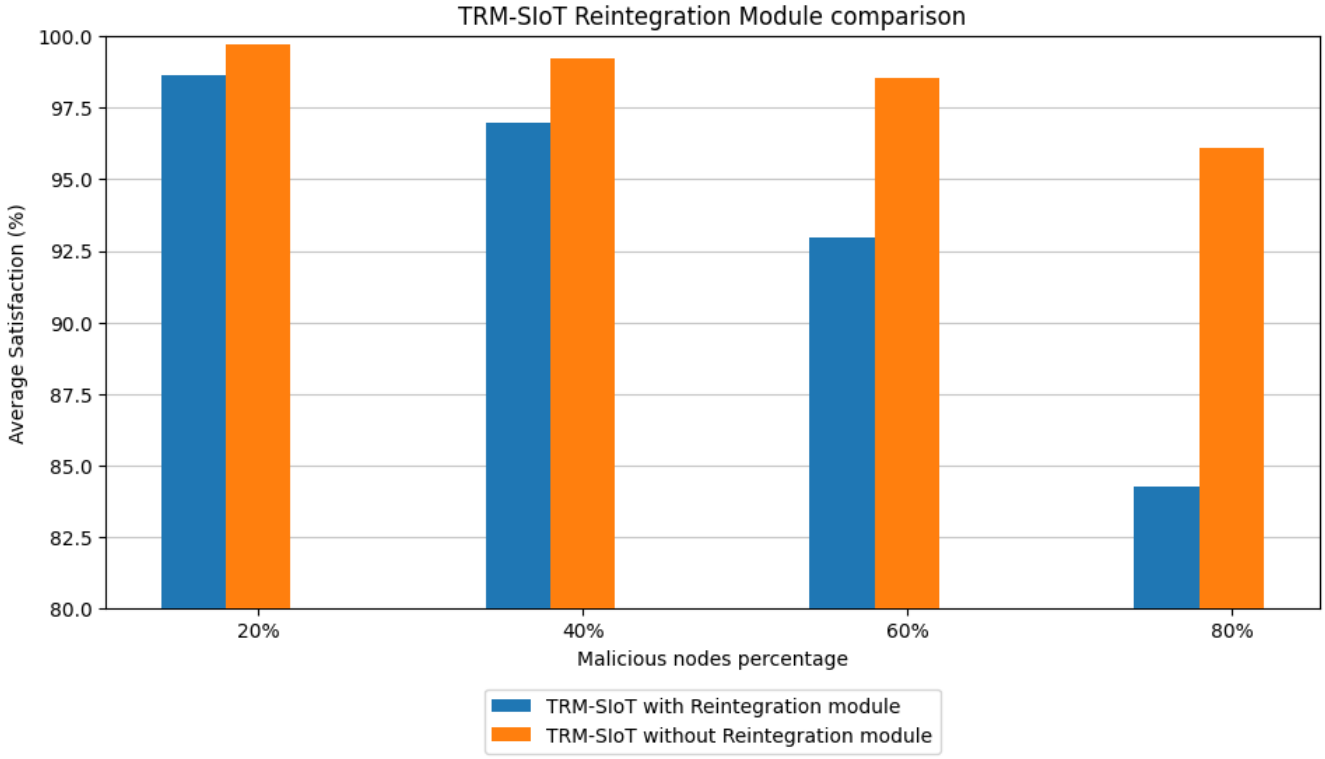
Το μοντέλο RDTM παρέχει τα πιο ικανοποιητικά αποτελέσματα σε σχέση με τα υπόλοιπα μοντέλα, και φαίνεται να αντιστέκεται πολύ αποτελεσματικά στα δύο είδη επιθέσεων που προσομοιώθηκαν. Μοναδικό του μειονέκτημα είναι η χρονική του πολυπλοκότητα. Το πρόβλημα αυτό θα μπορούσε να περιοριστεί αρχικά θέτοντας ένα μέγιστο όριο ως προς τον αριθμό των συναλλαγών που θα λαμβάνονται υπ’ όψη για τον υπολογισμό της Φήμης. Επιπροσθέτως, σε ένα σύστημα σαν το RDTM,

όπου λίγοι κόμβοι του συστήματος – οι PowerNodes στη συγκεκριμένη περίπτωση – αναλαμβάνουν μεγάλο φόρτο στο κομμάτι της επικοινωνίας, θα πρέπει να εξασφαλίζεται πως οι κόμβοι αυτοί έχουν τη δυνατότητα να ανταποκριθούν στον φόρτο αυτό. Ειδάλλως, θα δημιουργούνται bottlenecks, τα οποία θα δυσχεραίνουν την ομαλή λειτουργία του συστήματος.

Τέλος, το μοντέλο TRM-SIoT διατηρεί και αυτό τη Μέση Ικανοποίηση σε αρκετά υψηλά επίπεδα σε όλες τις περιπτώσεις, με εξαίρεση τις περιπτώσεις εκείνες στις οποίες το ποσοστό των κακόβουλων κόμβων ξεπερνάει το 80%. Ωστόσο, ακόμη και τότε, η Μέση Ικανοποίηση διατηρείται σε ποσοστά υψηλότερα του 80%. Επιπλέον, είναι πολύ πιο αποδοτικό από πλευράς χρόνου σε σχέση με το RDTM.

Όσον αφορά τη μείωση της Μέσης Ικανοποίησης στα συστήματα με υψηλά ποσοστά κακόβουλων κόμβων, αυτή ενδεχομένως να οφείλεται στον παράγοντα Επανένταξης που χρησιμοποιεί το μοντέλο. Με βάση το σχεδιασμό του TRM-SIoT, κατά την επιλογή ενός παρόχου υπηρεσίας, υπάρχει 10% πιθανότητα να επιλεγεί ένας τυχαίος κόμβος – ο οποίος δεν είναι ανάμεσα τους καλύτερους βάσει Φήμης. Με αυτόν τον τρόπο δίνεται η ευκαιρία σε πρώην κακόβουλους ή δυσλειτουργικούς κόμβους να επανενταχθούν στο σύστημα.

Ωστόσο, στον συγκεκριμένο προσομοιωτή δεν υποστηρίζεται κάποια τέτοια μετάβαση συμπεριφοράς. Οι κακόβουλοι κόμβοι παραμένουν κακόβουλοι καθ' όλη τη διάρκεια της προσομοίωσης – με εξαίρεση την επίθεση Εναλλασσόμενης Συμπεριφοράς, η οποία δεν είναι ταιριαστό παράδειγμα. Έτσι, με τον παράγοντα Επανένταξης ενεργό, το μόνο που επιτυγχάνεται στις συγκεκριμένες προσομοιώσεις είναι να ευνοούνται οι κακόβουλοι κόμβοι.



Αυτό επιβεβαιώνεται και πειραματικά, καθώς διαπιστώθηκε πως όταν ο παράγοντας αυτός απενεργοποιηθεί, το μοντέλο γίνεται ακόμη πιο αποτελεσματικό. Σε κάθε περίπτωση ωστόσο, ο παράγοντας Επανένταξης είναι μία λειτουργία που σε αρκετές περιπτώσεις μπορεί να λειτουργεί υπέρ του συστήματος και όχι σε βάρος του.

8

Επίλογος

Ολοκληρώνοντας, κρίνεται σκόπιμο να γίνει μια συνοπτική παρουσίαση του περιεχομένου της παρούσας διπλωματικής προκειμένου να μπορέσουν να εξαχθούν τα ανάλογα συμπεράσματα.

8.1 Σύνοψη και συμπεράσματα

Συνοψίζοντας, στη συγκεκριμένη διπλωματική παρουσιάστηκε μία ποσοτική σύγκριση μεταξύ αρκετών μοντέλων Εμπιστοσύνης και Φήμης. Με βάση τα πειραματικά αποτελέσματα φάνηκε πως όλα τα μοντέλα (EigenTrust, PowerTrust, PeerTrust, TRAVOS, RDTM, TRM-SIoT) λειτουργούν σε πολύ καλό βαθμό υπό κανονικές συνθήκες.

Ωστόσο, στις περιπτώσεις που το σύστημα δέχεται κάποια από τις επιθέσεις που μελετήθηκαν, η απόδοση ορισμένων μοντέλων πέφτει. Συγκεκριμένα, κατά το Collusion Attack, η απόδοση των PeerTrust και PowerTrust μειώνεται κατά μεγάλο βαθμό. Κατά την Επίθεση Εναλλασσόμενης Συμπεριφοράς, τα μοντέλα TRAVOS και PeerTrust δυσκολεύονται να ανταπεξέλθουν. Οι πιο αξιόπιστες λύσεις σε όλες τις περιπτώσεις είναι τα μοντέλα RDTM και TRM-SIoT, με το τελευταίο να υπερισχύει εάν ληφθεί υπ' όψη και ο παράγοντας της πολυπλοκότητας.

Έχοντας αναλύσει πλέον τα θετικά και αρνητικά χαρακτηριστικά κάθε μοντέλου, καθώς και τις επιδόσεις τους σε διάφορα είδη επιθέσεων, έχει δημιουργηθεί μια στέρεη βάση η οποία μπορεί να φανεί χρήσιμη σε κάθε μελλοντική επιλογή του πλέον κατάλληλου μοντέλου Εμπιστοσύνης και Φήμης.

8.2 Μελλοντικές επεκτάσεις

Λόγω της φύσης του αλλά και της χρησιμότητάς του, καθώς και του επίκαιρου χαρακτήρα του, το αντικείμενο της παρούσας διπλωματικής αφήνει ευρύ περιθώριο επέκτασης.

Αρχικά, μία πρώτη επέκταση της παρούσας εργασίας θα μπορούσε να αποτελέσει η υλοποίηση επιπλέον μοντέλων Εμπιστοσύνης και Φήμης με σκοπό τη σύγκρισή τους με τα ήδη υπάρχοντα.

Επίσης, μία πολύ σημαντική προσθήκη θα ήταν η υλοποίηση περισσότερων ειδών επιθέσεων στον προσομοιωτή TRMSiM-WSN, ώστε να εξάγεται μία ακόμη πιο πλήρης εικόνα όσον αφορά την αξιοπιστία των μοντέλων. Ενδεικτικά παραδείγματα αποτελούν το White-Washing Attack, κατά το οποίο οι κακόβουλοι κόμβοι φεύγουν από το σύστημα και επανέρχονται χρησιμοποιώντας διαφορετική ταυτότητα, ώστε να αγνοηθεί η προηγούμενη κακή τους Φήμη, και το Discriminatory Attack, κατά το οποίο ομάδες κόμβων, ενώ συμπεριφέρονται σωστά ως προς το μεγαλύτερο σύνολο του συστήματος, μπορεί να παρέχουν κακές υπηρεσίες σε κάποιες συγκεκριμένες ομάδες κόμβων.

Τέλος, θα ήταν σημαντικό να υλοποιηθεί στον προσομοιωτή μία λειτουργικότητα η οποία να υποστηρίζει την ένταξη/αφαίρεση κόμβων από το σύστημα κατά τη διάρκεια μίας προσομοίωσης. Η λειτουργικότητα αυτή θα συμβάλει στη μελέτη της διαχείρισης των νεοεισελθέντων κόμβων του συστήματος, η οποία αποτελεί σημαντικό αντικείμενο μελέτης.

9

Βιβλιογραφία και Αναφορές

[1] A. I. A. Ahmed, S. H. Ab Hamid, A. Gani, S. khan, and M. K. Khan, "Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges," *Journal of Network and Computer Applications*, vol. 145. Academic Press, Nov. 01, 2019. doi: 10.1016/j.jnca.2019.102409.

[2] Z. Noorian and M. Ulieru, "The state of the art in trust and reputation systems: A framework for comparison," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 5, no. 2, pp. 97–117, 2010, doi: 10.4067/S0718-18762010000200007.

[3] O. Khalid *et al.*, "Comparative study of trust and reputation systems for wireless sensor networks," *Security and Communication Networks*, vol. 6, no. 6, pp. 669–688, Jun. 2013, doi: 10.1002/SEC.597.

[4] F. G. Mármol and G. M. Pérez, "Trust and reputation models comparison," *Internet Research*, vol. 21, no. 2, pp. 138–153, Jan. 2011, doi: 10.1108/10662241111123739.

[5] "Gnutella - Wikipedia." Accessed: Jan. 28, 2023. [Online]. Available: https://en.wikipedia.org/wiki/Gnutella

[6] "BitTorrent (software) - Wikipedia." Accessed: Jan. 28, 2023. [Online]. Available: https://en.wikipedia.org/wiki/BitTorrent_(software)

[7] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Accessed: May 20, 2023. [Online]. Available: www.bitcoin.org

[8] M. Laeequddin, B. S. Sahay, V. Sahay, and K. A. Waheed, "Measuring trust in supply chain partners' relationships", doi: 10.1108/13683041011074218.

[9] Q. Ding, "Trust Management in the P2P Grid," *International Journal of Digital Content Technology and its Applications*, vol. 3, no. 1, Mar. 2009, doi: 10.4156/JDCTA.VOL3.ISSUE1.DING.

[10] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, “The EigenTrust Algorithm for Reputation Management in P2P Networks.”

[11] R. Zhou and K. Hwang, “PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing”, doi: 10.1109/TPDS.2007.1015.

[12] L. Xiong and L. Liu, “PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities,” *IEEE Trans Knowl Data Eng*, vol. 16, no. 7, pp. 843–857, Jul. 2004, doi: 10.1109/TKDE.2004.1318566.

[13] W. T. L. Teacy, J. Patel, N. R. Jennings, and M. Luck, “TRAVOS: Trust and reputation in the context of inaccurate information sources,” in *Autonomous Agents and Multi-Agent Systems*, Mar. 2006, pp. 183–198. doi: 10.1007/s10458-006-5952-x.

[14] “Beta distribution - Wikipedia.” Accessed: Jan. 10, 2023. [Online]. Available: https://en.wikipedia.org/wiki/Beta_distribution

[15] Z. Song, J. Pu, L. Jiang, F. Wei, and D. Wang, “A Reputation-based Dynamic Trust Model in P2P E-commerce Environment,” in *Proceeding - 2021 China Automation Congress, CAC 2021*, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 6432–6438. doi: 10.1109/CAC53003.2021.9727778.

[16] E. Kokoris-Kogias, O. Voutyras, and T. Varvarigou, “TRM-SIoT: A scalable hybrid trust & reputation model for the social Internet of Things,” in *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, Institute of Electrical and Electronics Engineers Inc., Nov. 2016. doi: 10.1109/ETFA.2016.7733612.

[17] L. Atzori, A. Iera, G. Morabito, and M. Nitti, “The social internet of things (SIoT) - When social networks meet the internet of things: Concept, architecture and network characterization,” *Computer Networks*, vol. 56, no. 16, pp. 3594–3608, Nov. 2012, doi: 10.1016/j.comnet.2012.07.010.

[18] F. G. Mármol and G. M. Pérez, “TRMSim-WSN, trust and reputation models simulator for wireless sensor networks,” in *IEEE International Conference on Communications*, 2009. doi: 10.1109/ICC.2009.5199545.

[19] F. Gómez Mármol and G. Martínez Pérez, “Providing trust in wireless sensor networks using a bio-inspired technique,” *Telecommun Syst*, vol. 46, no. 2, pp. 163–180, Feb. 2011, doi: 10.1007/S11235-010-9281-7/METRICS.

[20] F. Gómez Mármol, J. G. Marín-Blázquez, and G. Martínez Pérez, “LFTM, linguistic fuzzy trust mechanism for distributed networks,” *Concurr Comput*, vol. 24, no. 17, pp. 2007–2027, Dec. 2012, doi: 10.1002/CPE.1825.

[21] F. Gómez Mármol and G. Martínez Pérez, “TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks,” *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 934–941, May 2012, doi: 10.1016/J.JNCA.2011.03.028.