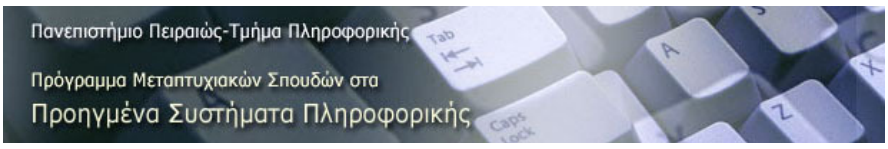
Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών
«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Μοντέλα Εμπιστοσύνης**
Ονοματεπώνυμο Φοιτητή	**Σταυρουλάκη Μαρία του Αντωνίου**
Αριθμός Μητρώου	**ΜΠΣΠ/07058**
Κατεύθυνση	**Δικτυοκεντρικά Πληροφοριακά Συστήματα**
Επιβλέπων	**Χρήστος Δουληγέρης, Καθηγητής**



Πέμπτη 10 Μαρτίου 2011

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Χρήστος Δουληγέρης Καθηγητής	Δημήτριος Βέργαδος Λέκτορας	Κοτζανικολάου Παναγιώτης Λέκτορας

Περιεχόμενα

Περίληψη

Μια έννοια η οποία έχει αποκτήσει εξαιρετική σημασία τα τελευταία χρόνια, λόγω της άνθησης των πάσης φύσεως δικτύων επικοινωνίας, είναι αυτή της εμπιστοσύνης. Καθώς τα ηλεκτρονικά μέσα επικοινωνίας πληθύνονται και γίνονται ολοένα και πιο προσβάσιμα στο ευρύ κοινό, αναπόφευκτα πολλαπλασιάζονται με εκρηκτικό τρόπο και οι συναλλαγές. Η ανάγκη διεξαγωγής αυτών των συναλλαγών με ασφαλή τρόπο, έχει αναδείξει την εμπιστοσύνη σε έννοια βαρύνουσας σημασίας, καθώς αυτή αποτελεί ένα μέσο με το οποίο μπορεί να εκτιμηθεί η αξιοπιστία ενός υποψηφίου προς συναλλαγή και η πιθανότητα της επιτυχίας μιας μελλοντικής δοσοληψίας με αυτόν.

Η έννοια της εμπιστοσύνης είναι πολύπλευρη και μπορεί να αποκτήσει διάφορες διαστάσεις, ανάλογα με το γνωστικό πλαίσιο στο οποίο εξετάζεται. Ανά περίπτωση, ο όρος εμπιστοσύνη μπορεί να αποκτήσει διάφορες εκφάνσεις, όπως η ειλικρίνεια των συναλλασσόμενων μερών, η αξιοπιστία ή η ικανότητά τους να εκπληρώσουν με επιτυχία τους όρους μιας συναλλαγής.

Προκειμένου να υλοποιηθεί ένας μηχανισμός διαχείρισης και αξιολόγησης της εμπιστοσύνης, είναι απαραίτητη η χρήση ενός μοντέλου, το οποίο τυποποιεί και ορίζει με ακρίβεια τόσο τον τρόπο με τον οποίο θεωρεί την έννοια της εμπιστοσύνης αυτή καθαυτή, όσο και τις εμπλεκόμενες διεργασίες. Τα μοντέλα αυτά και οι υλοποιήσεις τους είναι συχνά ευάλωτα σε επιθέσεις από κακόβουλες οντότητες, οι οποίες προσπαθούν να καταστρατηγήσουν τους όρους συναλλαγής με στόχο το προσωπικό τους όφελος, κάτι το οποίο αναδεικνύει ως σημαντικό παράγοντα την ευρωστία του μοντέλου.

Στην παρούσα διατριβή γίνεται προσπάθεια να αποσαφηνιστεί η έννοια της εμπιστοσύνης και να περιγραφούν τα χαρακτηριστικά της και οι σχετιζόμενες με αυτή διεργασίες. Επίσης θα παρουσιαστούν ορισμένα από τα σημαντικότερα μοντέλα εμπιστοσύνης που χρησιμοποιούνται κατά κύριο λόγο σε δίκτυα υπολογιστών και θα εξεταστεί η ευρωστία τους απέναντι στις πιο διαδεδομένες επιθέσεις.

Abstract

A concept that has lately gained prominence due to the wide development of communication networks is trust. The emergence of an increasing number of widely accessible public electronic means of communication has correspondingly been followed by a tremendous growth in the number of transactions that take place globally using such means. The need to conduct these transactions in a secure way has given importance to the notion of trust, as it can be used as a means to assess the credibility of a potential transaction party and to estimate the probability of success of a future dealing with it.

The notion of trust is multifaceted and may have various dimensions depending on the context. According to the context used, the term “trust” may focus on different aspects, such as the sincerity of the trading parties, their credibility or their capacity to successfully conclude a transaction.

In order to implement a mechanism that adequately manages and evaluates trust, it is necessary to utilize a model that formalizes and explicitly defines the concept itself, as well as the relevant processes. Such models and implementations are often susceptible to attacks from malicious entities that try to take advantage of the shortcomings of the model to gain profit. This makes robustness an important factor for every trust model.

In the present dissertation we attempt to clarify the notion of trust and to describe its characteristics as well as processes relevant to trust. We will also present selected trust models that are used mainly in computer networks and examine their robustness against the most widely known attacks.

1. Εισαγωγή

Ένα στοιχείο που χαρακτηρίζει το σύγχρονο κόσμο είναι η εκτεταμένη διασύνδεση των ανθρώπων, γνωστών ή αγνώστων, οι οποίοι συναλλάσσονται μεταξύ τους καθημερινά για διάφορους λόγους, συχνά από εξαιρετικά απομακρυσμένα σημεία, χρησιμοποιώντας ποικίλα μέσα επικοινωνίας και ιδίως το διαδίκτυο. Οι ηλεκτρονικές αγοραπωλησίες, ο διαμοιρασμός αρχείων και δεδομένων και η παροχή υπηρεσιών, είναι λίγες μόνο από τις δραστηριότητες των σημερινών χρηστών. Η μεγάλη διάδοση της χρήσης του διαδικτύου έχει αναδείξει την ανάγκη για ασφαλείς online συναλλαγές μεταξύ των χρηστών. Καθώς το μέγεθος του δικτύου είναι πολύ μεγάλο, οι πιθανότητες ένας χρήστης να έχει πραγματοποιήσει συναλλαγή με κάποιον άλλο είναι μηδαμινές. Έτσι, όταν συναλλάσσεται με κάποιο χρήστη, το πιθανότερο είναι να μην έχει εμπειρία και γνώση για τη συμπεριφορά του. Για το λόγο αυτό πρέπει να μπορεί να αποτιμήσει την αξιοπιστία του και να πάρει ανάλογες αποφάσεις.

Η εμπιστοσύνη αποτελεί τον πυρήνα τον περισσότερων σχέσεων μεταξύ των ατόμων και η ύπαρξή της είναι απαραίτητη για την ύπαρξη της συνεργασίας μεταξύ τους. Οι παράμετροι με βάση τους οποίους διαμορφώνεται η εμπιστοσύνη είναι συχνά προσωπικοί, δίνοντάς της ένα κατανεμημένο χαρακτήρα. Καθένας σχηματίζει τη δική του άποψη για κάποιο άτομο, βασιζόμενος σε κάποια χαρακτηριστικά που θεωρεί εκείνος σημαντικά. Σε αντίθεση με τα κοινωνικά δίκτυα, τα δίκτυα υπολογιστών απαιτούν η εμπιστοσύνη να έχει καθαρή φυσική έννοια, κάτι που θα βοηθήσει κατά τη μοντελοποίησή της στα μοντέλα εμπιστοσύνης.

Τα μοντέλα εμπιστοσύνης αναλαμβάνουν να τυποποιήσουν την έννοια της εμπιστοσύνης και να περιγράψουν πώς αυτή μπορεί να χρησιμοποιηθεί και να διαχειριστεί, προκειμένου να βοηθήσει κάποια οντότητα να αποφασίσει εάν κάποια άλλη είναι αξιόπιστη. Πολλά μοντέλα εμπιστοσύνης χρησιμοποιούν την έννοια της πεποίθησης για μια έμπιστη οντότητα ότι θα είναι αξιόπιστη, ειλικρινής ή ικανή να πραγματοποιήσει μια συναλλαγή. Άλλα πάλι την έννοια της φήμης, που ορίζει μια προσδοκία για τη συμπεριφορά της οντότητας βάσει παρατηρήσεων άλλων οντοτήτων ή παλαιότερης συμπεριφοράς της μέσα σε κάποιο χρονικό διάστημα. Όποια έννοια και να χρησιμοποιούν τα μοντέλα εμπιστοσύνης, οι οντότητες έχουν ως απώτερο σκοπό τη συναλλαγή, η οποία μπορεί να υπάρξει μόνο εάν οι συναλλασσόμενες οντότητες είναι αξιόπιστες. Κάτι τέτοιο όμως δεν υφίσταται πάντα.

Κάθε δίκτυο υπολογιστών, όπως και κάθε κοινωνία, ελκύει πολλές φορές κακόβουλες οντότητες, οι οποίες προσπαθούν να πραγματοποιήσουν επιθέσεις, τόσο εις βάρος των μελών του δικτύου, όσο και του μοντέλου εμπιστοσύνης γενικότερα. Πολύ συχνά θα προσπαθήσουν να αλλοιώσουν τη φήμη οντοτήτων παρουσιάζοντάς τες ως αναξιόπιστες, θα παρέχουν κακής ποιότητας υπηρεσίες, θα εκδηλώσουν αντιφατικές συμπεριφορές με στόχο να πλήξουν την αξιοπιστία άλλων οντοτήτων, θα συνωμοτήσουν με άλλες κακόβουλες οντότητες και τελικά θα προσπαθήσουν να αποφύγουν τις επιπτώσεις των πράξεών τους, αποχωρώντας από το δίκτυο την κατάλληλη στιγμή. Εν όψει της αυξανόμενης αβεβαιότητας και του κινδύνου που επιφέρουν τέτοιες επιθέσεις, οι οντότητες πρέπει να μπορούν να κρίνουν αποτελεσματικά την αξιοπιστία των υπόλοιπων οντοτήτων που βρίσκονται συνδεδεμένες στο δίκτυο και να μπορούν να αναγνωρίσουν τις κακόβουλες οντότητες, ώστε να αποφεύγουν τις συναλλαγές μαζί τους.

Στο επόμενο κεφάλαιο παρουσιάζεται η έννοια της εμπιστοσύνης, αναλύονται οι βασικές της δομές, περιγράφονται τα χαρακτηριστικά της, η σχέση της με τη συνεργασία και εισάγεται η χρήση της κατά τη λήψη αποφάσεων μεταξύ οντοτήτων σε δίκτυα υπολογιστών. Στη συνέχεια παρουσιάζονται κάποια από τα γνωστότερα μοντέλα εμπιστοσύνης που χρησιμοποιούνται σε δίκτυα υπολογιστών για να τυποποιήσουν την έννοια της εμπιστοσύνης και να μοντελοποιήσουν τις διαδικασίες που ακολουθούνται μεταξύ οντοτήτων, προκειμένου αυτές να πάρουν αποφάσεις βασιζόμενες στην αξιοπιστία και την εμπιστοσύνη προς άλλες οντότητες. Ακολουθεί η αξιολόγηση των μοντέλων αυτών και των χαρακτηριστικών τους, καθώς και ο τρόπος που αντιμετωπίζουν κάποιες συγκεκριμένες επιθέσεις ασφαλείας. Η διατριβή καταλήγει με τα συμπεράσματα, όπου παρατίθεται ένας πίνακας ποιοτικής αξιολόγησης των μοντέλων εμπιστοσύνης σε σχέση με την ανθεκτικότητά τους στις επιθέσεις που αναφέρθηκαν.

2. Η έννοια της εμπιστοσύνης

Οι περισσότερες μελέτες που έχουν γίνει κατά το παρελθόν και αφορούν στο θέμα της εμπιστοσύνης, προέρχονται από τρεις κύριους τομείς των επιστημών, την κοινωνιολογία, την ψυχολογία και τη φιλοσοφία. Ο όρος εμπιστοσύνη είναι όπως αναφέρεται στο [1] ένα πολύ πολύπλοκο και πολυδιάστατο φαινόμενο. Πρόκειται αναμφισβήτητα για ένα πολύ σημαντικό στοιχείο την καθημερινής μας ζωής. Όπως έχει ειπωθεί, χωρίς την ύπαρξη της εμπιστοσύνης η ανθρωπότητα θα υπέφερε από έλλειψη αποδοτικότητας και δυναμισμού [2], ή χειρότερα, θα ήταν πολύ δύσκολο ακόμα και να σηκωθεί κανείς όρθιος το πρωί, μιας και δεν θα μπορούσε να αντιμετωπίσει τις πολυπλοκότητες της ζωής και να εξετάσει με λογική τις προοπτικές της καθημερινής ζωής [3], με μοιραίο αποτέλεσμα την κατάρρευση της κοινωνίας [4].

Τι είναι όμως η εμπιστοσύνη; Κατά καιρούς έχουν δοθεί πολλοί ορισμοί που είχαν ως στόχο να δώσουν απάντηση σε αυτό το ερώτημα. Το γεγονός όμως αυτό αποτελεί ισχυρή ένδειξη ότι η ερώτηση δεν έχει απαντηθεί ικανοποιητικά μέχρι τώρα [5]. Όπως παρατήρησαν οι Lewicki και Bunker [6], ο καθορισμός του όρου εμπιστοσύνη στη βιβλιογραφία τείνει να επηρεάζεται από τα παραδείγματα του προσωπικού ακαδημαϊκού κλάδου του εκάστοτε ερευνητή. Για παράδειγμα, ενώ οι κοινωνιολόγοι τείνουν να θεωρούν την εμπιστοσύνη ως μια δομή στη φύση [7], [8], [9], κάποιοι ψυχολόγοι βλέπουν την εμπιστοσύνη ως ένα προσωπικό χαρακτηριστικό [10], [56]. Αντίστοιχα, οι κοινωνικοί ψυχολόγοι είναι πιθανότερο να θεωρήσουν την εμπιστοσύνη ως ένα διαπροσωπικό φαινόμενο [11], [12], ενώ οι οικονομολόγοι ως μια λογική επιλογή μηχανισμού [13]. Ο Marsh [5] θεωρεί ότι υπάρχουν αρκετοί λόγοι για την ύπαρξη των τόσο διαφορετικών απόψεων για την εμπιστοσύνη. Καταρχήν, δεδομένου ότι η εμπιστοσύνη απαντάται παντού, όλοι είναι «ειδικοί» σε αυτή και εκεί εντοπίζεται το πρόβλημα: όλοι μπορούν να ορίσουν την εμπιστοσύνη με διαφορετικό τρόπο και έτσι μπορούν να υπάρξουν πολλές διαφορετικές απόψεις γι' αυτήν. Κατά δεύτερον, όλες αυτές οι διαφορετικές απόψεις περί εμπιστοσύνης πηγάζουν από τα τόσα διαφορετικά είδη εμπιστοσύνης που υπάρχουν [9], [11] και από τους τόσους τομείς που εξετάζουν το φαινόμενο. Έτσι ο όρος εμπιστοσύνη απαντάται σε τομείς όπως η εξελικτική βιολογία [14], η κοινωνιολογία [3], η κοινωνική ψυχολογία [15], τα οικονομικά [16], η ιστορία [17] και η φιλοσοφία [4].

Ο ορισμός που έδωσε ο Deutsch το 1962 [15] φαίνεται να είναι από τους πιο αποδεκτούς μέχρι σήμερα. Σύμφωνα με τον συγγραφέα, η συμπεριφορά εμπιστοσύνης εμφανίζεται όταν ένα άτομο διακρίνει ένα αμφιλεγόμενο μονοπάτι, το αποτέλεσμα του οποίου μπορεί να είναι καλό ή κακό, και η εμφάνιση του καλού ή του κακού αποτελέσματος εξαρτάται από τις πράξεις κάποιου άλλου προσώπου. Σε αυτή την περίπτωση, το κακό αποτέλεσμα είναι περισσότερο ζημιογόνο από τα οφέλη του καλού αποτελέσματος. Εάν το πρώτο άτομο αποφασίσει να ακολουθήσει το μονοπάτι, τότε έχει κάνει μια επιλογή εμπιστοσύνης, ενώ σε διαφορετική περίπτωση θεωρείται δύσπιστο. Όπως αναφέρεται στο [5], υπάρχει διαφωνία για τον ορισμό αυτό ως προς την ιδέα ότι τα οφέλη πρέπει να είναι λιγότερα από τη ζημία που προκαλείται, αν και όπως συνεχίζει, οι Golembiewski and McConkie [2] έδωσαν έναν παρόμοιο ορισμό, ορίζοντας όμως ότι η απώλεια ή ο πόνος που επακολουθεί την ανεκπλήρωτη εμπιστοσύνη είναι μερικές φορές μεγαλύτερος από την ανταμοιβή της ευχαρίστησης της εκπληρωμένης εμπιστοσύνης. Πολλοί άλλοι ορισμοί προέρχονται από τον ορισμό του Deutsch, ο οποίος το 1973 τον επέκτεινε παρουσιάζοντας διευκρινίσεις και κατέληξε να ορίσει την εμπιστοσύνη ως πεποίθηση ότι κάποιος θα βρει αυτό που επιθυμεί από κάποιον άλλο και όχι αυτό που φοβάται [11].

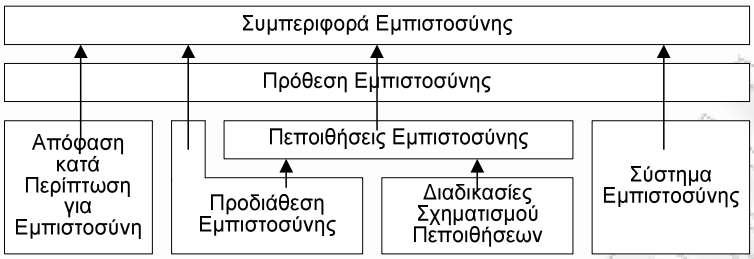
Η εμπιστοσύνη είναι ένα σύνηθες φαινόμενο. Πολλοί ερευνητές αναφέρονται στην εμπιστοσύνη ως ένα μέσο αντιμετώπισης του κινδύνου. Όπως αναφέρει και ο Luhmann [3], «πράγματι, η εμπιστοσύνη προαπαιτεί μία κατάσταση κινδύνου». Για το λόγο αυτό οι άνθρωποι προσπαθούν να απαλλαγούν από την ανάγκη να εμπιστεύονται ο ένας τον άλλο, χρησιμοποιώντας περιορισμούς και δεσμεύσεις και για τις δύο πλευρές. Σύμφωνα όμως με τους Boon και Holmes [18], η διακινδύνευση είναι αναγκαία στις σχέσεις όταν υπάρχει συνεργασία, προκειμένου να επιβεβαιώσει και να δυναμώσει την υπάρχουσα εμπιστοσύνη ή να δημιουργήσει εμπιστοσύνη εκεί όπου δεν υπήρχε. Στις περιπτώσεις όπου δεν υπάρχει τελικά συνεργασία, εμφανίζεται ο κίνδυνος της εμπιστοσύνης. Εάν η τελευταία ήταν αρχικά μεγάλη και ο κίνδυνος της απόρριψης επίσης μεγάλος, η ανυπαρξία συνεργασίας θα κατέληγε σε μεγάλη

απώλεια εμπιστοσύνης η οποία θα ήταν δύσκολο να κερδηθεί ξανά [19]. Για πολλούς ερευνητές ο κίνδυνος αυτός συνδέεται στενά με τα μεγέθη του διακρινόμενου κόστους και οφέλους μιας κατάστασης. Όσο υψηλότερο είναι το ενδεχόμενο κόστος, τόσο μεγαλύτερος είναι ο κίνδυνος, με το όφελος να δίνει σχεδόν αντίστροφο αποτέλεσμα στον κίνδυνο. Μια απλή σχέση που θα συνέδεε τα τρία μεγέθη είναι $\text{Κίνδυνος} = \text{Κόστος} / \text{Όφελος}$ [20].

Ο Marsh αναφέρει [5] ότι όταν κάποιος εμπιστεύεται κάποιον άλλο, επαφίεται στα χέρια του και το τελικό αποτέλεσμα εξαρτάται από αυτόν. Η εμπιστοσύνη περιλαμβάνει ρίσκο, αβεβαιότητα και τις πράξεις κάποιου άλλου. Έτσι, είτε το θετικό αποτέλεσμα είναι μεγαλύτερο από το αρνητικό είτε όχι, όταν επαφιέμεθα μερικώς ή ολοκληρωτικά στα χέρια άλλων, κάνουμε επιλογές εμπιστοσύνης. Ο Yamamoto αναφέρει ότι οι επιλογές αυτές βασίζονται σε ενδείξεις που πιστεύει κάποιος ή για τις οποίες είναι σίγουρος ότι κάποιος ή κάτι έχει καλές προθέσεις απέναντί του [21]. Οι επιλογές εμπιστοσύνης που κάνει κανείς βασίζονται σε υποκειμενικές απόψεις σχετικά με τον κόσμο. Έτσι, εάν η εμπιστοσύνη βασίζεται στην ατομική πεποίθηση, είναι πιθανό σε κάθε κατάσταση, διαφορετικά άτομα να τη δουν διαφορετικά [5]. Οι περισσότερες από τις επιλογές εμπιστοσύνης που γίνονται, αφορούν άλλους και περιστασιακά τους εαυτούς μας ή το περιβάλλον μας [3]. Υπό αυτή την έννοια, η εμπιστοσύνη είναι κοινωνικό φαινόμενο και υπάρχει όπου υπάρχουν και οι κοινωνίες [21]. Πράγματι, εάν η εμπιστοσύνη είναι στην πραγματικότητα μια μέθοδος για την αντιμετώπιση της ελευθερίας των άλλων [3], [22], τότε δεν μπορεί να είναι τίποτε άλλο, εκτός από κοινωνικό φαινόμενο. Σε αυτή την περίπτωση, η εμπιστοσύνη δε λειτουργεί μόνο σε προσωπικό επίπεδο, αλλά και σε κοινωνικό. Συμπερασματικά, η εμπιστοσύνη μέσα σε μια κοινωνία είναι μια αναδυόμενη ιδιότητα των συναλλαγών των ατόμων της κοινωνίας αυτής [5].

Το 1996, οι McKnight και Chervany παρουσίασαν στην εργασία τους “The meanings of trust” [23] ένα σύστημα ταξινόμησης των διαφόρων διαστάσεων που έχει η έννοια της εμπιστοσύνης και έδωσαν τους ορισμούς έξι συνδεόμενων βασικών δομών που την απαρτίζουν, οι οποίες διαμορφώνουν ένα μοντέλο. Η εργασία τους προήλθε από τη μελέτη 60 ερευνητικών άρθρων και βιβλίων από διάφορους τομείς των επιστημών, όπως η διοίκηση και οι επικοινωνίες, η κοινωνιολογία, η οικονομική και πολιτική επιστήμη, καθώς και η ψυχολογία. Αρχικά κατηγοριοποίησαν την έννοια της εμπιστοσύνης σε τέσσερις βασικούς τύπους, την απρόσωπη ή δομική, την εμπιστοσύνη που αναφέρεται στη διάθεση (dispositional trust), την προσωπική και τη διαπροσωπική εμπιστοσύνη. Η απρόσωπη εμπιστοσύνη είναι εκείνη που συναντάται στις κοινωνικές ή θεσμικές δομές μιας κατάστασης και όχι σε κάποιο άτομο ή στα προσωπικά χαρακτηριστικά των εμπλεκομένων. Αυτός ο τύπος εμπιστοσύνης είναι εκείνος που τη διαφοροποιεί από το να είναι ιδιότητα ή κατάσταση κάποιου ατόμου ή ατόμων. Η εμπιστοσύνη που αναφέρεται στη διάθεση, βασίζεται στα χαρακτηριστικά της προσωπικότητας της οντότητας που δείχνει εμπιστοσύνη και η οποία έχει μια γενική τάση να εμπιστεύεται τους άλλους στις διάφορες καταστάσεις ή έχει μια γενική πίστη στην ανθρώπινη φύση. Η προσωπική εμπιστοσύνη αναφέρεται στην περίπτωση όπου ένα άτομο εμπιστεύεται ένα άλλο, ή πολλά άτομα ή ακόμα και πράγματα σε μια συγκεκριμένη κατάσταση. Έτσι η εμπιστευόμενη οντότητα είναι το ένα άτομο, ενώ η εμπιστοσύνη απευθύνεται σε ένα άλλο πρόσωπο ή πρόσωπα. Τέλος, η διαπροσωπική εμπιστοσύνη υφίσταται όταν δύο ή περισσότερα άτομα ή ομάδες ατόμων εμπιστεύονται ο ένας τον άλλο σε μια συγκεκριμένη κατάσταση. Έτσι η εμπιστευόμενη οντότητα περιλαμβάνει τουλάχιστον δύο άτομα ή ομάδες.

Το [23] συνεχίζει παρουσιάζοντας τις έξι συνδεόμενες βασικές δομές, οι οποίες απαρτίζουν την έννοια της εμπιστοσύνης. Οι δομές αυτές είναι οι εξής: Πρόθεση Εμπιστοσύνης (Trusting Intention), Συμπεριφορά Εμπιστοσύνης (Trusting Behavior), Πεποιθήσεις Εμπιστοσύνης (Trusting Beliefs), Σύστημα Εμπιστοσύνης (System Trust), Προδιάθεση Εμπιστοσύνης (Dispositional Trust) και Απόφαση κατά Περίπτωση για Εμπιστοσύνη (Situational Decision to Trust). Στο σχήμα 1 φαίνεται πώς οι παραπάνω δομές εμπιστοσύνης συσχετίζονται μεταξύ τους. Τα βέλη αναπαριστούν σχέσεις και ενδιάμεσες σχέσεις.



Σχήμα 1: Σχέσεις μεταξύ δομών εμπιστοσύνης

Σε γενικές γραμμές, ένα σύνολο από τις σχέσεις αυτές ακολουθεί το μοτίβο της θεωρίας των Fishbein & Ajzen [24] περί αιτιολογημένης δράσης, δηλαδή οι πεποιθήσεις/συμπεριφορές (στην περίπτωσή μας οι Πεποιθήσεις Εμπιστοσύνης) οδηγούν σε προθέσεις (Πρόθεση Εμπιστοσύνης), οι οποίες γίνονται με τη σειρά τους ενδείξεις συμπεριφοράς (Συμπεριφορά Εμπιστοσύνης). Η λογική είναι απλή: όταν κάποιος έχει Πεποιθήσεις Εμπιστοσύνης για κάποιον άλλον, τότε είναι πρόθυμος να βασιστεί στο άτομο αυτό και άρα έχει Πρόθεση Εμπιστοσύνης. Εάν σκοπεύει να βασιστεί στο άτομο αυτό, τότε θα συμπεριφερθεί με τέτοιους τρόπους οι οποίοι φανερώνουν την πρόθεσή του αυτή (Συμπεριφορά Εμπιστοσύνης).

Πιο συγκεκριμένα, η δομή Πρόθεση Εμπιστοσύνης είναι ο βαθμός στον οποίο κάποιος είναι πρόθυμος να βασιστεί σε κάποιον άλλο σε μια δεδομένη κατάσταση, έχοντας ένα αίσθημα σχετικής ασφάλειας, ακόμα και αν είναι πιθανές τυχόν αρνητικές συνέπειες. Όπως φαίνεται και στο παραπάνω σχήμα, η Πρόθεση Εμπιστοσύνης βοηθάει τη δομή Συμπεριφορά Εμπιστοσύνης. Η προθυμία κάποιου να βασιστεί σε κάποιον άλλο οδηγεί πράγματι στο να βασιστεί τελικά σε αυτόν. Η Συμπεριφορά Εμπιστοσύνης είναι ο βαθμός στον οποίο κάποιος βασίζεται οικειοθελώς σε κάποιον άλλο σε μια δεδομένη κατάσταση, έχοντας ένα αίσθημα σχετικής ασφάλειας, ακόμα και αν είναι πιθανές τυχόν αρνητικές συνέπειες. Η Πρόθεση Εμπιστοσύνης βασίζεται αρχικά στις γνωστικές πεποιθήσεις του ατόμου για κάποιο άλλο άτομο. Οι Πεποιθήσεις Εμπιστοσύνης είναι ο βαθμός στον οποίο κάποιος πιστεύει (και αισθάνεται σιγουριά) ότι κάποιος άλλος είναι αξιόπιστος σε μια κατάσταση, δηλαδή είναι ικανός και πρόθυμος να ενεργήσει με βάση τα συμφέροντα του άλλου ατόμου. Το Σύστημα Εμπιστοσύνης είναι ο βαθμός στον οποίο κάποιος πιστεύει ότι βρίσκονται στη θέση τους οι σωστές απρόσωπες δομές, οι οποίες θα του επιτρέψουν να προσδοκεί μια επιτυχημένη μελλοντική προσπάθεια. Οι απρόσωπες αυτές δομές μπορεί να είναι είτε δομικές εγγυήσεις, όπως κανονισμοί, εγγυήσεις ή συμβόλαια, είτε η κανονικότητα της κατάστασης, δηλαδή η αντίληψη ότι η κατάσταση φαίνεται φυσιολογική και ομαλή ή «σε σωστή σειρά». Το Σύστημα Εμπιστοσύνης βοηθάει την Πρόθεση Εμπιστοσύνης, μιας και η ασφάλεια που παρέχει στο άτομο, το κάνει να αισθάνεται σίγουρο να βασιστεί σε κάποιο άλλο άτομο και να πάρει ρίσκα.

Η εμπιστοσύνη όμως δεν εξαρτάται πάντα από την εκάστοτε κατάσταση. Οι άνθρωποι αναπτύσσουν κατά τη διάρκεια της ζωής τους γενικευμένες προσδοκίες σχετικά με την αξιοπιστία των άλλων ανθρώπων. Έτσι η δομή Προδιάθεση Εμπιστοσύνης αναφέρεται στο βαθμό στον οποίο κάποιος έχει τη σταθερή τάση να εμπιστεύεται, ανεξαρτήτως καταστάσεων ή προσώπων. Από την άλλη, η δομή Απόφαση κατά Περίπτωση για Εμπιστοσύνη αναφέρεται στο βαθμό στον οποίο κάποιος προτίθεται να βασιστεί σε κάποιον άλλο σε μία δεδομένη κατάσταση, χωρίς να λαμβάνει υπόψη τα πιστεύω του για το άλλο άτομο, και αυτό γιατί τα οφέλη που θα αποκομίσει από την εμπιστοσύνη του στη συγκεκριμένη περίπτωση είναι πολύ περισσότερα από τα πιθανά αρνητικά αποτελέσματά της.

Πολλές φορές, αυτός τον οποίο εμπιστευόμαστε μάς απογοητεύει ή προδίδει την εμπιστοσύνη μας, οπότε είτε στο μέλλον τον εμπιστευόμαστε λιγότερο, είτε και καθόλου. Μια τέτοια προδοσία δεν είναι ευθύνη εκείνου που έδειξε εμπιστοσύνη αλλά εκείνου που τη δέχτηκε [25]. Ο Deutsch προχωράει ένα βήμα παραπέρα στο [15] προτείνοντας κάποια βασικά συμπεράσματα, τα οποία έχουν τις ρίζες τους στην ψυχολογία και τα οποία φαίνεται να ακολουθούν εκείνοι που εμφανίζουν στοιχεία εμπιστοσύνης. Μερικά από τα συμπεράσματα αυτά είναι τα εξής:

- Τα άτομα τείνουν να συμπεριφέρονται θετικά απέναντι σε πρόσωπα και γεγονότα από τα οποία αντιλαμβάνονται ότι έχουν όφελος και αρνητικά απέναντι σε αυτά από τα οποία δεν έχουν.
- Η ισχύς της τάσης αυτής σχετίζεται με το μέγεθος του οφέλους που αντιλαμβάνεται το άτομο ότι θα αποκομίσει, την αύξηση/μείωση της πιθανότητας του γεγονότος που αντιλαμβάνεται ότι θα υπάρξει εάν δράσει θετικά/αρνητικά απέναντι σε αυτό, την αντιλαμβανόμενη πιθανότητα του γεγονότος μετά από μια τέτοια θετική/αρνητική συμπεριφορά, την εσωτερική χρησιμότητα των δραστηριοτήτων που εμπλέκονται στη θετική/αρνητική συμπεριφορά και την αντιλαμβανόμενη αμεσότητα της εμφάνισης του γεγονότος.
- Τα άτομα είναι με το δικό τους τρόπο «θεωρητικοί ψυχολόγοι» και τείνουν να βγάζουν συμπεράσματα για τους άλλους.

Δεν είναι όλοι έμπιστοι και μάλιστα πολλοί είναι κακόβουλοι. Η κατανόηση της εμπιστοσύνης από κάποιον θα του έδινε δύο πλεονεκτήματα [5]:

- Θα του επέτρεπε τη θεώρηση των άλλων με βάση την εμπιστοσύνη, επιτρέποντας το σχηματισμό λογικών και αποτελεσματικών αποφάσεων σχετικά με το ποιος είναι και ποιος δεν είναι έμπιστος.
- Θα του επέτρεπε τη θεώρηση των πλευρών μιας συγκεκριμένης κατάστασης, σε σχέση ειδικά με το από ποιον να δεχτεί ή να ζητήσει βοήθεια και με ποιον να συνεργαστεί σε περίπτωση ανάγκης.

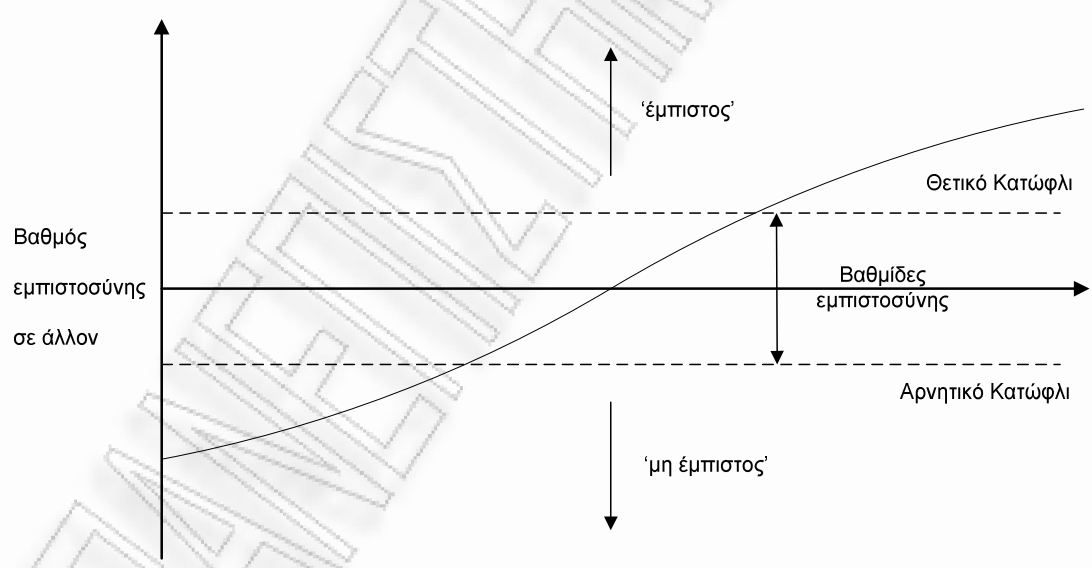
Τα άτομα σχηματίζουν γενικά ομάδες, που έχουν ως σκοπό την επίτευξη κάποιου συγκεκριμένου στόχου [26]. Τα άτομα που απαρτίζουν την ομάδα έχουν εμπιστοσύνη σε αυτή και τη θεωρούν ικανή να επιτύχει το σκοπό της. Όσο για το εάν η ομάδα εμπιστεύεται τα μέλη της, δεν υπάρχει απάντηση στο ερώτημα αυτό [5]. Σύμφωνα με τον Brown [27], η συνεργασία εντός μιας ομάδας αυξάνει τα θετικά συναισθήματα εντός αυτής όσο το αποτέλεσμα είναι θετικό, ενώ εάν το αποτέλεσμα δεν είναι το επιθυμητό, η κατάσταση είναι διαφορετική. Τα οφέλη όμως από την ύπαρξη της εμπιστοσύνης είναι πολλά. Καταρχήν, επιτυγχάνονται περισσότερα κατά την εκτέλεση εργασιών, υπάρχει μεγαλύτερη και υγιέστερη προσωπική ανάπτυξη [2], κατανόηση ή τουλάχιστον αποδοχή της πολυπλοκότητας της κοινωνίας [3], ικανότητα συνεργασίας [28] και μπορεί τελικά να γίνει καθορισμός και επιμερισμός εξουσιών.

Στην περίπτωση των ηλεκτρονικών υπολογιστών οι σχέσεις εμπιστοσύνης είναι πολύ πιο απλές από ό,τι ορίστηκε παραπάνω για τις σχέσεις μεταξύ ανθρώπων. Σύμφωνα με τους Sun et al. [29] η έννοια της εμπιστοσύνης στα δίκτυα υπολογιστών δεν εμπεριέχει τις έξι δομές που παρουσιάστηκαν στο [23]. Οι δομές Συμπεριφορά Εμπιστοσύνης, Πρόθεση Εμπιστοσύνης, Προδιάθεση Εμπιστοσύνης και Απόφαση κατά Περίπτωση για Εμπιστοσύνη δεν βρίσκουν εφαρμογή στα δίκτυα. Μόνο οι δομές Πεποίθηση Εμπιστοσύνης και Σύστημα Εμπιστοσύνης, οι οποίες δημιουργούνται μέσω μιας διαδικασίας σχηματισμού πεποίθησης και αποκαλούνται από τους συγγραφείς διαχείριση εμπιστοσύνης, σχετίζονται με την έννοια της εμπιστοσύνης που υπάρχει στα δίκτυα υπολογιστών. Το αποτέλεσμα της διαχείρισης εμπιστοσύνης παρέχεται σε διαδικασίες λήψης αποφάσεων, οι οποίες θα πάρουν τελικά αποφάσεις αξιολογώντας την εμπιστοσύνη, καθώς και άλλες συνθήκες που σχετίζονται με την εφαρμογή. Εδώ το Σύστημα Εμπιστοσύνης μπορεί να ερμηνευτεί ως ένας ειδικός τύπος πεποίθησης, όπου μια οντότητα πιστεύει ότι το δίκτυο θα λειτουργήσει όπως ακριβώς έχει σχεδιαστεί. Για το λόγο αυτό, η καταλληλότερη ερμηνεία του όρου εμπιστοσύνη για τα δίκτυα υπολογιστών είναι η πεποίθηση. Έτσι, μια οντότητα πιστεύει ότι η άλλη οντότητα θα αντιδράσει με έναν συγκεκριμένο τρόπο ή πιστεύει ότι το δίκτυο θα λειτουργήσει με έναν συγκεκριμένο τρόπο.

Η εμπιστοσύνη είναι σημαντική για πολλές αποφάσεις που αφορούν στην ασφάλεια, όπως η παραχώρηση ή η ανάκληση προνομίων και ο έλεγχος εισόδου σε ευαίσθητες πληροφορίες ή πόρους. Συχνά οι καταστάσεις περιπλέκονται, μιας και οι οντότητες καλούνται να πάρουν αποφάσεις χωρίς να έχουν άμεσες σχέσεις εμπιστοσύνης με όλες τις οντότητες των οποίων την αξιοπιστία καλούνται να αξιολογήσουν. Η εμπιστοσύνη επιτρέπει στις οντότητες να βγάζουν γενικά συμπεράσματα για καταστάσεις στις οποίες αγνοούν κάτι, είτε αυτό είναι η ύπαρξη άλλων οντοτήτων, είτε αποτελέσματα άλλων καταστάσεων, είτε γενικότερες

πληροφορίες [5]. Οι αποφάσεις που λαμβάνονται με βάση αυτά τα συμπεράσματα, δεν επιφέρουν τις περισσότερες φορές τα ίδια αποτελέσματα που θα είχε μια πλήρης ενημέρωση. Η εμπιστοσύνη όμως επιτρέπει στις οντότητες να κρίνουν τις άλλες οντότητες και το περιβάλλον τους και έτσι να γίνονται πιο εύρωστες απέναντι σε καταστάσεις αβεβαιότητας, να βοηθούνται σε τυχόν καταστάσεις συνεργασίας όταν δεν υπάρχει αρκετή πληροφόρηση και να ανταπεξέρχονται όταν οι καταστάσεις απαιτούν ταχύτατες και ακριβείς αποφάσεις. Είναι προφανές ότι η εμπιστοσύνη είναι παρούσα, ρητά ή άρρητα, οπουδήποτε χρειάζεται η συνεργασία ενός συνόλου οντοτήτων και παίζει σημαντικό ρόλο στη σύναψη και τη διατήρηση συνεργατικών σχέσεων μεταξύ οντοτήτων [5].

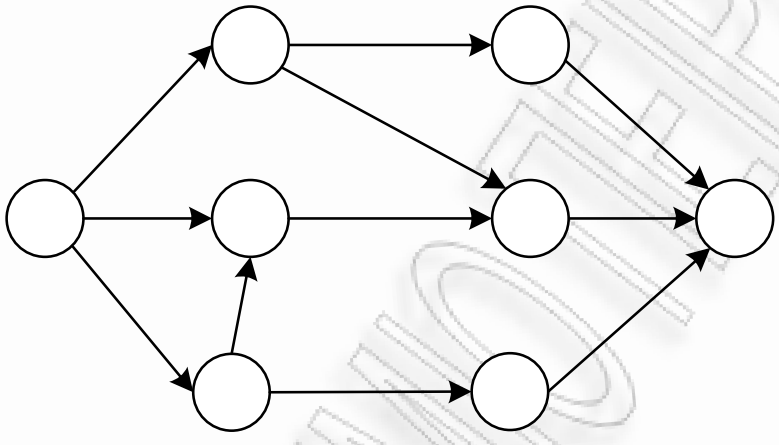
Πολλοί ερευνητές προσπάθησαν να χρησιμοποιήσουν την έννοια της εμπιστοσύνης και να την τυποποιήσουν με τέτοιο τρόπο, ώστε να μπορεί να χρησιμοποιηθεί σε μοντέλα και αλγορίθμους για την εξυπηρέτηση της συνεργασίας μεταξύ οντοτήτων σε δίκτυα υπολογιστών. Η χρήση ρητών τιμών για την εμπιστοσύνη μπορεί να θεωρηθεί πρόβλημα όπως αναφέρεται στο [5], μιας και πρόκειται για μέγεθος πολύ υποκειμενικό. Έτσι, μια τιμή εμπιστοσύνης μπορεί να σημαίνει διαφορετικό επίπεδο εμπιστοσύνης για κάποια οντότητα και διαφορετικό για κάποια άλλη. Από την άλλη, η χρήση τιμών επιτρέπει την περιεκτική και ακριβή περιγραφή συγκεκριμένων καταστάσεων στη συμπεριφορά που σχετίζεται με την εμπιστοσύνη και επιτρέπει την άμεση χρήση τυποποιήσεων. Ο Marsh [5] αναφέρει ότι η εμπιστοσύνη είναι ένα μέγεθος χωρίς μονάδες μέτρησης και κάνει χρήση της ιδέας του θετικού και του αρνητικού κατωφλίου. Μια τιμή εμπιστοσύνης πάνω από την τιμή του θετικού κατωφλίου θα σήμαινε ότι η οντότητα είναι έμπιστη, ενώ μία τιμή κάτω από την τιμή του αρνητικού κατωφλίου θα σήμαινε ότι η οντότητα είναι μη έμπιστη. Οι τιμές εμπιστοσύνης που βρίσκονται ανάμεσα στα δύο κατώφλια είναι όλα τα επίπεδα εμπιστοσύνης που μπορούν να υπάρξουν, όπως δείχνει και το σχήμα 2. Ο Gambetta βέβαια [30] αναφέρει ότι τα κατώφλια είναι διαφορετικά όχι μόνο για διαφορετικούς ανθρώπους, αλλά και για τους ίδιους ανθρώπους σε διαφορετικές καταστάσεις.



Σχήμα 2: Θετικό και αρνητικό κατώφλι εμπιστοσύνης

Υπάρχουν όμως και ερευνητές οι οποίοι μελέτησαν την ουσιαστική συμπεριφορά της εμπιστοσύνης, τον τρόπο με τον οποίο λειτουργεί βασιζόμενοι στην εμπειρία, τις προσδοκίες που υπάρχουν διαισθητικά για την εμπιστοσύνη από υποκειμενική άποψη και τα συμπεράσματα που υπάρχουν στη βιβλιογραφία και σχετίζονται με αυτή στους τομείς της κοινωνιολογίας, της ψυχολογίας και της φιλοσοφίας, και κατέληξαν σε ένα συνονθύλευμα παρατήρησης και διαίσθησης, δημιουργώντας τυποποιήσεις, οι οποίες συμπεριφέρονται με τον ίδιο τρόπο που συμπεριφέρεται και η εμπιστοσύνη. Στη συνέχεια χρησιμοποίησαν τις

τυποποιήσεις αυτές και δημιούργησαν μοντέλα που τις υιοθετούν και τα οποία προσφέρονται για χρήση σε δίκτυα υπολογιστών. Τα περισσότερα από τα μοντέλα αυτά μπορούν να αναπαρασταθούν χρησιμοποιώντας γραφήματα, όπου οι κορυφές αντιστοιχούν στις οντότητες και οι ακμές μεταξύ των κόμβων στις σχέσεις μεταξύ των οντοτήτων, οι οποίες εμφανίζονται πολλές φορές με βάρη ανάλογα το μοντέλο, για να δηλώσουν την τιμή της εμπιστοσύνης, της άποψης, κ.ά.. Τα γραφήματα αυτά είναι συνήθως κατευθυνόμενα, δεδομένου ότι όταν κάποια οντότητα εμπιστεύεται κάποια άλλη, δεν συνεπάγεται απαραίτητα ότι και η δεύτερη εμπιστεύεται την πρώτη. Ένα τέτοιο γράφημα φαίνεται στο σχήμα 3.



Σχήμα 3: Αναπαράσταση μοντέλου εμπιστοσύνης με χρήση γραφήματος

Στην επόμενη ενότητα θα έχουμε τη δυνατότητα να δούμε κάποια από τα πιο γνωστά μοντέλα εμπιστοσύνης και να παρακολουθήσουμε τον τρόπο με τον οποίο γίνεται η μοντελοποίηση, ο υπολογισμός και η χρήση της εμπιστοσύνης για την εξυπηρέτηση των στόχων των οντοτήτων του κάθε δικτύου. Τα μοντέλα αυτά επιλέχθηκαν βάσει των ιδιαίτερων χαρακτηριστικών που τα διαφοροποιούσαν από τα υπόλοιπα μοντέλα εμπιστοσύνης.

3. Μοντέλα Εμπιστοσύνης

Στα δίκτυα υπολογιστών οι οντότητες παρέχουν υπηρεσίες η μία στην άλλη, πραγματοποιούν συναλλαγές, ανταλλάσσουν αρχεία και δεδομένα, σχηματίζοντας απόψεις τόσο για τις συναλλαγές τους, όσο και για τις οντότητες με τις οποίες πραγματοποίησαν τις συναλλαγές αυτές. Οι απόψεις αυτές συλλέγονται, ανταλλάσσονται, ενημερώνονται και αξιολογούνται, προκειμένου να βοηθήσουν στην ανεύρεση πληροφοριών ή να χρησιμοποιηθούν ως συστάσεις προς άλλες οντότητες, για να διαμορφώσουν και εκείνες τη δική τους άποψη και να λάβουν αποφάσεις συνεργασίας με οντότητες που δεν γνωρίζουν. Στη συνέχεια παρουσιάζονται κάποια από τα μοντέλα που χρησιμοποιούνται για το σκοπό αυτό και περιγράφονται οι διαδικασίες και η μοντελοποίηση που εφαρμόζουν. Τα μοντέλα έχουν κατηγοριοποιηθεί προς ευκολία του αναγνώστη σύμφωνα με κάποια βασικά χαρακτηριστικά που τα διαφοροποιούν μεταξύ τους.

3.1. Χρήση μετρικών εμπιστοσύνης κατά τη λήψη αποφάσεων

Προκειμένου μια οντότητα να αλληλεπιδράσει με κάποια άλλη οντότητα, προσπαθεί να προσδιορίσει μια τιμή εμπιστοσύνης για την οντότητα αυτή, για να βεβαιωθεί ότι μια συναλλαγή μαζί της θα έχει τα επιθυμητά αποτελέσματα. Όταν η τιμή αυτή υπολογιστεί, συγκρίνεται με ένα κατώφλι εμπιστοσύνης, πάνω από το οποίο η δεύτερη οντότητα θεωρείται αξιόπιστη.

3.1.1. Το μοντέλο του Marsh

Ο Marsh [5] προσπάθησε να ενοποιήσει τις διάφορες πλευρές της εμπιστοσύνης, βασιζόμενος στις αρχές της οικονομίας, της ψυχολογίας, της κοινωνιολογίας και της φιλοσοφίας, και να τυποποιήσει τελικά, χρησιμοποιώντας μαθηματικούς τύπους, την έννοια της εμπιστοσύνης μεταξύ πρακτόρων στον τομέα της κατανεμημένης τεχνητής νοημοσύνης.

Ο Marsh ασχολήθηκε και ανέλυσε την εμπιστοσύνη που υπάρχει μεταξύ δύο πρακτόρων σε συγκεκριμένες καταστάσεις, κάτι που υφίσταται σε περιπτώσεις συνεργασίας. Αρχικά όρισε ως πεδίο ορισμού της μεταβλητής της εμπιστοσύνης το διάστημα $[-1,1)$. Στη συνέχεια όρισε ότι η εμπιστοσύνη $T_x(y,\alpha)$ ενός πράκτορα x σε έναν άλλο γνωστό του πράκτορα y σε μια κατάσταση α, εξαρτάται από την ωφέλεια $U_x(\alpha)$ την οποία αποκομίζει ο x από την κατάσταση α, καθώς και από τη σπουδαιότητα $I_x(\alpha)$ της κατάστασης αυτής για τον x, σε συνδυασμό με την εκτίμηση της γενικής εμπιστοσύνης $\widehat{T_x(y)}$ που έχει ο x στον y. Ο τύπος που περιγράφει τα παραπάνω είναι ο:

$$T_x(y,\alpha) = U_x(\alpha) \times I_x(\alpha) \times \widehat{T_x(y)}.$$

Εάν ληφθεί υπόψη και η εκτίμηση $(\widehat{T_y(x)})^x$ του x για το πόσο τον εμπιστεύεται ο πράκτορας y, τότε ο παραπάνω τύπος μετασχηματίζεται στον τύπο:

$$T_x(y,\alpha) = (U_x(\alpha) + \widehat{T_x(y)}) \times I_x(\alpha) \times (\widehat{T_y(x)})^x.$$

Ο Marsh όρισε επίσης ότι η εκτίμηση της τιμής της γενικής εμπιστοσύνης $\widehat{T_x(y)}$ ενός πράκτορα x σε έναν άλλο y, στηριζόμενος σε ένα σύνολο A παρόμοιων καταστάσεων με την κατάσταση α, τις οποίες έχει βιώσει ο x με τον y, δίνεται από τον τύπο:

$$\widehat{T_x(y)} = \frac{1}{|A|}\sum_{a\in A} T_x(y).$$

Η συνεργασία από την άλλη μεταξύ δύο πρακτόρων x και y σε μια κατάσταση, μπορεί να υπάρξει μόνο εάν η τιμή της εμπιστοσύνης του x βρίσκεται πάνω από ένα ορισμένο κατώφλι συνεργασίας. Το κατώφλι αυτό εξαρτάται μεταξύ άλλων από τον κίνδυνο που εμπεριέχει η κατάσταση, σε συνδυασμό με την ικανότητα του πράκτορα y και την εκτίμηση της γενικής εμπιστοσύνης που έχει ο x στον y. Στον παρακάτω τύπο υπολογίζεται το κατώφλι εμπιστοσύνης μεταξύ δύο πρακτόρων x και y για μια κατάσταση α:

$$Κατώφλι\_Συνεργασίας_x(\alpha) = \frac{Διακρινόμενος\_Κίνδυνος_x(\alpha)}{Διακρινόμενη\_Ικανότητα_x(y,\alpha)+\widehat{T_x(y)}} \text{ x } I_x(\alpha).$$

Στον τύπο αυτό, η μεταβλητή της εμπιστοσύνης παίζει σημαντικό ρόλο στην τελική τιμή του κατωφλίου, αφού μια πολύ χαμηλή τιμή εμπιστοσύνης θα εξασφαλίσει ότι η συνεργασία θα είναι λιγότερο πιθανή, σε σχέση με το αν η εμπιστοσύνη ήταν υψηλή. Παράλληλα, η σπουδαιότητα μιας κατάστασης παίζει επίσης σημαντικό ρόλο, μιας και όσο πιο σημαντική είναι μια κατάσταση, τόσο πιο πολύ υπάρχει ανάγκη για συνεργασία στην κατάσταση αυτή.

Ο Marsh αναφέρει ότι για τον καθορισμό του διακρινόμενου κινδύνου χρησιμοποιούνται διαφορετικές μέθοδοι και διακρίνει τρεις περιπτώσεις κατά τις οποίες ένας πράκτορας αποτιμά τους κινδύνους σε μια κατάσταση α: ο πράκτορας να μην έχει γνώση ή εμπειρία από την α, να έχει ημιτελή γνώση ή εμπειρία της α ή τέλος να έχει σημαντική εμπειρία ή γνώση της κατάστασης α. Στην πρώτη περίπτωση, η οποία εμφανίζει και τα περισσότερα προβλήματα, ο πράκτορας πρέπει να χρησιμοποιήσει την εμπιστοσύνη που έχει στον εαυτό του για να πάρει μια τέτοια απόφαση, βασιζόμενος σε παλαιότερες εμπειρίες του. Στη δεύτερη περίπτωση ο πράκτορας μπορεί να γνωρίζει τις πιθανές καταστάσεις που μπορούν να προκύψουν από την κατάσταση α, καθώς και κάποιες από τις πιθανότητες των πιθανών αυτών καταστάσεων. Εάν καμία από τις πιθανότητες αυτές δεν είναι γνωστή, τότε θα πρέπει και πάλι να εμπιστευτεί τον εαυτό του όπως και στην πρώτη περίπτωση. Τέλος, στην τρίτη περίπτωση ο πράκτορας θα αποτιμήσει απλά τους εμπλεκόμενους κινδύνους, χρησιμοποιώντας κάποια μορφή Μπεϋζιανής θεωρίας και θα καταλήξει σε κάποια χρησιμοποιήσιμη μετρική.

Όσον αφορά στη διακρινόμενη ικανότητα του πράκτορα y, ο πράκτορας x πρέπει να πάρει μια απόφαση για αυτόν, ακόμα και αν δεν τον γνωρίζει. Κάτι τέτοιο βέβαια διευκολύνεται εάν ο y ανήκει σε μια κοινωνία πρακτόρων, οι οποίοι είναι γνωστό ότι διαθέτουν συγκεκριμένες ικανότητες. Ο Marsh ορίζει τρεις επίσης περιπτώσεις για τη γνώση όσον αφορά στην ικανότητα ενός πράκτορα: ο πράκτορας να μην είναι γνωστός ούτε σε αυτή, ούτε σε άλλες παρόμοιες καταστάσεις, ο πράκτορας να είναι γνωστός αλλά όχι σε αυτή ή σε παρόμοιες καταστάσεις ή τέλος ο πράκτορας να είναι γνωστός και έμπιστος σε αυτή ή σε παρόμοιες καταστάσεις. Στην πρώτη περίπτωση, ένα πιθανό λογικό μέτρο της ικανότητας του πράκτορα y είναι η γενική διάθεση για εμπιστοσύνη T_x του πράκτορα x ο οποίος παίρνει την απόφαση, μετριασμένη από τη σπουδαιότητα της κατάστασης, όπως δείχνει και ο τύπος:

$$Διακρινόμενη\_Ικανότητα_x = T_x I_x(\alpha).$$

Στη δεύτερη περίπτωση, η γνώση του πράκτορα x περιορίζεται στην ικανότητα του y σε κάποιες καταστάσεις και μετριάζεται από το σύνολο της γενικής εμπιστοσύνης που έχει ο πράκτορας x

στον y. Ο Marsh δίνει τον επόμενο τύπο για τον υπολογισμό της διακρινόμενης ικανότητας της δεύτερης αυτής περίπτωσης:

$$Διακρινόμενη\_Ικανότητα_x(y,\alpha) = \frac{1}{|A|}\sum_{\beta \in B}((Βιωμένη\_Ικανότητα_x(y,\beta)^{t'}) \times \widehat{T_x(y)},$$

όπου το t' δηλώνει ότι η τιμή της ικανότητας έχει δοθεί μετά το τέλος της κατάστασης, ενώ το B είναι το σύνολο όλων των καταστάσεων στις οποίες οι δύο πράκτορες είχαν αλληλεπιδράσει. Είναι προφανές ότι οι καταστάσεις α και β θα είναι ανόμοιες.

Για την τρίτη περίπτωση ο Marsh εστιάζει στις παρόμοιες καταστάσεις του παρελθόντος. Με βάση τις τιμές ικανότητας που είχε ο πράκτορας σε εκείνες τις καταστάσεις, καταλήγει στον παρακάτω τύπο για τον υπολογισμό της εκτίμησης της ικανότητας για την υπό εξέταση κατάσταση:

$$Διακρινόμενη\_Ικανότητα_x(y,\alpha) = \frac{1}{|A|}\sum_{\alpha \in A}(Βιωμένη\_Ικανότητα_x(y,\alpha)^{t'}.$$

Ο Marsh χρησιμοποιεί τη μνήμη κάθε πράκτορα και την έννοια της ανταπόδοσης μιας χάρης μεταξύ δύο γνωστών πρακτόρων x και y, προκειμένου να εμβαθύνει και πιθανόν να διευκολύνει τη λήψη μιας απόφασης από τον x σε κάποια συγκεκριμένη κατάσταση. Τέλος, λαμβάνοντας υπόψη την ανταπόδοση πριν και μετά από ένα γεγονός, ο Marsh καταλήγει σε δύο συνθήκες – τύπους για την τυποποίηση της αύξησης και της μείωσης την τιμής της εμπιστοσύνης μεταξύ δύο γνωστών μεταξύ τους πρακτόρων:

Εάν $Βοήθησε(x,y,\alpha)^{t-\delta} \wedge Αποστάτησε(y,\beta)^{t}$ τότε $T_x(y)^{t+1} \ll T_x(y)^{t}$.

Εάν $Βοήθησε(x,y,\alpha)^{t-\delta} \wedge Συνεργάστηκε(y,\beta)^{t}$ τότε $T_x(y)^{t+1} \geq T_x(y)^{t}$,

δηλαδή εάν ο x βοήθησε στο παρελθόν τον y, ενώ ο y αποστάτησε τώρα που του ζητήθηκε η συνεργασία του, η εμπιστοσύνη που έχει ο x στον y θα μειωθεί κατά πολύ. Αντίθετα, εάν ο x βοήθησε στο παρελθόν τον y, και ο y ανταπέδωσε τώρα που του ζητήθηκε η συνεργασία του, η εμπιστοσύνη που έχει ο x στον y θα παραμείνει ίδια ή θα αυξηθεί κατά λίγο.

3.1.2. Το μοντέλο των Levien και Aiken

Οι Levien and Aiken ασχολήθηκαν στο [31] με το ρόλο που έχουν οι μετρικές εμπιστοσύνης στην ανθεκτικότητα των πιστοποιητικών δημοσίου κλειδιού σε επιθέσεις. Παρουσίασαν ένα αναλυτικό πλαίσιο για την κατανόηση της αποτελεσματικότητας των μετρικών αυτών ενάντια στις επιθέσεις και παρουσίασαν μια πρακτική μετρική εμπιστοσύνης η οποία βασίζεται στη ροή δικτύου (network flow).

Το μοντέλο των Levien and Aiken περιέχει δύο είδη πιστοποιητικών, το πιστοποιητικό δέσμευσης το οποίο ορίζει ότι ο εκδότης πιστεύει ότι το κλειδί k ανήκει σε έναν χρήστη n και υπογράφεται από το κλειδί του εκδότη του πιστοποιητικού, και το πιστοποιητικό εξουσιοδότησης το οποίο ορίζει ότι ο εκδότης εμπιστεύεται τα πιστοποιητικά που είναι υπογεγραμμένα από το κλειδί k και το οποίο επίσης υπογράφεται από το κλειδί του εκδότη του

πιστοποιητικού. Το μοντέλο δεν κάνει διαχωρισμό μεταξύ των διαφορετικών εκδοτών πιστοποιητικών, είτε πρόκειται για απλούς χρήστες είτε για έμπιστες τρίτες οντότητες.

Η απεικόνιση του μοντέλου γίνεται μέσω ενός κατευθυνόμενου γραφήματος, του οποίου οι κόμβοι είναι κλειδιά ή ζεύγη κλειδιού-χρήστη. Κάθε πιστοποιητικό απεικονίζεται ως ακμή-διάνυσμα το οποίο ξεκινάει από τον κόμβο κλειδί του εκδότη του πιστοποιητικού και καταλήγει στον κόμβο κλειδί που αναφέρεται μέσα σ' αυτό για το πιστοποιητικό εξουσιοδότησης, ή στον κόμβο ζεύγος κλειδιού-χρήστη που αναφέρεται μέσα σ' αυτό για το πιστοποιητικό δέσμευσης. Έτσι, οι κόμβοι ενός γραφήματος πιστοποιητικών G μπορεί να είναι είτε κόμβοι κλειδιά V_k, είτε κόμβοι στόχοι V_t, και άρα το γράφημα μπορεί να γραφεί ως (V_k U V_t, E).

Η εργασία ερευνά δύο διαφορετικούς τύπους επιθέσεων σε συστήματα πιστοποίησης. Ο πρώτος τύπος επίθεσης θεωρεί ότι ο επιτιθέμενος μπορεί να παράγει αυθαίρετα πιστοποιητικά έχοντας κλέψει τα ιδιωτικά κλειδιά των θυμάτων του, όπως για παράδειγμα έναν μυστικό κωδικό, και καλείται επίθεση κόμβου. Έτσι μπορεί να προσθέτει αυθαίρετα ακμές στο γράφημα, αναπαριστώντας πιστοποιητικά δέσμευσης ή εξουσιοδότησης. Ο δεύτερος τύπος επίθεσης είναι πολύ αποτελεσματικός ενάντια στις περισσότερες μετρικές εμπιστοσύνης και μπορεί να επιτευχθεί χωρίς την υποκλοπή μυστικών κλειδιών. Στην επίθεση αυτή, η οποία ονομάζεται επίθεση ακμής, ο επιτιθέμενος κόμβος καταφέρνει, εκμεταλλευόμενος αδυναμίες του συστήματος, να εξαπατά τους χρήστες με τα μυστικά κλειδιά και να τους πείθει να πιστοποιούν ως αξιόπιστα κλειδιά τα οποία δεν είναι. Έτσι, ο κόμβος που επιχειρεί μια τέτοια επίθεση είναι σε θέση να παράξει πιστοποιητικά εξουσιοδότησης από τα κλειδιά των χρηστών αυτών. Σε γενικές γραμμές, ένας επιτιθέμενος κόμβος είναι ικανός να καταργήσει αυθαίρετα πιστοποιητικά από οποιοδήποτε κλειδί, καθώς και να παράξει αυθαίρετα πιστοποιητικά από νεοδημιουργηθέντα κλειδιά. Το νέο γράφημα G' που προκύπτει μετά από μια επίθεση, περιέχει τουλάχιστον ένα νέο κόμβο στόχο x, ο οποίος αναπαριστά την απάτη. Στην περίπτωση της επίθεσης κόμβου, το νέο γράφημα περιέχει νέες ακμές από κόμβους που ανήκαν στο παλαιό γράφημα και οι οποίοι βρίσκονται υπό επίθεση. Κατά συνέπεια, όλες οι νέες ακμές του νέου γραφήματος προέρχονται είτε από επίθεση σε κόμβο, είτε από κάποιο νέο κόμβο. Αντίθετα, στην περίπτωση της επίθεσης ακμής, οι ακμές στο νέο γράφημα είναι πιο περιορισμένες, έτσι ώστε κανένας κόμβος υπό επίθεση να μην έχει ακμή κατευθείαν με κόμβο στόχο, αλλά μόνο με άλλο κόμβο κλειδί, δημιουργώντας έτσι μονοπάτι τουλάχιστον δύο βημάτων μέχρι τον κόμβο στόχο.

Στη συνέχεια, οι συγγραφείς παρουσίασαν μια μετρική εμπιστοσύνης, η οποία βασίζεται στις μέγιστες ροές δικτύου στο γράφημα πιστοποιητικών. Στο γράφημα αυτό θεωρούν ως s τον κόμβο πηγή και ως t τον κόμβο στόχο. Κάθε κόμβος του γραφήματος έχει αριθμό ακμών που καταλήγουν σε αυτόν ίσο με μια σταθερά d, ο αριθμός των πιστοποιητικών δηλαδή τα οποία εκδόθηκαν για αυτόν τον κόμβο-κλειδί, και κάθε κόμβος s έχει μια τιμή κατωφλίου $\theta(s)$, τέτοια ώστε να δέχεται ένα κλάσμα από όλους τους κόμβους στόχους. Σε κάθε κόμβο n του γραφήματος εκχωρείται μια χωρητικότητα (capacity):

$$C_{(s,t)}(n) = \max\left(f_s\big(dist(s,n)\big), g_t\big(dist(n,t)\big)\right),$$

όπου $dist(s,t)$ το μήκος του μικρότερου μονοπατιού από τον s μέχρι τον t. Οι συναρτήσεις f_s και g_t, οι οποίες είναι σχεδιασμένες να αντιστέκονται στις επιθέσεις κόμβου, αλλά δεν είναι πολύ αποτελεσματικές στις επιθέσεις ακμής, ορίζονται ως:

$$f_s(l) = \begin{cases} \max\left(\frac{1}{d}, \frac{1}{|succ(s)|}\right) & \alpha\nu\ l = 1 \\ \frac{1}{d} & \alpha\nu\ l \geq 2 \end{cases},$$

$$g_t(l) = \frac{1}{d}$$

Ως $succ(s)$ ορίζεται η ομάδα των διαδόχων του s. Οι τιμές αυτές είναι υπολογισμένες ώστε να καταλήγουν σε μέγιστες ροές δικτύου μεγέθους 1 για τα περισσότερα ζεύγη κόμβων πηγής – στόχου του γραφήματος. Οι τιμές αυτές για τις συναρτήσεις f_s και g_t εγγυώνται ότι ο αριθμός των κόμβων με χωρητικότητα $C(n) > 1/d$ δεν ξεπερνούν το d.

Οι Levien και Aiken υποστηρίζουν ότι αυξάνοντας τη χωρητικότητα των κόμβων που βρίσκονται κοντά στον κόμβο πηγή, αυξάνεται και η ασφάλεια. Σε μια τυχαία επίθεση, καθώς το γράφημα μεγαλώνει, η πιθανότητα επιλογής κόμβων οι οποίοι θα βρίσκονται όλοι κοντά στον κόμβο πηγή, είναι αρκετά μικρή, ενώ ακόμα και μια επιλεγμένη επίθεση προς κόμβους που θα είναι κοντά σε κάποιον κόμβο πηγή, δεν θα είναι γενικά αποτελεσματική όσον αφορά άλλους κόμβους πηγές. Τελικά, σε ένα καλά συνδεδεμένο γράφημα κόμβων με σταθερές χωρητικότητες για τον καθένα, η μετρική εμπιστοσύνης που περιγράφηκε, περιορίζεται από το ελάχιστο του συνόλου των ακμών που ξεκινούν από τον κόμβο πηγή και του συνόλου των ακμών που καταλήγουν στον κόμβο στόχο, ενώ θέτοντας αυξημένες χωρητικότητες στους κόμβους που βρίσκονται κοντά στην πηγή, η μετρική περιορίζεται μόνο από τον αριθμό ακμών που καταλήγουν στον κόμβο στόχο.

Στη συνέχεια, ορίζονται οι συναρτήσεις f_s και g_t ώστε η μετρική ροής δικτύου να ανταπεξέρχεται στις επιθέσεις ακμής:

$$f_s(l) = \begin{cases} \max\left(\frac{1}{d}, \frac{1}{|succ(s)|}\right) & \alpha\nu\ l = 1 \\ \max\left(\frac{1}{ad^2}, \frac{1}{|succ^2(s)|}\right) & \alpha\nu\ l = 2 \\ \frac{1}{ad^2} & \alpha\nu\ l \geq 3 \end{cases},$$

$$g_t(l) = \begin{cases} \frac{1}{d} & \alpha\nu\ l = 1 \\ \frac{1}{ad^2} & \alpha\nu\ l \geq 2 \end{cases}$$

Και σε αυτή την περίπτωση, οι τιμές των συναρτήσεων αναμένεται να καταλήγουν σε μέγιστες ροές δικτύου μεγέθους 1 για τα περισσότερα ζεύγη κόμβων πηγής – στόχου του γραφήματος. Το μέγεθος a είναι μια σταθερά, η οποία απεικονίζει το ποσοστό διαμοίρασης των κλειδιών και παίρνει τιμές μέσα στο διάστημα $[0{,}5..1]$. Για γραφήματα πιστοποιητικών που προκύπτουν στην πράξη, μία τιμή για το μέγεθος a μέσα στο διάστημα αυτό, οδηγεί σε υψηλά ποσοστά αποδοχής, ενώ για τυχαία γραφήματα το a προσεγγίζει τη μονάδα.

Ο υπολογισμός της μετρικής εμπιστοσύνης καταλήγει σε έναν πραγματικό αριθμό, ο οποίος απεικονίζει το βαθμό στον οποίο ένας κόμβος s του συνόλου V_k πρέπει να εμπιστεύεται έναν κόμβο στόχο t του συνόλου V_t. Ο κόμβος όμως πηγή s δεν χρησιμοποιεί απευθείας την πραγματική τιμή, αλλά απλώς τη συγκρίνει με ένα κατώφλι $\theta(s)$ που είναι ορισμένο για τον κόμβο αυτό, προκειμένου να αποφασίσει εάν ο κόμβος στόχος t είναι αξιόπιστος.

3.2. Χρήση μετρικών εμπιστοσύνης στη διαδικασία ταυτοποίησης

Πιστοποιητικά δημοσίου κλειδιού, ψηφιακές υπογραφές και συναρτήσεις κατακερματισμού χρησιμοποιούνται για διάφορους λόγους, μεταξύ των οποίων για την εξασφάλιση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων, για την επιβεβαίωση ή και την προστασία της ταυτότητας κάποιου χρήστη, για την προστασία της επικοινωνίας μεταξύ δύο χρηστών ή και για την εξασφάλιση της αξιοπιστίας κάποιου από αυτούς. Προκειμένου να αποφευχθούν περιπτώσεις ψευδών πιστοποιητικών, έχουν προταθεί κάποια μοντέλα εμπιστοσύνης, τα οποία επιτρέπουν στους χρήστες να αξιολογήσουν την αυθεντικότητα των παραπάνω πιστοποιητικών.

3.2.1. Το μοντέλο PGP (Pretty Good Privacy)

Το PGP (Pretty Good Privacy) δημιουργήθηκε αρχικά για την κρυπτογράφηση μηνυμάτων ηλεκτρονικού ταχυδρομείου, χρησιμοποιώντας κρυπτογράφηση δημοσίου ή συμβατικού κλειδιού [32], και παρέχοντας στο χρήστη μυστικότητα, πιστοποίηση και ευκολία. Στη συνέχεια χρησιμοποιήθηκε για την κρυπτογράφηση τοπικών αρχείων. Αποτελούσε όπως έχει λεχθεί ένα εργαλείο παροχής κρυπτογράφησης για τις μάζες [33]. Η απουσία ασφαλών καναλιών για την ανταλλαγή κλειδιών μεταξύ των χρηστών, έκανε το PGP ιδιαίτερα ευέλικτο. Το PGP δε χρησιμοποιεί κάποια κεντρική αρχή διαχείρισης πιστοποιητικών, αλλά οι χρήστες υπογράφουν ο ένας το κλειδί του άλλου, δημιουργώντας έτσι ένα δίκτυο από δημόσια κλειδιά, τα οποία είναι συνδεδεμένα μεταξύ τους μέσω των υπογραφών αυτών.

Χρησιμοποιώντας τη συμβατική κρυπτογράφηση, το PGP παράγει αρχικά ένα τυχαίο κλειδί συνόδου και κρυπτογραφεί με αυτό το κείμενο προς αποστολή. Ακολουθεί η κρυπτογράφηση του κλειδιού αυτού, χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη και μαζί με το κρυπτογραφημένο κείμενο, αποστέλλονται σε αυτόν. Ο παραλήπτης ανακτά το κλειδί συνόδου, χρησιμοποιώντας το ιδιωτικό του κλειδί και με αυτό αποκρυπτογραφεί τελικά το απεσταλμένο κείμενο. Κάθε χρήστης διαθέτει τα πιστοποιητικά δημοσίου και ιδιωτικού του κλειδιού, καθένα από τα οποία έχει το δικό του αναγνωριστικό κλειδιού. Σε κάθε πιστοποιητικό περιέχεται εκτός από το κλειδί για το οποίο δημιουργήθηκε, το αναγνωριστικό του χρήστη στον οποίο ανήκουν, το οποίο είναι συνήθως η διεύθυνση ηλεκτρονικού ταχυδρομείου του, και μια χρονική σφραγίδα, η οποία δείχνει την ημερομηνία δημιουργίας του κλειδιού. Κάθε χρήστης διατηρεί επιπλέον μια λίστα, τη λεγόμενη keyring, η οποία περιέχει όλα τα δημόσια κλειδιά που διαθέτει, μαζί τα αναγνωριστικά των χρηστών στους οποίους ανήκει το καθένα και η οποία υπογράφεται με το ιδιωτικό του κλειδί για λόγους ασφαλείας.

Κάθε χρήστης A, ο οποίος εμπιστεύεται κάποιον άλλο χρήστη B, μπορεί να πιστοποιήσει τη γνησιότητα του δημοσίου κλειδιού του, υπογράφοντάς το με το ιδιωτικό του κλειδί και δημιουργώντας έτσι υπογεγραμμένα πιστοποιητικά δημοσίου κλειδιού. Κάθε χρήστης Γ, ο οποίος διαθέτει το πραγματικό δημόσιο κλειδί του χρήστη A και άρα τον εμπιστεύεται, είναι σε θέση να διαπιστώσει, όταν του στείλει ο χρήστης B το υπογεγραμμένο πιστοποιητικό του, ότι η ηλεκτρονική υπογραφή προέρχεται πράγματι από τον A και άρα να εμπιστευτεί και εκείνος το δημόσιο κλειδί του χρήστη B. Με αυτό τον τρόπο, ο χρήστης A συστήνει το δημόσιο κλειδί του χρήστη B σε έναν τρίτο χρήστη Γ ως αυθεντικό.

Το PGP επιτρέπει σε κάθε χρήστη να εκχωρεί και να διατηρεί ως εμπιστευτικό, ένα επίπεδο αξιοπιστίας σε καθένα από τα δημόσια κλειδιά που εισάγει στο keyring του, δείγμα της εμπιστοσύνης του στον ιδιοκτήτη του δημοσίου αυτού κλειδιού για να πιστοποιεί την αυθεντικότητα άλλων δημοσίων κλειδιών. Έτσι, ένα δημόσιο κλειδί μπορεί να χαρακτηρίζεται ως άγνωστο, μη έμπιστο, μερικώς έμπιστο ή απολύτως έμπιστο. Το PGP μπορεί στη συνέχεια να υπολογίζει την εγκυρότητα ενός νέου δημοσίου κλειδιού, με βάση τα επίπεδα εμπιστοσύνης που διαθέτει ο χρήστης για τα δημόσια κλειδιά που υπογράφουν το λαμβανόμενο υπογεγραμμένο πιστοποιητικό δημοσίου κλειδιού, καθώς και συγκεκριμένους κανόνες οριζόμενους από αυτόν, όπως για παράδειγμα αποδοχή ως έγκυρο το πιστοποιητικό δημοσίου κλειδιού, εάν είναι υπογεγραμμένο από τουλάχιστον δύο μερικώς έμπιστα δημόσια κλειδιά. Με τον τρόπο αυτό, κάθε χρήστης συλλέγει δημόσια κλειδιά και ορίζει χρήστες που εμπιστεύεται ως πιστοποιητές

(certifiers), υπογράφει ο ίδιος άλλα πιστοποιητικά δημοσίου κλειδιού και τελικά δημιουργείται ένα δίκτυο υπογεγραμμένων πιστοποιητικών, των οποίων οι παραλήπτες εμπιστεύονται τουλάχιστον έναν από τους πιστοποιητές.

3.2.2. Το μοντέλο του Maurer

Το 1996, ο U. Maurer [34] παρουσίασε ένα ντετερμινιστικό και πιθανοτικό μοντέλο για την άποψη που έχει ένας χρήστης για την Υποδομή Δημοσίου Κλειδιού (PKI). Χάρη στη δομή αυτή ένας χρήστης A μπορεί να αποκτήσει το δημόσιο κλειδί ενός χρήστη B, συνοδευόμενο από πληροφορίες σχετικά με την αυθεντικότητά του, ενώ ένας άλλος χρήστης μπορεί να πιστοποιήσει το δημόσιο κλειδί κάποιου άλλου χρήστη ή να δώσει συστάσεις. Το μοντέλο του Maurer ασχολείται με τις διαδικασίες που μπορεί να ακολουθήσει κατά τη γνώμη του ένας χρήστης, προκειμένου να βγάλει συμπεράσματα από τις πληροφορίες που έχει ανακτήσει από τη δομή δημοσίου κλειδιού.

Σύμφωνα με το μοντέλο αυτό, ένα πιστοποιητικό δημοσίου κλειδιού το οποίο έχει εκδοθεί από κάποια τρίτη οντότητα για κάποιο χρήστη B, δηλώνοντας ότι ένα συγκεκριμένο δημόσιο κλειδί ανήκει σε αυτόν, μπορεί να χρησιμοποιηθεί από έναν χρήστη A, μόνο εάν γνωρίζει το δημόσιο κλειδί της τρίτης οντότητας – για να επαληθεύσει το πιστοποιητικό – και είναι βέβαιος ότι είναι αυθεντικό, ενώ συγχρόνως την εμπιστεύεται ότι είναι ειλικρινής και πιστοποιεί σωστά τον ιδιοκτήτη ενός δημοσίου κλειδιού πριν να το υπογράψει. Στην περίπτωση που ο χρήστης A δεν γνωρίζει το δημόσιο κλειδί της τρίτης οντότητας, μπορεί να χρησιμοποιήσει ένα πιστοποιητικό για την οντότητα αυτή, το οποίο έχει εκδώσει κάποια άλλη οντότητα. Η διαδικασία αυτή μπορεί να επαναληφθεί, σχηματίζοντας μια αλυσίδα πιστοποιητικών, μόνο εάν ο χρήστης A εμπιστεύεται κάθε οντότητα που έχει μεσολαβήσει στην αλυσίδα μέχρι το χρήστη B.

Κάθε χρήστης του μοντέλου έχει μια άποψη, βάσει της οποίας βγάζει συμπεράσματα για την αυθεντικότητα των δημόσιων κλειδιών των άλλων χρηστών, καθώς και για την αξιοπιστία των ίδιων των χρηστών. Κάθε άποψη αποτελείται από δηλώσεις για το ποια κλειδιά θεωρεί αρχικά ο χρήστης αυθεντικά και ποιους χρήστες θεωρεί αρχικά αξιόπιστους, καθώς και έναν αριθμό από πιστοποιητικά και συστάσεις, τα οποία έχουν αποκτηθεί από την Υποδομή Δημοσίου Κλειδιού. Όπως επισημαίνει ο συγγραφέας, οι συστάσεις είναι πιο πολύπλοκες από τα πιστοποιητικά. Υπάρχουν διάφορα επίπεδα εμπιστοσύνης και συστάσεων στα πλαίσια της πιστοποίησης δημοσίου κλειδιού. Μία σύσταση πρώτου επιπέδου προορίζεται για κάποια οντότητα, η οποία είναι αξιόπιστη στο να πιστοποιήσει δημόσια κλειδιά, ενώ μία σύσταση δευτέρου επιπέδου προορίζεται για κάποια οντότητα, η οποία είναι αξιόπιστη στο να συστήσει άλλες οντότητες για πιστοποίηση. Γενικά, μια σύσταση επιπέδου i αναφέρεται σε μια οντότητα, όταν αυτή είναι αξιόπιστη για να δώσει συστάσεις επιπέδου $i - 1$. Με την ίδια λογική, κάθε πιστοποιητικό μπορεί να θεωρηθεί ως σύσταση μηδενικού επιπέδου. Ενώ όμως μία οντότητα μπορεί να συστήσει μια άλλη οντότητα, ακόμα και αν δεν γνωρίζει το δημόσιο κλειδί της, ένα πιστοποιητικό μπορεί να εκδοθεί μόνο εάν ο χρήστης διαθέτει ένα αυθεντικό αντίγραφο του δημοσίου κλειδιού το οποίο θέλει να πιστοποιήσει.

Η αρχική άποψη $View_A$ ενός χρήστη είναι το σύνολο των αξιωμάτων, δηλαδή οι δηλώσεις, τα πιστοποιητικά και οι συστάσεις που θεωρεί αρχικά ως αληθή. Κάθε δήλωση μπορεί να πάρει μία από τις παρακάτω τέσσερεις μορφές:

- αυθεντικότητα δημοσίου κλειδιού $Aut_{A,X}$: δηλώνει την πίστη του χρήστη A για την αυθεντικότητα ενός συγκεκριμένου δημοσίου κλειδιού P_X που ανήκει στην οντότητα X.
- εμπιστοσύνη $Trust_{A,X,1}$: δηλώνει την πίστη του χρήστη A για την αξιοπιστία μιας συγκεκριμένης οντότητας X στο να εκδίδει πιστοποιητικά, ενώ η άποψή του για την αξιοπιστία της X να δίνει συστάσεις επιπέδου $i - 1$ ορίζεται ως $Trust_{A,X,i}$.

- πιστοποιητικό $Cert_{X,Y}$: δηλώνει ότι ο χρήστης A διαθέτει ένα πιστοποιητικό για το δημόσιο κλειδί της οντότητας Y, το οποίο έχει εκδοθεί και υπογραφεί από την οντότητα X.
- σύσταση $Rec_{X,Y,i}$: δηλώνει ότι ο χρήστης A διαθέτει μία σύσταση επιπέδου i για την οντότητα Y, η οποία έχει εκδοθεί και υπογραφεί από την οντότητα X.

Μια άκυρη δήλωση δεν είναι απαραίτητα λάθος, αλλά μπορεί απλά ο χρήστης να μην έχει αποδείξεις γι' αυτή. Μία δήλωση μπορεί να είναι έγκυρη κατά την άποψη κάποιου χρήστη, αν και μόνο εάν περιέχεται στην αρχική άποψή του ή εάν μπορεί να προκύψει από τους δύο παρακάτω κανόνες εξαγωγής συμπερασμάτων, με τη βοήθεια των οποίων προκύπτουν νέες δηλώσεις:

$$\forall\, X, Y: \quad Aut_{A,X}, Trust_{A,X,1}, Cert_{X,Y} \vdash Aut_{A,Y},$$

και

$$\forall\, X, Y, i \geq 1: \quad Aut_{A,X}, Trust_{A,X,i+1}, Rec_{X,Y,i} \vdash Trust_{A,Y,i}.$$

Σύμφωνα με τον πρώτο κανόνα, ένας χρήστης A μπορεί να αντλήσει την αυθεντικότητα ενός πιστοποιημένου δημόσιου κλειδιού ενός άλλου χρήστη Y, εάν υπάρχει μια οντότητα X, η οποία διαθέτει το πιστοποιημένο δημόσιο κλειδί του Y και για την οποία ο A μπορεί να αντλήσει την αυθεντικότητα του δημόσιου κλειδιού της και να της έχει εμπιστοσύνη επιπέδου 1. Επιπλέον, σύμφωνα με τον δεύτερο κανόνα, εάν ένας χρήστης A έχει εμπιστοσύνη σε μια οντότητα X επιπέδου τουλάχιστον 2, τότε μπορεί να δεχτεί από αυτή μία σύσταση επιπέδου κατά 1 μικρότερο για μία άλλη οντότητα Y, αν και μόνο αν θεωρεί ότι διαθέτει το αυθεντικό δημόσιο κλειδί της X. Τέλος, ο συγγραφέας του [34] θεωρεί τη συνεπαγωγή της εμπιστοσύνης και των συστάσεων για τα χαμηλότερα επίπεδα όταν αυτές υπάρχουν, για κάποιο ανώτερο επίπεδο.

Το δίκτυο των πιστοποιητικών, της εμπιστοσύνης και των συστάσεων που διαθέτει κάθε οντότητα, απεικονίζονται σε ένα κατευθυνόμενο γράφημα, του οποίου κορυφές είναι οι οντότητες, ενώ οι ακμές οι δηλώσεις. Η αυθεντικότητα και τα πιστοποιητικά αναπαριστώνται με συμπαγείς ακμές, ενώ η εμπιστοσύνη και οι συστάσεις με διακεκομμένες ακμές. Τα επίπεδα σύστασης αναγράφονται σε καθεμία από τις διακεκομμένες ακμές.

Όπως αναφέρεται στο μοντέλο, εάν ένας χρήστης A δε διαθέτει στοιχεία για την αυθεντικότητα του δημοσίου κλειδιού κάποιου κόμβου B και δεν μπορεί να βγάλει συμπεράσματα για αυτήν, μπορεί να μεγαλώσει την αρχική του άποψη, ζητώντας περισσότερα πιστοποιητικά και συστάσεις από την Υποδομή Δημοσίου Κλειδιού. Έτσι η αυθεντικότητα του δημοσίου κλειδιού του κόμβου B μπορεί να προκύψει, εάν ο A αποκτήσει μια πλήρη αλυσίδα πιστοποιητικών από αυτόν μέχρι τον B και εμπιστεύεται κάθε ενδιάμεσο κόμβο ότι μπορεί να δώσει μια πιστοποίηση. Σε καμία όμως περίπτωση, όπως αναφέρεται, δεν θα πρέπει μια οντότητα να πιστοποιεί δημόσια κλειδιά, των οποίων η αυθεντικότητα έχει προκύψει μέσω του μοντέλου, και αυτό γιατί μπορεί να δημιουργήσει ανεπιθύμητα αποτελέσματα σε άλλες οντότητες, εάν οι πολιτικές τους δεν είναι από πριν γνωστές.

Όπως αναφέρεται στο [34], καμία διαδικασία αυθεντικοποίησης δεν είναι τέλεια και καμία οντότητα δεν είναι απόλυτα αξιόπιστη. Για το λόγο αυτό, είναι λογικό να χρησιμοποιούνται οι τεχνικές της επιβεβαίωσης πολλών διαφορετικών αλυσίδων πιστοποιητικών για το ίδιο δημόσιο κλειδί, προκειμένου να αυξηθεί η βεβαιότητα της αυθεντικότητας ενός δημοσίου κλειδιού, και του συνδυασμού πολλών ανεξάρτητων συστάσεων για την απόκτηση ισχυρότερης σύστασης. Προκειμένου όμως να μπορούν να συνδυαστούν και να αξιοποιηθούν πολλά ανεξάρτητα μονοπάτια πιστοποίησης ή συστάσεις, είναι απαραίτητη η μέτρηση της βεβαιότητας. Έτσι ο Maurer συνεχίζει, εισάγοντας στο μοντέλο την έννοια της βεβαιότητας της ισχύος μιας δήλωσης και τη μέτρησή της σε μια συνεχή κλίματα του διαστήματος $[0, 1]$, όπου η κάθε τιμή μεταφράζεται ως η πιθανότητα η δήλωση αυτή να είναι ορθή. Έτσι το μοντέλο ορίζει στη θέση της αρχικής άποψης μιας οντότητας, μια κατανομή πιθανότητας για ένα πεπερασμένο σύνολο

πιθανών αρχικών απόψεων και η τιμή βεβαιότητας μιας δήλωσης ορίζεται ως η πιθανότητα να προκύψει από την αρχική άποψη.

Ο συγγραφέας ορίζει στη συνέχεια την παράμετρο βεβαιότητας $p(S)$ την οποία δίνει αρχικά ο χρήστης σε μία δήλωση S, η οποία ανήκει σε ένα υποσύνολο δηλώσεων της αρχικής του άποψης. Η τιμή βεβαιότητας $conf(S)$ της δήλωσης αυτής ισούται με την αρχική παράμετρο βεβαιότητας $p(S)$, εάν από το υποσύνολο των δηλώσεων στο οποίο ανήκει η δήλωση S δεν μπορούν να προκύψουν άλλες δηλώσεις, ενώ σε αντίθετη περίπτωση ισούται με το άθροισμα της $p(S)$ και της συνολικής πιθανότητας όλων των υποσυνόλων των δηλώσεων από τα οποία μπορεί να προκύψει η δήλωση S.

Με τη βοήθεια της παραμέτρου $p(S)$ ορίζεται τέλος η πιθανότητα ένα συγκεκριμένο υποσύνολο δηλώσεων V, από το οποίο μπορεί να προκύψει η δήλωση $Aut_{A,X}$, να ανήκει στην αρχική άποψη του χρήστη. Εάν στο υποσύνολο αυτό δεν υπάρχουν δηλώσεις εμπιστοσύνης και συστάσεις επιπέδου μεγαλύτερο από 1, τότε η παραπάνω πιθανότητα ισούται με το γινόμενο των παραμέτρων βεβαιότητας $p(S)$ των δηλώσεων που ανήκουν στο σύνολο V. Εάν όμως υπάρχουν δηλώσεις εμπιστοσύνης και συστάσεις οι οποίες προκύπτουν από αντίστοιχες δηλώσεις μεγαλύτερου επιπέδου, τότε η παραπάνω πιθανότητα υπολογίζεται με τον ίδιο τρόπο, αφού πρώτα αφαιρεθούν από το σύνολο V οι δηλώσεις αυτές και παραμείνουν μόνο οι δηλώσεις εμπιστοσύνης και οι συστάσεις του μεγαλύτερου επιπέδου.

3.2.3. Το μοντέλο των Reiter και Stubblebine

Στο [35] οι συγγραφείς, αναλύοντας διάφορες μετρικές που συνάντησαν στη βιβλιογραφία, προτείνουν ένα σύνολο κανόνων για τον σχεδιασμό μετρικών, οι οποίες θα αποτιμούν τη βεβαιότητα ενός συνόλου μονοπατιών, μιας και αντιλαμβάνονται ότι ο προσδιορισμός του ιδιοκτήτη ενός δημοσίου κλειδιού ή το ανάποδο, αποτελεί το βασικό συστατικό για την εκτέλεση ασφαλών συναλλαγών σε κάθε μεγάλης κλίμακας ανοιχτό σύστημα. Έτσι, καταλήγουν στη σύνταξη τριών γενικών κατηγοριών κανόνων, τους οποίους πρέπει να ικανοποιούν όλες οι μετρικές οι οποίες θα αποτιμούν τη βεβαιότητα ενός συνόλου μονοπατιών. Οι τρεις κατηγορίες αφορούν στη σημασία των αποτελεσμάτων μιας μετρικής, στην ευαισθησία της απέναντι στην κακή συμπεριφορά των οντοτήτων και, τέλος, στην πρακτική αποτελεσματικότητά της. Οι κανόνες που εμπίπτουν σε καθεμία από αυτές, φαίνονται παρακάτω.

Σημασία

1. Το μοντέλο στο οποίο εφαρμόζεται μια μετρική δεν πρέπει να απαιτεί ο χρήστης να βγάζει συμπεράσματα για δεσμούς μεταξύ κλειδιών και των ιδιοκτητών τους πριν την εφαρμογή της μετρικής, αλλά πρέπει να χρησιμοποιεί τη μετρική για την εξαγωγή τέτοιων συμπερασμάτων.

2. Η σημασία των παραμέτρων του μοντέλου πρέπει να είναι σαφής και ειδικότερα εκείνη των πιθανοτήτων και των τιμών εμπιστοσύνης στα μοντέλα που τα χρησιμοποιούν.

3. Μία μετρική πρέπει να λαμβάνει υπόψη της όσο το δυνατόν περισσότερες πληροφορίες, οι οποίες είναι σχετικές με την απόφαση εξουσιοδότησης που προσπαθεί να πάρει ο χρήστης.

4. Μία μετρική πρέπει να συμβουλεύεται το χρήστη για κάθε απόφαση που σχετίζεται με πιστοποίηση και η οποία δεν μπορεί να αυτοματοποιηθεί επακριβώς. Μια απόφαση η οποία θα μπορούσε να επηρεάσει την πιστοποίηση, θα πρέπει να αποκρυβεί από το χρήστη, μόνο εφόσον μπορεί να ληφθεί χρησιμοποιώντας σαφείς, καλά τεκμηριωμένους και διαισθητικούς κανόνες.

5. Το αποτέλεσμα μιας μετρικής πρέπει να είναι διαισθητικό, δηλαδή θα πρέπει να μπορεί να αποδοθεί η σημασία του, χρησιμοποιώντας μια απλή πρόταση φυσικής γλώσσας.

Ευαισθησία

6. Μια μετρική πρέπει να σχεδιάζεται με τρόπο, ώστε να είναι ανθεκτική σε χειρισμούς του μοντέλου από οντότητες με ανάρμοστη συμπεριφορά, ενώ η ευαισθησία της σε μορφές ανάρμοστης συμπεριφοράς πρέπει να είναι σαφής.

Αποτελεσματικότητα

7. Μια μετρική πρέπει να μπορεί να υπολογιστεί αποτελεσματικά.

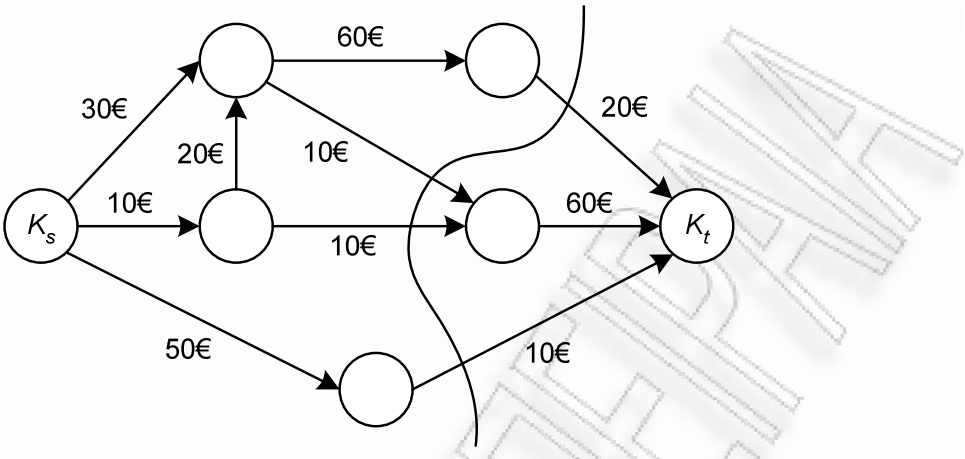
8. Το αποτέλεσμα μιας μετρικής για τμηματικές (μερικές) πληροφορίες πρέπει να βγάζει νόημα.

Οι Reiter και Stubblebine χρησιμοποιούν ένα μοντέλο, προκειμένου να δείξουν ότι οι υπόλοιπες μετρικές της βιβλιογραφίας παρουσιάζουν προβλήματα ως προς τους παραπάνω κανόνες, τα οποία έχουν δυσμενείς συνέπειες στην πιστοποίηση των χρηστών. Στο μοντέλο αυτό, ο χρήστης εντοπίζει ένα μονοπάτι από πηγές πιστοποίησης, στο οποίο μπορεί να πιστοποιήσει την πρώτη πηγή, ενώ κάθε πηγή μπορεί να πιστοποιήσει την επόμενη πηγή του μονοπατιού. Η τελική πηγή του μονοπατιού είναι τελικά το άτομο ή το κλειδί για το οποίο ενδιαφέρεται ο χρήστης. Εάν ο χρήστης εμπιστεύεται κάθε πηγή πιστοποίησης του μονοπατιού, τότε μπορεί να εξασφαλιστεί μια σωστή σύνδεση μεταξύ ονόματος και κλειδιού.

Οι συγγραφείς καταλήγουν να προτείνουν τη χρήση μιας μετρικής, η οποία βασίζεται στην έννοια της ασφάλειας για τις συνδέσεις μεταξύ ονομάτων και κλειδιών. Το μοντέλο που χρησιμοποιούν είναι ένα κατευθυνόμενο γράφημα, του οποίου οι κόμβοι είναι δημόσια κλειδιά και μια ακμή μεταξύ δύο κόμβων K_1 και K_2 υπάρχει μόνο εφόσον ο χρήστης διαθέτει ένα πιστοποιητικό, το οποίο προσδιορίζει χαρακτηριστικά στο K_2 και του οποίου η υπογραφή μπορεί να πιστοποιηθεί χρησιμοποιώντας το K_1. Κάθε ακμή έχει ως ετικέτα τα χαρακτηριστικά που περιέχονται στο πιστοποιητικό που αναπαριστά η ακμή αυτή, καθώς και μια αριθμητική τιμή, η οποία εκφράζει το ποσό των χρημάτων για το οποίο ο ιδιοκτήτης του K_1 ασφαλίζει την ορθότητα των χαρακτηριστικών και τη σωστή συμπεριφορά του K_2, εξασφαλίζοντας έτσι το χρήστη σε περιπτώσεις απωλειών, λόγω λανθασμένων πιστοποιήσεων ή κακής συμπεριφοράς. Η αριθμητική αυτή τιμή συμπεριλαμβάνεται μέσα στο πιστοποιητικό που αναπαριστά κάθε ακμή.

Δεδομένου ότι κάποιος κόμβος K_1 μπορεί να χρησιμοποιηθεί για να διαδώσει λανθασμένες πληροφορίες μέσω πιστοποιητικών, σε κάθε μονοπάτι από ένα εμπιστευμένο κλειδί πηγή έως ένα κλειδί στόχο, όπου η τελευταία ακμή εκχωρεί λανθασμένα χαρακτηριστικά στο κλειδί στόχο, οι συγγραφείς ορίζουν ως υπόλογο ακμή την πρώτη ακμή $K_1 \rightarrow K_2$ στην οποία εντοπίζονται ανακριβή χαρακτηριστικά ή το πιστοποιημένο κλειδί στόχος K_2 δεν συμπεριφέρεται σωστά, όπως για παράδειγμα παραπλανεί το χρήστη. Άρα, είναι υπόλογος ο ιδιοκτήτης του K_1, ο οποίος προσδιορίζεται από το κλειδί που πιστοποίησε το K_1.

Έτσι, αποκτώντας μια λανθασμένη σύνδεση μεταξύ ονόματος και κλειδιού για το κλειδί στόχο, προκύπτει ότι σε κάθε μονοπάτι μεταξύ των κλειδιών πηγής και στόχου υπάρχει κάποια υπόλογος ακμή και άρα οι ιδιοκτήτες των κλειδιών που δημιούργησαν τις ακμές αυτές, είναι υπόλογοι για το ποσό των χρημάτων που αναγράφεται σε αυτές. Σε αυτή την περίπτωση, οι συγγραφείς υπολογίζουν μια μετρική, η οποία αναπαριστά το ελάχιστο ποσό χρημάτων το οποίο μπορεί να περιμένει ένας χρήστης να ανακτήσει, ακολουθώντας ένα από όλα τα μονοπάτια που υπάρχουν από ένα εμπιστευόμενο κλειδί πηγή μέχρι ένα κλειδί στόχο. Ο υπολογισμός του ποσού αυτού, προκύπτει από τη θεωρία γραφημάτων και καλείται ελάχιστη χωρητικότητα τομής (capacity cut). Θεωρούμε ως K_s το εμπιστευμένο κλειδί πηγής, ως K_t το κλειδί στόχο και ως χωρητικότητα $c(K, K')$ κάθε ακμής $K \rightarrow K'$ το ασφαλισμένο ποσό χρημάτων της ακμής αυτής. Είναι προφανές ότι για ακμές που δεν υφίστανται, η χωρητικότητα είναι μηδενική. Η τομή χωρίζει το σύνολο των κόμβων σε δύο υποσύνολα A και B, τέτοια ώστε το K_s να ανήκει στο υποσύνολο A και το K_t στο B, όπως φαίνεται και στο σχήμα 4.



Σχήμα 4: Η ελάχιστη τομή αποφέρει ασφάλεια 50€ στη σύνδεση μεταξύ ονόματος και κλειδιού στόχου

Η χωρητικότητα $c(A, B)$ της τομής αυτής ισούται με τη συνολική χωρητικότητα των ακμών που ενώνουν το A με το B, δηλαδή:

$$c(A, B) = \sum_{K \in A, K' \in B} c(K, K'),$$

ενώ η ελάχιστη χωρητικότητα τομής ισούται με την ελάχιστη χωρητικότητα όλων των πιθανών τομών, αλλά και με το ελάχιστο ποσό για το οποίο έχει ασφαλιστεί η σύνδεση μεταξύ ονόματος και κλειδιού στόχου. Στο παραπάνω σχήμα, φαίνεται η τομή του συνόλου των κόμβων, η οποία δίνει την ελάχιστη χωρητικότητα τομής από όλες τις πιθανές τομές του συνόλου αυτού. Αυτή η χωρητικότητα τομής ισούται, όπως είπαμε, με τη συνολική χωρητικότητα των ακμών που ενώνουν τα δύο υποσύνολα που προέκυψαν και άρα ισούται, ξεκινώντας την πρόσθεση των ποσών ανά ακμή από πάνω προς τα κάτω, με $20€ + 10€ + 10€ + 10€ = 50€$.

3.2.4. Το μοντέλο του Jøsang

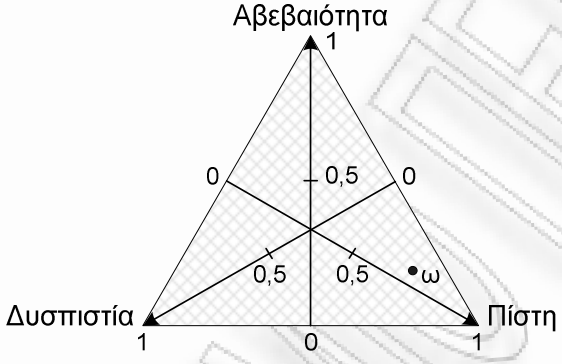
Το μοντέλο εμπιστοσύνης που προτείνεται στο [36] είναι βασισμένο σε ένα γενικό μοντέλο έκφρασης πεποιθήσεων και πιο συγκεκριμένα έκφρασης των σχετικά αβέβαιων πεποιθήσεων για την αλήθεια των δηλώσεων. Το μοντέλο βασίζεται σε πιστοποιητικά δημοσίου κλειδιού στα οποία όμως το κλειδί που χρησιμοποιείται συνδέεται με τον ιδιοκτήτη του, καθώς και με τις σχέσεις εμπιστοσύνης μεταξύ των χρηστών. Το μοντέλο αυτό μπορεί να χρησιμοποιηθεί σε περιπτώσεις όπου δεν υπάρχει κεντρική αρχή έκδοσης και διαχείρισης πιστοποιητικών, αλλά ο χρήστης είναι εκείνος που εκδίδει το πιστοποιητικό του, αποφασίζει σε ποιον θα εμπιστευτεί το κλειδί του, καθώς και ποια πιστοποιητικά και κλειδιά άλλων χρηστών είναι αυθεντικά. Ο συγγραφέας έχει αναπτύξει μία απλή άλγεβρα για την εμπιστοσύνη, η οποία μπορεί να χρησιμοποιηθεί για να πιστοποιήσει την αξιοπιστία των ίδιων των χρηστών και να καθορίσει την αυθεντικότητα των λαμβανόμενων κλειδιών.

Όπως ορίζεται στην εργασία, η εμπιστοσύνη είναι μια ανθρώπινη πεποίθηση, η οποία περιλαμβάνει ένα υποκείμενο (την εμπιστευόμενη ομάδα) και ένα αντικείμενο (την έμπιστη ομάδα). Η εμπιστοσύνη της σχέσης μεταξύ κλειδιού και ιδιοκτήτη μπορεί να εκφραστεί ως η πεποίθηση ότι το κλειδί είναι αυθεντικό, ενώ η εμπιστοσύνη απέναντι στον πιστοποιούντα

(recommender) ως η πεποίθηση ότι θα πιστοποιήσει μόνο κλειδιά τα οποία θεωρεί αυθεντικά. Οι χρήστες μπορούν να έχουν μόνο μία άποψη για τις σχέσεις αυτές, δίνοντας έτσι ένα βαθμό πίστης b, δυσπιστίας d ή αβεβαιότητας u, συστατικά τα οποία συνθέτουν το στοιχείο της άποψης $\mathrm{w}\{b,d,u\}$. Σύμφωνα με τον συγγραφέα, για κάθε άποψη ισχύει η σχέση:

$$b + d + u = 1.$$

Από την εξίσωση αυτή μπορεί να οριστεί το τρίγωνο του σχήματος 5, όπου μία άποψη ενός χρήστη μπορεί να αναπαρασταθεί ως ένα σημείο $\{b,d,u\}$ του τριγώνου.



Σχήμα 5: Τρίγωνο άποψης

Όπως αναφέρεται, μία άποψη που ορίζεται από την παραπάνω εξίσωση είναι στην πραγματικότητα ένα διδιάστατο κριτήριο, μιας και περιέχει τη διάσταση της πιθανότητας και εκείνη της αβεβαιότητας. Οι απόψεις μπορούν να μπουν σε σειρά, κατατάσσοντας πρώτα τις απόψεις με βάση την εκτιμώμενη πιθανότητα και στη συνέχεια να καταταχθούν εκείνες με την ίδια εκτιμώμενη πιθανότητα αλλά διαφορετική αβεβαιότητα.

Ο Jøsang εισάγει μία άλγεβρα για τον καθορισμό της εμπιστοσύνης στις αλυσίδες πιστοποίησης, η οποία βασίζεται σε ένα πλαίσιο τεχνητής λογικής, την οποία ονομάζει υποκειμενική λογική. Σύμφωνα με αυτή, η άποψη ενός πράκτορα A για μία δήλωση p ορίζεται ως:

$$\omega_p^A = \{b_p^A, d_p^A, u_p^A\},$$

δηλαδή η δήλωση p είναι αληθής στο βαθμό που εκφράζουν τα συστατικά πίστης b_p^A, δυσπιστίας d_p^A και αβεβαιότητας u_p^A αντίστοιχα.

Η υποκειμενική λογική περιέχει τελεστές αντίστοιχους με τους παραδοσιακούς (AND, OR και NOT), καθώς και τους τελεστές σύζευξης, σύστασης και συναίνεσης. Εάν θεωρήσουμε τις απόψεις $\omega_p^A = \{b_p^A, d_p^A, u_p^A\}$ και $\omega_q^A = \{b_q^A, d_q^A, u_q^A\}$ του πράκτορα A για δύο ξεχωριστές δηλώσεις p και q δυαδικού χαρακτήρα, η σύζευξη των δύο απόψεων ώστε και οι δύο απόψεις να είναι ταυτόχρονα αληθείς ορίζεται ως:

$$\omega_{p\wedge q}^A = \omega_p^A \wedge \omega_q^A = \{b_{p\wedge q}^A, d_{p\wedge q}^A, u_{p\wedge q}^A\},$$

όπου
$$\begin{cases} b^A_{p\wedge q} = b^A_p b^A_q, \\ d^A_{p\wedge q} = d^A_p + d^A_q - d^A_p d^A_q, \\ u^A_{p\wedge q} = b^A_p u^A_q + u^A_p b^A_q + u^A_p u^A_q. \end{cases}$$

Εάν θεωρήσουμε την άποψη $\omega^A_B = \{b^A_B, d^A_B, u^A_B\}$ ενός πράκτορα A για τις συστάσεις ενός πράκτορα B, p μία δήλωση δυαδικού χαρακτήρα και $\omega^B_p = \{b^B_p, d^B_p, u^B_p\}$ την άποψη του B για την p ως σύσταση στον A, τότε η άποψη του A για την p ως αποτέλεσμα της σύστασης από τον B ορίζεται ως:

$$\omega^{AB}_p = \omega^A_B \otimes \omega^B_p = \{b^{AB}_p, d^{AB}_p, u^{AB}_p\},$$

όπου
$$\begin{cases} b^{AB}_p = b^A_B b^B_p, \\ d^{AB}_p = b^A_B d^B_p, \\ u^{AB}_p = d^A_B + u^A_B + b^A_B u^B_p \end{cases} .$$

Η σύσταση του B πρέπει να μεταφραστεί ως το τι πραγματικά συστήνει ο B στον A και όχι αναγκαστικά ως η πραγματική άποψη του B. Ο τελεστής της σύστασης έχει νόημα μόνο στην περίπτωση που μπορεί να υποτεθεί ότι η σύσταση είναι μεταβατική ή πιο συγκεκριμένα όταν οι κόμβοι μιας αλυσίδας συστάσεων δεν αλλάζουν τη συμπεριφορά τους ανάλογα με τους κόμβους που αλληλεπιδρούν. Εάν τώρα θεωρήσουμε τις απόψεις ω^A_p και ω^B_p των κόμβων A και B αντίστοιχα για την ίδια δήλωση δυαδικού χαρακτήρα p, η συναινετική άποψη ενός φανταστικού πράκτορα $[A, B]$ που αναπαριστά τους A και B ορίζεται ως:

$$\omega^{A,B}_p = \omega^A_p \oplus \omega^B_p = \{b^{A,B}_p, d^{A,B}_p, u^{A,B}_p\},$$

όπου
$$\begin{cases} b^{A,B}_p = \left(b^A_p u^B_p + b^B_p u^A_p\right)/\left(u^A_p + u^B_p - u^A_p u^B_p\right), \\ d^{A,B}_p = \left(d^A_p u^B_p + d^B_p u^A_p\right)/\left(u^A_p + u^B_p - u^A_p u^B_p\right), \\ u^{A,B}_p = \left(u^A_p u^B_p\right)/\left(u^A_p + u^B_p - u^A_p u^B_p\right). \end{cases}$$

Η συναίνεση απόψεων απαιτεί ανεξάρτητα ορίσματα έτσι ώστε να μην έχει νόημα η συναίνεση μιας άποψης με τον εαυτό της. Στόχος του τελεστή της συναίνεσης είναι να μειώσει την αβεβαιότητα. Δύο πράκτορες που έχουν αντικρουόμενες απόψεις θα μπορέσουν να φτάσουν σε συναίνεση μόνο εάν οι απόψεις αυτές περιέχουν αβεβαιότητα. Είναι πιθανό αρκετές αλυσίδες συστάσεων να δίνουν απόψεις για την ίδια δήλωση. Δεδομένης της προϋπόθεσης της ανεξαρτησίας των απόψεων, οι απόψεις αυτές μπορούν να συνδυαστούν με τον κανόνα της συναίνεσης για να δώσουν μία άποψη για τη δήλωση αυτή. Θα υπάρχουν όμως και περιπτώσεις οι οποίες δε θα μπορούν να αναλυθούν απευθείας.

Το [36] αναλύει τον τρόπο που γίνονται οι πιστοποιήσεις των πρακτόρων και πώς η διαδικασία μπορεί να ενισχυθεί με έναν συνδυασμό του κλειδιού που χρησιμοποιείται για την πιστοποίηση και του ιδιοκτήτη του. Κατά την ηλεκτρονική διανομή κλειδιών, τα κλειδιά πρέπει να προτείνονται και να πιστοποιούνται από κάποιον τον οποίο εμπιστεύεται κάθε παραλήπτης για τη δουλεία αυτή και του οποίου διαθέτουν το πιστοποιημένο δημόσιο κλειδί. Ο συγγραφέας

χρησιμοποιεί το επόμενο παράδειγμα: εάν ο κόμβος A_1 διαθέτει το δημόσιο κλειδί k_{A2} του κόμβου A_2 και ο κόμβος A_2 διαθέτει με τη σειρά του το δημόσιο κλειδί k_{A3} του κόμβου A_3, τότε ο A_2 μπορεί να στείλει το δημόσιο κλειδί του A_3 στον A_1 πιστοποιημένο με το ιδιωτικό του κλειδί k_{A2}^{-1}. Όταν ο A_1 το λάβει, θα πιστοποιήσει το πιστοποιητικό του A_2 και εάν είναι αυθεντικό, θα ξέρει ότι και το δημόσιο κλειδί του κόμβου A_3 είναι αυθεντικό, ώστε να εγκαταστήσει ασφαλή επικοινωνία με τον A_3. Το πρόβλημα όμως είναι ότι τα πιστοποιητικά από μόνα τους δεν αρκούν.

Ο συγγραφέας συνεχίζει αναφέροντας ότι προκειμένου να υπάρξει ο συνδυασμός του κλειδιού που χρησιμοποιείται και του ιδιοκτήτη του, ο παραλήπτης κάθε πιστοποιητικού πρέπει να έχει κάποια άποψη για την αυθεντικότητα του κλειδιού (KA – Key Authenticity) που καλείται να χρησιμοποιήσει για να εξακριβώσει την αυθεντικότητα του πιστοποιητικού, και άρα μια άποψη για το κλειδί και τον ιδιοκτήτη του (στο παραπάνω παράδειγμα είναι η άποψη $\omega_{KA(k_{A2})}^{A1}$ του A_1 για το κλειδί k_{A2} του κόμβου A_2). Επιπλέον, ο παραλήπτης πρέπει να έχει μια άποψη για την αξιοπιστία των συστάσεων (RT – Recommendation Trustworthiness) που δίνει ο πιστοποιών (η άποψη $\omega_{RT(A2)}^{A1}$ του A_1 για τις συστάσεις του A_2), δηλαδή κατά πόσο τον εμπιστεύεται για να δίνει συστάσεις και να πιστοποιεί κλειδιά τρίτων. Τέλος, ο πιστοποιών πρέπει να ενσωματώνει στο πιστοποιητικό που στέλνει στον παραλήπτη την άποψή του για την αυθεντικότητα κάποιου πιστοποιημένου κλειδιού που ήδη κατέχει (η άποψη $\omega_{KA(k_{A3})}^{A2}$ του κόμβου A_2 για το κλειδί k_{A3} του κόμβου A_3).

Όπως αναφέρεται, σε ένα περιβάλλον ανταλλαγής ηλεκτρονικών μηνυμάτων, ένας πράκτορας μπορεί να θεωρηθεί έμπιστος, μόνο εάν κάποιος εμπιστεύεται την αυθεντικότητα του κλειδιού του (KA) και την αξιοπιστία των συστάσεών του (RT). Έτσι εισάγεται ο όρος συνδετική σύσταση για να αποδώσει τη σημασία της αξιόπιστης σύστασης σε ένα κανονικό διαπροσωπικό περιβάλλον, η οποία ορίζεται ως:

$$\omega_{A2}^{A1} = \left(\omega_{RT(A2)}^{A1} \wedge \omega_{KA(k_{A2})}^{A1}\right).$$

Εάν θεωρήσουμε τους πράκτορες A_1, A_2 και A_3 με αντίστοιχα δημόσια κλειδιά k_{A1}, k_{A2} και k_{A3}, $\omega_{KA(k_{A2})}^{A1}$ η άποψη του A_1 για το κλειδί k_{A2}, $\omega_{RT(A2)}^{A1}$ η άποψή του για τις συστάσεις του A_2 και $\omega_{KA(k_{A3})}^{A2}$ η άποψη του A_2 για το κλειδί k_{A3}, τότε η άποψη του A_1 για την αυθεντικότητα του κλειδιού k_{A3}, δηλαδή η απλή αυθεντικοποίηση, ορίζεται ως:

$$\omega_{KA(k_{A3})}^{A1\ A2} = \omega_{A2}^{A1} \otimes \omega_{KA(k_{A3})}^{A2} = \left(\omega_{RT(A2)}^{A1} \wedge \omega_{KA(k_{A2})}^{A1}\right) \otimes \omega_{KA(k_{A3})}^{A2}.$$

Όπως φαίνεται και στον τύπο, όταν ένα μονοπάτι πιστοποιήσεων περιλαμβάνει πολλούς ενδιάμεσους πιστοποιούντες, οι απόψεις για την αξιοπιστία των συστάσεων ω_{RT} πρέπει να δοθούν επίσης κατά μήκος του μονοπατιού και να περιληφθούν στο πιστοποιητικό μαζί με το πιστοποιημένο κλειδί. Δηλαδή, η αξιοπιστία των συστάσεων RT δεν εφαρμόζεται μόνο στις άμεσες πιστοποιήσεις των κλειδιών, αλλά και στη σύσταση άλλων πρακτόρων για παραπέρα συστάσεις. Στον παραπάνω τύπο μπορούν να εισαχθούν και άλλοι πράκτορες, οι οποίοι έχουν αλυσιδωτές σχέσεις εμπιστοσύνης και πιστοποίησης, δίνοντας έτσι την άποψη του A_1 για την αυθεντικότητα του τελικού κλειδιού ως αλυσιδωτή αυθεντικοποίηση των ενδιάμεσων πρακτόρων. Με τον τρόπο αυτό μπορεί να υπολογιστεί η σχετική αξιοπιστία των κλειδιών που λαμβάνονται σε ένα ανοιχτό δίκτυο υπολογιστών. Επιπλέον, όταν υπάρχουν πολλά μονοπάτια πιστοποιήσεων για το ίδιο κλειδί, η συνολική άποψη για την αυθεντικότητα του κλειδιού αυτού υπολογίζεται ως η συναίνεση των αντίστοιχων απόψεων που έχουν προκύψει από κάθε

μονοπάτι. Οι απόψεις όμως που στηρίζονται σε συστάσεις από άλλους πράκτορες δεν πρέπει ποτέ να μεταφέρονται σε άλλους πράκτορες, και αυτό γιατί οι παραλήπτες μπορεί να λάβουν συστάσεις από τους ίδιους πράκτορες, προκαλώντας εξαρτήσεις απόψεων όταν χρησιμοποιηθεί ο τελεστής της συναίνεσης. Για το λόγο αυτό, πρέπει να προτείνονται σε άλλους πράκτορες μόνο απόψεις οι οποίες βασίζονται σε άμεσες μαρτυρίες και εμπειρίες.

Ο συγγραφέας καταλήγει ότι μια αξιόπιστη αυθεντικοποίηση δημοσίων κλειδιών πρέπει να βασίζεται πάντα σε μια συνεχή αλυσίδα πιστοποιητικών και συστάσεων, δημιουργώντας βέβαια πολλές φορές προβλήματα στην ανεύρεση του κατάλληλου μονοπατιού. Για το λόγο αυτό αναφέρει ότι η εισαγωγή ιεραρχιών αρχών πιστοποίησης θα μπορούσε να βοηθήσει στο να ξεπεραστούν τέτοια προβλήματα, χωρίς να αντιτίθεται στη φιλοσοφία των ανοιχτών δικτύων. Η απαίτηση για συστάσεις που στηρίζονται σε άμεσες μαρτυρίες, οδηγεί σε δραματική μείωση του προβλήματος ανάκλησης πιστοποιητικών, μιας και ο πράκτορας που δίνει μια σύσταση γνωρίζει πάντα όλους τους παραλήπτες κάθε πιστοποιητικού και άρα μπορεί πολύ αποτελεσματικά να τους ενημερώσει για τυχόν ανάκληση κάποιου από αυτά. Τέλος, οι πράκτορες δεν χρειάζεται να ανησυχούν για περιπτώσεις κατά τις οποίες η αρχή πιστοποίησης την οποία εμπιστεύονται εμπιστεύεται κάποια άλλη αρχή, την οποία οι ίδιοι δεν εμπιστεύονται, και αυτό γιατί οι πράκτορες ενημερώνονται πάντα για την ταυτότητα κάθε ενδιάμεσου κόμβου σε μια αλυσίδα και μπορούν να αγνοήσουν μια σύσταση τιμής αξιοπιστίας που μπορεί να λάβουν, εάν έχουν άλλη άποψη για τη συγκεκριμένη αρχή πιστοποίησης.

3.3. Αξιοποίηση αξιολογήσεων συναλλαγών

Οι αξιολογήσεις συναλλαγών περιγράφουν την ποιότητα μιας συναλλαγής μεταξύ δύο χρηστών. Κάθε χρήστης είναι άγνωστος προς τους υπόλοιπους και μόνο οι αξιολογήσεις που τού έχουν δοθεί από άλλους χρήστες μετά από προηγούμενες συναλλαγές του, μπορούν να δώσουν κάποια στοιχεία για την αξιοπιστία του. Με την ανάλυση των αξιολογήσεων μπορεί να υπολογιστεί στη συνέχεια η τιμή εμπιστοσύνης για έναν οποιοδήποτε χρήστη του δικτύου.

3.3.1. Το μοντέλο eBay

Το eBay [37] αποτελεί μια από τις μεγαλύτερες παγκοσμίως online αγορές με πάνω από 50 εκατομμύρια εγγεγραμμένους χρήστες [38]. Τα περισσότερα αντικείμενα πωλούνται στο eBay μέσω αγγλικών δημοπρασιών και χρησιμοποιείται ένα σύστημα φήμης, στο οποίο τόσο οι αγοραστές, όσο και οι πωλητές μπορούν να βαθμολογούν οι μεν τους δε μετά από την ολοκλήρωση κάθε συναλλαγής. Το σύστημα αυτό βοηθάει τους υπόλοιπους χρήστες του eBay να γνωρίζουν τη συμπεριφορά που έχει επιδείξει ένας χρήστης κατά το παρελθόν, έτσι ώστε να τον προτιμήσουν ή όχι για μια μελλοντική συναλλαγή. Το eBay δεν παρέχει καμία εγγύηση για τις συναλλαγές που γίνονται μέσω αυτού, αλλά λειτουργεί μόνο ως μια υπηρεσία κατάταξης σε μια λίστα δημοπρασιών, όπου οι πωλητές και οι αγοραστές αναλαμβάνουν τον κίνδυνο που αποπνέουν οι συναλλαγές.

Κάθε χρήστης μπορεί εάν θέλει μετά την ολοκλήρωση της συναλλαγής του, να δώσει ένα σύντομο σχόλιο και να βαθμολογήσει με τρεις διαφορετικές τιμές την αξιοπιστία του άλλου χρήστη, δηλαδή θετική (1) εάν έχει μείνει ευχαριστημένος από τη συναλλαγή τους, ουδέτερη (0) ή αρνητική (-1) εάν κάτι στη συναλλαγή τους τον δυσαρέστησε. Η τιμή της θετικής ανάδρασης (Positive Feedback) κάθε χρήστη είναι το ποσοστό των θετικών βαθμολογιών σε διάστημα ενός έτους. Αυτό υπολογίζεται με βάση το συνολικό αριθμό των θετικών και αρνητικών βαθμολογιών ανάδρασης για τις συναλλαγές που ολοκληρώθηκαν μέσα στον τελευταίο χρόνο, αφαιρώντας τις τυχόν επαναλαμβανόμενες αναδράσεις από τον ίδιο χρήστη για συναλλαγές που έγιναν εντός της ίδιας ημερολογιακής εβδομάδας. Κάτι τέτοιο σημαίνει ότι εάν ένας χρήστης έχει δώσει περισσότερες από μια φορές ίδια βαθμολογία για κάποιον άλλο χρήστη, τότε αυτές θα μετρηθούν μία μόνο φορά, εκτός και αν οι βαθμολογίες αυτές έχουν δοθεί σε διαφορετικές εβδομάδες, οπότε και μετρώνται ανεξάρτητα. Το eBay ορίζει ως διάρκεια μιας εβδομάδας αυτή μεταξύ Δευτέρας και Κυριακής.

Τα θετικά ή αρνητικά σχόλια, καθώς και όλες οι βαθμολογίες των χρηστών, συλλέγονται, επεξεργάζονται, συσχετίζονται με το αναγνωριστικό του χρήστη στον οποίο ανήκουν και εμφανίζονται στους υπόλοιπους χρήστες δίπλα από κάθε αντικείμενο που πωλεί. Έτσι οι χρήστες βλέπουν τη φήμη του πωλητή πριν κάνουν μια προσφορά για κάποιο από τα προϊόντα του. Μια κεντρική έμπιστη αρχή είναι υπεύθυνη για την αποθήκευση, διαχείριση και δημοσίευση των βαθμολογιών αυτών. Ο τρόπος που λειτουργεί το σύστημα φήμης του eBay υπέρ ενός χρήστη μπορεί να φανεί από το επόμενο παράδειγμα. Ας θεωρήσουμε ότι μια ομάδα αγοραστών αγοράζουν προϊόντα από έναν πωλητή. Στη συνέχεια, του δίνουν θετική βαθμολογία, κάνουν θετικά σχόλια και μετά δεν συναλλάσσονται ξανά μαζί του. Ο πωλητής, παρ' όλο που «χάνει» τους πελάτες αυτούς, αποκτά θετική φήμη, κάτι που θα τον βοηθήσει στη μετέπειτα πορεία του. Οι μελλοντικοί του αγοραστές δεν έχουν καμία προσωπική επαφή με τον πωλητή αυτόν και λαμβάνουν αποφάσεις για αγορές από εκείνον στηριζόμενοι μόνο στις πολύ καλές κριτικές που έχει λάβει στο παρελθόν. Έτσι η καλή φήμη του πωλητή επηρεάζει τις μελλοντικές του πωλήσεις, κάτι που τον κάνει να την αποζητά όλο και περισσότερο.

Δεδομένου ότι το σύστημα φήμης που χρησιμοποιεί το eBay, επιτρέπει στους χρήστες να εκφράζουν το επίπεδο ικανοποίησής τους από έναν άλλο χρήστη μετά από κάθε συναλλαγή, έχει προταθεί η χρήση του σε συστήματα ομότιμων κόμβων, στα οποία οι κόμβοι κρατούν ιστορικό των συναλλαγών με τους υπόλοιπους κόμβους και μοιράζονται τις πληροφορίες αυτές με τους κόμβους του δικτύου [39].

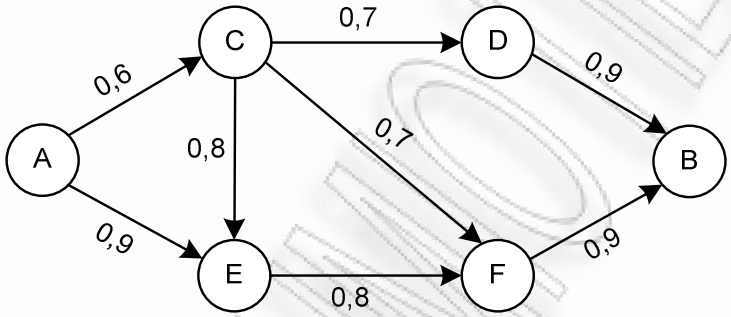
3.3.2. Το μοντέλο των Sherwood et al.

Οι Sherwood et al. [40] παρουσίασαν ένα σχήμα εξαγωγής συμπερασμάτων εμπιστοσύνης για το NICE, μια πλατφόρμα εκτέλεσης συνεργατικών εφαρμογών για το Διαδίκτυο. Οι εφαρμογές αυτές αποκτούν πρόσβαση σε απομακρυσμένους πόρους, ανταλλάσσοντας τοπικούς πόρους. Το NICE προσφέρει υπηρεσίες διαφήμισης πόρων, ασφαλείς ανταλλαγές και εμπόριο πόρων, καθώς και κατανεμημένη αξιολόγηση εμπιστοσύνης. Οι συναλλαγές στο NICE αποτελούνται από ασφαλείς ανταλλαγές πιστοποιητικών πόρων, τα οποία «εξαγοράζουν» τους απομακρυσμένους αυτούς πόρους. Οι κόμβοι ανταλλάσσουν μηνύματα συναλλαγών, τα οποία περιέχουν μία υπογεγραμμένη κατακερματισμένη τιμή, ικανή να εγγυηθεί την ακεραιότητα του μηνύματος. Κάθε χρήστης του NICE επιλέγει ένα αναγνωριστικό το οποίο περιέχει ένα αναγνωριστικό αλφαριθμητικό κείμενο και ένα δημόσιο κλειδί για την υπογραφή πιστοποιητικών πόρων, προκειμένου να εμπορεύεται πόρους και να εκχωρεί τιμές εμπιστοσύνης. Από αυτά, κανένα δεν χρειάζεται να καταχωρηθεί σε κάποια κεντρική αρχή. Το πρωτόκολλο ανταλλαγής των πιστοποιητικών πόρων διασφαλίζει ότι κανένας συμμετέχων δεν αποκτά ένα χρησιμοποιήσιμο πιστοποιητικό, χωρίς πρώτα να εκδώσει ένα έγκυρο πιστοποιητικό. Υπάρχουν όμως μη συνεργατικοί χρήστες, οι οποίοι μπορεί να αποκτήσουν πρόσβαση στους πόρους αυτούς εκδίδοντας πιστοποιητικά, τα οποία τελικά δεν εξοφλούν. Ο βασικός σκοπός των πολιτικών του NICE είναι να μπορούν οι καλοί χρήστες να αναγνωρίζουν γρήγορα και αποτελεσματικά τους υπόλοιπους καλούς χρήστες και να οργανώνονται σε δυνατές συνεργαζόμενες ομάδες, μην επιτρέποντας να χαθούν μεγάλες ποσότητες πόρων σε κακόβουλους χρήστες.

Το [40] εστιάζει σε κατανεμημένες λύσεις για το πρόβλημα της εξαγωγής συμπερασμάτων σχετικά με την εμπιστοσύνη και το χωρίζει σε δύο μέρη, μια συνιστώσα κατανεμημένης αναζήτησης, η οποία συλλέγει αποτελεσματικά πληροφορίες εμπιστοσύνης μεταξύ των συμμετεχόντων του συστήματος και μια συνιστώσα εξαγωγής συμπερασμάτων τοπικού επιπέδου, της οποίας οι αλγόριθμοι απαιτούν ως δεδομένα εισόδου τις παραπάνω πληροφορίες. Η μελέτη προσπαθεί να αναπτύξει μηχανισμούς ανταλλαγής και κοστολόγησης, οι οποίοι θα αναγνωρίζουν τους κόμβους που εκδίδουν αξιόπιστα και τελικά εξοφλούμενα πιστοποιητικά, προστατεύοντας έτσι την ακεραιότητα της ομάδας. Σύμφωνα με το μηχανισμό κοστολόγησης που βασίζεται στην εμπιστοσύνη, οι πόροι κοστολογούνται αναλογικά προς την αμοιβαία αντιλαμβανόμενη εμπιστοσύνη. Η πολιτική αυτή στηρίζεται στο ότι καθώς ένας κόμβος A συναλλάσσεται με έναν άλλο κόμβο μικρότερης εμπιστοσύνης, διατρέχει μεγαλύτερο κίνδυνο να μην εξυπηρετηθεί, κάτι που αντικατοπτρίζεται τελικά στην κοστολόγηση. Έτσι ο κόμβος A θα

συναλλαχθεί με τον κόμβο B, εάν ο τελευταίος προσφέρει σημαντικά περισσότερους πόρους από εκείνους που θα λάβει ως ανταπόδοση. Βέβαια, καθώς ο κόμβος B θα διεξάγει περισσότερες επιτυχημένες συναλλαγές με τον κόμβο A, η διαφορά του κόστους θα μειώνεται. Σύμφωνα με τον μηχανισμό ανταλλαγής που βασίζεται στην εμπιστοσύνη, αυτό που μεταβάλλεται δεν είναι η τιμή του πόρου, αλλά η ποσότητα που ανταλλάσσεται. Η πολιτική αυτή εγγυάται ότι όταν ένας κόμβος συναλλάσσεται με έναν άλλο με μικρή εμπιστοσύνη, ο πρώτος περιορίζει την ποσότητα των πόρων που μπορεί να χάσει.

Όταν ολοκληρωθεί μια συναλλαγή, ο χρήστης που εξυπηρετήθηκε παράγει μια υπογεγραμμένη δήλωση, το λεγόμενο cookie, η οποία περιγράφει την ποιότητα της συναλλαγής και μπορεί να χρησιμοποιηθεί μελλοντικά από τον χρήστη εξυπηρετητή για να αποδείξει την αξιοπιστία του σε άλλους χρήστες. Με τα cookies που συγκεντρώνονται, οι Sherwood et al. [40] κατασκευάζουν ένα κατευθυνόμενο γράφημα T, του οποίου οι κόμβοι είναι οι χρήστες του συστήματος, όπως φαίνεται στο σχήμα 6.



Σχήμα 6: Δίκτυο εμπιστοσύνης

Εάν ένας χρήστης B διαθέτει ένα cookie από έναν άλλο χρήστη A, αυτό απεικονίζεται στο γράφημα με μια κατευθυνόμενη ακμή με αρχή τον κόμβο A και τέλος τον κόμβο B. Η τιμή της ακμής, η οποία κυμαίνεται στο διάστημα $[0, 1]$, δηλώνει πόσο εμπιστεύεται ο κόμβος A τον B ότι θα είναι συνεργάσιμος και εξαρτάται από το σύνολο των cookies του A που διαθέτει ο B. Οι συναλλαγές συνεχίζονται με τα cookies να αποθηκεύονται σε διαφορετικούς χρήστες και άρα είτε να προστίθενται νέες ακμές μεταξύ κόμβων, είτε να αλλάζουν οι τιμές των ήδη υπαρχουσών ακμών.

Στην περίπτωση που ένας κόμβος A δεν έχει συναλλαχθεί ξανά με έναν κόμβο B, μπορεί να εξάγει μια τιμή εμπιστοσύνης γι' αυτόν, μέσω των κατευθυνόμενων μονοπατιών που τους ενώνουν. Επειδή όμως μπορεί να υπάρχουν πολλά συνδεόμενα μονοπάτια που ενώνουν τους κόμβους αυτούς, οι Sherwood et al. [40] παρουσιάζουν δύο διαφορετικούς αλγορίθμους συγκεντρωτικής εξαγωγής συμπερασμάτων σχετικά με την τιμή εμπιστοσύνης μεταξύ των κόμβων αυτών. Σύμφωνα με τον αλγόριθμο του ισχυρότερου μονοπατιού, ο κόμβος A επιλέγει το ισχυρότερο μονοπάτι ανάμεσα σε εκείνα που τον συνδέουν με τον κόμβο B και χρησιμοποιεί την ελάχιστη τιμή εμπιστοσύνης του μονοπατιού ως τιμή εμπιστοσύνης για τον κόμβο B. Η ισχύς ενός μονοπατιού υπολογίζεται ως η ελάχιστη από τις τιμές ή το γινόμενο όλων των τιμών των ακμών του μονοπατιού. Δεδομένης της ύπαρξης του γραφήματος εμπιστοσύνης, η μετρική της εμπιστοσύνης μπορεί εύκολα να υπολογιστεί χρησιμοποιώντας την κατά βάθος διάσχιση. Από την άλλη, ο αλγόριθμος σταθμισμένου αθροίσματος των ισχυρότερων ασύνδετων μονοπατιών ορίζει ότι ο κόμβος A μπορεί να επιλέξει να καταλήξει στην τιμή εμπιστοσύνης για τον κόμβο B, υπολογίζοντας το σταθμισμένο σύνολο της ισχύος των ισχυρότερων ασύνδετων μεταξύ τους μονοπατιών. Το σύνολο των ισχυρότερων ασύνδετων αυτών μεταξύ τους μονοπατιών είναι μοναδικό, και μπορεί να βρεθεί χρησιμοποιώντας ροές δικτύων με περιορισμούς ροών στις κορυφές.

Οι Sherwood et al. προχωράνε ένα βήμα παραπέρα, περιγράφοντας ένα διαφορετικό πρωτόκολλο για την κατανεμημένη αυτή τη φορά εξαγωγή τιμών εμπιστοσύνης. Σύμφωνα με το πρωτόκολλο, έστω ότι ένας κόμβος A επιθυμεί να χρησιμοποιήσει κάποιους από τους πόρους ενός άλλου κόμβου B. Εάν ο A διαθέτει cookies από τον B, τα στέλνει σε αυτόν. Ο B με τη σειρά του μπορεί να εξακριβώσει εάν του ανήκουν, χάρη στην ψηφιακή υπογραφή που περιέχουν και να υπολογίσει μια τιμή εμπιστοσύνης για τον κόμβο A. Εάν όμως ο κόμβος A δε διαθέτει cookies από τον κόμβο B, τότε ξεκινάει μια αναζήτηση για τα cookies αυτά με τη μέθοδο της πλημμύρας αιτημάτων προς τους γειτονικούς κόμβους για τους οποίους διαθέτει ήδη cookies. Τελικά, προκύπτει μια ένωση κατευθυνόμενων μονοπατιών, τα οποία ξεκινούν από τον κόμβο B και τελειώνουν στον κόμβο A. Με την ύπαρξη των συνόλων των cookies, ο κόμβος B μπορεί να χρησιμοποιήσει ένα από τα παραπάνω συγκεντρωτικά σχήματα για την εξαγωγή μιας τιμής εμπιστοσύνης για τον κόμβο A.

Τέλος, η εργασία παρουσιάζει κάποιες βελτιώσεις όσον αφορά στην αποτελεσματικότερη εύρεση μονοπατιών μεταξύ του χρήστη που εκκινεί την αναζήτηση και του κόμβου του οποίου επιθυμεί να χρησιμοποιήσει τους πόρους, στα αρνητικά cookies και, τέλος, εισάγει τη λίστα προτίμησης. Για την εύρεση μονοπατιού, υιοθετείται η χρήση σύνοψης όλων των cookies σε κάθε κόμβο, κάθε φορά που λαμβάνεται ένα cookie από κάποιο χρήστη. Κάθε χρήστης διατηρεί μία σύνοψη με όλες τις τελευταίες αναζητήσεις, με αποτέλεσμα ένα αίτημα να προωθείται στους κόμβους που φαίνονται από τη σύνοψη ότι διαθέτουν το επιθυμητό cookie και η εύρεσή του να μπορεί να γίνεται με μεγάλη ακρίβεια, αποφεύγοντας τα επαναλαμβανόμενα αιτήματα. Στην περίπτωση κατά την οποία το cookie δεν υπάρχει στη σύνοψη του κόμβου, το αίτημα προωθείται σε έναν αριθμό τυχαίων κόμβων. Επιπλέον, παρουσιάζεται μία βελτίωση για το θέμα της πιθανής μη καταγραφής από τους κόμβους των συναλλαγών τους που συνοδεύονται από χαμηλή τιμή εμπιστοσύνης. Μία λύση που παρέχεται στο πρόβλημα είναι η καταγραφή τέτοιων cookies και από τον άλλο χρήστη της συναλλαγής. Στη συνέχεια, όταν ο κακόβουλος χρήστης ζητήσει μια συναλλαγή με κόμβο με τον οποίο δεν έχει συναλλαχθεί ξανά, παρουσιάζοντάς του πολύ αξιόπιστα cookies, ο υποψήφιος συνεργάτης μπορεί να ξεκινήσει αναζήτηση για τυχόν υπάρχοντα αρνητικά cookies από τους κόμβους που εμπιστεύεται και να απορρίψει την υποψήφια συναλλαγή όταν τα λάβει. Τέλος, γίνεται χρήση μιας λίστας προτίμησης σε κάθε κόμβο, με τη βοήθεια της οποίας ανακαλύπτονται πιθανοί αξιόπιστοι χρήστες με τους οποίους ο κόμβος δεν έχει πραγματοποιήσει ξανά συναλλαγή. Οι κόμβοι της λίστας είναι εκείνοι που έχουν τη μέγιστη τιμή εμπιστοσύνης και ανήκουν στα μονοπάτια που έχουν προκύψει από τη διαδικασία αναζήτησης κάθε cookie.

3.4. Κατανεμημένα μοντέλα εμπιστοσύνης

Στη βιβλιογραφία συναντάμε πολλά κατανεμημένα μοντέλα εμπιστοσύνης, τα οποία επιτρέπουν στους κόμβους ενός δικτύου να υπολογίσουν τοπικά κάποιες τιμές εμπιστοσύνης. Ο τοπικός υπολογισμός τιμών εμπιστοσύνης δεν απαιτεί την ύπαρξη κεντρικού συστήματος διαχείρισης για τις τιμές αυτές και επιτρέπει στους κόμβους να διατηρούν διαφορετικές τιμές εμπιστοσύνης προς τον ίδιο κόμβο του δικτύου.

3.4.1. Το μοντέλο των Abdul-Rahman και Hailes

Στο [41] προτείνεται ένα κατανεμημένο μοντέλο εμπιστοσύνης που βασίζεται σε ένα πρωτόκολλο σύστασης. Οι συγγραφείς προτείνουν μία μεταβατικότητα της εμπιστοσύνης, η οποία όμως μπορεί να υπάρξει μόνο υπό προϋποθέσεις. Έτσι, προκειμένου ένας κόμβος A, ο οποίος εμπιστεύεται τον κόμβο B, να εμπιστευτεί και έναν κόμβο Γ επειδή τον εμπιστεύεται ο κόμβος B, θα πρέπει να ισχύουν οι εξής προϋποθέσεις:

- Ο κόμβος B να συστήσει ρητά στον A την εμπιστοσύνη του στον κόμβο Γ.

- Ο κόμβος A να μπορεί να εμπιστευτεί τις συστάσεις που δίνει ο κόμβος B ανάλογα με τις δικές του πολιτικές.
- Ο κόμβος A να μπορεί να κρίνει τις συστάσεις του κόμβου B και να αποφασίζει πόσο θα εμπιστευτεί τον κόμβο Γ, ασχέτως εάν ο κόμβος B τον εμπιστεύεται πλήρως ή όχι.

Επιπλέον, ορίζεται ότι μια σχέση εμπιστοσύνης, εκτός από μεταβατική υπό τις παραπάνω προϋποθέσεις, υφίσταται μεταξύ δύο μόνο οντοτήτων και είναι μη συμμετρική. Οι συγγραφείς διακρίνουν δύο είδη σχέσης εμπιστοσύνης, την άμεση σχέση, όπου ένας κόμβος εμπιστεύεται έναν άλλο κόμβο και την σχέση σύστασης, όπου ένας κόμβος εμπιστεύεται έναν άλλο κόμβο για να δώσει συστάσεις για την αξιοπιστία άλλων κόμβων.

Το προτεινόμενο μοντέλο βασίζεται σε πράκτορες, οι οποίοι κάνουν χρήση του πρωτοκόλλου σύστασης και μπορούν να προτείνουν οποιαδήποτε οντότητα του δικτύου στέλνοντας και λαμβάνοντας συστάσεις διαφόρων βαθμών εμπιστοσύνης, αποκτώντας πληροφορίες από τις πηγές που εμπιστεύονται, χωρίς να βασίζονται σε κεντρικούς μηχανισμούς. Η ποιότητα των πληροφοριών αυτών υπολογίζεται στη συνέχεια με βάση την παρατηρούμενη αξιοπιστία των πρακτόρων που κάνουν τις συστάσεις, και η εμπιστοσύνη αναθεωρείται κάθε φορά που λαμβάνονται νέες συστάσεις ή εμπειρίες. Οι πράκτορες χρησιμοποιούν κατηγορίες εμπιστοσύνης για να εκφράσουν την εμπιστοσύνη τους για άλλους πράκτορες με διαφορετικούς τρόπους, ανάλογα με το ιδιαίτερο χαρακτηριστικό του καθενός το οποίο είναι υπό εξέταση. Το μοντέλο χρησιμοποιεί επίσης διακριτές τιμές εμπιστοσύνης για να αναπαραστήσει τα πιθανά επίπεδα εμπιστοσύνης για έναν πράκτορα. Οι διακριτές αυτές τιμές περιορίζονται στην κάθε κατηγορία εμπιστοσύνης την οποία χαρακτηρίζουν και είναι ανεξάρτητες από τις τιμές άλλων κατηγοριών. Χρησιμοποιούνται δύο τύποι τιμών, ανάλογα με τον τύπο σχέσης εμπιστοσύνης που υπάρχει, η άμεση για τις άμεσες σχέσεις και η τιμή συνιστώντος, αντίστοιχα, για τις σχέσεις σύστασης. Οι τιμές για κάθε σχέση και οι περιγραφές τους φαίνονται στους παρακάτω πίνακες 1 και 2.

Τιμή	***Σημασία***	***Περιγραφή***
-1	Δυσπιστία	Εντελώς αναξιόπιστη
0	Άγνοια	Χωρίς κρίση σχετική με την εμπιστοσύνη για την οντότητα
1	Ελάχιστη	Ελάχιστη δυνατή εμπιστοσύνη
2	Μέση	Μέση αξιοπιστία. Οι περισσότερες οντότητες έχουν αυτό το επίπεδο εμπιστοσύνης
3	Καλή	Πιο αξιόπιστη από τις περισσότερες οντότητες
4	Απόλυτη	Απόλυτη εμπιστοσύνη σε αυτή την οντότητα

Πίνακας 1: Σημασιολογία τιμής άμεσης εμπιστοσύνης

Τιμή	***Σημασία***	***Περιγραφή***
-1	Δυσπιστία	Εντελώς αναξιόπιστος
0	Άγνοια	Χωρίς κρίση σχετική με την εμπιστοσύνη για τον πράκτορα
1	Η οντότητα κρίνει μόνη της την αξιοπιστία της σύστασης του συνιστώντος	
2		
3		
4		

Πίνακας 2: Σημασιολογία τιμής εμπιστοσύνης συνιστώντος

Οι συγγραφείς ορίζουν την έννοια της φήμης ως μία τριάδα στοιχείων: της ταυτότητας ή του ονόματος ενός πράκτορα, της κατηγορίας εμπιστοσύνης και της τιμής εμπιστοσύνης. Οι πληροφορίες φήμης περιέχονται στη συνέχεια στις συστάσεις, στις μεταδιδόμενες δηλαδή πληροφορίες εμπιστοσύνης. Κάθε πράκτορας κάνει συστάσεις σε άλλους πράκτορες βασιζόμενος σε αρχεία φήμης που διατηρεί στη βάση δεδομένων του και μπορεί είτε να στέλνει, είτε να λαμβάνει συστάσεις για μια οποιαδήποτε οντότητα του δικτύου.

Όταν κάποιος πράκτορας επιθυμεί να του δοθεί μια σύσταση, στέλνει ένα μήνυμα αίτησης σύστασης, το λεγόμενο RRQ, στο σύνολο των πρακτόρων τους οποίους εμπιστεύεται να του δώσουν σύσταση για τη συγκεκριμένη κατηγορία και λαμβάνει στη συνέχεια το μήνυμα σύστασης, το οποίο μπορεί να ανανεωθεί ή να ανακληθεί με ένα μήνυμα ανανέωσης. Στην περίπτωση που οι πράκτορες αυτοί δεν διαθέτουν πληροφορίες για την κατηγορία που τους ζητείται, προωθούν το μήνυμα RRQ στους πράκτορες τους οποίους εμπιστεύονται οι ίδιοι ότι μπορούν να δώσουν μία τέτοια σύσταση. Η προώθηση του μηνύματος προχωράει μέχρι να φτάσει σε κάποιο πράκτορα ο οποίος να διαθέτει τις επιθυμητές πληροφορίες. Μέσα στο μήνυμα RRQ περιλαμβάνονται, μεταξύ άλλων, οι ταυτότητες του αποστολέα που προωθεί κάθε φορά το μήνυμα και του κόμβου για τον οποίο ζητείται η σύσταση, τα ονόματα των κατηγοριών για τις οποίες ζητούνται τιμές, το πιστοποιητικό δημοσίου κλειδιού του αποστολέα και μια ημερομηνία λήξης του μηνύματος, η οποία βοηθάει στην αναγνώριση και απόρριψη παλαιών μηνυμάτων RRQ.

Στο μήνυμα σύστασης που αποστέλλεται, περιλαμβάνονται τα ονόματα των κατηγοριών για τις οποίες ζητήθηκε σύσταση και οι αντίστοιχες κρυπτογραφημένες τιμές τους, ένα πεδίο με την διατεταγμένη ακολουθία των ταυτοτήτων των κόμβων από τους οποίους πέρασε το μήνυμα, καθώς και μια ένδειξη για την περίοδο ισχύος της σύστασης. Το μήνυμα σύστασης επιστρέφεται μέσω του μονοπατιού από το οποίο προωθήθηκε το μήνυμα RRQ, το οποίο περιέχει έναν τουλάχιστον αξιόπιστο πράκτορα, αυτόν που κάνει τη σύσταση. Εάν το μήνυμα RRQ δε βρει κάποιον παραλήπτη που να μπορεί να δώσει σύσταση, επιστρέφεται στον αρχικό αποστολέα με τιμές NULL στα αντίστοιχα πεδία όπου θα δίνονταν οι πληροφορίες εμπιστοσύνης. Η τιμή εμπιστοσύνης $tv_p(T)$ ενός κόμβου για ένα μονοπάτι συστάσεων p δίνεται από τον τύπο:

$$tv_p(T) = \frac{tv(R1)}{4} \times \frac{tv(R2)}{4} \times \dots \times \frac{tv(Rn)}{4} \times rtv(T),$$

όπου $tv(Ri)$ η τιμή εμπιστοσύνης των συνιστώντων στο μονοπάτι συστάσεων, συμπεριλαμβανομένου του πρώτου και του τελευταίου συνιστώντος, δηλαδή εκείνου που έκανε την πρώτη σύσταση και εκείνου που ζήτησε αρχικά τη σύσταση, και $rtv(T)$ η τιμή εμπιστοσύνης η οποία συστήθηκε για τον κόμβο που ζητήθηκε στο μήνυμα RRQ. Στην περίπτωση που ο κόμβος αποστολέας λάβει περισσότερες από μία συστάσεις για τον κόμβο που ζήτησε μέσω διαφορετικών μονοπατιών, τότε η τελική τιμή εμπιστοσύνης του κόμβου υπολογίζεται ως η μέση τιμή των επιμέρους τιμών εμπιστοσύνης $tv_i(T)$ από κάθε μονοπάτι i.

Η φήμη κάποιου κόμβου μπορεί να αλλάξει και έτσι να χρειαστεί να ενημερωθούν οι πληροφορίες φήμης και κατ' επέκταση οι συστάσεις που διαθέτουν οι υπόλοιποι για αυτόν. Αυτό επιτυγχάνεται με ένα μήνυμα ανανέωσης, που αποστέλλεται από τον κόμβο που έκανε τη σύσταση για τον υπό εξέταση κόμβο και για την κατηγορία που ζητήθηκε, προς όλους τους κόμβους που τη ζήτησαν. Το μήνυμα αυτό περιέχει αλλαγμένη την τιμή εμπιστοσύνης, ώστε να ανταποκρίνεται στη νέα φήμη του κόμβου για τον οποίο έγινε η σύσταση. Εάν η νέα τιμή εμπιστοσύνης είναι 0, δηλαδή η κόμβος είναι πλέον αναξιόπιστος, τότε η σύσταση δε λέμε ότι ανανεώνεται αλλά ότι ανακαλείται.

3.5. Χρήση ιδιοδιανυσμάτων για τον προσδιορισμό της εμπιστοσύνης

Τα διανύσματα χρησιμοποιούνται συχνά για την αναπαράσταση μεγεθών τα οποία αποτελούνται από πολλές συνιστώσες. Η καθολική εμπιστοσύνη ενός κόμβου αποτελεί ένα τέτοιο μέγεθος. Το μοντέλο που ακολουθεί αξιοποιεί τις ιδιότητες των ιδιοδιανυσμάτων προκειμένου να υπολογίσει καθολικές τιμές εμπιστοσύνης.

3.5.1. Το μοντέλο του EigenTrust

Οι Kamvar et al. [42] ασχολήθηκαν με το πρόβλημα των επιθέσεων κακόβουλων κόμβων σε δίκτυα ομότιμων κόμβων. Οι κακόβουλοι ομότιμοι κόμβοι χρησιμοποιούν τα δίκτυα αυτά για να εισάγουν ιούς ή να κάνουν επιθέσεις μη αυθεντικών αρχείων, κατά τις οποίες απαντούν σε οποιοδήποτε αίτημα αποστολής αρχείου αποστέλλοντας παραποιημένα ή μη λειτουργικά αρχεία. Οι συγγραφείς επιχειρούν να αναγνωρίσουν τους κακόβουλους αυτούς κόμβους χρησιμοποιώντας μια μέθοδο κατά την οποία εκχωρείται σε κάθε κόμβο μια μοναδική τιμή καθολικής εμπιστοσύνης, η οποία εκφράζει τις εμπειρίες όλων των ομότιμων κόμβων του δικτύου με τον κόμβο αυτό. Στον υπολογισμό κάθε τέτοιας τιμής συμμετέχουν όλοι οι ομότιμοι κόμβοι με κατανεμημένο και συμμετρικό τρόπο, ώστε να μην επιβαρύνεται πολύ το δίκτυο.

Αρχικά οι Kamvar et al. θέτουν κάποιες προϋποθέσεις για τον τρόπο λειτουργίας των δικτύων ομότιμων κόμβων. Σύμφωνα με τις προϋποθέσεις αυτές, το δίκτυο δεν πρέπει να διοικείται από κάποια κεντρική αρχή, αλλά οι πολιτικές που ακολουθούν οι χρήστες του δικτύου πρέπει να προέρχονται από τους ίδιους. Επιπλέον, κάθε χρήστης πρέπει να παραμένει ανώνυμος και η φήμη του να συνδέεται μόνο με ένα αδιαφανές αναγνωριστικό, ενώ οι νέοι χρήστες δεν πρέπει να λαμβάνουν κάποιο κέρδος όταν εισέρχονται στο δίκτυο. Έτσι δεν θα ενθαρρύνονται συμπεριφορές διαρκούς αλλαγής αναγνωριστικού από κόμβους με χαμηλή τιμή εμπιστοσύνης για να την αυξήσουν με πλαστό τρόπο. Συγχρόνως, οι επιβαρύνσεις στο δίκτυο όσον αφορά στους υπολογισμούς, την υποδομή, την αποθήκευση και την πολυπλοκότητα των μηνυμάτων, πρέπει να είναι ελάχιστες. Τέλος, το δίκτυο πρέπει να είναι εύρωστο απέναντι σε ομάδες κακόβουλων ομότιμων κόμβων, οι οποίοι γνωρίζονται μεταξύ τους και προσπαθούν να καταστρέψουν συλλογικά το δίκτυο.

Στο μοντέλο EigenTrust [42], κάθε φορά που κάποιος ισότιμος κόμβος κατεβάζει ένα αρχείο από κάποιον άλλο, βαθμολογεί τη συναλλαγή ως θετική $(+1)$ ή ως αρνητική (-1). Αρνητική τιμή αποδίδεται, για παράδειγμα, εάν το αρχείο είναι πλαστό, παραποιημένο ή ακόμα και αν η μεταφορά του αρχείου διεκόπη. Κάθε ισότιμος κόμβος i αποθηκεύει τον αριθμό των ικανοποιητικών συναλλαγών που είχε με έναν άλλο κόμβο j και τον αριθμό των ανικανοποίητων

συναλλαγών που είχε με τον ίδιο κόμβο και υπολογίζει την τοπική τιμή εμπιστοσύνης s_{ij} από τη διαφορά των δύο τιμών. Το EigenTrust συγκεντρώνει τις τοπικές τιμές εμπιστοσύνης όλων των χρηστών με ελάχιστες επιβαρύνσεις για το δίκτυο. Το μοντέλο βασίζεται στη μεταβατική εμπιστοσύνη. Έτσι, ένας ισότιμος κόμβος εμπιστεύεται πολύ τους κόμβους οι οποίοι τού παρείχαν αυθεντικά αρχεία, αλλά επιπλέον είναι πολύ πιθανό να εμπιστευτεί και την άποψή τους για τις τοπικές τιμές εμπιστοσύνης που διαθέτουν, δεδομένου ότι ήταν ήδη ειλικρινείς για τα αρχεία που παρείχαν.

Προκειμένου να χρησιμοποιηθούν για την παραγωγή των αντίστοιχων καθολικών τιμών εμπιστοσύνης, οι τοπικές τιμές εμπιστοσύνης κανονικοποιούνται και παίρνουν τιμές που ανήκουν στο διάστημα $[0..1]$, αποφεύγοντας έτσι περιπτώσεις κακόβουλων κόμβων, οι οποίοι αποδίδουν μεγάλες τιμές εμπιστοσύνης σε άλλους κακόβουλους κόμβους και μικρές σε καλούς ισότιμους κόμβους. Η κανονικοποίηση γίνεται με τη βοήθεια του τύπου:

$$c_{ij} = \frac{\max(s_{ij}, 0)}{\sum_j \max(s_{ij}, 0)}.$$

Στη συνέχεια το μοντέλο βρίσκει την εμπιστοσύνη t_{ik} που έχει ο κόμβος i για τον κόμβο k βασιζόμενος στις απόψεις των φίλων του. Η εμπιστοσύνη αυτή, η οποία επηρεάζεται από την εμπιστοσύνη που έχει ο κόμβος i στους φίλους του, δίνεται από τον τύπο:

$$t_{ik} = \sum_j c_{ij} c_{jk}.$$

Εάν ορίσουμε ως C τη μήτρα $|c_{ij}|$ και ως $\vec{t_\iota}$ το διάνυσμα που περιέχει τις τιμές t_{ik}, τότε ισχύει $\vec{t_\iota} = C^T \vec{c_\iota}$. Έτσι, χρησιμοποιώντας τον τύπο αυτό και ζητώντας τις απόψεις των φίλων των φίλων του για τους υπόλοιπους κόμβους, ο κόμβος i μπορεί να αποκτήσει συνολική άποψη για όλο το δίκτυο. Εάν δε το δίκτυο είναι αρκετά μεγάλο, το διάνυσμα εμπιστοσύνης $\vec{t_\iota}$ θα συγκλίνει στο ίδιο διάνυσμα για κάθε κόμβο, δηλαδή στο αριστερό βασικό ιδιοδιάνυσμα (principal eigenvector) του C. Άρα το διάνυσμα $\vec{t}$ είναι το διάνυσμα καθολικής εμπιστοσύνης και τα στοιχεία του αναπαριστούν την εμπιστοσύνη που έχει το σύστημα ως σύνολο στον κάθε κόμβο.

Οι Kamvar et al. περιέγραψαν το βασικό αλγόριθμο EigenTrust [42] θεωρώντας αρχικά ότι κάποιος κεντρικός υπολογιστής γνωρίζει όλες τις κανονικοποιημένες τοπικές τιμές εμπιστοσύνης και πραγματοποιεί τους υπολογισμούς. Οι συγγραφείς ορίζουν ως $\vec{e}$ το m-διάνυσμα που αναπαριστά μια ομοιόμορφη κατανομή πιθανότητας σε όλους τους κόμβους m του δικτύου, δηλαδή $e_i = 1/m$. Ο αλγόριθμος αυτός δεν συμπεριλάμβανε περιπτώσεις όπως η ύπαρξη εξ' ορισμού αξιόπιστων κόμβων, περιπτώσεις όπου κόμβοι δεν κατεβάζουν αρχεία από άλλους κόμβους ή βαθμολογούν όλους τους υπόλοιπους με 0, καθώς και περιπτώσεις ύπαρξης ομάδων κακόβουλων κόμβων. Για το λόγο αυτό ο αλγόριθμος τροποποιήθηκε με τον ορισμό μιας κατανομής $\vec{p}$ των από πριν αξιόπιστων κόμβων P, καθώς και με την εισαγωγή συναρτήσεων από τις οποίες προκύπτουν το μέγεθος c_{ij} και το διάνυσμα $\vec{t}$, σύμφωνα με τους τύπους:

$$c_{ij} = \begin{cases} \dfrac{\max(s_{ij}, 0)}{\sum_j \max(s_{ij}, 0)} & \text{εάν } \sum_j \max(s_{ij}, 0) \neq 0 \\ p_j & \text{διαφορετικά} \end{cases}$$

$$\vec{t}^{(k+1)} = (1-\alpha)C^T\vec{t}^{(k)} + \alpha\vec{p}\,,$$

όπου $p_i = 1/|P|$, εάν $i \in P$ και $p_i = 0$ διαφορετικά, και όπου a μια σταθερά με τιμή μικρότερη από 1.

Ο παραπάνω αλγόριθμος επεκτείνεται στη συνέχεια για να συμπεριλάβει και την περίπτωση του κατανεμημένου δικτύου, όπου όλοι οι ισότιμοι κόμβοι συνεργάζονται για να υπολογίσουν το διάνυσμα καθολικής εμπιστοσύνης και οι επιβαρύνσεις κάθε κόμβου λόγω υπολογισμών, αποθήκευσης και ανταλλαγής μηνυμάτων είναι ελάχιστες. Κάθε κόμβος υπολογίζει και αποθηκεύει τη δική του καθολική τιμή εμπιστοσύνης με τη βοήθεια του τύπου:

$$t_i^{(k+1)} = (1-\alpha)\left(c_{1i}t_1^{(k)} + \cdots + c_{ni}t_n^{(k)}\right) + \alpha p_i\,,$$

στον οποίο n είναι το σύνολο των κόμβων του δικτύου, ενώ πολλοί όροι της συνάρτησης είναι μηδενικοί, λόγω της περιορισμένης αλληλεπίδρασης του κάθε κόμβου με τους υπόλοιπους κόμβους του δικτύου. Στον αλγόριθμο αυτό, η τιμή της κατανομής p_i για κάθε εξ' ορισμού αξιόπιστο κόμβο είναι γνωστή μόνο στον ίδιο τον κόμβο, κάτι που τον διατηρεί ανώνυμο απέναντι στους υπόλοιπους κόμβους του δικτύου.

Οι συγγραφείς, εντοπίζοντας το πρόβλημα των κακόβουλων κόμβων, οι οποίοι μπορεί να δηλώσουν λανθασμένες τιμές εμπιστοσύνης στην προσπάθειά τους να υπονομεύσουν το σύστημα, χρησιμοποιούν βασικές αλλαγές στον αλγόριθμο για τα κατανεμημένα περιβάλλοντα δικτύων, εισάγοντας έτσι το ασφαλές EigenTrust. Σύμφωνα με τις αλλαγές αυτές, η τιμή εμπιστοσύνης ενός κόμβου δεν υπολογίζεται από τον ίδιο τον κόμβο, αλλά από ένα σύνολο άλλων κόμβων, τους λεγόμενους διαχειριστές βαθμολογίας. Έτσι, εάν κάποιος κόμβος χρειάζεται την τιμή εμπιστοσύνης κάποιου άλλου κόμβου, στέλνει αιτήματα στους διαχειριστές βαθμολογίας του κόμβου αυτού. Η τιμή εμπιστοσύνης είναι τότε εκείνη που παρουσιάζει πλειοψηφία έναντι τυχόν άλλων τιμών, οι οποίες θα έχουν δοθεί από κακόβουλους κόμβους που μπορεί να βρίσκονται ανάμεσα στους διαχειριστές. Για την επιλογή των διαχειριστών, χρησιμοποιείται ένας κατανεμημένος πίνακας κατακερματισμού (DHT-Distributed Hash Table). Οι κατανεμημένοι πίνακες κατακερματισμού χρησιμοποιούν μια συνάρτηση κατακερματισμού για να χαρτογραφήσουν με ντετερμινιστικό τρόπο κλειδιά, όπως ονόματα αρχείων, και να τα αναπαραστήσουν ως σημεία σε ένα διάστημα λογικών συντεταγμένων. Κάθε στιγμή το διάστημα συντεταγμένων χωρίζεται δυναμικά μεταξύ των κόμβων του συστήματος, έτσι ώστε κάθε κόμβος να καλύπτει κάποια περιοχή του διαστήματος, ενώ είναι υπεύθυνος για την αποθήκευση ζευγών κλειδί-τιμή, τα κλειδιά των οποίων έχουν κατακερματιστεί και αναπαριστούν κάποιο σημείο που βρίσκεται στην περιοχή τους.

Στην περίπτωση του ασφαλούς EigenTrust, ένας διαχειριστής βαθμολογίας κάποιου κόμβου προκύπτει από τον κατακερματισμό ενός μοναδικού αναγνωριστικού τού κόμβου αυτού, όπως η διεύθυνση δικτύου και η πόρτα TCP του, και η αναπαράστασή του σε ένα σημείο στο κατακερματισμένο διάστημα του πίνακα κατανεμημένου κατακερματισμού. Ο κόμβος ο οποίος καλύπτει το διάστημα στο οποίο ανήκει το σημείο αυτό, ορίζεται ως διαχειριστής βαθμολογίας του κόμβου. Έτσι, όλοι οι κόμβοι του συστήματος, οι οποίοι γνωρίζουν τη διεύθυνση δικτύου του κόμβου, μπορούν να εντοπίσουν το διαχειριστή βαθμολογίας του. Οι συγγραφείς βασίζουν την εφαρμογή του ασφαλούς EigenTrust σε ένα καλοσχεδιασμένο κατανεμημένο πίνακα κατακερματισμού, όπου οι διαχειριστές βαθμολογίας που αποχωρούν από το δίκτυο, προωθούν τις τιμές εμπιστοσύνης που διαθέτουν ή τον τρέχοντα υπολογισμό τιμών στον κόμβο που βρίσκεται δίπλα τους στο ισότιμο διάστημα του πίνακα, ενώ χρησιμοποιούνται και τα αντίγραφα δεδομένων για την αποφυγή απωλειών όταν χαθεί κάποιος διαχειριστής.

Οι καθολικές τιμές εμπιστοσύνης που δίνει ο ασφαλής αλγόριθμος EigenTrust μπορούν να χρησιμοποιηθούν για να απομονώσουν τους κακόβουλους κόμβους από το δίκτυο. Αυτό μπορεί να γίνει επιλέγοντας πιθανοτικά τους κόμβους από τους οποίους κάποιος άλλος κόμβος

θα κατεβάσει αρχεία, βασιζόμενος στις τιμές εμπιστοσύνης τους. Έτσι, η πιθανότητα ότι ένας κόμβος θα κατεβάσει ένα αρχείο από τον κόμβο j θα είναι ανάλογη προς την τιμή εμπιστοσύνης του t_j. Με αυτό τον τρόπο περιορίζονται τα κατεστραμμένα αρχεία που υπάρχουν στο δίκτυο και εξισορροπείται ο φόρτος του δικτύου, επιτρέποντας και σε νέους κόμβους να αποκτήσουν καλή φήμη. Υπάρχει όμως και η περίπτωση κατά την οποία ένας κόμβος παρέχει κακή εξυπηρέτηση σε κάποιον κόμβο, παρόλο που γενικά διαθέτει καλή καθολική τιμή εμπιστοσύνης. Σε αυτήν την περίπτωση, ο δεύτερος κόμβος μπορεί να επηρεάσει την επιλογή του για τον κόμβο από τον οποίο θα κατεβάσει κάποιο αρχείο, συνδυάζοντας τις καθολικές τιμές εμπιστοσύνης με τη δική του τοπική αποτίμηση εμπιστοσύνης για τους άλλους κόμβους και χρησιμοποιώντας τις τιμές εμπιστοσύνης που προκύπτουν από το διάνυσμα $\vec{t}_{προσωπικό} = d\vec{t} + (1-d)\vec{c}$, όπου d μια σταθερά στο διάστημα $[0..1]$. Επιπλέον, το σύστημα μπορεί να επιβραβεύει τους κόμβους που έχουν υψηλές τιμές εμπιστοσύνης, παρέχοντάς τους αυξημένη συνδεσιμότητα με άλλους αξιόπιστους κόμβους ή μεγαλύτερο εύρος ζώνης. Έτσι, οι χρήστες αποκτούν κίνητρο για να μοιράζονται τα αρχεία τους και μάλιστα να διαγράφουν όποια μη αυθεντικά αρχεία έχει τύχει να κατεβάσουν από κάποιον κακόβουλο χρήστη, εμποδίζοντάς την επανάληψή τους στο δίκτυο.

3.6. Υπολογισμός εμπιστοσύνης βάσει κοινών χαρακτηριστικών

Δεδομένου ότι η εμπιστοσύνη έχει πολλές πλευρές και περιεχόμενα, πολλά μοντέλα υπολογίζουν τις τιμές εμπιστοσύνης με βάση τα κοινά ενδιαφέροντα των κόμβων.

3.6.1. Το μοντέλο Poblano

Οι Chen και Yeager [43] πρότειναν ένα αποκεντρωμένο μοντέλο εμπιστοσύνης για εφαρμογές σε JXTA, το Poblano. Η JXTA είναι μια γλώσσα προγραμματισμού και πρωτόκολλο ανοιχτού κώδικα, ανεξάρτητο πλατφόρμας, για δίκτυα ομότιμων κόμβων που ξεκίνησε η Sun Microsystems το 2001. Το μοντέλο παρέχει εκτός από τις σχέσεις εμπιστοσύνης μεταξύ των ομότιμων κόμβων και σχέσεις μεταξύ αυτών και υποδοχέων αντικειμένων της Java (codat). Οι συγγραφείς περιγράφουν τα πρωτόκολλα για τη διάδοση της εμπιστοσύνης και τους αλγορίθμους για την ανανέωσή της. Μια δεύτερη εφαρμογή του μοντέλου Poblano είναι η δημιουργία ενός συστήματος σύστασης για λόγους ασφαλείας.

Όπως αναφέρουν οι συγγραφείς, η εμπιστοσύνη έχει πολλούς παράγοντες και περιεχόμενα και ασχολήθηκαν με τον παράγοντα της εμπιστοσύνης που βασίζεται στα ενδιαφέροντα της ομάδας. Για το λόγο αυτό, κάθε ομότιμος κόμβος στο μοντέλο Poblano αξιολογεί την εμπιστοσύνη του σε codats, προκειμένου στη συνέχεια να δημιουργήσει σχέσεις εμπιστοσύνης με αυτά. Για να αξιολογηθεί η εμπιστοσύνη στα ενδιαφέροντα ενός ομότιμου κόμβου, αυτά αναπαρίστανται με λέξεις κλειδιά. Στη συνέχεια, τα αποτελέσματα της αξιολόγησης των λέξεων κλειδιών του συνόλου του codat αποστέλλονται από έναν ομότιμο κόμβο σε έναν άλλο, προκειμένου ο δεύτερος να αξιολογήσει την εμπιστοσύνη του προς τον πρώτο μέσω της αξιολόγησης του λαμβανόμενου συνόλου ενδιαφερόντων. Έτσι, η αξιολόγηση της εμπιστοσύνης για έναν ομότιμο κόμβο βασίζεται στα ενδιαφέροντα ενός άλλου κόμβου.

Το μοντέλο Poblano χρησιμοποιεί τρεις κλάσεις για να αναπαραστήσει τα διαφορετικά συστατικά εμπιστοσύνης, τις κλάσεις CodatConfidence, PeerConfidence και Risk. Η πρώτη κλάση χρησιμοποιείται για να αξιολογήσει το συστατικό εμπιστοσύνης codat (codat trust component) με βάση μια λέξη κλειδί, η δεύτερη για να αξιολογήσει το συστατικό εμπιστοσύνης codat ομότιμου κόμβου (codat peer trust component) με βάση μια λέξη κλειδί και η τρίτη για να αξιολογήσει το συστατικό εμπιστοσύνης κίνδυνος ομότιμου κόμβου (peer's risk trust component). Οι δύο τελευταίες κλάσεις και οι πιο σημαντικές και χρησιμοποιούνται για να καθορίσουν εάν ένας ομότιμος κόμβος στόχος είναι ικανός να συνεργαστεί και άρα να είναι αξιόπιστος. Κάθε κόμβος έχει πίνακες PeerConfidence και τόσους πίνακες CodatConfidence όσες και οι ομάδες ομότιμων κόμβων στις οποίες ανήκει. Επίσης, κάθε ομάδα ομότιμων κόμβων διαθέτει πίνακα CodatConfidence, δεδομένου ότι το codat συσχετίζεται με ομάδες ομότιμων

κόμβων. Ο πρώτος πίνακας PeerConfidence περιέχει τους ομότιμους κόμβους που ανήκουν σε μια ομάδα και για τους οποίους ο κόμβος έχει πληροφορίες για τη λέξη κλειδί και το codat. Ο δεύτερος πίνακας PeerConfidence βρίσκεται σε όλες τις ομάδες στις οποίες ανήκει ο κόμβος, προκύπτει από τον πρώτο πίνακα και επιτρέπει τους υπολογισμούς μιας τιμής PeerConfidence ανεξαρτήτως των ομάδων στις οποίες ανήκει ο ομότιμος κόμβος. Επίσης, κάθε ομότιμος δεν είναι μέλος σε όλα τα PeerGroups, όπως και κάθε νέος ομότιμος δεν ανήκει απαραίτητα σε κάποιο PeerGroup.

Οι συγγραφείς αναφέρουν ότι προκειμένου ένας ομότιμος κόμβος να βρει μια λέξη κλειδί ακολουθεί τα επόμενα βήματα. Αρχικά ψάχνει για τη λέξη κλειδί στον πίνακά του CodatConfidence και αν βρει ένα codat που να σχετίζεται με τη λέξη που θέλει, τότε η διαδικασία τελειώνει. Σε διαφορετική περίπτωση, ψάχνει στον πίνακά του PeerConfidence. Εάν υπάρχουν εκεί κόμβοι που να συνδέονται πολύ με αυτή τη λέξη κλειδί, τους αποστέλλει το αίτημά του. Όταν λάβουν το αίτημα, καθένας από τους κόμβους αυτούς θα επαναλάβει τις προηγούμενες διαδικασίες στους δικούς τους πίνακες. Εάν κάποιος βρει ένα codat που να σχετίζεται με τη λέξη, ενημερώνει τον ομότιμο κόμβο που απέστειλε το αίτημα και η διαδικασία ολοκληρώνεται. Εάν όμως και πάλι η αναζήτηση αποτύχει, τότε ο αρχικός κόμβος αναζητά στους πίνακες με τις λέξεις κλειδιά των ομάδων ομότιμων κόμβων άλλες πιθανές πηγές για αυτό που ψάχνει.

Ο τρόπος υπολογισμού του CodatConfidence έχει ως εξής: καθώς ο ομότιμος κόμβος που έχει κάνει το αίτημα προσπελαύνει το codat, η τιμή της δημοτικότητας του παρόχου αυξάνεται κατά μία μονάδα. Το παλιό αντικείμενο confidence για τον πάροχο, σε αναφορά με τη λέξη κλειδί, ενημερώνεται με βάση την εκτίμηση του codat από τον αιτώντα. Τώρα ο αιτών έχει μια νέα εγγραφή στο δικό του πίνακα CodatConfidence. Όλες οι εκτιμήσεις codat για το δεδομένο ομότιμο θα χρησιμοποιηθούν για τη δημιουργία μιας τιμής PeerConfidence για τον πάροχο σε σχέση με το δεδομένο ζεύγος λέξη κλειδί και codat. Η ίδια εκτίμηση codat θα σταλεί επίσης στον πάροχο, ο οποίος μπορεί να ενημερώσει το δικό του πίνακα CodatConfidence με μια συνάρτηση που βασίζεται στην προηγούμενη τιμή, στη νέα τιμή και στην εμπιστοσύνη του στον αιτώντα.

Οι Chen και Yeager παρουσιάζουν στη συνέχεια έναν απλό αλγόριθμο για την εκτίμηση του βαθμού της διαδιδόμενης εμπιστοσύνης. Η τιμή της εμπιστοσύνης παίρνει τις τιμές -1, 0, 1, 2, 3 και 4, οι οποίες περιγράφουν τη δυσπιστία, την άγνοια, την ελάχιστη εμπιστοσύνη, τη μέση εμπιστοσύνη, την καλή εμπιστοσύνη και, τέλος, την απόλυτη εμπιστοσύνη αντίστοιχα. Όταν η εμπιστοσύνη έχει τιμές -1 ή 0, το αντίστοιχο codat δεν προσπελαύνεται ποτέ. Ο υπολογισμός της τιμής της εμπιστοσύνης $V_{path}(T)$ για έναν ομότιμο κόμβο στόχο T, η οποία διαδίδεται μέσω ενός μονοπατιού από τον ομότιμο s και μέσω των ομότιμων κόμβων P_i, όπου i = 1, 2, ..., n δίνεται από τον τύπο:

$$V_{path}(T) = \frac{1}{4n} \left(\sum_{i=1}^{n} V(P_i)\right) \times V(T) \ ,$$

όπου $V(P_i)$ η τιμή εμπιστοσύνης του ομότιμου P_i ο οποίος παρέχει την πληροφορία και $V(T)$ η τιμή εμπιστοσύνης του ομότιμου T. Στην περίπτωση που υπάρχουν περισσότερα από ένα μονοπάτια μεταξύ των δύο κόμβων, τότε η τελική τιμή εμπιστοσύνης είναι η μέση τιμή όλων των μεταδιδόμενων τιμών εμπιστοσύνης. Στο μοντέλο Poblano οι τιμές PeerConfidence και CodatConfidence αποτελούν τις μετρικές συνάφειας για ένα codat μέσα σε ένα δεδομένο PeerGroup. Έτσι, ο παραπάνω τύπος μετασχηματίζεται χρησιμοποιώντας την τιμή CodatConfidence, η οποία είναι η πληροφορία που μεταδίδεται, και την τιμή PeerConfidence, η οποία είναι η πληροφορία του μεταφορέα που χρησιμοποιείται για το βάρος και καταλήγει στον τύπο:

$$CodatConf_{path} = \frac{1}{4n}\left(\sum_{i=1}^{n} PeerConf(P_i)\right) \text{ x } CodatConf.$$

Η τιμή της μετάδοσης αυτής μέσω του μονοπατιού υπολογίζεται σε δύο περιπτώσεις. Αρχικά, εάν ένας απομακρυσμένος κόμβος ζητήσει μια πληροφορία, ο πάροχος του αποστέλλει το αντικείμενο CodatConfidence. Εάν μετά τον υπολογισμό της τιμής $CodatConf_{path}$ ο αιτών θέλει ακόμα το codat, ο πάροχος τού το αποστέλλει. Η δεύτερη περίπτωση είναι μετά τη χρήση του codat, όπου ο κόμβος που το αιτήθηκε στέλνει ως ανάδραση το νέο αντικείμενο CodatConfidence στον πάροχο μέσω του ίδιου μονοπατιού από το οποίο το έλαβε.

Στην περίπτωση της ενημέρωσης της τιμής της εμπιστοσύνης, κάθε ομότιμος ενημερώνει τρία είδη πινάκων πεποίθησης και οι ενημερώσεις βασίζονται, εκτός από τις εκτιμήσεις του κόμβου, στις αναδράσεις που λαμβάνει. Εάν ένας ομότιμος θελήσει να ενημερώσει το CodatConfidence που διαθέτει χρησιμοποιώντας τη δική του εκτίμηση και την τιμή του CodatConfidence που έλαβε από άλλους ομότιμους, χρησιμοποιεί τον παρακάτω τύπο:

$$\begin{aligned} &\textit{νέο\_CodatConf} = F\left(\textit{παλιό\_CodatConf, διαδιδόμενο\_CodatConf, εκτίμηση\_ομότιμου}\right) = \\ &a \text{ x } \textit{παλιό\_CodatConf} + b \text{ x } \textit{διαδιδόμενο\_CodatConf} + c \text{ x } \textit{εκτίμηση\_ομότιμου}\,, \end{aligned}$$

όπου $a + b + c = 1$ και a, b, c θετικοί πραγματικοί αριθμοί. Επειδή η προσωπική εκτίμηση του ομότιμου έχει μεγαλύτερη σημασία, τίθεται $c = 0{,}7$, ενώ εάν η νέα τιμή δημοτικότητας είναι μεγαλύτερη από την παλιά, τότε τίθεται $a = 0{,}1$ και $b = 0{,}2$. Σε διαφορετική περίπτωση, οι τιμές είναι ανάποδα. Εάν όμως ένας ομότιμος κόμβος θελήσει να ενημερώσει την τιμή CodatConfidence που διαθέτει χρησιμοποιώντας μια ανάδραση που έλαβε από κάποιον άλλο ομότιμο για τον οποίο διαθέτει τιμή PeerConfidence, χρησιμοποιεί τον τύπο:

$$\begin{aligned} &\textit{νέο\_CodatConf} = F\left(\textit{παλιό\_CodatConf, ανάδραση, PeerConf\_ομότιμου}\right) = \\ &\frac{\textit{παλιό}_{CodatConf} + \textit{ανάδραση} * \dfrac{PeerConf\_\textit{ομότιμου}}{4}}{2}. \end{aligned}$$

Εάν η τιμή του PeerConfidence δεν είναι γνωστή τότε τίθεται ίση με τη μονάδα. Τέλος, εάν ένας ομότιμος κόμβος θελήσει να ενημερώσει την τιμή PeerConfidence για έναν πάροχο στην ομάδα, διαθέτοντας μόνο την τιμή CodatConfidence σχετική με όλο το codat που παρέχει ο πάροχος, χρησιμοποιεί τον τύπο:

$$\begin{aligned} &\textit{νέο\_PeerConf} = F\left(\textit{παλιό\_PeerConf, CodatConf\_σχετικό\_με\_codat\_παρόχου}\right) = \\ &\frac{\textit{παλιό\_PeerConf} + \dfrac{\sum_{a \in K} CodatConf\_\textit{παρόχου}}{|K|}}{2}, \end{aligned}$$

όπου $|K|$ ο αριθμός των λέξεων κλειδιών που σχετίζονται με τον πάροχο.

Οι Chen και Yeager ορίζουν μια συνθήκη κάτω από την οποία ένας κόμβος είναι συνεργάσιμος. Η συνθήκη αυτή, η οποία φαίνεται στον τύπο παρακάτω, εξαρτάται από μια στατιστική τιμή κινδύνου, η οποία κυμαίνεται από 0 μέχρι 4, με το 4 να σημαίνει μέγιστος κίνδυνος, τις τιμές CodatConfidence και μια τιμή σπουδαιότητας, η οποία δηλώνει το πόσο σημαντική είναι η συνεργασία για τον κόμβο και παίρνει τις τιμές -1, 0, 1, 2, 3 και 4:

$$PeerConf_{keyword} \text{ x } Σπουδαιότητα > \frac{Κίνδυνος_{κόμβου}}{\frac{\sum_{a \in K} CodatConf_{κόμβου}}{|K|}},$$

όπου |K| το σύνολο των λέξεων κλειδιών για τον συγκεκριμένο κόμβο για τον οποίο υπάρχουν τιμές CodatConfidence σε όλες τις ομάδες κόμβων. Οι τιμές CodatConfidence χρησιμοποιούνται για να δείξουν την ικανότητα που έχει επιδείξει ο κόμβος.

Οι συγγραφείς παρουσιάζουν στη συνέχεια μια λύση για δημιουργία ενός φάσματος εμπιστοσύνης (trust spectrum), στο οποίο θα δημιουργούνται και θα διανέμονται υπογεγραμμένα πιστοποιητικά. Οι κόμβοι θα έχουν μοναδικά αναγνωριστικά για να επιτρέπεται η αυθεντικοποίηση και θα τους εκχωρούνται πολιτικές πρόσβασης εντός των ομάδων στις οποίες ανήκουν, όπως ο ρόλος της αυθεντικοποίησης και της εξουσιοδότησης. Σύμφωνα με το φάσμα αυτό εμπιστοσύνης, κοντά στο ένα καταληκτικό σημείο υπάρχουν υπογεγραμμένα πιστοποιητικά CA, ενώ κοντά στο άλλο αυτό-υπογεγραμμένα πιστοποιητικά. Τα μέλη κάθε ομάδας θα αποφασίζουν σε ποιο σημείο εμπιστοσύνης του φάσματος θα επιλέγουν να επικοινωνούν. Οποιοσδήποτε κόμβος θα μπορεί να μπει σε μια ομάδα και να προσφέρει τις υπηρεσίες του. Όλα τα μέλη της ομάδας θα έχουν ένα PeerConfidence και θα μπορούν να μεταβιβάσουν την εξουσία υπογραφής πιστοποιητικών σε επιλεγμένα μέλη της ομάδας, κάτι που σε συνδυασμό με την αυστηρή αυθεντικοποίηση και την εξουσιοδότηση, θα μπορεί να αποτρέψει την κλοπή ρόλων εντός μιας ομάδας.

Οι Chen και Yeager προχωρούν ένα βήμα παραπέρα, θεωρώντας το πιστοποιητικό ως μια μορφή codat και εφαρμόζουν το μοντέλο Poblano στη συλλογή υπογεγραμμένων πιστοποιητικών μιας ομάδας που διαθέτει κάθε μέλος της για την ομάδα αυτή. Έτσι, κάθε κόμβος ο οποίος ψάχνει για ένα υπογεγραμμένο πιστοποιητικό κάποιου κόμβου, το ψάχνει ως λέξη κλειδί στη συλλογή υπογεγραμμένων πιστοποιητικών της ομάδας που διαθέτουν οι υπόλοιπου κόμβοι. Σε κάθε PeerGroup υπάρχουν πλέον οι πίνακες CertConf και PeerConf, από τους οποίους στον πρώτο υπάρχουν όλοι οι κόμβοι της ομάδας με το υπογεγραμμένο πιστοποιητικό τους και η τιμή εμπιστοσύνης σε αυτά, ενώ στον δεύτερο πίνακα υπάρχουν δύο τιμές για κάθε κόμβο, μια για τη βεβαιότητα στη χρήση του πιστοποιητικού του συγκεκριμένου κόμβου ($PeerConf_{πιστοπ}$) και μια για την εκτίμηση της ικανότητας του κόμβου να συστήνει ή να συνυπογράφει πιστοποιητικά ($PeerConf_{συστ}$). Τέλος, οι συγγραφείς δίνουν έναν τύπο για την ανανέωση της τιμής του $PeerConf_{συστ}$ ενός κόμβου με την πάροδο του χρόνου, υπολογίζοντας τη μέση τιμή των συστάσεων για τον κόμβο αυτό:

$$coPeerConf_{rec}\ (P_0) = \frac{1}{|K|} \sum_{a \in K} (CertConf_{path})_a\ ,$$

όπου K το σύνολο των CertConf για τα οποία δεν υπάρχουν προεπιλεγμένες τιμές στον πίνακα PeerConf για πιστοποιητικά που έχει συστήσει ή έχει συνυπογράψει ο κόμβος P_0.

3.7. Χρήση Μπεϋζιανών δικτύων για την αναπαράσταση της εμπιστοσύνης

Πολλά μοντέλα εμπιστοσύνης χρησιμοποιούν Μπεϋζιανά δίκτυα για να αναπαραστήσουν τις σχέσεις μεταξύ ομότιμων κόμβων και να βοηθήσουν στον εύκολο υπολογισμό της διαφοροποιημένης εμπιστοσύνης.

3.7.1. Το μοντέλο των Wang και Vassileva

Οι Wang και Vassileva [44] πρότειναν ένα μοντέλο για τα δίκτυα ομότιμων κόμβων, το οποίο βασίζεται σε Μπεϋζιανά δίκτυα. Τα Μπεϋζιανά δίκτυα παρέχουν μια ευέλικτη μέθοδο αναπαράστασης της διαφοροποιημένης εμπιστοσύνης, συνδυάζοντας διαφορετικές πλευρές της. Το μοντέλο που παρουσιάζεται είναι αρκετά γενικό και μπορεί να εφαρμοστεί σε πολλούς τομείς, όπως σε υπηρεσίες διαδικτύου, στο ηλεκτρονικό εμπόριο, σε συμβουλευτικά συστήματα ή σε κατανεμημένα υπολογιστικά συστήματα ομότιμων κόμβων για εφαρμογές διαμοιρασμού αρχείων.

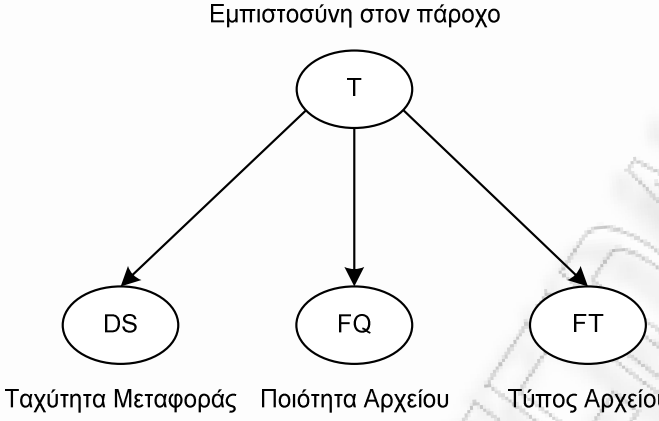
Στα συστήματα διαμοιρασμού αρχείων σε δίκτυα ομότιμων κόμβων κάθε ομότιμος παίζει το ρόλο του παρόχου αρχείων σε άλλους κόμβους και το ρόλο του χρήστη των αρχείων που του παρέχουν άλλοι κόμβοι. Έτσι αναπτύσσει δύο είδη εμπιστοσύνης, εκείνο της εμπιστοσύνης στην αξιοπιστία άλλων κόμβων να παρέχουν συστάσεις για άλλους κόμβους και εκείνο της εμπιστοσύνης στην ικανότητα του παρόχου να παρέχει σωστά τα αρχεία που του ζητούνται. Η ικανότητα αυτή μπορεί να έχει πολλές απόψεις, όπως η ταχύτητα μεταφοράς του αρχείου, η ποιότητά του και το είδος του. Κάποιος για παράδειγμα μπορεί να είναι πολύ αξιόπιστος στο να παρέχει μουσικά αρχεία, αλλά να είναι πλήρως αναξιόπιστος στο να παρέχει αρχεία βίντεο. Οι ομότιμοι χρειάζεται πολλές φορές να αναπτύσσουν διαφορετική εμπιστοσύνη για καθεμία από τις ικανότητες ενός παρόχου αρχείων, μιας και μπορεί να ενδιαφέρονται για διαφορετική άποψη κάθε φορά της ικανότητάς του.

Οι συγγραφείς χρησιμοποιούν στο μοντέλο τους τα Μπεϋζιανά δίκτυα, μιας και αυτά αποτελούν δίκτυα σχέσεων που χρησιμοποιούν στατικές μεθόδους για την αναπαράσταση πιθανοτικών σχέσεων μεταξύ διαφορετικών ομότιμων. Ένα απλοϊκό Μπεϋζιανό δίκτυο αποτελείται από έναν κόμβο ρίζα και πολλούς κόμβους φύλλα και αναπαριστά ακριβώς τη σχέση εμπιστοσύνης μεταξύ ενός χρήστη και ενός παρόχου αρχείων. Τα Μπεϋζιανά δίκτυα στηρίζονται στον κανόνα του Bayes [45] σύμφωνα με τον οποίο

$$p(h|e) = \frac{p(e|h)p(h)}{p(e)},$$

όπου $p(h)$ και $p(e)$ οι πρότερες πιθανότητες της υπόθεσης h και της απόδειξης e αντίστοιχα, όπου $p(h|e)$ η πιθανότητα της h δεδομένης της e και όπου $p(e|h)$ η πιθανότητα της e δεδομένης της h.

Κάθε κόμβος αναπτύσσει για κάθε πάροχο με τον οποίο έχει αλληλεπιδράσει ένα απλοϊκό Μπεϋζιανό δίκτυο, με κόμβο ρίζα T ο οποίος μπορεί να λάβει τις τιμές 1 και 0 για να δηλώσει την ικανοποίηση ή τη δυσαρέσκειά του. Οι κόμβοι φύλλα αναπαριστούν τις διάφορες απόψεις για την ικανότητα του παρόχου αρχείων, όπως φαίνεται και στο σχήμα 7.



Σχήμα 7: Μοντέλο Μπεϋζιανού δικτύου

Η τιμή της συνολικής εμπιστοσύνης που έχει ο κόμβος στην ικανότητα του παρόχου να παρέχει αρχεία, συμβολίζεται με $p(T=1)$ και αποτελεί το ποσοστό των ικανοποιητικών συναλλαγών m, διαιρούμενο από το συνολικό αριθμό n των συναλλαγών, όπως φαίνεται και στον επόμενο τύπο. Αντίστοιχα, το $p(T=0)$ αποτελεί το ποσοστό των μη ικανοποιητικών συναλλαγών.

$$p(T=1) = \frac{m}{n},$$
$$p(T=1) + p(T=0) = 1.$$

Κάθε κόμβος φύλλο συνδέεται με έναν πίνακα δεσμευμένων πιθανοτήτων (conditional probability table – CPT). Κάθε πιθανότητα αναπαριστά την εμπιστοσύνη που έχει ο ομότιμος κόμβος σε κάποια πλευρά της ικανότητας του παρόχου αρχείων. Εάν υποθέσουμε ότι ένας κόμβος φύλλο μπορεί να πάρει πέντε τιμές, ο πίνακας CPT του θα αποτελείται από πέντε γραμμές για κάθε τιμή και από δύο στήλες, από τις οποίες στην πρώτη θα υπάρχουν οι πιθανότητες να είναι ικανοποιητικές οι συναλλαγές, ενώ στη δεύτερη στήλη οι πιθανότητες να μην είναι ικανοποιητικές. Όπως φαίνεται και από τον παραπάνω τύπο, το άθροισμα των πιθανοτήτων ανά γραμμή θα ισούται με τη μονάδα. Με τη χρήση των πινάκων CPT, κάθε ομότιμος κόμβος μπορεί να υπολογίσει τις πιθανότητες ένας πάροχος αρχείων να είναι αξιόπιστος από διάφορες απόψεις, κάνοντας χρήση των παραπάνω τύπων και άρα να βγάλει συμπεράσματα για την εμπιστοσύνη που πρέπει να έχει απέναντί του. Οι ομότιμοι μπορούν να θέσουν διάφορες συνθήκες ανάλογα με τις ανάγκες τους και να προσθέσουν αργότερα περισσότερες πλευρές της ικανότητας ενός παρόχου στο Μπεϋζιανό δίκτυο.

Μετά από κάθε συναλλαγή, κάθε ομότιμος ενημερώνει το αντίστοιχο Μπεϋζιανό δίκτυο. Όταν ένας ομότιμος κρίνει μια συναλλαγή, έχει κατά νου δύο παράγοντες, τους βαθμούς της ικανοποίησής του για την ταχύτητα μεταφοράς s_{ds} και την ποιότητα του μεταφερόμενου αρχείου s_{fq}. Ο συνολικός βαθμός ικανοποίησης ενός ομότιμου για μια συναλλαγή s δίνεται από τον τύπο:

$$s = w_{ds} * s_{ds} + w_{fq} * s_{fq},$$
$$w_{ds} + w_{fq} = 1,$$

όπου w_{ds} και w_{fq} είναι βάρη τα οποία δηλώνουν τη σπουδαιότητα που έχει κάθε βαθμός ικανοποίησης για έναν ομότιμο κόμβο. Κάθε ομότιμος έχει ένα κατώφλι ικανοποίησης s_t, πάνω από το οποίο μια συναλλαγή θεωρείται ικανοποιητική.

Στην εφαρμογή διαμοιρασμού αρχείων στην οποία εφαρμόζουν το μοντέλο τους οι Wang και Vassileva, οι χρήστες βρίσκουν τα αρχεία τους χρησιμοποιώντας τη λειτουργία της αναζήτησης. Μέσω αυτής τούς επιστρέφεται μια λίστα με όλους τους παρόχους για το αρχείο που ζήτησαν. Προκειμένου να επιλέξουν μέσα από τη λίστα αυτή, χρησιμοποιούν ένα μηχανισμό εμπιστοσύνης και φήμης, ο οποίος κατατάσσει τους παρόχους με βάση την εμπιστοσύνη που έχει σε αυτούς ο ομότιμος κόμβος και ο τελευταίος επιλέγει να κατεβάσει το αρχείο που ψάχνει από τον πάροχο που εμπιστεύεται περισσότερο. Εάν ο ομότιμος κόμβος δεν έχει συναλλαχθεί με κάποιον πάροχο στο παρελθόν, μπορεί να στείλει αιτήματα σύστασης ανάλογα με τις ανάγκες του σε άλλους ομότιμους κόμβους. Εκείνοι, λαμβάνοντας το αίτημα, θα ελέγξουν τα Μπεϋζιανά τους δίκτυα και αν έχουν στοιχεία για τον πάροχο για τον οποίο ζητείται η σύσταση, θα αποστείλουν την ανάλογη τιμή εμπιστοσύνης που έχουν για την πλευρά της ικανότητας που τους ζητείται. Ο ομότιμος που ζήτησε τις συστάσεις, συλλέγει όσες του έχουν αποσταλεί και εξαιρεί εκείνες που προέρχονται από αναξιόπιστους κόμβους. Στη συνέχεια συνδυάζει τις προερχόμενες από αξιόπιστους και άγνωστους κόμβους με τη βοήθεια του παρακάτω τύπου, για να καταλήξει στη συνολική τιμή σύστασης για τον πάροχο:

$$r_{ij} = w_t * \frac{\sum_{l=1}^{k} tr_{il} * t_{lj}}{\sum_{l=1}^{k} tr_{il}} + w_s * \frac{\sum_{z=1}^{g} t_{zj}}{g}, \text{ όπου } w_t + w_s = 1 ,$$

όπου r_{ij} η συνολική τιμή σύστασης για τον j–οστό πάροχο αρχείων που λαμβάνει ο i–οστός ομότιμος κόμβος. Τα k και g είναι τα σύνολα των αξιόπιστων και των άγνωστων αντίστοιχα κόμβων που έστειλαν συστάσεις. Το tr_{il} είναι η εμπιστοσύνη που έχει ο i–οστός ομότιμος κόμβος στην l–οστή αξιόπιστη σύσταση, το t_{lj} είναι η εμπιστοσύνη που η l–οστή αξιόπιστη σύσταση έχει στον j–οστό πάροχο αρχείων και το t_{zj} είναι η εμπιστοσύνη που η z–οστή αξιόπιστη σύσταση έχει στον j–οστό πάροχο αρχείων. Τα βάρη w_t και w_s χρησιμοποιούνται για να δείξουν πόσο αξιολογεί ο χρήστης τις συστάσεις από τους αξιόπιστους και από τους άγνωστους κόμβους. Ο κόμβος θα προτιμήσει τον πάροχο αυτόν, εάν τελικά η συνολική τιμή σύστασης για αυτόν είναι μεγαλύτερη από ένα δεδομένο κατώφλι θ.

Κάθε φορά που ένας κόμβος αλληλεπιδρά με έναν πάροχο μετά από την παραπάνω διαδικασία, ενημερώνει την εμπιστοσύνη του σε αυτόν στο αντίστοιχο Μπεϋζιανό δίκτυο, αλλά και την εμπιστοσύνη του στους άλλους κόμβους που του έστειλαν σύσταση για τον πάροχο αυτόν, χρησιμοποιώντας τον τύπο:

$$tr_{ij}^{n} = \alpha * tr_{ij}^{0} + (1 - \alpha) * e_{\alpha}, \text{ όπου } 0 \leq \alpha \leq 1 .$$

tr_{ij}^{n} είναι η νέα τιμή εμπιστοσύνης που έχει ο i–οστός ομότιμος κόμβος στην j–οστή σύσταση μετά την ενημέρωση, ενώ το tr_{ij}^{0} είναι η παλιά τιμή της εμπιστοσύνης. Η σταθερά α είναι ένας ρυθμός εκμάθησης. Το e_{α} καλείται νέα τιμή απόδειξης και μπορεί να πάρει τις τιμές -1 και 1. Εάν η τιμή της σύστασης που έδωσε ο κόμβος ήταν μεγαλύτερη από το κατώφλι και η αλληλεπίδραση με τον πάροχο ήταν ικανοποιητική, το e_{α} παίρνει την τιμή 1, ενώ εάν υπάρξει δυσαναλογία μεταξύ των δύο τιμών, το e_{α} παίρνει την τιμή -1.

Οι συγγραφείς παρέχουν έναν τρόπο για την ανεύρεση αναξιόπιστων ομότιμων κόμβων, τον οποίο αναφέρουν ως «κουτσομπολιό». Σύμφωνα με αυτόν, όταν οι ομότιμοι βρίσκονται σε αδράνεια, μπορούν να ανταλλάσσουν και να συγκρίνουν περιοδικά τα Μπεϋζιανά

τους δίκτυα που αναφέρονται στους ίδιους παρόχους αρχείων. Έτσι βρίσκουν γρηγορότερα και πιο αποτελεσματικά άλλους ομότιμους κόμβους, οι οποίοι έχουν τις ίδιες προτιμήσεις με αυτούς. Μετά από κάθε σύγκριση, καθένας ενημερώνει την εμπιστοσύνη του στον άλλο, με τη βοήθεια ενός παρόμοιου τύπου με τον προηγούμενο, χρησιμοποιώντας όμως την τιμή e_β αντί της e_α, η οποία παίρνει τιμές στο διάστημα [-1, 1] και τη σταθερά β αντί της α, με $\beta > \alpha$. Αυτό συμβαίνει γιατί συγκρίνοντας τα Μπεϋζιανά τους δίκτυα, οι δύο κόμβοι είναι σαν να συγκρίνουν όλες τις συναλλαγές που έχουν πραγματοποιήσει. Έτσι η απόδειξη e_β επηρεάζει περισσότερο την εμπιστοσύνη του κόμβου σε κάποιον άλλο κόμβο, από ό,τι έκανε η απόδειξη e_α η οποία βασιζόταν σε μια συναλλαγή. Η σύγκριση των Μπεϋζιανών δικτύων των δύο κόμβων γίνεται με τη σύγκριση των τιμών τους. Κάθε κόμβος υπολογίζει την ομοιότητα κάθε ζεύγους κόμβων, καθορίζοντας έτσι το βαθμό ομοιότητας των δύο Μπεϋζιανών δικτύων με τη βοήθεια του μέτρου ομοιότητας που δίνεται από τους παρακάτω τύπους και στη συνέχεια συνδυάζουν μεταξύ τους τα αποτελέσματα ομοιότητας του κάθε ζεύγους κόμβων:

$$e_\beta = 1 - 2 * \sum_{i=1}^{4}(w1_i * c_i), \text{ όπου } w1_1 + w1_2 + w1_3 + w1_4 = 1 ,$$

$$c_1 = \sqrt{\frac{(v1_{11} - v2_{11})^2}{(v1_{11} + v2_{11})^2} + \frac{(v1_{12} - v2_{12})^2}{(v1_{12} + v2_{12})^2}} ,$$

$$c_i = \frac{\sum_{j=1}^{2} \sqrt{\sum_{l=1}^{h_i} \frac{\left(v1_{ijl} - v2_{ijl}\right)^2}{\left(v1_{ijl} + v2_{ijl}\right)^2}}}{2}, \text{ όπου } i = 2, 3, 4 .$$

Τα $w1_i$ αποτελούν βάρη για τους κόμβους του δικτύου του πρώτου ομότιμου κόμβου και χρησιμοποιούνται για να δείξουν τη σπουδαιότητα των κόμβων αυτών στη σύγκριση των δύο Μπεϋζιανών δικτύων. Τα c_i είναι τα αποτελέσματα της σύγκρισης των πινάκων των δύο ομότιμων για τους κόμβους του δικτύου. Δεδομένου ότι ο πίνακας CPT του κόμβου ρίζα T έχει μόνο μια στήλη τιμών, σε αντίθεση με τους υπόλοιπους κόμβους οι οποίοι έχουν δύο στήλες, χρησιμοποιούνται δύο διαφορετικοί τύποι για τον υπολογισμό των c_i. Το h_i χρησιμοποιείται για να δηλώσει τον αριθμό των τιμών που μπορεί να πάρει κάθε κόμβος του Μπεϋζιανού δικτύου. Τα $v1_{11}$ και $v1_{12}$ είναι οι τιμές των $p(T=1)$ και $p(T=0)$ για τον πρώτο ομότιμο, τα $v2_{11}$ και $v2_{12}$ είναι οι αντίστοιχες τιμές για το δεύτερο ομότιμο και τα $v1_{ijl}$ και $v2_{ijl}$ είναι οι τιμές των πινάκων CPT του πρώτου και του δεύτερου ομότιμου αντίστοιχα. Χρησιμοποιώντας τις παραπάνω μετρικές, οι ομότιμοι υπολογίζουν εκτός από τις τιμές εμπιστοσύνης τους, τους πίνακες CPT τους, λαμβάνοντας υπόψη και τις προσωπικές τους προτιμήσεις, έτσι ώστε ομότιμοι με όμοιες προτιμήσεις να αξιολογούν με μεγαλύτερες τιμές τις απόψεις ο ένας του άλλου.

3.8. Η εντροπία ως έκφραση της αβεβαιότητας

Η εμπιστοσύνη συνεπάγεται μια πεποίθηση και αυτή με τη σειρά της εμπεριέχει ένα ποσοστό αβεβαιότητας. Από την άλλη, η εντροπία αποτελεί μέτρο αβεβαιότητας και ως τέτοιο μπορεί να χρησιμοποιηθεί για να εκφράσει την εμπιστοσύνη.

3.8.1. Το μοντέλο των Sun et al.

Οι Sun, Han, Yu και Liu παρουσίασαν στην έρευνά τους [29] ένα πλαίσιο για την ποσοτική μέτρηση της εμπιστοσύνης, τη μοντελοποίηση της διάδοσής της και την προστασία των

συστημάτων αξιολόγησης της εμπιστοσύνης ενάντια στις κακόβουλες επιθέσεις. Όπως αναφέρουν και οι ίδιοι, η απόδοση των κατανεμημένων δικτύων εξαρτάται από τη συνεργασία μεταξύ των κατανεμημένων οντοτήτων τους. Έτσι, η αξιολόγηση της εμπιστευτικότητας των τελευταίων είναι το βασικό στοιχείο, μιας και η εμπιστοσύνη είναι η κινητήριος δύναμη της συνεργασίας.

Οι συγγραφείς χρησιμοποιούν την τριάδα {υποκείμενος : πράκτορας, ενέργεια} προκειμένου να αναπαραστήσουν μια σχέση εμπιστοσύνης μεταξύ δύο πλευρών, του υποκείμενου (subject) και του πράκτορα για να εκτελέσει ο δεύτερος μια ενέργεια. Ο υποκείμενος αντιπροσωπεύει συνήθως μια οντότητα αλλά μπορεί να είναι και μια ομάδα οντοτήτων. Το ίδιο ισχύει και για τον πράκτορα, ο οποίος μπορεί να είναι ακόμα και ολόκληρο το δίκτυο. Η ενέργεια τέλος μπορεί να είναι είτε μια ενέργεια που εκτελείται από τον πράκτορα, είτε μια ιδιότητα την οποία αυτός κατέχει.

Οι συγγραφείς υποστηρίζουν ότι η αβεβαιότητα στην πεποίθηση αποτελεί μέτρο εμπιστοσύνης. Εάν ο υποκείμενος πιστεύει ότι ο πράκτορας θα εκτελέσει την ενέργεια, τότε ο πρώτος εμπιστεύεται απόλυτα τον δεύτερο και δεν υπάρχει αβεβαιότητα. Το ίδιο ισχύει και στην περίπτωση που ο υποκείμενος πιστεύει ότι ο πράκτορας δεν θα εκτελέσει την ενέργεια και άρα δεν τον εμπιστεύεται καθόλου. Η μεγαλύτερη αβεβαιότητα εντοπίζεται όταν ο υποκείμενος δεν γνωρίζει τον πράκτορα και άρα δεν τον εμπιστεύεται. Για το λόγο αυτό οι μετρικές της εμπιστοσύνης πρέπει να περιγράφουν τα επίπεδα αβεβαιότητας σε μια σχέση εμπιστοσύνης. Η νέα μετρική που ορίζεται βασίζεται στην εντροπία και παίρνει τις τιμές 1, -1 και 0. Ως T{υποκείμενος, πράκτορας, ενέργεια} ορίζεται η τιμή εμπιστοσύνης μιας σχέσης εμπιστοσύνης και ως P{υποκείμενος, πράκτορας, ενέργεια} η πιθανότητα ότι ο πράκτορας θα εκτελέσει την ενέργεια κατά την άποψη του υποκειμένου. Η τιμή εμπιστοσύνης που βασίζεται στην εντροπία δίνεται από τον τύπο:

$$T = \begin{cases} 1 - H(p), & \gamma\iota\alpha\ 0{,}5 \le p \le 1 \\ H(p) - 1, & \gamma\iota\alpha\ 0 \le p \le 0{,}5 \end{cases},$$

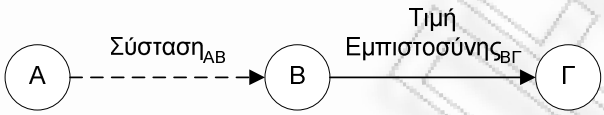
όπου T=T{υποκείμενος, πράκτορας, ενέργεια}, p=P{υποκείμενος, πράκτορας, ενέργεια}, $H(p) = -plog_2(p) - (1-p)log_2(1-p)$ και H η συνάρτηση εντροπίας. Αυτός ο ορισμός περικλείει τόσο την εμπιστοσύνη όσο και τη δυσπιστία και δείχνει ότι η τιμή της εμπιστοσύνης δεν είναι γραμμική συνάρτηση της πιθανότητας. Γενικά, η τιμή της εμπιστοσύνης είναι θετική όταν ο πράκτορας είναι πιθανότερο να πραγματοποιήσει την ενέργεια (p>$0{,}5$), και αρνητική όταν είναι πιθανότερο να μην την πραγματοποιήσει (p<$0{,}5$).

Όταν ο υποκείμενος μπορεί να κάνει απευθείας παρατήρηση, εκτιμά την τιμή της πιθανότητας και υπολογίζει την τιμή της εμπιστοσύνης για έναν πράκτορα, ενώ όταν δεν αλληλεπιδρά απευθείας μαζί του μπορεί και πάλι να έχει σχέση εμπιστοσύνης μέσω της διάδοσης της εμπιστοσύνης από τις λαμβανόμενες συστάσεις. Προκειμένου όμως οι συστάσεις εμπιστοσύνης να χρησιμοποιούνται σωστά από ένα δίκτυο υπολογιστών εισάγονται βασικοί κανόνες και αξιώματα.

Αν θεωρήσουμε ότι οι κόμβοι A και B ενός δικτύου έχουν μια σχέση $\{A : B,$ ενέργεια$_A\}$ και οι B και Γ μια σχέση $\{B : \Gamma,$ ενέργεια$_B\}$. Οι κόμβοι A και Γ μπορούν να εγκαταστήσουν μια σχέση $\{A : \Gamma,$ ενέργεια$_B\}$ μεταξύ τους εάν η ενέργεια$_A$ μπορεί να δώσει συστάσεις σε άλλους κόμβους για την εκτέλεση της ενέργειας$_B$ και είναι θετική η τιμή της εμπιστοσύνης της σχέσης $\{A:B,$ ενέργεια$_A\}$. Η πρώτη προϋπόθεση είναι αναγκαία γιατί οι κόμβοι που εκτελούν την ενέργεια δεν έχουν απαραίτητα σωστές συστάσεις, ενώ η δεύτερη προϋπόθεση προλαμβάνει τις περιπτώσεις όπου οι αναξιόπιστοι κόμβοι δίνουν ψευδείς συστάσεις. Ο πιο εγγυημένος τρόπος βέβαια είναι να μην λαμβάνονται υπόψη οι συστάσεις αναξιόπιστων μελών.

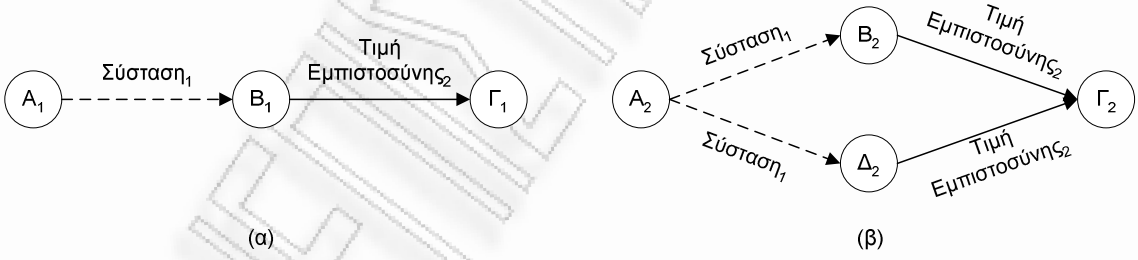
Με την ικανοποίηση των προϋποθέσεων αυτών οι συγγραφείς εισήγαγαν τρία αξιώματα:

1. *Η αλληλουχία συστάσεων εμπιστοσύνης δεν αυξάνει την εμπιστοσύνη.*
   Όταν ο υποκείμενος εγκαθιστά μια σχέση εμπιστοσύνης με έναν πράκτορα μέσω της σύστασης ενός τρίτου κόμβου, η τιμή της εμπιστοσύνης μεταξύ τους δεν μπορεί να είναι μεγαλύτερη από εκείνη μεταξύ του υποκείμενου και του τρίτου κόμβου, ούτε και από εκείνη μεταξύ του πράκτορα και του τρίτου κόμβου επίσης. Όπως δείχνει και το σχήμα 8, μία σχέση εμπιστοσύνης μεταξύ δύο κόμβων μπορεί να αναπαρασταθεί από ένα κατευθυνόμενο γράφημα, όπου η τιμή της εμπιστοσύνης αναπαρίσταται από το βάρος κατά μήκος της ακμής που ενώνει τους δύο κόμβους. Το είδος της γραμμής που ενώνει τους δύο κόμβους αναπαριστά τον τύπο της ενέργειας. Εάν η γραμμή είναι διακεκομμένη, τότε γίνεται σύσταση, ενώ όταν η γραμμή είναι συνεχόμενη, τότε πραγματοποιείται μια ενέργεια.



Σχήμα 8: Διάσχιση εμπιστοσύνης κατά μήκος αλυσίδας

2. *Η σύσταση εμπιστοσύνης από πολλαπλές διαδρομές δε μειώνει την εμπιστοσύνη.*
   Αυτό σημαίνει ότι εάν ο υποκείμενος λάβει πολλές συστάσεις για έναν πράκτορα από πολλές πηγές, η τιμή της εμπιστοσύνης δεν μπορεί να είναι μικρότερη από εκείνη που θα είχε στην περίπτωση που λάμβανε λιγότερες συστάσεις για τον ίδιο πράκτορα. Έτσι ο υποκείμενος θα είναι σιγουρότερος ή τουλάχιστον θα παραμείνει το ίδιο σίγουρος εάν λάβει κάποια σύσταση που συμφωνεί με την ήδη υπάρχουσα γνώμη του για τον πράκτορα, όπως φαίνεται και στο σχήμα 9.



Σχήμα 9: Μετάδοση συστάσεων εμπιστοσύνης

3. *Η εμπιστοσύνη που βασίζεται σε συστάσεις από πολλαπλές διαδρομές από μια πηγή δεν πρέπει να είναι μεγαλύτερη από εκείνη που προκύπτει από ανεξάρτητες πηγές.*
   Στην περίπτωση που μια σχέση εμπιστοσύνης εγκαθίσταται και η διάδοση της εμπιστοσύνης γίνεται μέσω συνεχόμενων βημάτων και πολλαπλών διαδρομών, μπορούν να υπάρξουν συστάσεις από την ίδια πηγή οι οποίες να έχουν διαδοθεί μέσω διαφορετικών μονοπατιών. Έτσι, οι συστάσεις από ανεξάρτητες πηγές μπορούν να μειώσουν την αβεβαιότητα πιο αποτελεσματικά από τις συστάσεις συσχετιζόμενων πηγών.

Με τη βοήθεια των αξιωμάτων αυτών, οι Sun et al. εισάγουν δύο μεθόδους υπολογισμού της εμπιστοσύνης οι οποίες βασίζονται στην αλληλουχία (concatenation) και στη μετάδοση μέσω πολλαπλών διαδρομών. Από τα μοντέλα αυτά, το ένα βασίζεται στην εντροπία και το άλλο στην πιθανότητα και αναλύονται στη συνέχεια.

α) Μοντέλο βασιζόμενο στην εντροπία

Στο μοντέλο αυτό, λαμβάνονται ως είσοδοι οι τιμές εμπιστοσύνης που βασίζονται στην εντροπία. Το μοντέλο λαμβάνει υπόψη του μόνο τις τιμές εμπιστοσύνης και όχι τη βεβαιότητα.

Για την αλληλουχία της διάδοσης της εμπιστοσύνης που φαίνεται στο σχήμα 8, ο κόμβος B παρατηρεί τη συμπεριφορά του κόμβου Γ και κάνει συστάσεις στον κόμβο A με μορφή $T_{B\Gamma}$ *= {B : Γ, ενέργεια}*. Ο κόμβος A όμως εμπιστεύεται τον κόμβο B με τιμή εμπιστοσύνηςR_{AB} *= T {A : B, να κάνει σύσταση}*. Έτσι, η τιμή της εμπιστοσύνης $T_{AB\Gamma}$ είναι σύμφωνα με το αξίωμα 1 $T_{AB\Gamma} = R_{AB}.T_{B\Gamma}$. Από αυτή την εξίσωση προκύπτει ότι εάν ο κόμβος B δεν γνωρίζει τον κόμβο Γ ή αντίστοιχα ο κόμβος A τον κόμβο B, η εμπιστοσύνη μεταξύ των A και Γ θα είναι μηδέν.

Στην περίπτωση της διάδοσης της εμπιστοσύνης μέσω πολλαπλών διαδρομών, θεωρούμε R_{AB} *= T {A : B, να κάνει σύσταση}*, $T_{B\Gamma}$ *= {B : Γ, ενέργεια}*, $R_{A\Delta}$ *= T {A : Δ, να κάνει σύσταση}* και $T_{\Delta\Gamma}$ *= {Δ : Γ, ενέργεια}*. Είναι προφανές ότι ο κόμβος A μπορεί να εγκαταστήσει σχέση εμπιστοσύνης με τον κόμβο Γ μεταξύ του μονοπατιού $A \rightarrow B \rightarrow \Gamma$ ή του $A \rightarrow \Delta \rightarrow \Gamma$. Εδώ το αποτέλεσμα του συνδυασμού των τιμών εμπιστοσύνης που λαμβάνονται από τα δύο μονοπάτια δίνεται από τον τύπο:

$$T_{A\Gamma} = \{A : \Gamma, ενέργεια\} = \frac{R_{AB}}{R_{AB} + R_{A\Delta}}(R_{AB}.T_{B\Gamma}) + \frac{R_{A\Delta}}{R_{AB} + R_{A\Delta}}(R_{A\Delta}.T_{\Delta\Gamma}).$$

Ο παραπάνω τύπος δεν θα επηρέαζε το τελικό αποτέλεσμα στην περίπτωση που κάποιο μονοπάτι έδινε τιμή εμπιστοσύνης ίση με το μηδέν.

β) Μοντέλο βασιζόμενο στην πιθανότητα

Εδώ χρησιμοποιούνται οι τιμές των πιθανοτήτων των σχέσεων εμπιστοσύνης με χρήση μέσων τιμών και τιμών διακύμανσης, προκειμένου να υπολογιστεί η μετάδοση της εμπιστοσύνης μέσω αλληλουχιών και πολλαπλών διαδρομών.

Για την αλληλουχία της διάδοσης της εμπιστοσύνης που είδαμε στο σχήμα 8, οι συγγραφείς ορίζουν τα παρακάτω στοιχεία:

- Η τυχαία μεταβλητή P είναι η πιθανότητα ότι ο κόμβος Γ θα εκτελέσει την ενέργεια. Κατά τη γνώμη του κόμβου A η τιμή εμπιστοσύνης T {$A : \Gamma$, ενέργεια} καθορίζεται από τη μέση τιμή $E(P)$ και η βεβαιότητα από την τιμή διακύμανσης *Var(P)*.
- Η τυχαία μεταβλητή X είναι δυαδική. Η τιμή 1 σημαίνει ότι ο κόμβος B παρέχει ειλικρινείς συστάσεις. Σε διαφορετική περίπτωση η τιμή της είναι 0.
- Η τυχαία μεταβλητή Θ είναι η πιθανότητα ότι $X = 1$, δηλαδή

$$Pr(X = 1 \mid \Theta = \theta) = \theta \text{ και}$$
$$Pr(X = 0 \mid \Theta = \theta) = 1 - \theta$$

  Κατά τη γνώμη του κόμβου A, η μέση τιμή της P{$A : B$, να κάνει σύσταση} είναι $B = p_{AB} = E(\theta)$, και η τιμή διακύμανσης είναι *Var(θ)* = σ_{AB}.
- Ο κόμβος B παρέχει συστάσεις για τον κόμβο Γ ως ακολούθως: η μέση τιμή της P{$B : \Gamma$, ενέργεια} είναι $p_{B\Gamma}$, ενώ η τιμή διακύμανσής της είναι $\sigma_{B\Gamma}$.

Τελικά, προκύπτουν οι ακόλουθοι τύποι οι οποίοι εκφράζουν το μοντέλο αλληλουχίας που βασίζεται στην πιθανότητα:

$$E(P) = p_{AB}\, p_{B\Gamma} + (1 - p_{AB})\,(1 - p_{B\Gamma}),$$

$$Var(P) = \int_{p=0}^{p=1} p^2 f(P = p)dp - E(P)^2$$
$$= p_{AB}\sigma_{B\Gamma} + (1 - p_{AB})\sigma_{\Gamma|X=0} + p_{AB}(1 - p_{AB}).\left(p_{B\Gamma} - p_{\Gamma|X=0}\right)^2,$$

όπου $\sigma_{\Gamma|X=0} = Var(P|X = 0)$ και $p_{\Gamma|X=0} = 1 - p_{B\Gamma}$. Η επιλογή της $\sigma_{\Gamma|X=0}$ εξαρτάται από το εκάστοτε σενάριο εφαρμογής. Για παράδειγμα, εάν υποθέσουμε ότι η P κατανέμεται ομοιόμορφα στο διάστημα $[0, 1]$, το $\sigma_{\Gamma|X=0}$ θα είναι η μέγιστη πιθανή διακύμανση. Εάν όμως η συνάρτηση πυκνότητας πιθανότητας της P είναι συνάρτηση Βήτα με μέσο $m = p_{\Gamma|X=0}$, έχουμε:

$$\sigma_{\Gamma|X=0} = \begin{cases} \dfrac{m(1-m)^2}{2-m}, \gamma\iota\alpha\ m \geq 0{,}5 \\ \dfrac{m^2(1-m)}{1+m}, \gamma\iota\alpha\ m < 0{,}5 \end{cases}$$

Για τη διάδοση της εμπιστοσύνης μέσω πολλαπλών διαδρομών, χρησιμοποιείται η συνάρτηση Βήτα. Ας θεωρήσουμε ότι ο κόμβος A μπορεί να εγκαταστήσει σχέση εμπιστοσύνης με τον κόμβο Γ μέσω δύο μονοπατιών, των A➔B➔Γ και A➔Δ➔Γ. Θεωρούμε ότι ο κόμβος A έχει αρχικά μόνο τη σύσταση για τον κόμβο Γ που λαμβάνει από τον κόμβο B. Στη συνέχεια λαμβάνει και τη σύσταση του κόμβου Δ για τον Γ. Σε περιπτώσεις όπου ο υποκείμενος λαμβάνει δυαδικής μορφής απόψεις για έναν κόμβο, δηλαδή θετικές ή αρνητικές, μπορεί να χρησιμοποιηθεί το μοντέλο της κατανομής Βήτα $B(a, \beta)$ με τύπο:

$$B(\alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1},$$

όπου a ο αριθμός των θετικών συστάσεων και β ο αριθμός των αρνητικών. Εάν συνδυάσουμε τις συστάσεις που έλαβε ο κόμβος A από τα δύο μονοπάτια με το Μπεϋζιανό μοντέλο, τότε όπως έδειξαν στο [29] προκύπτει η συνάρτηση Βήτα $B(a_1 + a_2 - 1, \beta_1 + \beta_2 - 1)$, ένας συνδυασμός των δύο συναρτήσεων Βήτα $B(a_1, \beta_1)$ και $B(a_2, \beta_2)$ που προκύπτουν με τη χρησιμοποίηση των δύο συστάσεων που λαμβάνει ο κόμβος από τα διαφορετικά μονοπάτια.

Η χρήση όμως του μοντέλου της συνάρτησης Βήτα μπορεί να γίνει και για μη δυαδικές συστάσεις, καθορίζοντας τις παραμέτρους a και β από το μέσο m και τη διακύμανση υ:

$$\alpha = m\left(\frac{m(1-m)}{\upsilon} - 1\right),$$

και $$\beta = (1-m)\left(\frac{m(1-m)}{\upsilon} - 1\right).$$

Μέσω του πρώτου μονοπατιού που αναφέραμε παραπάνω, ο κόμβος A αποκτά εμπιστοσύνη και βεβαιότητα που αναπαριστούνται από το μέσο m_1 και την τιμή διακύμανσης υ_1. Μέσω του δεύτερου μονοπατιού, τα ίδια δεδομένα αναπαριστούνται με το μέσο m_2 και την

τιμή διακύμανσης v_2. Μέσω των παραπάνω εξισώσεων τα (m_1, v_1) και (m_2, v_2) μετατρέπονται σε (a_1, β_1) και (a_2, β_2) αντίστοιχα. Ο συνδυασμός των δύο ζευγών δίνει ένα νέο ζεύγος (a, β) όπου $a = a_1 + a_2 - 1$ και $\beta = \beta_1 + \beta_2 - 1$, από το οποίο μπορεί να προκύψει ο νέος μέσος και η νέα τιμή διακύμανσης με τη βοήθεια των εξισώσεων που παρουσιάσαμε παραπάνω. Οι συγγραφείς χρησιμοποίησαν το μοντέλο τους αυτό και για τον καθορισμό του κατά πόσο κάποιος κόμβος του δικτύου είναι κακόβουλος ή όχι.

Οι Sun et al. χρησιμοποίησαν στη συνέχεια τα αξιώματα και τα μοντέλα αυτά για να σχεδιάσουν ένα πλαίσιο διαχείρισης της εμπιστοσύνης για κατανεμημένα δίκτυα. Στο πλαίσιο αυτό υπάρχουν πέντε βασικές δομές. Το αρχείο εμπιστοσύνης κατασκευάζεται μέσω της διαδικασίας εγκατάστασης εμπιστοσύνης. Η διαδικασία αυτή δημιουργεί τιμές άμεσης εμπιστοσύνης μέσω παρατηρήσεων και τιμές έμμεσης εμπιστοσύνης μέσω συστάσεων και μέσω ενημερώσεων από τη διαδικασία διατήρησης αρχείου, η οποία εκχωρεί αρχικές τιμές εμπιστοσύνης και δίνει δυναμικές ιδιότητες στην εμπιστοσύνη. Η διαχείριση αιτημάτων εμπιστοσύνης χρησιμοποιείται ως διεπαφή μεταξύ εφαρμογών, οι οποίες αιτούνται τιμών εμπιστοσύνης και διαχείρισης εμπιστοσύνης, ενώ επιπλέον διαχειρίζεται τα αιτήματα για τις συστάσεις εμπιστοσύνης. Τέλος, η ανακάλυψη κακόβουλων κόμβων γίνεται με βάση το αρχείο εμπιστοσύνης και τα αποτελέσματά της επηρεάζουν κάποιες οντότητες του αρχείου αυτού. Το πλαίσιο αυτό μπορεί να χρησιμοποιηθεί σε πολλές εφαρμογές και για πολλά είδη δικτύων.

Οι συγγραφείς παρουσιάζουν μία τέτοια χρήση σε δίκτυα ad hoc όπου κάθε κόμβος διατηρεί ένα αρχείο εμπιστοσύνης, το οποίο σχετίζεται με δύο ενέργειες, την προώθηση πακέτων και την παροχή συστάσεων. Όταν ένας κόμβος πηγή θελήσει να εγκαταστήσει μια διαδρομή με έναν άλλο κόμβο στόχο, ψάχνει να βρει όλες τις διαδρομές που τους ενώνουν και στη συνέχεια προσπαθεί να βρει την πιο αξιόπιστη από αυτές, υπολογίζοντας την αξιοπιστία των ενδιάμεσων κόμβων στο να προωθούν πακέτα, μέσω του δικού του αρχείου εμπιστοσύνης ή ζητώντας συστάσεις για τους κόμβους αυτούς. Προκειμένου να αποστείλει ένα αίτημα σύστασης για ένα σύνολο κόμβων A, ο κόμβος πηγή κοιτάει πρώτα το αρχείο εμπιστοσύνης του και επιλέγει ένα σύνολο κόμβων B, των οποίων οι τιμές εμπιστοσύνης για να παρέχουν συστάσεις είναι μεγαλύτερες από κάποιο κατώφλι. Το σύνολο B μπορεί να είναι μεγαλύτερο από αυτό που χρειάζεται για να του παρέχουν τις επιθυμητές συστάσεις, έτσι ώστε να αποφευχθούν τυχόν κακόβουλοι κόμβοι οι οποίοι θα προσπαθήσουν να εκμεταλλευτούν αυτή την πληροφορία, αλλά και για να κρατήσει ένα μέτρο σύγκρισης για την ποιότητα των συστάσεων που δίνουν οι κόμβοι του συνόλου B, σε περίπτωση που κάποια στιγμή τύχει να έχει ο κόμβος πηγή άμεση συναλλαγή με το ζητούμενο σύνολο κόμβων A. Ο κόμβος πηγή αποστέλλει στη συνέχεια ένα μήνυμα αιτήματος σύστασης εμπιστοσύνης στους γείτονές του που βρίσκονται στην εμβέλειά του, το οποίο περιέχει τα αναγνωριστικά των κόμβων των δύο συνόλων A και B, το μέγιστο μήκος του μονοπατιού μεταφοράς εμπιστοσύνης και το χρόνο ζωής του μηνύματος.

Οι κόμβοι οι οποίοι λαμβάνουν το μήνυμα και δεν ανήκουν στο σύνολο B, το προωθούν στους γείτονές τους. Εάν όμως ανήκουν στο σύνολο αυτό, είτε στέλνουν τις ζητούμενες τιμές εμπιστοσύνης στον κόμβο πηγή μέσω του ανάποδου μονοπατιού απ' όπου ήρθε το αίτημα, είτε ζητάνε από τους δικούς τους έμπιστους κόμβους να τους παρέχουν τις συστάσεις που ζητούνται. Οι κόμβοι του συνόλου B μπορούν ακόμα και να μην απαντήσουν στο αίτημα, εάν δεν θέλουν να αποκαλύψουν τις εγγραφές εμπιστοσύνης τους, αν για παράδειγμα θεωρούν ότι ο κόμβος πηγή είναι κακόβουλος. Αφού βρεθεί το πιο αξιόπιστο μονοπάτι χρησιμοποιώντας τα παραπάνω στοιχεία και τις μεθόδους υπολογισμού της εμπιστοσύνης που περιγράφτηκαν προηγουμένως, γίνεται η μετάδοση των δεδομένων.

Ο κόμβος πηγή ενημερώνει μετά τις εγγραφές εμπιστοσύνης του βασιζόμενος στις παρατηρήσεις του για την ποιότητα της διαδρομής και τα πακέτα που τελικά προώθησε κάθε ενδιάμεσος κόμβος με τον οποίο δεν έχει σχέση εμπιστοσύνης. Ένας διακριτικός μηχανισμός αυτό-αξιολόγησης επιτρέπει στον κόμβο πηγή να συλλέγει στατιστικά προώθησης πακέτων και να τα επιβεβαιώνει κάνοντας ελέγχους συνέπειας. Έτσι, για κάθε ενδιάμεσο κόμβο του μονοπατιού, εάν η απόλυτη τιμή της διαφοράς της παρατηρούμενης τιμής εμπιστοσύνης που προκύπτει από τον παραπάνω μηχανισμό, με την τιμή της διαδιδόμενης εμπιστοσύνης που

υπολογίστηκε από τις μεθόδους υπολογισμού εμπιστοσύνης, είναι ίση ή μικρότερη από ένα κατώφλι, ο ενδιάμεσος κόμβος που παρείχε τη σύσταση θεωρείται αξιόπιστος. Σε διαφορετική περίπτωση θεωρείται ότι παρείχε μια κακή σύσταση και η εγγραφή του στο αρχείο του κόμβου πηγή παίρνει ανάλογη τιμή.

3.9. Ανώνυμος υπολογισμός μετρικών εμπιστοσύνης

Ο υπολογισμός των τιμών εμπιστοσύνης απαιτεί συχνά την επικοινωνία μεταξύ κόμβων για την ανταλλαγή στοιχείων εμπιστοσύνης. Πολλές φορές η αποκάλυψη της ταυτότητας των κόμβων αυτών δεν είναι επιθυμητή από το σύστημα. Για το λόγο αυτό, έχουν προταθεί μοντέλα εμπιστοσύνης, τα οποία υπολογίζουν τις τιμές εμπιστοσύνης κατά τέτοιο τρόπο, ώστε να διασφαλίζεται η ανωνυμία μεταξύ των κόμβων του δικτύου.

3.9.1. Το μοντέλο TrustMe

Οι Singh και Liu [46] παρουσίασαν ένα ασφαλές και ανώνυμο πρωτόκολλο υποστήριξης για τη διαχείριση της εμπιστοσύνης σε αποκεντρωμένα δίκτυα ομότιμων κόμβων, το λεγόμενο TrustMe, το οποίο χρησιμοποιεί μηχανισμούς κρυπτογράφησης δημοσίου κλειδιού. Το πρωτόκολλο αυτό παρέχει ανωνυμία και για τον κόμβο που αναζητά την τιμή εμπιστοσύνης κάποιου κόμβου, αλλά και για τον κόμβο ο οποίος τού την παρέχει. Οι συγγραφείς αποδεικνύουν μέσω προσομοιώσεων ότι το πρωτόκολλο είναι πολύ ασφαλές απέναντι σε διάφορες πιθανές επιθέσεις.

Στο μοντέλο TrustMe, υπάρχει καταρχήν ένας bootstrap server ο οποίος διαθέτει ένα ζεύγος κλειδιών, από τα οποία το δημόσιο κλειδί του είναι γνωστό στους ομότιμους κόμβους του δικτύου. Επίσης, κάθε κόμβος που εισέρχεται στο δίκτυο πρέπει να διαθέτει δύο ζεύγη κλειδιών, το πρώτο για την παροχή και λήψη υπηρεσιών, ενώ το δεύτερο ζεύγος χρησιμεύει όταν εκτελεί χρέη Πράκτορα Διατήρησης Εμπιστοσύνης – ΠΔΕ (Trust – Holding Agent – THA). Ένας ΠΔΕ είναι ένας ομότιμος κόμβος ο οποίος διατηρεί τις τιμές εμπιστοσύνης ενός συγκεκριμένου κόμβου και χρησιμοποιεί μηχανισμούς έξυπνου δημοσίου κλειδιού, προκειμένου να διατηρήσει την ανωνυμία και να διασφαλίσει την ασφάλεια των επικοινωνιών. Κάθε ομότιμος ΠΔΕ διατηρεί επιπλέον μια χρονική σφραγίδα (timestamp), έτσι ώστε εάν κάποιες από τις πληροφορίες που διαθέτει δεν προσπελαθούν μέχρι τη λήξη της σφραγίδας, τότε αυτές διαγράφονται από τη βάση δεδομένων του. Όταν ένας νέος ομότιμος κόμβος έρθει σε επαφή με τον bootstrap server, εκείνος παράγει γι' αυτόν ένα αναγνωριστικό και ένα νέο ζεύγος ειδικών κλειδιών και του παρέχει μόνο το ειδικό ιδιωτικό κλειδί. Στη συνέχεια επιλέγει από μια λίστα ομότιμων τους κόμβους εκείνους οι οποίοι θα εκτελούν χρέη ΠΔΕ για το νέο κόμβο και τους αποστέλλει ένα μήνυμα, στο οποίο περιέχεται μεταξύ άλλων και το ειδικό δημόσιο κλειδί του νέου κόμβου. Με τη λήψη του μηνύματος αυτού, κάθε ΠΔΕ κόμβος ενημερώνει την τοπική βάση δεδομένων του και εισάγει σε αυτή τα στοιχεία του νέου κόμβου που έλαβε μέσω του μηνύματος.

Όταν ένας ομότιμος κόμβος s θελήσει να μάθει την τιμή εμπιστοσύνης ενός άλλου ομότιμου t του δικτύου, εκπέμπει ένα μήνυμα αιτήματος εμπιστοσύνης με το αναγνωριστικό του ομότιμου αυτού. Κάθε ΠΔΕ κόμβος ο οποίος διαθέτει την τιμή εμπιστοσύνης για τον κόμβο t στέλνει μια κωδικοποιημένη απάντηση με την τιμή εμπιστοσύνης του t στον κόμβο s. Η κωδικοποίηση γίνεται με το ειδικό ιδιωτικό κλειδί του κόμβου t που έχει κάθε ΠΔΕ του και στο μήνυμα περιλαμβάνεται το ειδικό δημόσιο κλειδί του ομότιμου t για να αποκωδικοποιηθεί το μήνυμα. Αυτό γίνεται προκειμένου να αποφευχθούν περιπτώσεις κακόβουλων κόμβων, οι οποίοι αποστέλλουν ψευδή μηνύματα, προσπαθώντας να μειώσουν την τιμή εμπιστοσύνης άλλων ομότιμων. Με τη λήψη της απάντησης και ανάλογα με τις τιμές εμπιστοσύνης που έλαβε, ο ομότιμος που έστειλε το αίτημα μπορεί να αποφασίσει να αλληλεπιδράσει με τον ομότιμο t ή όχι.

Στην περίπτωση που ο s αλληλεπιδράσει με τον ομότιμο t, ανταλλάσσουν μεταξύ τους μηνύματα – αποδείξεις της αλληλεπίδρασής τους αυτής, τα οποία δεν μπορούν να

δημιουργηθούν με κάποιο άλλο τρόπο, αφού απαιτούν τη γνώση του ιδιωτικού κλειδιού του άλλου κόμβου. Μετά την αλληλεπίδραση των δύο ομότιμων, ο κόμβος s μπορεί να εκπέμψει ένα μήνυμα αναφοράς και να δώσει μια νέα τιμή εμπιστοσύνης για τον ομότιμο t στους ΠΔΕ οι οποίοι είναι υπεύθυνοι γι' αυτόν. Το μήνυμα αυτό είναι κωδικοποιημένο με τέτοιο τρόπο, ώστε να διασφαλίζεται ότι ο αποστολέας έχει σίγουρα αλληλεπιδράσει με τον ομότιμο στον οποίο αναφέρεται και ότι μόνο οι ΠΔΕ που είναι υπεύθυνοι για τον ομότιμο αυτόν μπορούν να το διαβάσουν και να αποθηκεύσουν τη νέα ατομική τιμή εμπιστοσύνης για τον κόμβο t από τον ομότιμο s. Η καθολική τιμή εμπιστοσύνης για τον κόμβο t θα προκύψει στη συνέχεια από όλες τις ατομικές τιμές εμπιστοσύνης που έχουν αποσταλεί από τους ομότιμους οι οποίοι έχουν αλληλεπιδράσει με τον ομότιμο t. Τέλος, όταν ένας ομότιμος ΠΔΕ θελήσει να αποχωρήσει από το δίκτυο, έρχεται σε επαφή με τον bootstrap server, ο οποίος αναθέτει την αρμοδιότητα του ΠΔΕ σε κάποιον άλλο ομότιμο.

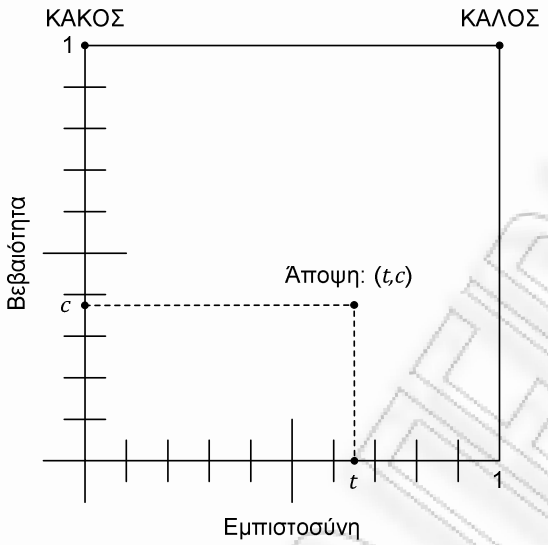
3.10. Χρήση δομών ημιδακτυλίου για το συνδυασμό απόψεων

Όταν δύο κόμβοι δεν έχουν άμεση αλληλεπίδραση αλλά επιθυμούν να εγκαταστήσουν μια έμμεση σχέση, οι απόψεις των υπόλοιπων κόμβων που βρίσκονται μεταξύ τους πρέπει να συνδυαστούν και να αξιολογηθούν. Οι αλγεβρικές δομές των ημιδακτυλίων μπορούν να χρησιμοποιηθούν για την εύρεση της τιμής εμπιστοσύνης την οποία πρέπει να εκχωρήσει ο κόμβος πηγή στον κόμβο στόχο.

3.10.1. Το μοντέλο των Theodorakopoulos και Baras

Οι Theodorakopoulos και Baras [47] εστίασαν στην αξιολόγηση των μαρτυριών χρηστών σχετικά με την εμπιστοσύνη σε δίκτυα ad hoc. Οι συγγραφείς μοντελοποίησαν τη διαδικασία αξιολόγησης ως ένα γενικευμένο πρόβλημα ελάχιστου μονοπατιού σε ένα σταθμισμένο (weighted) κατευθυνόμενο γράφημα. Χρησιμοποιώντας τη θεωρία των ημιδακτυλίων (semirings) έδειξαν πώς μπορούν δύο κόμβοι να εγκαταστήσουν μια έμμεση σχέση εμπιστοσύνης χωρίς να έχουν προηγούμενη άμεση αλληλεπίδραση.

Στο κατευθυνόμενο γράφημα $G = (V, E)$ που χρησιμοποιείται στο μοντέλο, οι κόμβοι αναπαριστούν οντότητες και οι ακμές άμεσες σχέσεις εμπιστοσύνης, με βάρος την τιμή της άποψης που έχει ο πρώτος κόμβος για το δεύτερο. Κάθε άποψη αποτελείται από το συνδυασμό δύο αριθμών, της τιμής εμπιστοσύνης και της τιμής βεβαιότητας και η περιοχή από την οποία παίρνει τιμές είναι ένα τετράγωνο στο καρτεσιανό επίπεδο, όπως φαίνεται και στο σχήμα 10. Η τιμή εμπιστοσύνης αποτελεί την εκτίμηση μιας οντότητας για την αξιοπιστία της οντότητας στόχου, ενώ η τιμή βεβαιότητας αντιστοιχεί στην ακρίβεια της εκχώρησης της τιμής εμπιστοσύνης. Καθεμία από τις τιμές αυτές εκχωρούνται από κάθε χρήστη σύμφωνα με τα δικά του κριτήρια και παρατηρήσεις, ακόμα και για γειτονικούς κόμβους με τους οποίους αλληλεπιδρούσαν στο παρελθόν, αλλά με τους οποίους δε συνδέονται πια. Είναι προφανές ότι στην περίπτωση αυτή, η τιμή της βεβαιότητας θα φθίνει με την πάροδο του χρόνου. Παράλληλα, μια άποψη για έναν κόμβο μπορεί μόνο να φθίνει κατά μήκος ενός μονοπατιού, μιας και περιορίζεται από την άποψη που έχει ο κόμβος πηγή για τον πρώτο κόμβο του μονοπατιού.



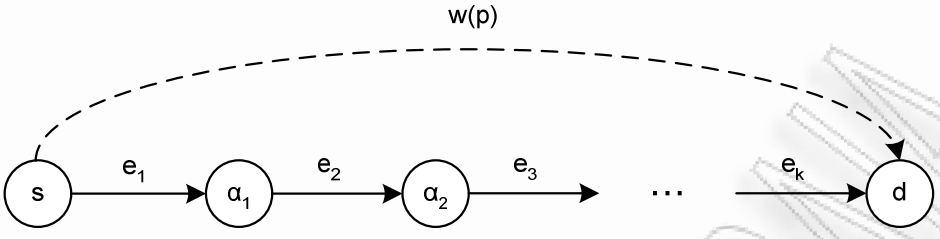
Σχήμα 10: Περιοχή τιμών άποψης

Κάθε οντότητα έχει άμεσες σχέσεις μόνο με τις οντότητες εκείνες με τις οποίες έχει αλληλεπιδράσει. Στόχος είναι η δημιουργία μιας έμμεσης σχέσης μεταξύ δύο χρηστών οι οποίοι δεν έχουν πρότερη αλληλεπίδραση, χρησιμοποιώντας τις άμεσες σχέσεις εμπιστοσύνης που έχουν μεταξύ τους οι ενδιάμεσοι χρήστες. Έτσι μπορεί να θεωρηθεί ότι η εμπιστοσύνη είναι μεταβατική.

Σε αυτό το πλαίσιο, οι Theodorakopoulos και Baras επιλύουν δύο εκδοχές του προβλήματος εξαγωγής συμπερασμάτων σχετικά με την εμπιστοσύνη. Η πρώτη εκδοχή είναι η εύρεση της τιμής εμπιστοσύνης-βεβαιότητας την οποία πρέπει να εκχωρήσει ένας κόμβος πηγή σε έναν κόμβο στόχο, βασιζόμενος τις αντίστοιχες τιμές των ενδιάμεσων κόμβων. Κάτι τέτοιο αντιστοιχεί στην εύρεση της γενικευμένης απόστασης μεταξύ των κόμβων A και B. Η δεύτερη εκδοχή είναι η εύρεση του πιο έμπιστου μονοπατιού μεταξύ δύο κόμβων A και B, η εύρεση δηλαδή μιας ακολουθίας κόμβων, η οποία έχει την υψηλότερη συνολικά τιμή εμπιστοσύνης μεταξύ όλων των μονοπατιών που συνδέουν τους δύο κόμβους.

Οι συγγραφείς, προκειμένου να συνδυάσουν τις απόψεις κόμβων, χρησιμοποιούν αλγεβρικές δομές με συγκεκριμένες ιδιότητες, τους λεγόμενους ημιδακτύλιους $(S,\oplus,\otimes)$, όπου S είναι ένα σύνολο και οι $\oplus$ και $\otimes$ είναι δυαδικοί τελεστές με συγκεκριμένες ιδιότητες. Ένας ημιδακτύλιος μπορεί να χρησιμοποιηθεί για τον υπολογισμό του βάρους της μικρότερης διαδρομής από έναν κόμβο s μέχρι έναν κόμβο d σε ένα κατευθυνόμενο γράφημα με βάρη. Σε αυτή την περίπτωση, εάν υπάρχει μόνο ένα μονοπάτι που ενώνει τους δύο κόμβους, ο τελεστής αλληλουχίας $\otimes$ συνδυάζει τα βάρη των ακμών που ακολουθούν το ένα το άλλο κατά μήκος του μονοπατιού p, από τον κόμβο πηγή ως τον κόμβο στόχο και δίνει το συνολικό βάρος για το μονοπάτι αυτό. Εάν για παράδειγμα σε ένα τέτοιο μονοπάτι $p = (s, a_1, a_2, \ldots, a_{k-1}, d)$ υπάρχουν οι ακμές $e_1 = (s, a_1)$, $e_2 = (a_1, a_2)$, …, $e_k = (a_{k-1}, d)$ όπως φαίνεται στο σχήμα 11, τότε το συνολικό βάρος από τον κόμβο s μέχρι τον κόμβο d κατά μήκος του μονοπατιού έχει τη μορφή:

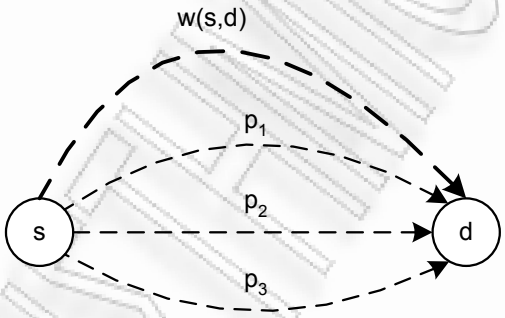
$$w(p) = w(e_1) \otimes w(e_2) \otimes \ldots \otimes w(e_k) \ .$$



Σχήμα 11: Ο τελεστής αλληλουχίας χρησιμοποιείται για να συνδυάσει βάρη κατά μήκος ενός μονοπατιού

Ο τελεστής σύνοψης ⊕ αντίθετα, μπορεί να χρησιμοποιηθεί για να συνδυάσει βάρη κατά μήκος παράλληλων μονοπατιών που ξεκινάνε από έναν κόμβο και καταλήγουν σε έναν άλλο. Έτσι, εάν έχουμε τα πολλαπλά μονοπάτια p_1, p_2, ..., p_n από έναν κόμβο πηγή s ως έναν κόμβο στόχο d με τα αντίστοιχα βάρη $w^{p_1}(s, d)$, $w^{p_2}(s, d)$, …, $w^{p_n}(s, d)$, όπως φαίνεται στο σχήμα 12, το συνολικό βάρος από όλα τα μονοπάτια είναι:

$$w(s, d) = w^{p_1}(s, d) \oplus w^{p_2}(s, d) \oplus \ldots \oplus w^{p_n}(s, d) .$$



Σχήμα 12: Ο τελεστής σύνοψης χρησιμοποιείται για να συνδυάσει βάρη κατά μήκος μονοπατιών

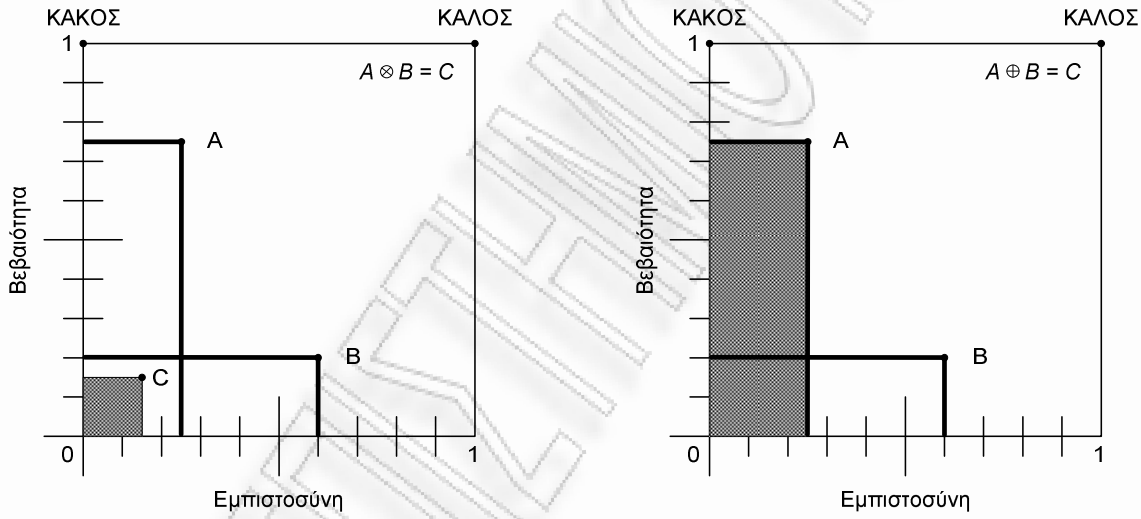
Επιπρόσθετα στις παραπάνω δομές, οι συγγραφείς όρισαν τη σημασία των στοιχείων ⓪ και ①. Όπως αναφέρουν, το στοιχείο ⓪ αντιστοιχεί στην άποψη «δεν γνωρίζω» και περιγράφει την απουσία σχέσης εμπιστοσύνης μεταξύ δύο κόμβων. Έτσι, η ύπαρξή του κατά μήκος ενός μονοπατιού θα δώσει το ίδιο αποτέλεσμα για όλο το μονοπάτι. Αντίθετα, το στοιχείο ① αποτελεί την καλύτερη άποψη που μπορεί να έχει ένας κόμβος για κάποιον άλλο.

Σχετικά με την εύρεση της τιμής εμπιστοσύνης-βεβαιότητας την οποία πρέπει να εκχωρήσει ένας κόμβος πηγή σε έναν κόμβο στόχο, βασιζόμενος στις αντίστοιχες τιμές των ενδιάμεσων κόμβων, οι συγγραφείς έδειξαν με τη βοήθεια των τελεστών αλληλουχίας και σύνοψης ότι ισχύει:

$$(t_{ik}, c_{ik}) \otimes (t_{kj}, c_{kj}) = (t_{ik}\, t_{kj}, c_{ik}\, c_{kj}) ,$$

$$\left(t_{ij}^{p1}, c_{ij}^{p1}\right) \oplus \left(t_{ij}^{p2}, c_{ij}^{p2}\right) = \begin{cases} \left(t_{ij}^{p1}, c_{ij}^{p1}\right) & \alpha\nu\ c_{ij}^{p1} > c_{ij}^{p2} \\ \left(t_{ij}^{p2}, c_{ij}^{p2}\right) & \alpha\nu\ c_{ij}^{p1} < c_{ij}^{p2} \\ \left(t_{ij}^{*}, c_{ij}^{p1}\right) & \alpha\nu\ c_{ij}^{p1} = c_{ij}^{p2} \end{cases}$$

όπου $\left(t_{ij}^{p1}, c_{ij}^{p1}\right)$ συμβολίζει την άποψη την οποία σχηματίζει ο κόμβος i για τον κόμβο j μέσω του μονοπατιού p_1. Το πεδίο από το οποίο παίρνει τιμές μια άποψη είναι το πεδίο S=[0,1]x[0,1], ενώ όπου $t_{ij}^{*} = max\left(t_{ij}^{p1}, t_{ij}^{p2}\right)$. Δεδομένου ότι οι τιμές της εμπιστοσύνης και της βεβαιότητας προκύπτουν από το διάστημα $[0,1]$, αυτές φθίνουν όταν συναθροίζονται κατά μήκος ενός μονοπατιού. Όταν όμως οι απόψεις συναθροίζονται για πολλά μονοπάτια, υπερισχύει εκείνο που διαθέτει τη μεγαλύτερη βεβαιότητα, ενώ όταν αυτή είναι ίδια σε όλα τα μονοπάτια, επιλέγεται εκείνο που διαθέτει τη μεγαλύτερη τιμή εμπιστοσύνης. Στα παρακάτω σχήματα φαίνεται ένα παράδειγμα εφαρμογής του ημιδακτυλίου μονοπατιού σε δύο απόψεις.



Σχήμα 13: Εφαρμογή των τελεστών αλληλουχίας και σύνοψης του ημιδακτυλίου μονοπατιού

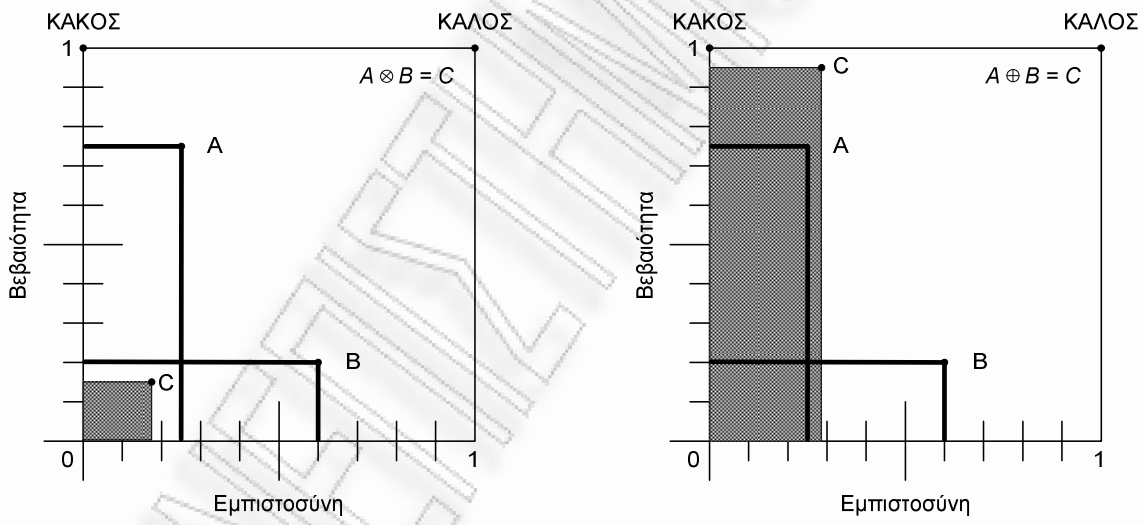
Ο παραπάνω ημιδακτύλιος μονοπατιού υπολογίζει ουσιαστικά την απόσταση εμπιστοσύνης (trust distance) κατά μήκος του βεβαιότερου μονοπατιού εμπιστοσύνης μέχρι τον κόμβο στόχο, μιας και ο τελεστής σύνοψης επιλέγει μόνο ένα μονοπάτι, αγνοώντας τις πληροφορίες των άλλων μονοπατιών και επιτρέποντας έτσι την ελαχιστοποίηση των μηνυμάτων για τη συλλογή πληροφοριών. Στην περίπτωση που προκύψει από τον ημιδακτύλιο αυτό μια αρκετά μεγάλη τιμή εμπιστοσύνης, τότε το μονοπάτι αυτό προς τον κόμβο στόχο είναι έμπιστο.

Για το πρόβλημα της εύρεσης του πιο έμπιστου μονοπατιού μεταξύ δύο κόμβων, οι Theodorakopoulos και Baras κατέληξαν στον ημιδακτύλιο απόστασης, στον οποίο το πεδίο από το οποίο παίρνει τιμές μια άποψη είναι το S=[0,∞]x[0,1]:

$$(t_{ik}, c_{ik}) \otimes (t_{kj}, c_{kj}) \rightarrow \left(\frac{1}{\frac{1}{t_{ik}} + \frac{1}{t_{kj}}}, c_{ik} c_{kj}\right),$$

$$\left(t_{ij}^{p1}, c_{ij}^{p1}\right) \oplus \left(t_{ij}^{p2}, c_{ij}^{p2}\right) \rightarrow \left(\frac{c_{ij}^{p1} + c_{ij}^{p2}}{\frac{c_{ij}^{p1}}{t_{ij}^{p1}} + \frac{c_{ij}^{p2}}{t_{ij}^{p2}}}, c_{ij}^{p1} + c_{ij}^{p2} \right).$$

Όπως φαίνεται, οι τιμές της εμπιστοσύνης αλλά και της βεβαιότητας φθίνουν όταν συναθροίζονται κατά μήκος ενός μονοπατιού. Επίσης, μια μηδενική τιμή εμπιστοσύνης θα δώσει μηδενική τιμή εμπιστοσύνης στην τελική άποψη, ενώ μια τιμή εμπιστοσύνης ίση με ∞ θα εξαφανίσει την αντίστοιχη άποψη από το τελικό αποτέλεσμα. Αντίθετα, οι τιμές βεβαιότητας βρίσκονται μέσα στο διάστημα $[0,1]$ και δεδομένου ότι πολλαπλασιάζονται μεταξύ τους, η τελική τιμή βεβαιότητας παρουσιάζεται μειωμένη. Από την άλλη, όταν η συνάθροιση γίνεται για πολλά μονοπάτια, η συνολική τιμή εμπιστοσύνης ισούται με το σταθμικό αρμονικό μέσο των συνιστωσών τιμών, με βάρη ανάλογα με τις τιμές βεβαιότητάς τους, δίνοντας ένα αποτέλεσμα μεταξύ των συνιστωσών τιμών αλλά κοντύτερα στην πιο βέβαιη. Επιπλέον, παρατηρείται ότι μια μηδενική τιμή βεβαιότητας μηδενίζει την αντίστοιχη άποψη στο αποτέλεσμα. Προκειμένου η τελική τιμή εμπιστοσύνης να είναι μέγιστη, θα πρέπει οι δύο απόψεις να έχουν επίσης μέγιστες τιμές. Στο σχήμα 14 φαίνεται ένα παράδειγμα εφαρμογής του ημιδακτυλίου απόστασης σε δύο απόψεις κόμβων.



Σχήμα 14: Εφαρμογή των τελεστών αλληλουχίας και σύνοψης του ημιδακτυλίου απόστασης

Οι Theodorakopoulos και Baras [47] παρουσίασαν τέλος έναν αλγόριθμο, ο οποίος υπολογίζει το άθροισμα ⊕ των βαρών όλων των μονοπατιών από έναν καθορισμένο κόμβο s προς όλους τους υπόλοιπους κόμβους ενός γραφήματος εμπιστοσύνης $G = (V, E)$. Ο αλγόριθμος αυτός, ο οποίος είναι μια επέκταση του αλγορίθμου Dijkstra, αξιολογεί όλες τις ενδείξεις που αφορούν στην εμπιστοσύνη. Ο κόμβος πηγή υπολογίζει απόψεις για όλους τους κόμβους σε κάθε κύκλο υπολογισμού. Στον αλγόριθμο αυτό υπάρχει περίπτωση να μην επιτραπεί σε κάποιους κόμβους να υποστηρίξουν κάποιον άλλο, και αυτό επειδή η τιμή εμπιστοσύνης των κόμβων αυτών δεν θα υπερβαίνει κάποιο προκαθορισμένο κατώφλι εμπιστοσύνης. Αντίθετα, δεν υπάρχει κανένας περιορισμός στην αντίστοιχη βεβαιότητα, επιτρέποντας έτσι αρχικά στους κακούς κόμβους να υποστηρίζουν άλλους κόμβους. Όταν όμως οι καλοί κόμβοι μαζέψουν αποδείξεις ότι οι κόμβοι αυτοί είναι κακοί, τους αποκλείουν. Επιπλέον,

είναι λογικό ότι κανένας κόμβος δεν επιτρέπεται να υποστηρίξει τον κόμβο πηγή, μιας και αυτός είναι που ξεκίνησε τη διαδικασία. Τέλος, απορρίπτονται οι ακμές που οδηγούν σε κυκλικά μονοπάτια.

3.11. Αξιοποίηση πολυδιάστατης φήμης

Πολλές φορές ένας πράκτορας είναι δύσκολο να προσδιορίσει τη φήμη ενός άλλου πράκτορα μόνο βάσει των συναλλαγών του με αυτόν, γιατί πιθανόν να μην υπάρχουν, είτε των μαρτυριών που λαμβάνει από άλλους πράκτορες. Σε αυτές τις περιπτώσεις χρησιμοποιούνται και οι τρεις διαστάσεις της φήμης για τον προσδιορισμό της, η ατομική, η κοινωνική και η οντολογική.

3.11.1. Το μοντέλο Regret

Οι Sabater και Sierra [48] παρουσίασαν ένα μοντέλο βασιζόμενο στη φήμη, το Regret, το οποίο εκμεταλλεύεται τις κοινωνικές σχέσεις μεταξύ των πρακτόρων. Κάθε πράκτορας διαθέτει ένα σύνολο κοινωνιογραμμάτων, τα οποία αναπαριστούν τις κοινωνικές του σχέσεις με το περιβάλλον που γνωρίζει. Το σύστημα Regret βασίζεται στις τρεις διαστάσεις της φήμης, στην ατομική, κατά την οποία ο πράκτορας χρησιμοποιεί τις άμεσες μόνο συναλλαγές του με τα υπόλοιπα μέλη της κοινωνίας για να δημιουργήσει δεδομένα για τη φήμη τους, στην κοινωνική, κατά την οποία ο πράκτορας χρησιμοποιεί τόσο τις άμεσες συναλλαγές, όσο και πληροφορίες που προέρχονται από άλλους πράκτορες του δικτύου και τις κοινωνικές σχέσεις για να εξάγει συμπεράσματα για τη φήμη τους, και τέλος την οντολογική διάσταση, κατά την οποία τα διαφορετικά είδη της φήμης συνδυάζονται μεταξύ τους και παράγουν νέα είδη.

Όπως αναφέρουν οι συγγραφείς, κάθε αποτέλεσμα ενός διαλόγου μεταξύ δύο πρακτόρων ορίζεται ως ένα συμβόλαιο, στο οποίο καθορίζονται οι ενέργειες που πρέπει να γίνουν και τα αποτελέσματα αυτών, ή ένα συμβόλαιο στο οποίο καθορίζονται οι συνθήκες μιας συναλλαγής, οι όροι και οι ακριβείς τιμές τους. Ένα αποτέλεσμα συμβολίζεται ως o=(a,b,I,X^c,X,t), όπου a και b οι πράκτορες του συμβολαίου, I ένα σύνολο δεικτών οι οποίοι ορίζουν τα θέματα του συμβολαίου, X^c και X διανύσματα που περιέχουν τις συμφωνημένες τιμές του συμβολαίου και τις τελικές τιμές μετά την ολοκλήρωσή του αντίστοιχα και t ο χρόνος στον οποίο υπογράφτηκε το συμβόλαιο. Επίσης, χρησιμοποιείται ένας υποδείκτης $i \in I$ για να αναφερθεί στη συγκεκριμένη τιμή του i στα X^c και X. Επιπλέον, ως ODB ορίζουν το σύνολο όλων των δυνατών αποτελεσμάτων, ενώ το $ODB^{a,b}_{\{i_1,\ldots,i_n\}}$ αποτελεί το σύνολο των αποτελεσμάτων του συμβολαίου μεταξύ των a και b, το οποίο έχει θέματα τα $\{i_1,\ldots, i_n\}$. Τα αποτελέσματα αυτά αποθηκεύονται σε μια βάση δεδομένων σε κάθε πράκτορα, τη λεγόμενη βάση δεδομένων αποτελεσμάτων, και αποτελούν τα βασικά κομμάτια από τα οποία υπολογίζεται η ατομική φήμη.

Οι Sabater και Sierra ορίζουν ως φήμη αποτελέσματος (outcome reputation) $R_{a\to b}^{o}(\varphi)$ τη φήμη τύπου φ, η οποία υπολογίζεται άμεσα από τη βάση δεδομένων αποτελεσμάτων ενός πράκτορα. Συγχρόνως ορίζουν τη βασική σχέση (grounding relation) gr η οποία συνδέει έναν τύπο φήμης φ με ένα σύνολο θεμάτων, τα οποία επιτρέπουν τη σωστή επιλογή των αντίστοιχων αποτελεσμάτων από τη βάση δεδομένων. Κάθε θέμα έχει τη μορφή (I_i, {+,-}, a_i), όπου η πρώτη παράμετρος ορίζει το θέμα, η δεύτερη καθορίζει το πώς επηρεάζει η αύξηση της τιμής του θέματος τη φήμη (+ την αυξάνει και – τη μειώνει), και τέλος η τρίτη παράμετρος αποτελεί το βάρος που έχει το θέμα αυτό στον υπολογισμό της φήμης. Έτσι, για τον υπολογισμό της φήμης αποτελέσματος χρησιμοποιείται ο παρακάτω τύπος:

$$R_{\substack{o \\ a\to b}}(\varphi) = \sum_{o_i \in ODB^{a,b}_{gr(\varphi)}} \rho(t, t_i) * Imp(o_i, gr(\varphi)) \,,$$

όπου $\rho(t, t_i) = \frac{f(t_i,t)}{\sum_{o_j \in ODB^{a,b}_{gr(\varphi)}} f(t_j,t)}$ και όπου t ο πραγματικός χρόνος. Η συνάρτηση $f(t_i, t)$, είναι χρονικά εξαρτώμενη και δίνει μεγαλύτερη βαρύτητα στα πιο πρόσφατα αποτελέσματα, ενώ η συνάρτηση $Imp(o_i, gr(\varphi))$ αξιολογεί το αποτέλεσμα o_i, λαμβάνοντας υπόψη τις πραγματικές τιμές των θεμάτων με τα οποία έχει συνδεθεί ο τύπος φήμης φ μέσω της σχέσης gr. Οι συγγραφείς ορίζουν την αξιολόγηση ενός αποτελέσματος ως τη διαφορά μεταξύ της χρησιμότητας ενός συμβολαίου και της χρησιμότητας της πραγματοποίησής του:

$$Imp\big(o, gr(\varphi)\big) = g\big(V(X^s) - V(X^c)\big),$$

όπου g μια συνάρτηση η οποία μοντελοποιεί τη συμπεριφορά ενός πράκτορα, σύμφωνα με το βαθμό εξαπάτησης ή ανταμοιβής που λαμβάνει μετά την ανάλυση του αποτελέσματος. Για το σκοπό αυτό μπορεί να χρησιμοποιηθεί η συνάρτηση $g(x) = \sin(\frac{\pi}{2}x)$, με τη βοήθεια της οποίας ο πράκτορας τιμωρεί την εξαπάτηση κατά την ολοκλήρωση ενός συμβολαίου δίνοντας τιμές κοντά στο -1 όταν $V(X^s) < V(X^c)$ ή τιμές κοντά στο 1 όταν συμβαίνει το αντίθετο. Ως $V(X^c)$ ορίζεται η συνάρτηση χρησιμότητας του διανύσματος X^c, ενώ το διάνυσμα X^s προκύπτει από τον τύπο:

$$X_i^s = \begin{cases} X_i, & \varepsilon\acute{\alpha}\nu\ i \in gr(\varphi) \\ X_i^c, & \delta\iota\alpha\varphi o\rho\varepsilon\tau\iota\kappa\acute{\alpha} \end{cases}$$

Το σύστημα Regret χρησιμοποιεί τον παράγοντα του αριθμού των αποτελεσμάτων No που χρησιμοποιούνται για τον υπολογισμό της φήμης και την απόκλιση της φήμης αποτελέσματος Dt, για να καθορίσει την αξιοπιστία της τιμής της φήμης. Όπως αναφέρεται, καθώς αυξάνεται ο αριθμός των αποτελεσμάτων, ο βαθμός αξιοπιστίας αυξάνεται μέχρι μιας μέγιστης τιμής itm, η οποία εξαρτάται από τη συχνότητα των συναλλαγών των μελών της κοινωνίας. Από την άλλη, όσο μεγαλύτερη είναι η μεταβλητότητα των τιμών εκτίμησης, τόσο πιο ασταθής θα είναι ο άλλος πράκτορας στην ολοκλήρωση της συμφωνίας. Για να μετρηθεί αυτή η μεταβλητότητα, λαμβάνεται υπόψη η επίδραση της πραγματικής εκτέλεσης των συμβολαίων στην αναμενόμενη χρησιμότητα. Τα παραπάνω μοντελοποιούνται με τη βοήθεια των τύπων:

$$\mathrm{No}\Big(ODB^{a,b}_{gr(\varphi)}\Big) = \begin{cases} \sin\left(\dfrac{\pi * \left|ODB^{a,b}_{gr(\varphi)}\right|}{2 * itm}\right), & \left|ODB^{a,b}_{gr(\varphi)}\right| \le itm \\ 1, & \delta\iota\alpha\varphi o\rho\varepsilon\tau\iota\kappa\acute{\alpha} \end{cases},$$

$$\mathrm{Dt}\Big(ODB^{a,b}_{gr(\varphi)}\Big) = \sum_{o_i} \rho(t, t_i) * \left|Imp(o_i, gr(\varphi)) - R_{\substack{o \\ a\to b}}(\varphi)\right| .$$

Το Dt παίρνει τιμές μεταξύ 0 και 1. Όταν η απόκλιση είναι κοντά στο 1, οι τιμές εκτίμησης έχουν μεγάλη μεταβλητότητα και άρα χαμηλή αξιοπιστία της τιμής της φήμης, ενώ το αντίθετο συμβαίνει όταν η απόκλιση είναι κοντά στο 0. Έχοντας ορίσει τα παραπάνω μεγέθη, ο παρακάτω τύπος ορίζει την αξιοπιστία μιας φήμης αποτελέσματος ως τον κυρτό (convex) συνδυασμό της συνάρτησης No και της απόκλισης της εκτίμησης αξιολόγησης αποτελεσμάτων Dt:

$$RL_{\underset{a\to b}{o}}(\varphi) = (1-\mu) * \mathrm{No}\left(ODB^{a,b}_{gr(\varphi)}\right) + \mu * \left(1 - \mathrm{Dt}\left(ODB^{a,b}_{gr(\varphi)}\right)\right).$$

Το Regret χρησιμοποιεί τρία είδη κοινωνικής φήμης ανάλογα με την πηγή των πληροφοριών για έναν πράκτορα: τη φήμη μάρτυρα $R_{\underset{a\to b}{w}}(\varphi)$ όπου οι πληροφορίες προέρχονται από άλλους πράκτορες, τη φήμη γειτονιάς $R_{\underset{a\to b}{N}}(\varphi)$ όπου οι πληροφορίες προέρχονται από τους γείτονες και τις σχέσεις τους με τον πράκτορα και τέλος τη φήμη συστήματος $R_{\underset{a\to b}{s}}(\varphi)$, η οποία έχει μια προκαθορισμένη τιμή ανάλογα με το ρόλο που έχει ο πράκτορας στη θεσμική δομή (institutional structure). Μια θεσμική δομή είναι μια κοινωνική δομή της οποίας τα μέλη έχουν ένα ή περισσότερα διακριτά χαρακτηριστικά, τα οποία τους καθορίζουν ως μέλη της δομής αυτής. Η φήμη συστήματος δεν είναι συνήθως τόσο αξιόπιστη, μιας και δεν λαμβάνει υπόψη τα χαρακτηριστικά του πράκτορα και του περιβάλλοντός του. Παρ' όλ' αυτά χρησιμεύει πολύ στις περιπτώσεις των νέων πρακτόρων, οι οποίοι δεν έχουν συναλλαγές ακόμα με άλλους πράκτορες. Αντίθετα, τα άλλα δύο είδη κοινωνικής φήμης απαιτούν μια πολύ καλή γνώση των κοινωνικών σχέσεων του εκάστοτε πράκτορα.

Στην περίπτωση της φήμης μάρτυρα, κάποιες πληροφορίες μπορεί να αποκρύπτονται, ή όσες μεταδίδονται τελικά από τους πράκτορες μάρτυρες μπορούν να είναι λανθασμένες, ακόμα και να συσχετίζονται μεταξύ τους όταν στηρίζονται στα ίδια γεγονότα ή διαμοιράζονται πολλές πληροφορίες, οι οποίες τείνουν να ενοποιούν τον τρόπο σκέψης των μαρτύρων. Στην τελευταία περίπτωση, η εμπιστοσύνη στις πληροφορίες αυτές δεν πρέπει να είναι τόσο μεγάλη όσο φαίνεται. Οι συγγραφείς ομαδοποιούν τους πράκτορες που είχαν συχνές αλληλεπιδράσεις με τον πράκτορα του οποίου ζητείται η φήμη, και αντιμετωπίζουν τον πιο αντιπροσωπευτικό πράκτορα κάθε ομάδας ως μοναδική πηγή φήμης, προκειμένου να ελαχιστοποιήσουν αυτή τη συσχέτιση. Το σύστημα Regret ακολουθεί μια ευρετική διαδικασία ώστε να βρεθεί από το σύνολο όλων όσοι έχουν αλληλεπιδράσει με τον πράκτορα στόχο, το υποσύνολο τον πρακτόρων οι οποίοι θα γίνουν μάρτυρες. Αρχικά, χρησιμοποιώντας ένα κοινωνιόγραμμα, βρίσκει τις συνιστώσες του και για κάθε μία από αυτές, το σύνολο των σημείων κοπής. Για κάθε συνιστώσα η οποία δε διαθέτει σημείο κοπής, επιλέγεται ο κόμβος με το μεγαλύτερο βαθμό. Η ένωση των συνόλων των κόμβων αυτών αποτελεί το σύνολο των μαρτύρων W.

Από το σύνολο των μαρτύρων, ένα υποσύνολο W' ανταποκρίνεται στο αίτημα του πράκτορα a και παρέχουν πληροφορίες με τη μορφή $\langle R_{w_i\to b}(\varphi), RL_{w_i\to b}(\varphi)\rangle$, όπου w_i ο πράκτορας που δίνει πληροφορίες στον a. Το πρώτο στοιχείο είναι η τιμή φήμης του πράκτορα στόχου κατά την άποψη του μάρτυρα, ενώ το δεύτερο στοιχείο δείχνει τη βεβαιότητα του μάρτυρα για την πρώτη τιμή. Δεδομένου ότι οι πληροφορίες αυτές μπορεί να είναι ψευδείς, ο πράκτορας a πρέπει να δώσει κάποιο βαθμό σπουδαιότητας σε καθεμία, προσδιορίζοντας μια τιμή εμπιστοσύνης $trust(a, w_i, b)$ για τον πράκτορα από τον οποίο προήλθε. Το σύστημα χρησιμοποιεί δύο διαφορετικές μεθόδους για να υπολογίσει την τιμή αυτή, μέσω της κοινωνικής εμπιστοσύνης $socialTrust(a, w_i, b)$ ή μέσω της φήμης εμπιστοσύνης αποτελέσματος (outcome trust reputation) $R_{\underset{a\to w_i}{o}}(trust)$. Η κοινωνική εμπιστοσύνη είναι ο βαθμός εμπιστοσύνης τον οποίο εκχωρεί ο πράκτορας a στον w_i, όταν ο δεύτερος τού παρέχει πληροφορίες για τον b λαμβάνοντας υπόψη τις κοινωνικές σχέσεις μεταξύ των τριών πρακτόρων. Το σύστημα Regret

χρησιμοποιεί ασαφείς κανόνες για να προσδιορίσει τον τρόπο με τον οποίο μια κοινωνική δομή παρέχει ένα βαθμό αξιοπιστίας σε μια πληροφορία που προέρχεται από κάποιο πράκτορα της δομής αυτής. Η είσοδος κάθε κανόνα είναι ο τύπος και ο βαθμός της κοινωνικής σχέσης, ενώ η έξοδος είναι η αξιοπιστία της πληροφορίας από την πλευρά της κοινωνικής σχέσης. Ανάλογα με τη σημασία που έχει κάθε σχέση στην κοινωνία του πράκτορα, επιλέγονται οι αντίστοιχες σχέσεις για τον υπολογισμό της αξιοπιστίας. Από την άλλη, η φήμη εμπιστοσύνης αποτελέσματος της «εμπιστοσύνης» που αξίζει ο μάρτυρας, υπολογίζεται όπως όλες οι φήμες αποτελέσματος και οι τιμές εμπιστοσύνης που υπολογίζονται είναι πιο χρήσιμες από εκείνες που προκύπτουν από τις κοινωνικές σχέσεις, αφού βασίζονται σε ατομικές εμπειρίες, σε αντίθεση με τις καθολικές αναμενόμενες συμπεριφορές. Βέβαια, είναι ευκολότερο να βρεθούν οι κοινωνικές σχέσεις απ' ότι ένα σύνολο αποτελεσμάτων, ειδικά εάν ο πράκτορας μόλις ξεκίνησε ένα νέο σενάριο. Έτσι, το Regret υπολογίζει το βαθμό εμπιστοσύνης που έχει ο πράκτορας a στο μάρτυρα w_i όταν ο δεύτερος του παρέχει πληροφορίες για τον b, χρησιμοποιώντας τη φήμη εμπιστοσύνης εάν είναι αξιόπιστη, διαφορετικά την κοινωνική εμπιστοσύνη:

$$trust(\alpha, w_i, b) = RL_{\underset{a\to w_i}{o}}(trust) * R_{\underset{a\to w_i}{o}}(trust) + \left(1 - RL_{\underset{a\to w_i}{o}}(trust)\right) * socialTrust(\alpha, w_i, b)\,.$$

Το Regret, έχοντας όλα τα παραπάνω στοιχεία, υπολογίζει τη φήμη μάρτυρα και την αξιοπιστία της, με βάση τον παρακάτω τύπο:

$$R_{\underset{a\to b}{w}}(\varphi) = \sum_{w_i \in W'} \omega^{w_i b} * R_{w_i \to b}(\varphi)\,,$$

$$RL_{\underset{a\to b}{w}}(\varphi) = \sum_{w_i \in W'} \omega^{w_i b} * min\left(trust(\alpha, w_i, b), RL_{w_i \to b}(\varphi)\right)\,,$$

όπου $\omega^{w_i b} = \frac{trust(\alpha, w_i, b)}{\sum_{w_j \in W'} trust(\alpha, w_j, b)}$. Ο πράκτορας χρησιμοποιεί την κανονικοποιημένη εμπιστοσύνη του μάρτυρα για να ζυγίσει κάθε άποψη στην τελική τιμή. Ο πράκτορας χρησιμοποιεί επίσης στον υπολογισμό της αξιοπιστίας τα ίδια βάρη με εκείνα στον υπολογισμό της φήμης. Τέλος, για να υπολογίσει την αξιοπιστία μιας ατομικής φήμης, χρησιμοποιεί το ελάχιστο μεταξύ της εμπιστοσύνης του μάρτυρα που έστειλε τη φήμη και της αξιοπιστίας που δίνει ο ίδιος ο μάρτυρας στη φήμη αυτή.

Για τον υπολογισμό της φήμης γειτονιάς χρησιμοποιούνται επίσης ασαφείς κανόνες, οι οποίοι συνδέουν τη φήμη αποτελέσματος ενός γείτονα του πράκτορα στόχου και την κοινωνική τους σχέση με τη φήμη που έχει ο πράκτορας στόχος. Η εφαρμογή των κανόνων αυτών παράγει ένα σύνολο από φήμες ατομικής γειτονιάς $R_{\underset{a\to b}{n_i}}(\varphi)$. Η αξιοπιστία κάθε φήμης ατομικής γειτονιάς χρησιμοποιείται για να ζυγίσει τη συμμετοχή στο τελικό αποτέλεσμα τόσο της φήμης, όσο και της αξιοπιστίας κάθε γείτονα, όπως φαίνεται στον τύπο υπολογισμού της φήμης γειτονιάς:

$$R_{\underset{a\to b}{N}}(\varphi) = \sum_{n_i \in N_b} \omega^{n_i b} * R_{\underset{a\to b}{n_i}}(\varphi) ,$$

$$RL_{\underset{a\to b}{N}}(\varphi) = \sum_{n_i \in N_b} \omega^{n_i b} * RL_{\underset{a\to b}{n_i}}(\varphi) ,$$

όπου $\omega^{n_i b} = \frac{RL_{\underset{a\to b}{n_i}}(\varphi)}{\sum_{n_j \in N_b} RL_{\underset{a\to b}{n_j}}(\varphi)}$ και όπου N_b =(n_1,n_2,…,n_n) το σύνολο των γειτόνων του πράκτορα b.

Για τον υπολογισμό της φήμης συστήματος, οι συγγραφείς θεωρούν ότι κάθε πράκτορας έχει ένα ρόλο κάθε φορά που εκτελεί μια ενέργεια και ότι η φήμη που αναλογεί σε κάθε ρόλο ανήκει στην αρχική γνώση κάθε πράκτορα. Ο υπολογισμός της φήμης γίνεται με τη βοήθεια ενός πίνακα για κάθε θεσμική δομή, του οποίου οι γραμμές είναι οι πιθανοί ρόλοι και οι στήλες όλοι οι εξειδικευμένοι τύποι φήμης.

Για την αναπαράσταση της τελευταίας διάστασης της φήμης, της οντολογικής, χρησιμοποιούνται δομές γραφημάτων, ενώ για τον υπολογισμό μιας φήμης, χρησιμοποιώντας τη διάστασή της αυτή, ο πράκτορας πρέπει να υπολογίσει τη φήμη όλων των συσχετιζόμενων πλευρών της συμπεριφοράς του πράκτορα, οι οποίες μπορούν με τη σειρά τους να είναι κόμβοι άλλων υπογραφημάτων με άλλες συσχετιζόμενες πλευρές. Η φήμη καθενός από τους κόμβους αυτούς, η οποία είναι συσχετισμένη με μια ατομική πλευρά της συμπεριφοράς του πράκτορα, υπολογίζεται χρησιμοποιώντας τις ατομικές και κοινωνικές διαστάσεις της. Έτσι, η φήμη ενός εσωτερικού κόμβου ψ ενός οντολογικού γραφήματος υπολογίζεται από τον τύπο:

$$R_{a\to b}(\varphi) = \sum_{\psi \in children(\varphi)} \omega_{\varphi\psi} * R_{a\to b}(\psi) ,$$

$$RL_{a\to b}(\varphi) = \sum_{\psi \in children(\varphi)} \omega_{\varphi\psi} * RL_{a\to b}(\psi) ,$$

όπου $\omega_{\varphi\psi}$ η σπουδαιότητα κάθε άποψης. Συνδυάζοντας όλα τα παραπάνω, καταλήγουμε στους παρακάτω τύπους με τους οποίους το σύστημα Regret υπολογίζει τη φήμη κάθε πράκτορα:

$$R_{a\to b}(\varphi) = \begin{cases} \sum_{i \in \{O,W,N,S\}} \xi_i * R_{\underset{a\to b}{i}}(\varphi) , & \text{εάν } \varphi \text{ είναι φύλλο} \\ \sum_{\psi \in children(\varphi)} \omega_{\varphi\psi} * R_{a\to b}(\psi) , & \text{διαφορετικά} \end{cases} ,$$

$$RL_{a\to b}(\varphi) = \begin{cases} \sum_{i\in\{O,W,N,S\}} \xi_i * RL_{\ \ a\to b}^{\ i}(\varphi) \ , & \varepsilon\acute{\alpha}\nu\ \varphi\ \epsilon\acute{\iota}\nu\alpha\iota\ \varphi\acute{\upsilon}\lambda\lambda o \\ \sum_{\psi\in children(\varphi)} \omega_{\varphi\psi} * RL_{a\to b}(\psi) \ , & \delta\iota\alpha\varphi o\rho\epsilon\tau\iota\kappa\acute{\alpha} \end{cases},$$

Όπως αναφέραμε, η πιο αξιόπιστη φήμη είναι κατά σειρά η φήμη αποτελέσματος, η φήμη μάρτυρα, η φήμη γειτονιάς και τέλος η φήμη συστήματος. Το σύστημα Regret δίνει μεγαλύτερη βαρύτητα στη φήμη αποτελέσματος και αν αυτή έχει χαμηλή αξιοπιστία, τότε ο πράκτορας χρησιμοποιεί τα επόμενα δύο είδη φήμης. Εάν όμως η γνώση του για τις κοινωνικές σχέσεις είναι μικρή, τότε θα χρησιμοποιήσει τη φήμη συστήματος. Έτσι, χρησιμοποιώντας τους παράγοντες $\{\xi_I, \xi_W, \xi_N, \xi_S\}$ η φόρμουλα που χρησιμοποιεί το Regret είναι η:

$$\begin{aligned} \xi_I &= RL_{\ \ a\to b}^{\ O}(\varphi)\,, \\ \xi_W &= RL_{\ \ a\to b}^{\ W}(\varphi) * (1-\xi_I)/2\,, \\ \xi_N &= RL_{\ \ a\to b}^{\ N}(\varphi) * (1-\xi_I)/2\,, \\ \xi_S &= 1-(\xi_I+\xi_W+\xi_N)\,. \end{aligned}$$

3.12. Περιορισμός μήκους μονοπατιού εμπιστοσύνης

Όλα τα μοντέλα εμπιστοσύνης προσπαθούν να υπολογίσουν τιμές εμπιστοσύνης μεταξύ κόμβων, οι οποίοι συνήθως συνδέονται μεταξύ τους μέσω έμμεσων σχέσεων. Κάποια μοντέλα θέτουν περιορισμό στο μήκος των μονοπατιών που συνδέουν τους κόμβους.

3.12.1. Το μοντέλο TwoHop

Οι Glynos, Argyroudis, Douligeris και O'Mahony [49] παρουσίασαν μια συνεργατική μετρική και έναν αλγόριθμο αξιολόγησης εμπιστοσύνης σε δίκτυα ομότιμων κόμβων, τον λεγόμενο TwoHop. Ο αλγόριθμος αυτός χρησιμοποιεί συστάσεις κόμβων, προκειμένου να αξιολογήσει την αξιοπιστία παρόχων υπηρεσιών. Χρησιμοποιώντας άμεσες σχέσεις μεταξύ κόμβων που είχαν αλληλεπιδράσει στο παρελθόν, εγκαθίστανται σχέσεις μεταξύ άγνωστων κόμβων.

Το πρόβλημα που καλείται να επιλύσει ο αλγόριθμος TwoHop μοντελοποιείται με τη βοήθεια ενός κατευθυνόμενου γραφήματος με βάρη, του οποίου οι κορυφές αναπαριστούν τους συμμετέχοντες, οι ακμές τις σχέσεις μεταξύ τους και τα βάρη των ακμών τη δύναμη της σχέσης αυτής. Οι κόμβοι μπορούν να συνδέονται μεταξύ τους με πολλές ακμές, καθεμία από τις οποίες αναπαριστά διαφορετικού τύπου σχέση και μπορούν να εγκαθιστούν έμμεσες σχέσεις μεταξύ τους μόνο όσοι απέχουν απόσταση ίση έως δύο βήματα. Το βάρος κάθε νέας εγκαθιστάμενης σχέσης μεταξύ μιας κορυφής πηγής και μιας δεύτερης κορυφής εξαρτάται από τον τύπο της ακμής και την απόσταση μεταξύ των κορυφών αυτών.

Οι συγγραφείς χρησιμοποιούν πέντε βασικές αρχές για την κατασκευή της αρχιτεκτονικής TwoHop. Αρχικά, επιβάλλουν τον περιορισμό των δύο βημάτων στα μονοπάτια συστάσεων κόμβων. Έτσι, οι κόμβοι που κάνουν τις συστάσεις, είτε συνδέονται άμεσα με τους κόμβους τους οποίους συστήνουν, είτε δέχονται από τους άμεσους γείτονές τους τις συστάσεις τους για κόμβους με τους οποίους είχαν άμεση επαφή στο παρελθόν. Δεύτερον, κάθε ακμή όπως αναφέραμε αναπαριστά διαφορετικού είδους σχέση εμπιστοσύνης και έτσι ένα βάρος ακμής μπορεί να περιγράφει την ποιότητα μιας υπηρεσίας που παρέχει ένας κόμβος, ενώ ένα άλλο την ποιότητα των αξιολογήσεων που αυτός παρέχει. Τρίτον, κάθε κόμβος διατηρεί ένα

τοπικό χαρτοφυλάκιο (portfolio) εμπιστοσύνης, όπου διατηρεί όλες τις σχέσεις εμπιστοσύνης που έχει δημιουργήσει τον τελευταίο καιρό, αλλά μπορεί να συμβουλευτεί και τα χαρτοφυλάκια άλλων κόμβων, των οποίων το περιεχόμενο όμως έγκειται σε περιορισμούς τοπικών βαρών. Τέταρτον, η μετρική που χρησιμοποιεί το σύστημα, η οποία περιγράφει την εμπιστοσύνη σε μια υπηρεσία μέσα από την εμπειρία των κόμβων που βρίσκονται σε ακτίνα δύο βημάτων από τον κόμβο που τη χρειάζεται, είναι το αλγεβρικό άθροισμα των σχετικών βαρών και αξιολογήσεων που βρίσκονται στα χαρτοφυλάκια των κόμβων αυτών. Τέλος, εάν για έναν πάροχο μιας υπηρεσίας βρεθούν περισσότεροι από ένας αξιολογητές, συμβάλλουν όλοι στον υπολογισμό της εμπιστοσύνης, ενώ εάν βρεθούν δύο ή περισσότερα μονοπάτια που διαθέτουν τον ίδιο αξιολογητή, επιλέγεται το συντομότερο, εκτός και αν έχουν το ίδιο μήκος, οπότε επιλέγεται εκείνο που ξεκινάει από τον πιο έμπιστο κόμβο.

Οι κόμβοι του συστήματος TwoHop μπορούν να έχουν έναν ή περισσότερους από τους εξής ρόλους: παροχείς υπηρεσιών, αξιολογητές υπηρεσιών, κριτές των αξιολογητών υπηρεσιών και τέλος κριτικοί συλλογών αξιολογητών. Το πόσους ρόλους θα έχει συγχρόνως ένας κόμβος εξαρτάται από τις δραστηριότητές του όσο είναι παρών στο δίκτυο. Για να καταλάβουμε τους ρόλους αυτούς θα πρέπει να τους αναλύσουμε τον έναν μετά τον άλλο. Ένας πάροχος υπηρεσίας είναι ένας κόμβος ο οποίος παρέχει μια υπηρεσία σε άλλους κόμβους. Κάθε υπηρεσία διαθέτει ένα αναγνωριστικό s με τη βοήθεια του οποίου αναγνωρίζεται ο τύπος της υπηρεσίας από τους κόμβους του δικτύου. Ο αξιολογητής υπηρεσίας είναι στη συνέχεια ένας κόμβος ο οποίος κάποια στιγμή χρησιμοποίησε την υπηρεσία που του προσέφερε ένας τέτοιος πάροχος και αξιολόγησε την ποιότητά της. Ο κριτής αξιολογητή υπηρεσίας είναι ο κόμβος εκείνος που αποτιμά την ποιότητα των αξιολογήσεων που έκανε ο αξιολογητής υπηρεσίας για την υπηρεσία αυτή, ενώ τέλος ο κριτικός συλλογής αξιολογητή εξετάζει τις εκτιμήσεις του προηγούμενου κριτή για τον τύπο της υπηρεσίας αυτής και απονέμει βαθμούς τόσο για την ποσότητα, όσο και για την ποιότητα των εκτιμήσεων αυτών. Έτσι, κάθε κόμβος του συστήματος διαθέτει τελικά ένα σύνολο χαρτοφυλακίων εμπιστοσύνης, με ένα χαρτοφυλάκιο για κάθε τύπο υπηρεσίας, το οποίο περιέχει όλες τις πληροφορίες αξιολογήσεων, αποτιμήσεων και κριτικών που έχει κάνει ο ιδιοκτήτης. Εάν κάποια από τις τιμές αυτές δεν είναι διαθέσιμη, τότε χρησιμοποιείται η τιμή 0.

Προκειμένου το σύστημα TwoHop να υπολογίσει τη συνολική τιμή εμπιστοσύνης για μια υπηρεσία, χρησιμοποιεί τρεις συναρτήσεις. Η συνάρτηση `getPortfolio(`i, s`)` ανακτά το χαρτοφυλάκιο για την υπηρεσία τύπου s από τον κόμβο με αναγνωριστικό i. Η συνάρτηση `peerExists(`P, i`)` επιστρέφει TRUE εάν βρεθεί ο κόμβος i στο χαρτοφυλάκιο P, ενώ η συνάρτηση `calculateTrust(`P_{root}, i, s`)` υπολογίζει την τιμή εμπιστοσύνης για την υπηρεσία τύπου s που προσέφερε ο κόμβος i, ξεκινώντας από το χαρτοφυλάκιο P_{root}, το λεγόμενο αρχικό χαρτοφυλάκιο εμπιστοσύνης, το οποίο είναι συνήθως το χαρτοφυλάκιο του ίδιου του κόμβου. Στην περίπτωση που το χαρτοφυλάκιο αυτό δεν περιέχει εγγραφές, μπορεί να χρησιμοποιηθεί το χαρτοφυλάκιο κάποιου έμπιστου κόμβου ως αρχικό.

Η τελευταία συνάρτηση είναι εκείνη που επιτελεί τη συνολική διαδικασία του υπολογισμού. Αρχικά, σαρώνει το αρχικό χαρτοφυλάκιο εμπιστοσύνης για καταχωρήσεις που αφορούν άλλους κόμβους εκτός του παρόχου. Έτσι αποφεύγεται να συνυπολογιστούν οι αξιολογήσεις που πιθανόν να έχει κάνει ο πάροχος για τη δική του υπηρεσία, αξιολογήσεις που πιθανόν να έχουν κάνει άλλες ομάδες που γνωρίζει ο πάροχος ή παλαιότερες αξιολογήσεις που είχε κάνει ο ιδιοκτήτης του αρχικού χαρτοφυλακίου. Στη συνέχεια εξάγεται και εξετάζεται σειριακά το χαρτοφυλάκιο (P_{onehop}) κάθε εναπομείναντα κόμβου που βρίσκεται στις καταχωρήσεις του αρχικού χαρτοφυλακίου. Οι κόμβοι αυτοί απέχουν ένα βήμα από τον κόμβο στον οποίο ανήκει το P_{root}. Σε καθένα από τα χαρτοφυλάκια αυτά αναζητούνται καταχωρήσεις αξιολογήσεων της υπηρεσίας του παρόχου και καταχωρήσεις εκτιμήσεων για κόμβους, οι οποίοι είναι ειδικοί στο συγκεκριμένο τύπο υπηρεσίας. Εάν βρεθεί κάποια τιμή αξιολόγησης, αυτή πολλαπλασιάζεται με την τιμή εκτίμησης με την οποία συνδέεται ο κόμβος αυτός στο P_{root} και η τιμή προστίθεται στη συνολική εμπιστοσύνη, ενώ η τιμή εκτίμησης προστίθεται στο συνολικό βάρος αντίστοιχα. Εάν βρεθεί κάποια εκτίμηση μέσα στα P_{onehop} η οποία αναφέρεται σε κόμβο ο οποίος ήδη περιέχεται μέσα στο P_{root}, η εκτίμηση αυτή απορρίπτεται. Γενικά, οι καταχωρήσεις

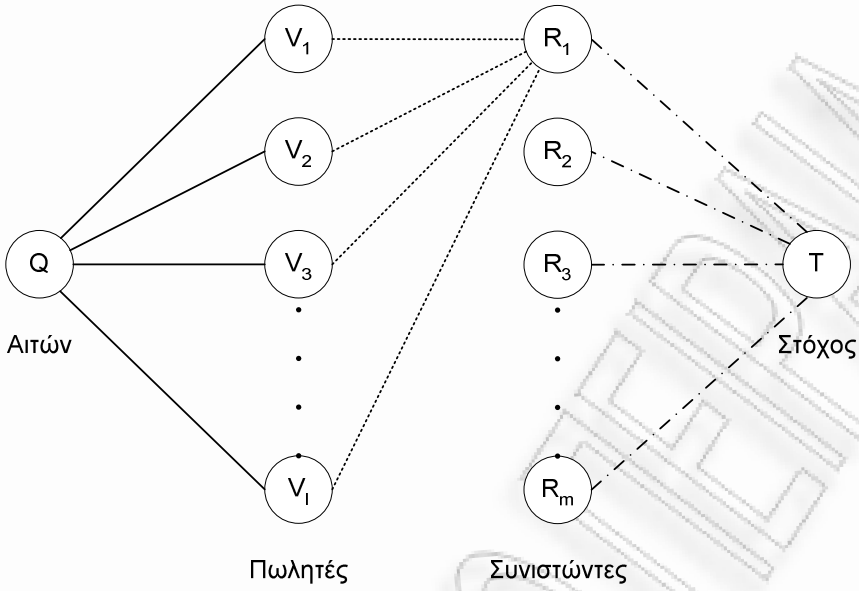
εκτιμήσεων στα P_{onehop} χρησιμοποιούνται ως δείκτες προς τα χαρτοφυλάκια δεύτερου βήματος (P_{twohop}). Για καθένα από τα P_{twohop} καταγράφεται η εκτίμηση που συνδέεται με τον ιδιοκτήτη του χαρτοφυλακίου, όπως περιγράφτηκε στο P_{onehop} και στη συνέχεια εξάγεται και εξετάζεται σειριακά κάθε P_{twohop} για καταχωρήσεις αξιολόγησης του ζητούμενου παρόχου. Η τιμή αυτή πολλαπλασιάζεται με ένα γινόμενο βάρους, το οποίο αποτελείται από την καταχώρηση εκτίμησης στο P_{onehop} και την τιμή της κριτικής του ιδιοκτήτη του P_{root} για τον κόμβο ο οποίος πρότεινε αυτό τον κόμβο που απέχει δύο βήματα. Το βάρος αυτό προστίθεται αντίστοιχα στο συνολικό βάρος. Η τιμή της εμπιστοσύνης που τελικά επιστρέφει η συνάρτηση `calculateTrust` είναι ο σταθμικός μέσος των συλλεγόμενων αξιολογήσεων.

3.12.2. Το μοντέλο των Prasad et al.

Οι Prasad et al. [50] παρουσίασαν ένα κατανεμημένο σύστημα υπολογισμού φήμης, το οποίο στηρίζεται στο σύστημα διαμοιρασμού αρχείων σε ένα δίκτυο ομότιμων κόμβων και εξαρτάται κυρίως από τις ομοιότητες των αναδράσεων και κάποια κατηγορία ομότιμων, καθώς και από την ομοιότητα και την παλαιότητα των συναλλαγών. Κάθε ομότιμος στο σύστημά τους έχει διπλό ρόλο. Μπορεί να είναι πάροχος αρχείων σε άλλους ομότιμους ή καταναλωτής, ο οποίος χρησιμοποιεί αρχεία παρεχόμενα από άλλους ομότιμους του δικτύου. Κάθε καταναλωτής αξιολογεί την υπηρεσία που έλαβε από έναν πάροχο, με βάση την ταχύτητα μεταφοράς, την ποιότητα, καθώς και τον αριθμό των συναλλαγών που πραγματοποίησαν. Ως αποτέλεσμα της συνάθροισης των αξιολογήσεων που έχουν οι καταναλωτές για κάποιον πάροχο, εκείνος διαμορφώνει μια φήμη.

Ένα δίκτυο ομότιμων κόμβων μπορεί από τη μία να διαθέτει πολλούς νέους κόμβους, οι οποίοι δε διαθέτουν καμία εκτίμηση για τους υπάρχοντες ομότιμους του δικτύου, ενώ οι παλαιοί ομότιμοι με τη σειρά τους είναι σχεδόν αδύνατον να αλληλεπιδράσουν με όλους τους υπόλοιπους ομότιμους του δικτύου. Δεδομένου ότι κάθε ομότιμος κόμβος υπολογίζει την εμπιστοσύνη του για έναν άλλο ομότιμο μόνο μετά από άμεση αλληλεπίδραση μαζί του, το σύστημα των Prasad et al. στηρίζεται στη φήμη και στις προσδοκίες της συνεργατικής συμπεριφοράς που έχουν κάποιοι ομότιμοι για κάποιους άλλους, προκειμένου να υπολογίσει την αξιοπιστία τους. Στην περίπτωση των νέων κόμβων, η φήμη τους μπορεί να υπολογιστεί μόνο μετά από τουλάχιστον μια αλληλεπίδραση με έναν τουλάχιστον ομότιμο κόμβο.

Στην περίπτωση που κάποιος ομότιμος δεν έχει πρότερη εμπειρία από κάποιον πάροχο, θα κάνει ένα ερώτημα στους υπόλοιπους ομότιμους για να βρει αν κάποιος έχει αλληλεπιδράσει με τον πάροχο αυτό. Οι συγγραφείς μοντελοποιούν το ζήτημα της φήμης, χρησιμοποιώντας ένα γράφημα κόμβων, στο οποίο εκτός από τον αιτώντα και τον ομότιμο στόχο, όπου ο πρώτος θέλει να κάνει μια συναλλαγή με τον δεύτερο, υπάρχουν οι ομότιμοι συνιστώντες (recommenders), οι οποίοι είχαν συναλλαχθεί στο παρελθόν με τον ομότιμο στόχο και οι οποίοι παρέχουν ανάδραση στον αιτώντα, καθώς και οι ομότιμοι πωλητές (vendors), οι οποίοι συναλλάσσονται τόσο με τους συνιστώντες, όσο και με τον αιτώντα. Το γράφημα αυτό φαίνεται στο σχήμα 15.



Σχήμα 15: Φήμη σε δίκτυα ομότιμων κόμβων

Όπως φαίνεται, ο αιτών ζητάει πληροφορίες για το στόχο από τον συνιστώντα και εκείνος τού παρέχει μια ανάδραση, με βάση τις συναλλαγές που έχει πραγματοποιήσει με τον ομότιμο στόχο. Η ανάδραση μπορεί να οριστεί ως η αναλογία της ικανοποίησης του ομότιμου σε σχέση με τον αριθμό των συναλλαγών που πραγματοποιήθηκαν. Η ικανοποίηση αυτή εξαρτάται από διάφορους παράγοντες, όπως η ποιότητα της παρεχόμενης υπηρεσίας. Εάν κάποιος κόμβος απαντήσει, αλλά δεν έχει πραγματοποιήσει κάποια συναλλαγή με τον κόμβο στόχο, αγνοείται. Οι συνιστώντες αποστέλλουν μια λίστα με τους πωλητές με τους οποίους έχουν αλληλεπιδράσει, μαζί με μια ανάδραση για καθέναν από αυτούς. Ο αιτών βρίσκει μια λίστα κοινών ομότιμων πωλητών για κάθε έναν από τους συνιστούντες και υπολογίζει την ομοιότητα που έχει με καθέναν από τους συνιστούντες αυτούς. Με βάση την ομοιότητα, υπολογίζει στη συνέχεια την αξιοπιστία καθενός. Η ανάδραση από κάθε συνιστώντα προσαρμόζεται, με βάση την αξιοπιστία του και παραλείπονται εκείνες που έχουν αποσταλεί από αναξιόπιστους κόμβους. Τελικά ο αιτών θα πάρει ο ίδιος μια απόφαση για να αλληλεπιδράσει με τον κόμβο στόχο, χωρίς να εξαρτάται από κάποιο κεντρικό σύστημα. Εάν θεωρήσουμε τους ομότιμους j και k τότε η ανάδραση f_{jk} που δίνει ο k για τον j δίνεται από τον τύπο:

$$f_{jk} = \frac{\sum_{i=1}^{n} s_{jk_i}}{n},$$

όπου n ο συνολικός αριθμός συναλλαγών που έχουν πραγματοποιηθεί από τον k με τον j. Το s_{jk_i} είναι η ικανοποίηση του k για τον j στην i–οστή συναλλαγή. Ανάλογα με την ποιότητα της συναλλαγής, η τιμή της ικανοποίησης που δίνεται από τον κόμβο, κυμαίνεται στο διάστημα μεταξύ 0 (ανικανοποίητος) και 1 (απόλυτα ικανοποιημένος). Καθώς όμως συνεχίζουν οι συναλλαγές μεταξύ των κόμβων, οι συγγραφείς διαχωρίζουν τη βαρύτητα της ικανοποίησης που είχαν οι παλαιότερες συναλλαγές και δίνουν μεγαλύτερο βάρος στις πιο πρόσφατες συναλλαγές, προσθέτοντας τις παραμέτρους int, ένα χρονικό διάστημα μέσα στο οποίο γίνεται ένα σύνολο συναλλαγών, t για την ακριβή στιγμή κατά την οποία πραγματοποιήθηκε η συναλλαγή και την παράμετρο tf, η οποία αποτελεί πλαίσιο χρόνου μέσα στο οποίο διαιρείται σε χρονικά διαστήματα int όλος ο χρόνος που έχει περάσει από τη στιγμή 0 μέχρι την tf. Αν

θεωρήσουμε ότι το $int=0$ αναπαριστά την πιο πρόσφατη περίοδο και η επόμενη πιο πρόσφατη περίοδος είναι η $int=1$, ενώ η i-οστή συναλλαγή πραγματοποιήθηκε σε κάποια περίοδο int, τότε η ανάδραση f_{jk} που δίνει ο k για τον j δίνεται από τον τύπο:

$$f_{jk} = \frac{\sum_{i=1,n \quad int=0,|tf|} \left[\frac{\left(t-2^{int}\right)+1}{t}\right] * s_{jk_i}}{n}.$$

Όπως δείχνει και ο τύπος, οι αναδράσεις και οι τιμές ικανοποίησης φθίνουν με την πάροδο του χρόνου, κάνοντας πιο σημαντικές τις πιο πρόσφατες εκτιμήσεις και καθιστώντας τον υπολογισμό της φήμης πιο δυναμικό. Ένας αξιόπιστος κόμβος θεωρείται εκείνος που θα δώσει σωστή ανάδραση, ενώ εκείνος που δίνει αναδράσεις οι οποίες δεν αντιστοιχούν στην εμπιστοσύνη του θεωρείται κακόβουλος κόμβος. Η εμπιστοσύνη ενός ομότιμου για έναν άλλο ομότιμο παραμένει στη γνώση του πρώτου και δεν γνωστοποιείται σε κάποιον άλλο, εάν ο τελευταίος δεν επικοινωνήσει μαζί του. Έτσι, είναι δύσκολο να βρεθεί εάν ένας ομότιμος είναι κακόβουλος ή όχι. Οι συγγραφείς αντιμετωπίζουν το πρόβλημα αυτό υπολογίζοντας, όπως είπαμε, την αξιοπιστία ενός ομότιμου ο οποίος δίνει ανάδραση για έναν δεδομένο κόμβο στόχο.

Το μοντέλο που παρουσιάζεται δίνει μεγάλη σημασία στην ομοιότητα των συναλλαγών, των αναδράσεων και στην ομοιότητα των ομότιμων πωλητών που επιλέγουν οι κόμβοι για τις συναλλαγές τους. Όπως αναφέρουν οι Prasad et al., όσο πιο συχνά συναλλάσσονται δύο ομότιμοι με τον ίδιο πωλητή, τόσο ομοιότεροι είναι μεταξύ τους. Άρα ένα μέτρο της ομοιότητάς τους αυτής είναι ο αριθμός των συναλλαγών που πραγματοποιούν με τον ίδιο πωλητή και δίνεται από τον τύπο:

$$Sim_{\in} = \frac{\left|I_{(Q,V)} - I_{(R,V)}\right|}{\left(I_{(Q,V)} + I_{(R,V)}\right)},\ 0 \le Sim_{\in} \le 1\ ,$$

όπου $I_{(Q,V)}$ και $I_{(R,V)}$ το σύνολο των συναλλαγών που πραγματοποιήθηκαν με τον ομότιμο πωλητή V από τον ομότιμο αιτώντα Q και από τον ομότιμο συνιστώντα R αντίστοιχα. Όσο η τιμή του $Sim_{\in}$ προσεγγίζει το 0, τόσο οι Q και R τείνουν να είναι όμοιοι, ενώ το αντίθετο συμβαίνει όσο η τιμή τείνει προς το 1. Η ομοιότητα των αναδράσεων των δύο παραπάνω ομότιμων κατά την εκτίμηση μιας συγκεκριμένης υπηρεσίας, προσδιορίζεται από τον τύπο:

$$Sim_{\mathrm{F}} = \sqrt{\frac{\sum_{i=1}^{N}\left(f_{v_i R_1} - f_{v_i Q}\right)}{N}},\ 0 < Sim_{\mathrm{F}} < 1\ ,$$

όπου N οι ομότιμοι πωλητές. Όπως και με την ομοιότητα των συναλλαγών, εάν η τιμή της Sim_{F} είναι μικρή, τότε η εκτίμηση των Q και R είναι όμοια, ενώ εάν είναι μεγάλη είναι ανόμοια. Τέλος, για την ομοιότητα των πωλητών, οι συγγραφείς αναφέρουν ότι όσο μεγαλύτερος είναι ο αριθμός των πωλητών για ένα ζεύγος κόμβων, τόσο περισσότερο όμοιοι είναι. Έτσι, εάν θεωρήσουμε τους αριθμούς των πωλητών NV_R και NV_Q με τους οποίους έχουν συναλλαχθεί οι R και Q αντίστοιχα, η ομοιότητα των τελευταίων ως προς την προτίμησή τους σε κάποιους ομότιμους πωλητές για να κάνουν τις συναλλαγές τους, δίνεται από τον τύπο:

$$Sim_{\text{cv}} = \frac{2*\left|NV_R - NV_Q\right|}{NV_R + NV_Q + 2*\left|NV_R - NV_Q\right|},\ 0 \le Sim_{\epsilon} \le 1\ .$$

Όπως αναφέραμε και παραπάνω, η αξιοπιστία αποτελεί ένα μέτρο για το κατά πόσο μια ανάδραση ενός κόμβου είναι έγκυρη και στην περίπτωση ενός ομότιμου συνιστώντα δίνεται από τον τύπο:

$$Cr = (1\text{-}\ Sim_{\text{F}}) * Sim_{\text{cv}},\ 0 < Cr < 1.$$

Όπως φαίνεται, όσο πιο όμοιες είναι οι αναδράσεις και μεγαλύτερος ο αριθμός των κοινών ομότιμων πωλητών, τόσο πιο αξιόπιστοι είναι οι κόμβοι.

Η εμπιστοσύνη ενός ομότιμου σε έναν άλλο βασίζεται συνήθως στον αριθμό των επιτυχημένων συναλλαγών που έχουν πραγματοποιήσει μεταξύ τους. Εάν μετά από τις πρώτες συναλλαγές δεν έχουν υπάρξει αρκετές πληροφορίες για τον προσδιορισμό της, υπολογίζεται η φήμη του ομότιμου κόμβου για να καθοριστεί το κατά πόσο μπορούν να γίνουν άλλες συναλλαγές. Η φήμη αποτελεί τη συνδυασμένη ανάδραση που αποδίδουν σε κάποιο κόμβο άλλοι κόμβοι. Οι Prasad et al. υπολόγισαν τη φήμη $Rep_{R_1R_2}$ ενός κόμβου R_1 σε σχέση με έναν άλλο R_2, συνυπολογίζοντας τον παράγοντα των αναξιόπιστων κόμβων και υποβαθμίζοντας τη συμμετοχή τους χρησιμοποιώντας μια σταθερά ρ:

$$Rep\_adj_{R_1R_2} = \frac{\sum_{i=1}^{N}\left(f_{R_1V_i} \times Cr_{R_2V_i}^{\rho}\right)}{\sum_{i=1}^{N} Cr_{R_2V_i}^{\rho}},$$

όπου N ο αριθμός των ομότιμων πωλητών V_{i} οι οποίοι έχουν ήδη συναλλαχθεί με τον κόμβο R_1, ενώ $Cr_{R_2V_i}$ ο παράγοντας αξιοπιστίας του R_2 σε σχέση με τον κόμβο V_{i}. Εάν η σταθερά ρ λάβει την τιμή 1, τότε η ανάδραση ορίζεται με βάρος τον παράγοντα αξιοπιστίας του κόμβου.

4. Αξιολόγηση μοντέλων εμπιστοσύνης

Τα μοντέλα εμπιστοσύνης που περιγράψαμε στο προηγούμενο κεφάλαιο είχαν ομαδοποιηθεί με βάση το κύριο χαρακτηριστικό που τα διακρίνει. Προκειμένου όμως να αξιολογηθούν τα μοντέλα, ώστε στη συνέχεια να συγκριθούν, πρέπει να εξεταστούν τα χαρακτηριστικά τους κάτω από ένα κοινό φάσμα. Οι Theodorakopoulos και Baras [51] προσπάθησαν να εφαρμόσουν μια τέτοια τακτική, τυποποιώντας τις μετρικές εμπιστοσύνης κάποιων μοντέλων και εισάγοντάς τες σε ένα αλγεβρικό πλαίσιο, μέσα από το οποίο προέκυψαν συγκρίσιμα συμπεράσματα για τις μετρικές αυτές. Το δεύτερο μέρος της αξιολόγησης έχει να κάνει με την ανθεκτικότητα κάθε μοντέλου εμπιστοσύνης σε γνωστές επιθέσεις κακόβουλων κόμβων και ο τρόπος που τις αντιμετωπίζει καθένα από αυτά.

4.1. Τυποποίηση και γενικά χαρακτηριστικά μετρικών εμπιστοσύνης

Οι Theodorakopoulos και Baras [51] παρείχαν ένα αλγεβρικό πλαίσιο μέσω του οποίου περιέγραψαν τρόπους για τη συνένωση πληροφοριών που σχετίζονται με την εμπιστοσύνη και τη δημιουργία μιας μοναδικής τιμής. Όπως αναφέρουν, η εμπιστοσύνη είναι μια σταθμισμένη δυαδική σχέση μεταξύ δύο μελών ενός δικτύου. Εάν για παράδειγμα έχουμε ένα ιεραρχικό δίκτυο πρακτόρων, τότε η εμπιστοσύνη ενός πράκτορα προς έναν άλλο πράκτορα θα μπορούσε να είναι η προσδοκία ότι ο δεύτερος είναι αξιόπιστος, ενώ το βάρος της σχέσης αυτής θα είναι η ποσοτικοποίηση της παραπάνω προσδοκίας, δηλαδή όσο μεγαλύτερο είναι, τόσο μεγαλύτερη είναι και η προσδοκία. Οι καθημερινές αλληλεπιδράσεις μεταξύ κάποιων μελών ενός δικτύου είναι εκείνες που δημιουργούν την άμεση εμπιστοσύνη ή δυσπιστία μεταξύ τους, κάτι όμως που δεν υπάρχει μεταξύ όλων των ζευγών των μελών του δικτύου αυτού. Κάθε μέλος που δεν έχει άμεση εμπιστοσύνη σε κάποιο άλλο μέλος, αλλά για το οποίο χρειάζεται να βγάλει κάποιο συμπέρασμα, πρέπει όπως έχουμε αναφέρει να υπολογίσει την αξιοπιστία του βασιζόμενο σε έμμεσες σχέσεις εμπιστοσύνης. Αυτό γίνεται συνδυάζοντας όλες τις σχετικές άμεσες σχέσεις εμπιστοσύνης και τα σχετιζόμενα με αυτές βάρη και καταλήγοντας σε έμμεσες τιμές εμπιστοσύνης.

Το μοντέλο των Theodorakopoulos και Baras κάνει χρήση της σύστασης εμπιστοσύνης ενός χρήστη για έναν άλλο χρήστη. Όπως αναφέρουν, οι τιμές δύο συστάσεων εμπιστοσύνης από δύο διαφορετικούς χρήστες για έναν τρίτο μπορεί να διαφέρουν, δεδομένου ότι καθένας έχει διαφορετική άποψη για τον άλλο. Οι συγγραφείς κάνουν χρήση των δύο τελεστών αλληλουχίας $\otimes$ και σύνοψης $\oplus$ για τον υπολογισμό των τιμών σύστασης εμπιστοσύνης $t(s, d)$ ενός κόμβου πηγή s για οποιοδήποτε άλλο κόμβο στόχο d του δικτύου. Με τη βοήθεια των δύο αυτών τελεστών, οι συγγραφείς τυποποιούν κάποιες από τις μετρικές υπολογισμού εμπιστοσύνης που υπάρχουν στη βιβλιογραφία, εντοπίζοντας με τον τρόπο αυτό τις ομοιότητες και τις διαφορές τους και καθιστούν ευκολότερη την υλοποίηση και αξιολόγηση των αλγορίθμων που τις χρησιμοποιούν. Οι τυποποιήσεις αυτές θα αναφερθούν κατά την αξιολόγηση των αντίστοιχων μοντέλων.

Οι Theodorakopoulos και Baras, μετά τις τυποποιήσεις των μετρικών των μοντέλων εμπιστοσύνης που μελέτησαν, κατέληξαν σε κάποιους κανόνες, τους οποίους πρέπει να ικανοποιούν γενικά οι μετρικές εμπιστοσύνης που χρησιμοποιούν τα μοντέλα εμπιστοσύνης. Σύμφωνα με τους κανόνες αυτούς, όταν μελετάται ένα μονοπάτι, ένας κόμβος A δεν μπορεί να αυξήσει την τιμή εμπιστοσύνης ενός κόμβου πηγή για έναν κόμβο στόχο περισσότερο από την τιμή εμπιστοσύνης που έχει ο κόμβος πηγή για τον ίδιο τον κόμβο A. Αυτό συμβαίνει γιατί οι τιμές εμπιστοσύνης ενός κόμβου για άλλους κόμβους δεν μπορούν να είναι περισσότερο έμπιστες από ότι είναι ο ίδιος ο κόμβος. Ακόμα και αν ο κόμβος A δώσει τη μέγιστη τιμή εμπιστοσύνης για τον κόμβο στόχο, ο κόμβος πηγή δεν μπορεί να αυξήσει την τιμή εμπιστοσύνης του περισσότερο από όσο εμπιστεύεται τον κόμβο A. Εάν πάλι σε ένα μονοπάτι ένας κόμβος πηγή γνωρίζει έναν κόμβο στόχο μόνο μέσω ενός κόμβου A, τότε ο κόμβος πηγή δεν μπορεί να εμπιστευτεί τον κόμβο στόχο περισσότερο από ότι τον εμπιστεύεται και του

συστήνει ο κόμβος A. Από αυτό προκύπτει ότι η εμπιστοσύνη κατά μήκος ενός μονοπατιού μπορεί είτε να μένει σταθερή, είτε να φθίνει, αλλά σε καμία περίπτωση να αυξάνει.

Στην περίπτωση τώρα που μελετώνται περισσότερα από ένα μονοπάτια, εάν συμφωνούν οι τιμές εμπιστοσύνης των διαφόρων μονοπατιών για έναν κόμβο, τότε η ακρίβεια της υπολογιζόμενης τιμής της εμπιστοσύνης που του αποδίδεται είναι πιο βέβαιη. Έτσι, εάν όλες οι συστάσεις που προέρχονται από τα μονοπάτια συγκλίνουν ότι ένας κόμβος είναι έμπιστος, τότε ο κόμβος αυτός δεν μπορεί παρά να είναι έμπιστος. Εάν όμως οι συστάσεις αυτές είναι αντικρουόμενες, τότε υπάρχουν δύο περιπτώσεις. Εάν η εμπιστοσύνη μπορεί να λάβει μόνο τις τιμές 0 και 1, δηλαδή ο υπό εξέταση κόμβος να είναι έμπιστος ή μη έμπιστος, το άθροισμα των αντικρουόμενων απόψεων θα μειώσει τη βεβαιότητα της ακρίβειας της υπολογιζόμενης τιμής εμπιστοσύνης. Εάν από την άλλη η εμπιστοσύνη μπορεί να λάβει τιμές μέσα σε ένα συνεχές διάστημα, οι αντικρουόμενες απόψεις θα θεωρηθούν ως απόψεις διαφορετικών πλευρών της συμπεριφοράς του ίδιου κόμβου και έτσι, η τιμή εμπιστοσύνης που θα υπολογιστεί θα προέρχεται από το μέσο όρο των συστάσεων πιθανόν βάσει των αντίστοιχων τιμών βεβαιότητας, ενώ η τιμή βεβαιότητας για την ακρίβεια της τιμής αυτής θα αυξηθεί.

4.2. Μοντέλα επιθέσεων

Ένα μοντέλο εμπιστοσύνης θεωρείται ότι επιτελεί επιτυχώς το στόχο του όταν εκπληρώνει το σκοπό για τον οποίο έχει δημιουργηθεί. Αυτό μπορεί να σημαίνει ότι βοηθάει τους συμμετέχοντες στο δίκτυο να πάρουν σωστές αποφάσεις για την εμπιστοσύνη που πρέπει να έχουν σε άλλους συμμετέχοντες, να πιστοποιεί τις ταυτότητες των συναλλασσόμενων, ή ακόμα και να εκμηδενίζει τις συναλλαγές μεταξύ συμμετεχόντων οι οποίες δυσαρεστούν κάποια από τις δύο πλευρές. Τα μοντέλα εμπιστοσύνης αποτελούν ελκυστικό στόχο για τους κακόβουλους κόμβους, εκείνους που θέλουν να εκμεταλλευτούν το σύστημα είτε προς όφελός τους επηρεάζοντας την ατομική τους φήμη, είτε για να βλάψουν το δίκτυο στοχεύοντας σε συγκεκριμένους κόμβους, ακόμα και επηρεάζοντας μεγάλα ποσοστά κόμβων αυτού. Μάλιστα, οι κόμβοι οι οποίοι σε ένα μοντέλο εμπιστοσύνης κατέχουν ένα συγκεκριμένο ίσως και κεντρικό ρόλο, αποτελούν από τους πιο μεγάλους στόχους επιθέσεων.

Υπάρχουν πολλά χαρακτηριστικά τα οποία καθορίζουν τις δυνατότητες ενός επιτιθέμενου κόμβου. Τέτοια χαρακτηριστικά περιλαμβάνουν τη θέση που έχει ο επιτιθέμενος κόμβος σε σχέση με το σύστημα, δηλαδή εάν είναι εσωτερικός ή εξωτερικός του συστήματος, εάν δρα ως μονάδα ή είναι μέλος κάποιας ομάδας και εάν οι επιθέσεις του είναι ενεργητικές, δηλαδή απαιτούν κάποια αλληλεπίδραση με το σύστημα, ή παθητικές [52]. Όταν οι κακόβουλοι κόμβοι είναι εσωτερικοί σε ένα σύστημα, έχουν νόμιμη είσοδο στο δίκτυο και μπορούν να συμμετάσχουν σε αυτό σύμφωνα με τις προϋποθέσεις που θέτει το σύστημα, ενώ εάν είναι εξωτερικοί τότε δεν έχουν εξουσιοδότηση για να βρίσκονται σε αυτό και ίσως να γίνουν αντιληπτοί. Όπως αναφέρουν οι Hoffman et al. [52], οι κακόβουλοι κόμβοι υποκινούνται από ιδιοτελείς ή δόλιους σκοπούς. Οι ιδιοτελείς επιτιθέμενοι κόμβοι προσπαθούν να παραποιήσουν τις τιμές φήμης για το δικό τους όφελος, ενώ οι δόλιοι επιτιθέμενοι προσπαθούν να υποβιβάσουν τη φήμη άλλων κόμβων ή να υπονομεύσουν τη διαθεσιμότητα του ίδιου του συστήματος. Μάλιστα, στην περίπτωση που οι κακόβουλοι κόμβοι δρουν σε ομάδες, είναι πιο δύσκολο να προσδιοριστούν και να αντιμετωπιστούν, μιας και εκδηλώνουν συνήθως πολύπλευρες συμπεριφορές, οι οποίες τους επιτρέπουν να καλύπτονται μερικώς μέσα στις ομάδες τους.

Μια από τις πιο συνηθισμένες επιθέσεις είναι η αυτό-προώθηση, κατά την οποία ένας κακόβουλος κόμβος δημιουργεί ψευδείς θετικές αναδράσεις για τον ίδιο, αυξάνοντας ψευδώς τη φήμη του. Χρησιμοποιώντας μια τέτοια επίθεση μπορούν οι κακόβουλοι κόμβοι να συνεργάζονται πραγματοποιώντας μεταξύ τους πολύ συχνά, αληθινά γεγονότα και παράγοντας αληθινές αλλά πολύ υψηλές αναδράσεις, βελτιώνοντας τις φήμες τους πολύ πιο γρήγορα από ότι οι υπόλοιποι κόμβοι του δικτύου [53]. Κάτι τέτοιο όμως εμπεριέχει πρώτα τη συνεργασία μεταξύ κακόβουλων κόμβων.

Μια άλλη επίθεση, η οποία περιλαμβάνει τη διάδοση ψευδών συστάσεων, είναι η επίθεση κακολόγησης (bad mouthing) [54]. Κατά την επίθεση αυτή ένας κακόβουλος κόμβος παρέχει ψευδείς συστάσεις για αξιόπιστους κόμβους στόχους, με σκοπό να μειώσει την τιμή εμπιστοσύνης που οι υπόλοιποι κόμβοι έχουν για τους κόμβους στόχους, αλλά παρέχει επιπλέον και ψευδείς καλές συστάσεις για άλλους κακόβουλους κόμβους, προκειμένου οι υπόλοιποι αξιόπιστοι κόμβοι να αυξήσουν την εμπιστοσύνη τους σε αυτούς.

Κατά την επίθεση αντιφατικής συμπεριφοράς [54] ένας κακόβουλος κόμβος επιδεικνύει αντιφατική συμπεριφορά σε ομάδες κόμβων, που έχει ως στόχο να πλήξει την εμπιστοσύνη που έχουν οι ομάδες αυτές μεταξύ τους στο να παρέχουν συστάσεις. Για το λόγο αυτό παρουσιάζει καλή συμπεριφορά σε μια ομάδα κόμβων, ενώ την ίδια στιγμή παρουσιάζει κακή συμπεριφορά σε κάποια άλλη ομάδα κόμβων. Όπως είναι φυσικό, η πρώτη ομάδα θα δώσει υψηλές τιμές εμπιστοσύνης στον κακόβουλο κόμβο, σε αντίθεση με τη δεύτερη ομάδα η οποία θα του εκχωρήσει χαμηλές τιμές. Όταν κάποια στιγμή οι κόμβοι της πρώτης ομάδας ζητήσουν συστάσεις από τη δεύτερη ομάδα αναφορικά με τον κακόβουλο κόμβο, οι συστάσεις που θα λάβουν δε θα συμφωνούν με τις τιμές εμπιστοσύνης που θα έχουν δώσει οι ίδιοι. Αυτό θα οδηγήσει τους κόμβους της πρώτης ομάδας στην πεποίθηση ότι οι συστάσεις που δίνουν οι κόμβοι της δεύτερης ομάδας δεν ανταποκρίνονται στην αλήθεια και έτσι θα μειώσουν την τιμή της εμπιστοσύνης που έχουν στις συστάσεις τους.

Η επίθεση on-off [54] συνοδεύεται επίσης από καλή και κακή συμπεριφορά των επιτιθέμενων κόμβων, αλλά αυτές εναλλάσσονται διαδοχικά κατά τη διάρκεια του χρόνου με στόχο να περάσουν απαρατήρητες οι κακόβουλές τους ενέργειες. Έτσι, όταν η επίθεση είναι σε κατάσταση on, ο κακόβουλος κόμβος πραγματοποιεί κακόβουλες ενέργειες σε κάποιο κόμβο στόχο, ενώ όταν η επίθεση είναι σε κατάσταση off, ο κακόβουλος κόμβος ενεργεί ως αξιόπιστος κόμβος και το δίκτυο λειτουργεί κανονικά [53]. Η επίθεση αυτή προσπαθεί να εκμεταλλευτεί το ρόλο που παίζουν οι ασύμβατες συμπεριφορές κατά τη διάρκεια του χρόνου στον υπολογισμό της τιμής της εμπιστοσύνης ενός κόμβου.

Ένα άλλο είδος επίθεσης είναι η επίθεση τύπου Sybil, κατά την οποία ένας κακόβουλος κόμβος μπορεί και παράγει μεγάλους αριθμούς ψευδών ταυτοτήτων και τις χρησιμοποιεί συγχρόνως εντός του δικτύου. Ελέγχοντας τις ταυτότητες αυτές, ο κακόβουλος κόμβος μπορεί στη συνέχεια να πραγματοποιεί κακόβουλες πράξεις, διαμοιράζοντας τις επιπτώσεις μεταξύ των ταυτοτήτων αυτών που σε διαφορετική περίπτωση θα έπρεπε να επωμιστεί ο ίδιος, ή ακόμα και να επηρεάζει ολόκληρη τη λειτουργία του δικτύου [55].

Η επίθεση αθώωσης στηρίζεται και αυτή στη δημιουργία ταυτοτήτων. Σε αυτή την επίθεση ο κακόβουλος κόμβος πραγματοποιεί τις κακόβουλες ενέργειες που επιθυμεί χωρίς να νοιάζεται για τις επιπτώσεις. Όταν η φήμη του μειωθεί κατά πολύ και άρα θα πρέπει να δεχτεί τις συνέπειες, αυτός επιλέγει να βγει από το δίκτυο και να αφήσει την παλιά του ταυτότητα και την παλιά του φήμη. Στη συνέχεια, δημιουργεί μια νέα ταυτότητα και εισέρχεται ξανά στο σύστημα με τη νέα του πια φήμη και διάθεση να ακολουθήσει την ίδια διαδικασία [52]. Όπως αναφέρουν οι Friedman και Resnick η επίθεση αυτή διευκολύνεται από τη διαθεσιμότητα φθηνών ψευδωνύμων και το γεγονός ότι η ανταποδοτικότητα είναι αρκετά δυσκολότερο να διατηρηθεί όταν οι ταυτότητες αλλάζουν εύκολα [57].

Μια άλλη επίθεση η οποία εμπεριέχει μια ή περισσότερες από τις παραπάνω επιθέσεις είναι η συνωμοσία. Οι επιθέσεις αυτές χρησιμοποιούν πολλές στρατηγικές, κατά τις οποίες για παράδειγμα οι επιτιθέμενοι κόμβοι αλλάζουν τη συμπεριφορά τους κατά τη διάρκεια του χρόνου ή υιοθετούν πολλές ταυτότητες [52], ενώ συγχρόνως οι επιτιθέμενοι κόμβοι σχηματίζουν συνωμοτικές ομάδες και βοηθούν ο ένας τον άλλο εκτελώντας πολυάριθμες ψευδείς συναλλαγές και δίνοντας έτσι καλές αξιολογήσεις μεταξύ τους [58]. Στη συνέχεια θα αποτιμήσουμε τα χαρακτηριστικά των μοντέλων που μελετήσαμε και θα δούμε πώς αντιμετωπίζουν τις παραπάνω επιθέσεις.

4.3. Αποτίμηση χαρακτηριστικών μοντέλων εμπιστοσύνης

4.3.1. Το μοντέλο του Marsh

Ο Marsh [5] μπόρεσε και τυποποίησε την έννοια της εμπιστοσύνης, λαμβάνοντας υπόψη πολλές από τις πλευρές της, σε σχέσεις μεταξύ πρακτόρων στον τομέα της κατανεμημένης τεχνητής νοημοσύνης. Ήταν από τους πρώτους που προσπάθησαν να δώσουν μια επίσημη αντιμετώπιση στην έννοια αυτή, η οποία να μπορεί να χρησιμοποιηθεί στην επιστήμη των υπολογιστών. Η προσέγγισή του περιλαμβάνει την προσθήκη του διακρινόμενου κινδύνου και της ωφέλειας μέσα σε μια συνεργατική σχέση. Η τυποποίηση αυτή είναι, όπως υποστηρίζει, σχετικά απλή και άρα εφαρμόζεται εύκολα με μικρές καθυστερήσεις. Σε περιπτώσεις με ελλιπή πληροφόρηση ή περιπτώσεις όπου απαιτούνται γρήγορες και ακριβείς αποφάσεις, η γνώση της εμπιστοσύνης μπορεί να βοηθήσει τους πράκτορες ενός δικτύου να λάβουν λογικές αποφάσεις συνεργασίας με άλλους πράκτορες. Όπως αναφέρει ο συγγραφέας, η κατανόηση της εμπιστοσύνης μπορεί να βοηθήσει τους πράκτορες με τεχνητή νοημοσύνη να αντιμετωπίσουν με στιβαρότητα την αβεβαιότητα και να τους δώσει ένα αναγνωρισμένο μέσο για τη διαχείριση της πολυπλοκότητας του περιβάλλοντος. Ο Marsh προσπάθησε να αναπτύξει μια μεγαλύτερη κατανόηση του τρόπου λειτουργίας της εμπιστοσύνης, έτσι ώστε να μπορέσει η έννοια να σχολιαστεί με ακριβή τρόπο και σημασία για να προσεγγίσει την αληθινή συμπεριφορά εμπιστοσύνης.

Το μοντέλο του Marsh έχει πολλούς περιορισμούς, όπως παρατηρούν άλλοι ερευνητές. Όπως αναφέρεται στο [59], η πολύ ισχυρή κοινωνιολογική βάση του μοντέλου το κάνει αρκετά πολύπλοκο και δεν μπορεί να υλοποιηθεί εύκολα. Επιπλέον, το μοντέλο δίνει μεγάλη βαρύτητα στις εμπειρίες των ίδιων των πρακτόρων, μην επιτρέποντάς τους να δημιουργήσουν συλλογικά ένα δίκτυο εμπιστοσύνης. Το μοντέλο δεν περιέχει κανένα κοινωνικό μηχανισμό και έτσι οι πράκτορες δεν μπορούν να δημιουργήσουν κάποια φήμη για τους υπόλοιπους πράκτορες [60]. Όπως αναφέρεται και στο [61], το μοντέλο του Marsh είναι πολύ θεωρητικό και εκτός από τις δυσκολίες στην υλοποίησή του, είναι ακατάλληλο για χρήση σε ηλεκτρονικές κοινωνίες. Οι Abdul-Rahman και Hailes [62] αναφέρουν τέλος ότι το μοντέλο περιέχει ένα μεγάλο αριθμό συνεχών μεταβλητών, οι οποίες προσπαθούν να αναπαραστήσουν αφηρημένες έννοιες, όπως ο κίνδυνος και η ικανότητα, χωρίς ιδιαίτερη επιτυχία, μιας και οι έννοιες αυτές είναι δύσκολο να αναπαρασταθούν μέσα από απλούς πραγματικούς αριθμούς. Έτσι το μοντέλο συνοδεύεται από ασάφεια, η οποία ενισχύεται όταν η μια μεταβλητή εφαρμόζεται σε άλλη.

Το μοντέλο του Marsh δεν λαμβάνει υπόψη την άποψη των πρακτόρων για τον εαυτό τους ή για τους άλλους, αλλά μόνο την εμπιστοσύνη που υπολογίζει ο κάθε πράκτορας για τους άλλους με βάση τις δικές του παρατηρήσεις. Άρα επιθέσεις αυτό-προώθησης και κακολόγησης δεν έχουν αποτέλεσμα. Επιπλέον, επειδή στο μοντέλο δε γίνεται χρήση τιμών εμπιστοσύνης μεταξύ ομάδων, μια επίθεση αντιφατικής συμπεριφοράς επίσης δεν θα αποδώσει. Από την άλλη, επειδή η εμπιστοσύνη υπολογίζεται με βάση τις παρατηρήσεις και το ιστορικό της συμπεριφοράς ενός πράκτορα, μια κακή συνεργασία θα αποτυπωθεί και η εμπιστοσύνη στον πράκτορα θα μειωθεί, κάνοντας σχετικά ανέφικτη μια επίθεση on-off. Επίσης, το μοντέλο δε διαθέτει μηχανισμό για έλεγχο ταυτοτήτων και άρα είναι ευάλωτο σε επιθέσεις τύπου Sybil και αθώωσης. Τέλος, επειδή κάθε πράκτορας έχει τις δικές του παρατηρήσεις και με βάση αυτές υπολογίζει την εμπιστοσύνη του σε άλλους πράκτορες, το μοντέλο είναι ανθεκτικό απέναντι σε επιθέσεις συνωμοσίας.

4.3.2. Το μοντέλο των Levien και Aiken

Οι Levien and Aiken [31] μελέτησαν τα πιστοποιητικά δημοσίου κλειδιού και εξέτασαν την ανθεκτικότητά τους σε διάφορες επιθέσεις, χρησιμοποιώντας μετρικές εμπιστοσύνης. Η μελέτη τους κατέληξε στην εισαγωγή μιας νέας μετρικής εμπιστοσύνης, η οποία βασίζεται στις μέγιστες ροές δικτύου ενός γραφήματος πιστοποιητικών. Όπως αναφέρουν, κάθε κόμβος διαθέτει μια χωρητικότητα (capacity) και κάθε κόμβος στόχος γίνεται αποδεκτός από τον κόμβο πηγή εάν η

μετρική ροής δικτύου βρίσκεται πάνω από ένα κατώφλι που έχει ορίσει ο κόμβος πηγή. Είναι προφανές ότι η ανθεκτικότητα της μετρικής εμπιστοσύνης απέναντι στις επιθέσεις εξαρτάται από τη διανομή των χωρητικοτήτων των κόμβων μέσα στο γράφημα [63]. Οι συγγραφείς υποστηρίζουν ότι αυξάνοντας τη χωρητικότητα των κόμβων που βρίσκονται κοντά σε έναν κόμβο πηγή, αυξάνεται και η ασφάλεια, αφού η μετρική εμπιστοσύνης περιορίζεται σε αυτή την περίπτωση μόνο από τον αριθμό των ακμών που καταλήγουν στον κόμβο στόχο.

Σύμφωνα με τους Theodorakopoulos και Baras [51], οι χωρητικότητες των κόμβων σε ένα γράφημα πιστοποιητικών, αντιπροσωπεύουν τα βάρη w των ακμών της τυποποίησής τους και παίρνουν τιμές στο διάστημα $[0,1]$. Στο γράφημα αυτό, κάθε κόμβος πηγή s έχει έναν αριθμό ακμών που ξεκινάνε από αυτόν. Η τιμή εμπιστοσύνης για έναν κόμβο στόχο d είναι το κλάσμα του αριθμού των ακμών οι οποίες καταλήγουν σε αυτόν. Σε αυτή την περίπτωση, ο τελεστής αλληλουχίας των Theodorakopoulos και Baras δίνει τον τύπο:

$$w(A,B) \otimes w(B,C) = min(w(A,B), w(B,C)) ,$$

ενώ ο τελεστής σύνοψης καταλήγει στον τύπο:

$$t^{p_1}(s, d) \oplus t^{p_2}(s, d) = t^{p_1}(s, d) + t^{p_2}(s, d) .$$

Όπως αναφέρουν οι Levien και Aiken, υπάρχουν επιθέσεις όπου οι κόμβοι οι οποίοι δέχονται την επίθεση έχουν επιλεγεί τυχαία και άλλες όπου οι κόμβοι επιλέγονται με βάση τη μέγιστη επιτυχία επίθεσης. Σε κάθε περίπτωση όμως, μια επιλεγμένη επίθεση είναι πιο αποτελεσματική από ότι μια τυχαία. Οι συγγραφείς μετράνε την επιτυχία μιας επίθεσης ως το κλάσμα των κλειδιών που δέχονται την απάτη. Είναι προφανές ότι αυτό το κλάσμα εξαρτάται από τις τιμές κατωφλίου $\theta(s)$ για κάθε τέτοιο κλειδί. Εάν ένα κλειδί είναι ορισμένο να δέχεται πολύ λίγους στόχους, μπορεί να απορρίψει τις περισσότερες απάτες. Για το λόγο αυτό, όλα τα κριτήρια επιτυχίας του μοντέλου υποθέτουν ότι υπάρχουν σταθερά ποσοστά αποδοχής στόχου. Με σταθερή τιμή κατωφλίου $\theta(s)$ για κάθε κλειδί, μπορούμε να μιλάμε για κλάσμα κλειδιών που αποδέχονται μια απάτη από μια συγκεκριμένη επίθεση. Οι συγγραφείς αποδεικνύουν ότι παρόλο που στην περίπτωση μιας επίθεσης κόμβου σε d κόμβους η επίθεση θα πετύχει ανεξαρτήτως της μετρικής που θα χρησιμοποιηθεί, η μετρική εμπιστοσύνης ροής δικτύου μπορεί να αντισταθεί σε μια επίθεση κόμβου σε $d - 1$ κόμβους. Ο αριθμός d αποτελεί τον αριθμό των ακμών που καταλήγουν σε έναν κόμβο. Ομοίως και στις επιθέσεις ακμής, αποδεικνύεται ότι η μετρική ροής δικτύου μπορεί να αντιμετωπίσει μια επίθεση ακμής που γίνεται σε λιγότερους από ad^2 κόμβους.

Τελικά, η μετρική ροής δικτύου που παρουσιάστηκε αποδεικνύεται πιο ανθεκτική απέναντι σε επιθέσεις ακμής, παρά κόμβου και αυτό γιατί τα κλειδιά που απαιτούνται για να επιτύχει η επίθεση είναι κατά πολύ πολλαπλάσια στην περίπτωση της πρώτης επίθεσης, αναλόγως την επιλογή της τιμής του μεγέθους a. Για το λόγο αυτό, σε κάθε υποδομή κλειδιού ο ιδιοκτήτης κάθε κλειδιού πρέπει να είναι πρόθυμος και ικανός να έχει άλλους χρήστες που να πιστοποιούν το κλειδί του, έτσι ώστε να μπορεί να αντιμετωπιστεί τυχόν επίθεση εναντίον του.

Όπως φαίνεται από το μοντέλο, ο αριθμός των ακμών που καταλήγουν σε κάθε κόμβο παραμένει σταθερός, κάτι που όμως δεν είναι αληθοφανές σε ένα δίκτυο όπου κόμβοι αποχωρούν και άλλοι κόμβοι εισέρχονται σε αυτό. Επιπλέον, όπως αναφέρθηκε, κάθε κόμβος έχει μια χωρητικότητα. Η τιμή της χωρητικότητας αυτής υπολογίζεται από τους υπόλοιπους κόμβους, μόνο εάν έχουν πλήρη γνώση όλου του δικτύου, κάτι που προφανώς πρέπει να ισχύει. Έτσι, οι ακμές του δικτύου είναι γνωστές σε όλους τους κόμβους και δεν μπορεί κάποιος να υποκριθεί την ύπαρξη ή την απουσία κάποιας ακμής.

Με τον τρόπο αυτό, το μοντέλο είναι ανθεκτικό σε επιθέσεις αυτό-προώθησης, δεδομένου ότι η αξιοπιστία των κλειδιών εξαρτάται μόνο από τα πιστοποιητικά εξουσιοδότησης που έχουν εκδοθεί από άλλους για τα κλειδιά αυτά. Το μοντέλο όμως είναι ανοικτό σε επιθέσεις κακολόγησης, δεδομένου ότι ένας κακόβουλος κόμβος μπορεί να εκδώσει ένα πιστοποιητικό δέσμευσης ή εξουσιοδότησης χωρίς να ανταποκρίνεται στην πραγματικότητα, ενώ είναι ευάλωτο και σε επιθέσεις on-off με κάποιον κόμβο να εκδίδει περιοδικά πιστοποιητικά για ψεύτικα κλειδιά ή για κλειδιά που δεν ανήκουν στους χρήστες που αναφέρεται μέσα στα πιστοποιητικά αυτά. Μπορεί αν ανακαλυφθεί από κάποιο χρήστη να ανακληθεί το πιστοποιητικό εξουσιοδότησης που του έχει εκδώσει, αλλά ο κακόβουλος χρήστης θα μπορέσει να ανακτήσει την εμπιστοσύνη των άλλων με την έκδοση επόμενων πιστοποιητικών που θα ανταποκρίνονται στην πραγματικότητα. Το μοντέλο όμως δεν επηρεάζεται από επιθέσεις αντιφατικής συμπεριφοράς, δεδομένου ότι εάν ένας κόμβος υπογράψει κάποιο ψεύτικο κλειδί, αυτό απλά θα αποτυπωθεί στο δίκτυο ως μια ακμή, αλλά δε θα επηρεάσει την αξιοπιστία των άλλων κόμβων. Από την άλλη, ενώ μπορούν να υπάρξουν επιθέσεις τύπου Sybil και αθώωσης, ο χρήστης που θα ανακαλυφθεί στην πρώτη περίπτωση θα ανακληθούν τα πιστοποιητικά που έχουν εκδοθεί για εκείνον και τα κλειδιά του, ενώ στη δεύτερη περίπτωση ο χρήστης που θα εισέλθει ως νέος στο δίκτυο δεν θα έχει καμία ακμή με κάποιον άλλο χρήστη. Τέλος, το μοντέλο είναι ανοικτό και σε επιθέσεις συνωμοσίας, με τους κακόβουλους κόμβους να εκδίδουν πιστοποιητικά ο ένας για τον άλλο και να πιστοποιούν την αξιοπιστία άλλων πιστοποιητικών από ψεύτικα κλειδιά. Όπως είπαμε και προηγουμένως, μπορούν οι χρήστες που ανακαλύπτουν την κακόβουλη συμπεριφορά να ανακαλέσουν τα πιστοποιητικά που έχουν εκδώσει για τους χρήστες αυτούς, αλλά το σύστημα δεν διαθέτει κάποιο είδος ιστορικότητας που να αποτυπώνει την κακόβουλη συμπεριφορά των χρηστών. Έτσι οι χρήστες που εκτελούν τις επιθέσεις είναι σε θέση μετά να αποκτήσουν ξανά τα πιστοποιητικά που έχασαν.

4.3.3. Το μοντέλο PGP (Pretty Good Privacy)

Στο PGP [33] γίνεται ρητός διαχωρισμός μεταξύ της εγκυρότητας ενός δημοσίου κλειδιού και του επιπέδου εμπιστοσύνης που του έχει εκχωρηθεί. Ενώ το επίπεδο εμπιστοσύνης ενός κλειδιού εκχωρείται από το χρήστη, η εγκυρότητά του διαπιστώνεται ανάλογα με τα επίπεδα εμπιστοσύνης που έχουν τα κλειδιά που το υπογράφουν. Το PGP εκμεταλλεύεται την αυθεντικότητα των πιστοποιητικών δημοσίου κλειδιού και την αξιοπιστία των κόμβων οι οποίοι παίζουν το ρόλο του πιστοποιητή κλειδιού και δημιουργεί δίκτυα εμπιστοσύνης μεταξύ των χρηστών του μέσω των ψηφιακών υπογραφών.

Παρόλο που το PGP είναι πολύ γρήγορο και προσέφερε πολλά για το σκοπό για τον οποίο υλοποιήθηκε, δεν αποτελεί κατάλληλο για εφαρμογές ηλεκτρονικού εμπορίου και για εφαρμογές που απαιτούν ισχυρή ταυτοποίηση χρηστών, καθώς η διεύθυνση ηλεκτρονικής αλληλογραφίας δεν μπορεί να αποτελέσει έναν ακριβή τρόπο προσδιορισμού της ταυτότητας ενός χρήστη, ενώ απουσιάζουν επίσημοι μηχανισμοί δημιουργίας, απόκτησης και διανομής πιστοποιητικών. Επιπλέον, το PGP δεν υποστηρίζει κάποια μέθοδο επαλήθευσης και ανάκλησης πιστοποιητικών. Οι διαδικασίες αυτές πραγματοποιούνται μόνο μέσω άμεσης επικοινωνίας των χρηστών, η οποία καθίσταται σχεδόν αδύνατη λόγω της μη ισχυρής ταυτοποίησής τους. Παρότι το πιστοποιητικό PGP είναι πολύ απλό, παρουσιάζει προβλήματα όταν πρόκειται να χρησιμοποιηθεί σε ανοιχτά κατανεμημένα περιβάλλοντα, αφού δεν παρουσιάζει ευελιξία σε περιβάλλοντα με κλιμακούμενες απαιτήσεις. Από την άλλη, το PGP κρατάει κρυφό το επίπεδο αξιοπιστίας που έχει κάθε χρήστης για καθένα από τα δημόσια κλειδιά που διαθέτει, επιτρέποντας στις πληροφορίες αυτές να αξιοποιούνται μόνο τοπικά και να μην προωθούνται στους χρήστες του υπόλοιπου δικτύου ώστε να εκχωρήσουν και αυτοί τιμές εμπιστοσύνης στα κλειδιά, τα οποία προέρχονται από άγνωστους για αυτούς χρήστες [49].

Το PGP είναι ανθεκτικό σε επιθέσεις αυτό-προώθησης, αφού κάθε κόμβος αποφασίζει ο ίδιος για το επίπεδο εμπιστοσύνης που θα δώσει σε ένα νέο κλειδί. Από την άλλη, μπορεί κάποιος κόμβος να υπογράψει το ψεύτικο δημόσιο κλειδί κάποιου άλλου κόμβου και να το συστήσει ως αυθεντικό σε κάποιον που τον εμπιστεύεται, πραγματοποιώντας έτσι μια επίθεση

κακολόγησης. Αυτό θα αποτελούσε και επίθεση συνωμοσίας, μιας και για τον ανυποψίαστο κόμβο ο τρίτος κόμβος θα θεωρείτο αξιόπιστος και θα μπορούσε να τον προτείνει και σε άλλους κόμβους. Επιπλέον, ένας κακόβουλος μπορεί να εκτελεί επιθέσεις on-off και να υπογράφει ανά διαστήματα ψευδή κλειδιά άλλων κακόβουλων κόμβων και να τα συστήνει σε άλλους κόμβους. Επειδή κάθε κόμβος έχει την άποψή του για τα κλειδιά που διαθέτει, μια αντιφατική συμπεριφορά κάποιου κακόβουλου κόμβου δεν θα έχει αποτέλεσμα. Τέλος, από τη στιγμή που το PGP δε διαθέτει έλεγχο ταυτοτήτων, οι κακόβουλοι κόμβοι μπορούν να πραγματοποιούν επιθέσεις τύπου Sybil και αθώωσης.

4.3.4. Το μοντέλο του Maurer

Το μοντέλο του Maurer [34] έχει ως στόχο την εγκατάσταση μιας έμμεσης σχέσης μεταξύ δύο οντοτήτων, οι οποίες δεν έχουν αλληλεπιδράσει στο παρελθόν, δημιουργώντας ένα ή περισσότερα μονοπάτια εμπιστοσύνης μεταξύ τους και η τιμή της εμπιστοσύνης υπολογίζεται μέσω αθροισμάτων κατά μήκος των μονοπατιών και συνδυασμών των τιμών αυτών. Το μοντέλο επιτρέπει τον προσδιορισμό αυθαίρετων εξαρτήσεων μεταξύ των δηλώσεων του συνόλου των πιθανών αρχικών απόψεων, ορίζοντας μια κατάλληλη τιμή πιθανότητας για τις δηλώσεις αυτές, ενώ επιπλέον προλαμβάνει εξαρτήσεις που οφείλονται σε επικαλυπτόμενα μονοπάτια πιστοποίησης.

Όπως αναφέρεται, οι παράμετροι βεβαιότητας θα μπορούσαν να χρησιμοποιηθούν στην περίπτωση των πιστοποιητικών, ώστε αυτά να λήγουν σταδιακά και όχι απότομα σε μια συγκεκριμένη μέρα. Για το λόγο αυτό, θα μπορούσαν οι παράμετροι βεβαιότητας να ελαττώνονται με την πάροδο του χρόνου. Βέβαια αποτελούν μειονεκτήματα για το μοντέλο το γεγονός ότι οι χρήστες πρέπει να εκχωρούν ακριβείς παραμέτρους βεβαιότητας σε όλες τις δηλώσεις που διαθέτουν, καθώς και η απουσία μηχανισμού επιβεβαίωσης και ανάκλησης πιστοποιητικών, μην επιτρέποντας στους συμμετέχοντες να λάβουν υπόψη τους τέτοια γεγονότα όταν λαμβάνουν αποφάσεις εμπιστοσύνης.

Το ντετερμινιστικό μοντέλο του Maurer είναι ελκυστικό, γιατί είναι απλό και ευέλικτο. Παρ' όλ' αυτά, όταν εφαρμόζεται σε πραγματικούς τύπους συστημάτων έχει κάποιους περιορισμούς. Όπως αναφέρεται στο [64], εκτός από το πρόβλημα της έλλειψης μηχανισμού ανάκλησης πιστοποιητικών που αναφέρει και ο Maurer, η χρήση της έννοιας της αυθεντικότητας ενός δημοσίου κλειδιού είναι λάθος, μιας και στην πράξη αυτό που απασχολεί τις οντότητες είναι η σύνδεση του δημόσιου κλειδιού και των πληροφοριών που περιέχει το πιστοποιητικό, οι πολιτικές χρήσης των κλειδιών, οι περιορισμοί, και όχι το τμήμα των πληροφοριών του πιστοποιητικού που αναφέρει τον ιδιοκτήτη του. Ένα άλλο μειονέκτημα που βρίσκουν οι Marchesini και Smith [64] είναι ότι οι συστάσεις του μοντέλου είναι απόλυτες, εννοώντας ότι εάν ένας χρήστης A έχει εκδώσει μία σύσταση σε έναν χρήστη B, τότε ο A αξιώνει τον B ως αξιόπιστο στο σύνολο των ενεργειών που είναι και ο ίδιος αξιόπιστος. Όπως αναφέρουν όμως, μπορεί κάποιος χρήστης να επιθυμεί να εκχωρήσει σε κάποιον άλλον το δικαίωμα να χρησιμοποιεί κάποια από τα χαρακτηριστικά του πιστοποιητικού του, έτσι ώστε να μπορεί να ενεργεί σαν να ήταν ο ίδιος ή μέλος της ομάδας του, κάτι που με το μοντέλο του Maurer δεν μπορεί να γίνει.

Οι Theodorakopoulos και Baras αναφέρουν ότι σύμφωνα με το μοντέλο τους [51], η μετρική του βάρους που όρισαν οι ίδιοι είναι στο μοντέλο του Maurer η βεβαιότητα της ισχύος μιας δήλωσης, η οποία αντιμετωπίζεται ως πιθανότητα και παίρνει πραγματικές τιμές εντός του διαστήματος $[0, 1]$. Ουσιαστικά, το βάρος $w(A, B)$ παίρνει τη μορφή της πιθανότητας ύπαρξης μιας κατευθυνόμενης ακμής (A, B). Έτσι, η τιμή της σύστασης εμπιστοσύνης ενός χρήστη s για έναν χρήστη d ισούται με την πιθανότητα ύπαρξης τουλάχιστον ενός κατευθυνόμενου μονοπατιού από τον πρώτο κόμβο στον δεύτερο. Εάν θεωρήσουμε ότι οι πιθανότητες των διαφορετικών ακμών είναι ανεξάρτητες μεταξύ τους, τότε για τρεις τυχαίους κόμβους A, B και C ενός δικτύου και τα βάρη w των δεσμών μεταξύ τους, ο τελεστής της αλληλουχίας των Theodorakopoulos και Baras δίνει τον απλό πολλαπλασιασμό:

$$w(A,B) \otimes w(B,C) = w(A,B)\ w(B,C)\ ,$$

ενώ ο τελεστής της σύνοψης δίνει τον τύπο:

$$t^{p_1}(s,\ d) \oplus t^{p_2}(s,\ d) = t^{p_1}(s,\ d) + t^{p_2}(s,\ d) - t^{p_1}(s,\ d)\ t^{p_2}(s,\ d)\ .$$

Αναφορικά με τις επιθέσεις, το μοντέλο βασίζεται σε συστάσεις αξιοπιστίας για τα δημόσια κλειδιά που δεν είναι γνωστά. Έτσι καμία οντότητα δεν μπορεί να δηλώσει την αυθεντικότητα του κλειδιού της και άρα δεν μπορεί να εκτελέσει επίθεση αυτό-προώθησης. Το μοντέλο χρησιμοποιεί μηχανισμό επιβεβαίωσης και αύξησης της βεβαιότητας της αυθεντικότητας ενός δημοσίου κλειδιού μέσα από το συνδυασμό πολλών διαφορετικών αλυσίδων πιστοποιητικών, καθώς και μηχανισμό συνδυασμού πολλών ανεξάρτητων συστάσεων για την απόκτηση ισχυρότερης σύστασης, κάνοντας χρήση της πιθανότητας μια δήλωση να είναι ορθή. Με τους μηχανισμούς αυτούς, το μοντέλο φαίνεται ανθεκτικό σε επιθέσεις κακολόγησης, αντιφατικής συμπεριφοράς και on-off. Ακόμα και στην περίπτωση που θα υπήρχε συνωμοσία μεταξύ κακόβουλων κόμβων για να διαδίδουν ψευδείς συστάσεις και πιστοποιητικά, το μοντέλο θα ήταν ανθεκτικό εάν οι κακόβουλοι αυτοί κόμβοι δεν ήταν πολλοί ώστε να επηρεάσουν όλα τα μονοπάτια μεταξύ των δύο οντοτήτων που θέλουν να επικοινωνήσουν. Τέλος, το μοντέλο δεν εξετάζει τη σύνδεση μεταξύ κλειδιών και ιδιοκτητών. Έτσι μπορεί να υπάρξει επίθεση Sybil, όπου κάποια οντότητα θα έχει πολλές ταυτότητες και πολλά κλειδιά στο ίδιο δίκτυο.

4.3.5. Το μοντέλο των Reiter και Stubblebine

Η μετρική που προτείνεται στο [35] παίρνει ως είσοδο ένα γράφημα, ένα εμπιστευμένο κλειδί πηγής και ένα κλειδί στόχο και επιστρέφει ένα ποσό για το οποίο έχει ασφαλιστεί η σύνδεση μεταξύ ονόματος και κλειδιού στόχου, υπολογίζοντας την ελάχιστη χωρητικότητα τομής του γραφήματος. Όπως αναφέρουν και οι συγγραφείς, η μετρική τους ικανοποιεί τους 8 κανόνες που έθεσαν. Έτσι, ο χρήστης δε χρειάζεται να εξακριβώσει τις συνδέσεις μεταξύ ονομάτων και κλειδιών για να κατασκευάσει το μοντέλο αυτό. Για την ακρίβεια, η μετρική δεν έχει ενσωματώσει κανέναν προσδιορισμό κλειδιού ή ανεξαρτησίας οντοτήτων για το σκοπό της πιστοποίησης και αντί να επιστρέφει κάποιο αφηρημένο μέγεθος, επιστρέφει κάτι απόλυτα αντιληπτό, ένα ποσό χρημάτων για το οποίο είναι ασφαλισμένη μια σύνδεση μεταξύ κλειδιού και ονόματος, ανεξαρτήτως των οντοτήτων που μπορεί να μην συμπεριφέρονται σωστά ή ποιών κλειδιών έχουν εκτεθεί - εκτός του εμπιστευμένου κλειδιού πηγής. Ακόμα και με ατελείς πληροφορίες, η μετρική των Reiter και Stubblebine είναι σε θέση να επιστρέψει ένα ποσό χρημάτων για το οποίο θα είναι ασφαλισμένη μια σύνδεση μεταξύ κλειδιού και ονόματος, παρόλο που το ποσό αυτό μπορεί να είναι τελικά μεγαλύτερο, και αυτό χρησιμοποιώντας οποιοδήποτε αλγόριθμο μέγιστης ροής [65]. Με τον τρόπο αυτό, ο χρήστης μπορεί να ζυγίζει το οικονομικό ρίσκο που συνοδεύεται από κάθε συναλλαγή και το ποσό των χρημάτων που θα μπορέσει να ανακτήσει εάν η σύνδεση στην οποία στηρίζεται η συναλλαγή αυτή είναι ψευδής. Έτσι, η έννοια της ασφάλισης επεκτείνεται φυσικά για την εφαρμογή αυτή, αφού είναι καλά ορισμένη σε νομικά θέματα και θέματα επιχειρήσεων.

Ο υπολογισμός της μετρικής θα μπορούσε να βελτιωθεί, επιτρέποντας στο χρήστη να περιορίσει τους κόμβους που περιέχονται στον υπολογισμό, βασιζόμενος στην εμπιστοσύνη που έχει στους ιδιοκτήτες των κλειδιών αυτών για το κατά πόσο θα πλήρωναν εάν βρίσκονταν υπόλογοι. Επιπλέον, η μετρική αυτή θα μπορούσε να χρησιμοποιήσει μονοπάτια τα οποία να ξεκινάνε από διαφορετικά εμπιστευμένα κλειδιά πηγής, τα οποία θα συνδυάζονταν σε μια «υπερ-πηγή» για το σκοπό ενός τέτοιου αλγορίθμου.

Οι Theodorakopoulos και Baras [51] τυποποίησαν την αριθμητική τιμή κάθε ακμής στο γράφημα του μοντέλου, αναφέροντας ότι αποτελεί το αριθμητικό βάρος *w* το οποίο αναφέρουν οι ίδιοι στο μοντέλο τους και το οποίο είναι προφανώς ένας αριθμός που ανήκει στο διάστημα $[0, \infty)$. Για το βάρος αυτό εφάρμοσαν τους τελεστές αλληλουχίας και σύνοψης καταλήγοντας αντίστοιχα στους παρακάτω τύπους:

$$w(A,B) \otimes w(B,C) = min(w(A,B),\ w(B,C)) \ ,$$

$$t^{p_1}(s,\ d) \oplus t^{p_2}(s,\ d) = t^{p_1}(s,\ d) + t^{p_2}(s,\ d) \ .$$

Η μετρική που προτείνουν οι Reiter και Stubblebine ξεπερνά κάποια εμπόδια που αντιμετωπίζουν άλλες μετρικές και αυτό γιατί τα αποτελέσματά της συσχετίζονται άμεσα με ποικίλες εμπορικές συναλλαγές, αλλά και γιατί θέτει ενώπιον των ευθυνών κάθε πιστοποιών για να θέσει και να αναλάβει τον κίνδυνο των πιστοποιητικών που δημιουργεί. Οι συγγραφείς οραματίζονται μάλιστα ένα ολοκληρωμένο σύστημα παρόχων ασφαλίσεων, καθένας από τους οποίους θα λαμβάνει τα έσοδά του από δύο είδη πελατών: τον δεσμευμένο και τον ασφαλισμένο. Ο πρώτος θα πληρώνει την ασφαλιστική εταιρεία για να παράξει ένα πιστοποιητικό για τη σύνδεση μεταξύ των χαρακτηριστικών και των κλειδιών του, ενώ ο δεύτερος θα πληρώνει την εταιρεία για να μπορεί να χρησιμοποιεί το πιστοποιητικό για την ασφάλιση μιας αυθεντικοποίησης. Στη συνέχεια ένας χρήστης, προκειμένου να πάρει την καλύτερη απόφαση, πρέπει να βρει ένα σύνολο μονοπατιών από πιστοποιητικά, των οποίων η ελάχιστη τομή να ικανοποιεί την απαιτούμενη ασφαλισμένη τιμή για τη σύνδεση μεταξύ ονόματος στόχου και κλειδιού και του οποίου το συνολικό κόστος να ελαχιστοποιείται ή να βρίσκεται κάτω από μια επιθυμητή τιμή.

Η παραπάνω μετρική αφήνει ανοιχτά κάποια προβλήματα, καθώς δεν αντιμετωπίζει τις περιπτώσεις όπου περιέχονται συγκρουόμενες αναφορές σχετικά με τον ιδιοκτήτη ενός δημοσίου κλειδιού, ούτε και εκείνη της ανάκλησης πιστοποιητικών. Αντιμετωπίζει όμως πολύ καλά τις επιθέσεις αυτό-προώθησης και κακολόγησης, αφού από τη μία δεν εκφέρει κάποιος άποψη για το δικό του κλειδί, ενώ από την άλλη καλείται να πληρώσει πρόστιμο όταν δίνει ψευδή στοιχεία για το κλειδί που ζητείται. Για τον ίδιο λόγο αντιμετωπίζονται και οι επιθέσεις αντιφατικής συμπεριφοράς, on-off και συνωμοσίας. Τέλος, για τις επιθέσεις τύπου Sybil δεν θα αποκόμιζε κάποιο συμφέρον εάν τις πραγματοποιούσε, όπως ισχύει και για τις επιθέσεις αθώωσης.

4.3.6. Το μοντέλο του Jøsang

Ο Jøsang [36] έδωσε μια αλγεβρική αντιμετώπιση στις μετρήσεις της εμπιστοσύνης και προσπάθησε να βρει το πώς αυτή μεταβάλλεται κατά μήκος μιας αλυσίδας συστάσεων. Χρησιμοποίησε ρητά τον παράγοντα της αμφιβολίας ως συστατικό της άποψης ενός πράκτορα και εφάρμοσε ουσιαστικά μια άλγεβρα για τον καθορισμό της εμπιστοσύνης, ως λύση στο πρόβλημα της πιστοποίησης των οντοτήτων σε ανοιχτά δίκτυα. Η άλγεβρα αυτή λαμβάνει υπόψη την εμπιστοσύνη στη σύνδεση μεταξύ ενός ιδιοκτήτη και του αυθεντικού κλειδιού του και την εμπιστοσύνη στην ικανότητά του να παρέχει μια σύσταση. Απαραίτητη προϋπόθεση είναι οι συστάσεις που παρέχονται να στηρίζονται μόνο σε προσωπικές εμπειρίες και παρατηρήσεις, έτσι ώστε να αποφεύγονται ανεπιθύμητες εξαρτήσεις μεταξύ τους. Κάτι τέτοιο δεν περιορίζει, όπως αναφέρει ο συγγραφέας, τα πιθανά μονοπάτια πιστοποίησης, αλλά απλώς επιβάλλει ένα συγκεκριμένο τρόπο δημιουργίας τους.

Οι Theodorakopoulos και Baras έδωσαν μια τυποποίηση του βάρους που όρισαν στο [51] για το μοντέλο του Jøsang [36]. Όπως αναφέρουν, η μετρική του βάρους στο μοντέλο [36] είναι η διατεταγμένη τριάδα πραγματικών θετικών αριθμών, οι οποίοι ανήκουν στο διάστημα

$[0,1]$ και οι οποίοι αναπαριστούν τη γνώμη που έχει ένας χρήστης για μια σχέση εμπιστοσύνης. Οι τρεις αριθμοί αυτοί είναι ο βαθμός πίστης b, δυσπιστίας d και αβεβαιότητας u, συστατικά τα οποία συνθέτουν το στοιχείο της γνώμης και των οποίων το άθροισμα δίνει τη μονάδα. Σε αυτή την περίπτωση, ο τελεστής της αλληλουχίας των Theodorakopoulos και Baras δίνει τον τύπο:

$$w(A,B) \otimes w(B,C) = (b_1, d_1, u_1) \otimes (b_2, d_2, u_2) = (b_1b_2, b_1d_2, d_1 + u_1 + b_1u_2) .$$

Αντίστοιχα, ο τελεστής της σύνοψης δίνει τον τύπο:

$$t^{p_1}(s,d) \oplus t^{p_2}(s,d) = \left(b_{sd}^{p1}, d_{sd}^{p1}, u_{sd}^{p1}\right) \oplus \left(b_{sd}^{p2}, d_{sd}^{p2}, u_{sd}^{p2}\right) = \left(\frac{b_{sd}^{p1}u_{sd}^{p2} + b_{sd}^{p2}u_{sd}^{p1}}{k}, \frac{d_{sd}^{p1}u_{sd}^{p2} + d_{sd}^{p2}u_{sd}^{p1}}{k}, \frac{u_{sd}^{p1}u_{sd}^{p2}}{k}, \right),$$

όπου $k = u_{sd}^{p1} + u_{sd}^{p2} - u_{sd}^{p1}u_{sd}^{p2}$.

Σύμφωνα με το μοντέλο, όταν παρέχονται συστάσεις από πολλά μονοπάτια, αυτές συνδυάζονται χρησιμοποιώντας τον τελεστή της συναίνεσης. Αυτό επιτρέπει στην τελική τιμή να διαμορφώνεται αυθαίρετα προς οποιαδήποτε τιμή, κάτι που σημαίνει ότι εάν υπάρξουν αρκετοί κακόβουλοι κόμβοι σε αντίστοιχα μονοπάτια συστάσεων, τότε η τελική τιμή σύστασης μπορεί να διαμορφωθεί σύμφωνα με τη βούλησή τους [63].

Όσον αφορά στις επιθέσεις που έχουμε αναφέρει, το μοντέλο του Jøsang θεωρεί ότι οι συστάσεις που παρέχουν οι πράκτορες είναι ανάλογες της εμπιστοσύνης που τους αποδίδεται για να κάνουν τη σύσταση. Μπορεί όμως κάποιος πράκτορας με μεγάλη εμπιστοσύνη για να παρέχει συστάσεις, να δώσει ψευδή σύσταση για το κλειδί κάποιου άλλου και να το παρουσιάσει ως μη αυθεντικό. Έτσι το μοντέλο είναι ευάλωτο σε επιθέσεις κακολόγησης. Επιπλέον, το μοντέλο είναι ανοικτό και σε επιθέσεις συνωμοσίας, δεδομένου ότι εάν κάποιοι κακόβουλοι πράκτορες συνωμοτήσουν μπορεί να πιστοποιεί ο ένας την αυθεντικότητα του κλειδιού του άλλου δίνοντας ψευδή σύσταση, ακόμα και να φτιάξουν αλυσίδες πιστοποίησης αν ο πρώτος κακόβουλος πράκτορας θεωρηθεί από κάποιον άλλο αξιόπιστος και ζητήσει τη σύστασή του. Βέβαια, η εμπιστοσύνη του κακόβουλου αυτού πράκτορα για να δίνει συστάσεις θα μειωθεί στη συνέχεια, αλλά μπορεί να επανέλθει με τον καιρό. Αλλά ούτε οι επιθέσεις τύπου Sybil και αθώωσης μπορούν να αποφευχθούν, δεδομένου ότι δεν αναφέρεται ότι υπάρχει τρόπος πιστοποίησης των ταυτοτήτων των πρακτόρων κατά την είσοδό τους στο δίκτυο. Έτσι μπορεί να υπάρχει κάποιος πράκτορας που να εμφανίζεται με πολλές ταυτότητες και κλειδιά μέσα στο δίκτυο, καθώς και κάποιος ο οποίος να φεύγει από το δίκτυο όταν μειωθεί πολύ η εμπιστοσύνη που του έχουν οι άλλοι πράκτορες στο να παρέχει συστάσεις και να επιστρέψει με νέα ταυτότητα και κλειδιά. Με το συνδυασμό μιας επίθεσης Sybil κάποιος κακόβουλος πράκτορας θα είναι σε θέση να πραγματοποιήσει και επίθεση αυτό-προώθησης, χρησιμοποιώντας τη μια του ταυτότητα για να συστήσει το κλειδί της άλλης του ταυτότητας. Έτσι μπορούμε να πούμε ότι είναι ευάλωτο το μοντέλο και σε μια τέτοια επίθεση. Συγχρόνως, κάποιος κακόβουλος πράκτορας μπορεί να εμφανίζει περιοδικά κακόβουλη συμπεριφορά έτσι ώστε να θεωρείται αξιόπιστος από κάποιους πράκτορες, οι οποίοι θα συνεχίζουν να ζητάνε τις συστάσεις του. Όσο για τις επιθέσεις αντιφατικής συμπεριφοράς, το μοντέλο εμφανίζεται ισχυρό, μιας και κάθε πράκτορας έχει την προσωπική του άποψη για την αξιοπιστία κάθε πράκτορα να παρέχει συστάσεις και δεν επηρεάζεται από απόψεις άλλων πρακτόρων.

4.3.7. Το μοντέλο eBay

Όπως αναφέρει και ο Dellarocas [67], η εμπορική επιτυχία των online ηλεκτρονικών αγορών είναι να έχουν επιτελέσει τον κύριο στόχο τους, να έχουν δηλαδή δημιουργήσει αρκετή εμπιστοσύνη μεταξύ των αγοραστών, έτσι ώστε να τους πείσουν να υποθέτουν τον κίνδυνο της συναλλαγής με παντελώς ξένους χρήστες. Το eBay [37] αποτελεί, όπως έχουν αποδείξει τα εκατομμύρια των χρηστών του, μια τέτοια αγορά και αυτό οφείλεται κατά πολύ στο σύστημα διαχείρισης φήμης που διαθέτει. Όπως αποδεικνύεται στο [68], το σύστημα φήμης που χρησιμοποιεί το eBay ενθαρρύνει τις συναλλαγές παρόλη την ύπαρξη αρνητικών συναλλαγών.

Εκτός από τα πολλά θετικά που προσφέρει, όπως τη μεγάλη ευκολία της αγοράς από το σπίτι, την εύρεση αντικειμένων που δεν πωλούνται πια ή τις καλύτερες τιμές που μπορεί να έχουν τα προϊόντα, έχει και κάποια μειονεκτήματα. Η διαδικασία της διαχείρισης των βαθμολογιών κάθε χρήστη, αντιμετωπίζει τη φήμη καθενός από αυτούς ως μια γενική ιδιότητα και της δίνει μια τιμή που δεν εξαρτάται και δεν εξηγεί το περιεχόμενό της. Υπάρχουν επίσης και οι κακόβουλοι χρήστες, οι οποίοι βαθμολογούν αρνητικά χρήστες με τους οποίους δεν είχαν κανένα πρόβλημα στη συναλλαγή τους. Σε αυτές τις περιπτώσεις το κεντρικό σύστημα της εφαρμογής αναλαμβάνει να διερευνήσει τις κατηγορίες και να βρει λύση, χωρίς να αποτρέπει τέτοια φαινόμενα επιθέσεων κακολόγησης. Από την άλλη όμως, δεδομένου ότι διατηρείται το ιστορικό των αξιολογήσεων, μπορεί να εντοπιστεί από χρήστες η κακόβουλη συμπεριφορά και να αποφευχθεί τυχόν συναλλαγή με έναν τέτοιο χρήστη. Σε κάθε περίπτωση, ο μόνος τρόπος για να μειωθεί ο αντίκτυπος μιας τέτοιας ενέργειας είναι η ύπαρξη πολλών θετικών βαθμολογιών, οι οποίες θα υπερκαλύψουν τελικά τη ζημία των αρνητικών και θα αυξήσουν την αξιοπιστία του χρήστη. Από την άλλη, πολλοί χρήστες αποφεύγουν να δώσουν μια αρνητική βαθμολογία σε κάποιο χρήστη, ακόμα και αν είναι βαθύτατα δυσαρεστημένοι από το αποτέλεσμα της συναλλαγής τους και αυτό γιατί φοβούνται τον κίνδυνο αντιποίνων, κάτι που θα ήταν εντελώς άδικο. Για το λόγο αυτό προτιμούν να μη δώσουν καμία βαθμολογία [69].

Υπάρχουν βέβαια και περιπτώσεις συνεργαζόμενων αναξιόπιστων χρηστών, οι οποίοι δίνουν ο ένας στον άλλο θετικές βαθμολογίες έτσι ώστε να αυξήσουν τη συνολική θετική τους ανάδραση και να εμφανίζονται πιο δημοφιλείς στους υπόλοιπους χρήστες. Επειδή όμως μια βαθμολογία μπορεί να δοθεί μόνο μετά από την ολοκλήρωση μιας συναλλαγής, ακόμα και αν η συναλλαγή αυτή γίνει για μικρής αξίας αντικείμενα, ο πωλητής θα πρέπει να πληρώσει ένα αντίτιμο για να μπορέσει αρχικά να διαφημίσει το προϊόν του. Έτσι, οι ψευδείς θετικές βαθμολογήσεις μεταξύ κακόβουλων συνεργαζόμενων χρηστών μπορούν μεν να υπάρξουν, αλλά γίνονται πολλές φορές ασύμφορες. Θεωρούμε όμως ότι το μοντέλο είναι ευάλωτο σε επιθέσεις συνωμοσίας. Άλλοι πάλι κακόβουλοι χρήστες μπορούν να εκβιάσουν και να αποσπάσουν θετικές βαθμολογίες από χρήστες, απειλώντας τους με αρνητική βαθμολόγηση [70], ενώ άλλοι εγκαταλείπουν την παλιά τους ταυτότητα όταν αυτή συγκεντρώσει αρνητική φήμη και δημιουργούν νέα ταυτότητα, η οποία όμως μπορεί να μην έχει αρνητική φήμη, δεν έχει όμως και θετική. Το σύστημα eBay προσπαθεί να αντιμετωπίσει τέτοια φαινόμενα με την απαίτησή του να δίνονται κάποιες προσωπικές πληροφορίες κατά την εγγραφή του νέου χρήστη, όπως ο αριθμός της πιστωτικής του κάρτας. Έτσι μπορεί να εντοπίσει την πραγματική ταυτότητα του κάθε χρήστη και να αντιμετωπίσει επιθέσεις αθώωσης. Η αναγκαία δήλωση προσωπικών πληροφοριών κατά την εγγραφή ενός νέου χρήστη αποτρέπει και τις επιθέσεις τύπου Sybil. Αυτό που είναι προφανές είναι ότι κανένας χρήστης δεν μπορεί να αλλάξει τη φήμη του με σκοπό να αυτό-προωθηθεί.

Επιπλέον, το eBay δεν φαίνεται ικανό να αντιμετωπίσει επιθέσεις τύπου karma suicide. Σύμφωνα με τις επιθέσεις αυτές, ένας κακόβουλος κόμβος πραγματοποιεί για αρκετό διάστημα συναλλαγές μικρής χρηματικής αξίας με άλλους χρήστες και επιδεικνύει καλή συμπεριφορά, οπότε και συγκεντρώνει μεγάλα ποσοστά θετικής ανάδρασης. Τελικά, θυσιάζει όλη τη θετική του βαθμολογία και εκδηλώνει την κακή του συμπεριφορά, κλέβοντας σε μια και μόνη συναλλαγή υψηλής όμως χρηματικής αξίας. Επίσης, οι επιθέσεις αντιφατικής συμπεριφοράς φαίνεται να είναι άλλο ένα πρόβλημα για το σύστημα eBay. Ένας κακόβουλος χρήστης μπορεί να έχει αρνητική συμπεριφορά απέναντι σε κάποιους και θετική απέναντι σε κάποιους άλλους, δηλαδή σε άλλους να στέλνει προϊόντα σε καλή κατάσταση και σε άλλους σε κακή. Σε κάποια επόμενη συναλλαγή και αφού βέβαια οι αγοραστές θα έχουν φροντίσει να αξιολογήσουν τον κακόβουλο

χρήστη, η αξιοπιστία των αξιολογήσεων αυτών είναι πιθανό να αμφισβητηθούν από χρήστες που έχουν διαφορετική άποψη για τον κακόβουλο χρήστη, αμφισβητώντας έτσι και τη φήμη των ανυποψίαστων χρηστών που έκαναν τις αξιολογήσεις. Δεδομένου όμως ότι οι συναλλαγές που γίνονται καθημερινά στο eBay είναι χιλιάδες, είναι πιθανό μια τέτοια επίθεση να περάσει απαρατήρητη από τους πολυάσχολους χρήστες. Τέλος, ένας κακόβουλος χρήστης μπορεί να παρουσιάζει περιοδικά κακόβουλη συμπεριφορά, εμφανίζοντας την καλή πλευρά του σε πολλές μικρές συναλλαγές και αυξάνοντας τη φήμη του και την κακόβουλη πλευρά του σε μεγάλες συναλλαγές. Κάτι τέτοιο βέβαια θα μειώσει τη φήμη του, την οποία θα μπορέσει να αυξήσει με αξιολογήσεις από καλές συναλλαγές.

4.3.8. Το μοντέλο των Sherwood et al.

Όπως αναφέρεται και στο [40], οι χρήστες του συστήματος NICE αποθηκεύουν μόνο πληροφορίες φήμης που μπορούν ρητά να χρησιμοποιήσουν για το δικό τους συμφέρον. Οι δύο αλγόριθμοι που παρουσιάστηκαν είναι αποτελεσματικοί, δεδομένου ότι όλες οι ακμές του γραφήματος χρησιμοποιούνται μόνο μια φορά, ενώ οι τιμές εμπιστοσύνης που υπολογίζονται περιορίζονται αριθμητικά από την ελάχιστη τιμή εμπιστοσύνης που υπάρχει στο μονοπάτι. Βέβαια, πριν εφαρμοστούν οι αλγόριθμοι αυτοί, πρέπει πρώτα το γράφημα να έχει κατασκευαστεί με κλιμακούμενο τρόπο και στις τιμές των ακμών να έχουν αποδοθεί οι τιμές των cookies. Έτσι, επιτρέπεται στους εκάστοτε χρήστες να υπολογίζουν τοπικές τιμές εμπιστοσύνης για άλλους χρήστες τις οποίες δεν διέθεταν πριν, χρησιμοποιώντας τον αλγόριθμο της επιλογής τους, υλοποιώντας με αυτό τον τρόπο ένα πλήθος διαφορετικών πολιτικών και ανακαλύπτοντας τελικά με μεγάλη αποτελεσματικότητα τους μη συνεργατικούς χρήστες του συστήματος.

Οι συγγραφείς αποδεικνύουν ότι οι αλγόριθμοί τους λειτουργούν καλά, ακόμα και με περιορισμένο αποθηκευτικό χώρο, επεξεργαστική ικανότητα και εύρος ζώνης σε κάθε κόμβο και μπορούν να χρησιμοποιηθούν για την αποτελεσματική υλοποίηση μεγάλων κατανεμημένων εφαρμογών, χωρίς τη συνδρομή άλλων αρχών στο σύστημα. Επιπλέον, αποδεικνύουν ότι οι χρήστες οδηγούνται στη δημιουργία συνεργατικών ομάδων, ακόμα και σε μεγάλα συστήματα όπου οι περισσότεροι χρήστες είναι κακόβουλοι, ασχέτως από τον αριθμό των θετικών ή αρνητικών cookies που αποθηκεύουν οι καλοί χρήστες, αρκεί οι χρήστες να επιλέγουν τυχαία άλλους χρήστες για να συναλλαχθούν.

Το σχήμα κατανεμημένης εξαγωγής τιμών εμπιστοσύνης έχει αρκετές επιθυμητές ιδιότητες. Όπως είπαμε, όταν ένας κόμβος A θέλει να χρησιμοποιήσει τους πόρους του κόμβου B ψάχνει να βρει τα cookies του μέσω των κόμβων που εμπιστεύεται. Οι γειτονικοί όμως αυτοί κόμβοι προωθούν αιτήματα άλλων κόμβων μόνο εφόσον τους εμπιστεύονται, αποφεύγοντας έτσι επιθέσεις άρνησης εξυπηρέτησης που μπορεί να επιχειρήσει κάποιος κακόβουλος κόμβος, ζητώντας επανειλημμένα από τους γειτονικούς του κόμβους να του βρουν δικά του cookies. Επιπλέον, παρέχεται κίνητρο στο σύστημα να αποθηκεύονται τα cookies, μιας και κάθε κόμβος αποθηκεύει και χρησιμοποιεί εκείνα τα cookies που είναι προς το δικό του συμφέρον, ενώ αποφεύγει να προωθεί μηνύματα από κόμβους που δεν εμπιστεύεται. Τέλος, το σύστημα έχει κατανεμημένη αποθήκευση του αρχείου συναλλαγών και εάν δύο κόμβοι διεξάγουν ένα μεγάλο αριθμό πλαστών συναλλαγών, αυτοί είναι οι μόνοι που μπορούν να επιλέξουν να διατηρήσουν την τελικά διαμορφούμενη κατάσταση. Εάν όμως η αποθήκευση των συναλλαγών γινόταν κεντρικά για όλους τους κόμβους, τότε μια ανάλογη επίθεση άρνησης εξυπηρέτησης θα μπορούσε να υπερχειλίσει το αρχείο συναλλαγών με πλαστές συναλλαγές.

Οι Theodorakopoulos και Baras [51] τυποποίησαν σύμφωνα με το μοντέλο τους τα cookies, τα οποία αποτελούν τα τυποποιημένα βάρη w όπως αναφέρουν, και κατασκεύασαν με αυτά ένα κατευθυνόμενο γράφημα. Τα βάρη αυτά παίρνουν τιμές εντός του διαστήματος $[0, 1]$ και για τον πρώτο αλγόριθμο του ισχυρότερου μονοπατιού, ο τελεστής αλληλουχίας των Theodorakopoulos και Baras δίνει τον παρακάτω τύπο:

$$w(A,B) \otimes w(B,C) = min(w(A,B),\ w(B,C)) \ ,$$

ο οποίος είναι ίδιος με εκείνον του μοντέλου [31], ενώ ο τελεστής σύνοψης καταλήγει αντίστοιχα στον τύπο:

$$t^{p_1}(s,\ d) \oplus t^{p_2}(s,\ d) = max(t^{p_1}(s,\ d),\ t^{p_2}(s,\ d)) \ .$$

Στην περίπτωση του δεύτερου αλγορίθμου, του σταθμισμένου αθροίσματος των ισχυρότερων ασύνδετων μονοπατιών, ο τελεστής αλληλουχίας δίνει τον ίδιο τύπο με αυτόν του πρώτου αλγορίθμου, ενώ ο τελεστής σύνοψης δίνει τον τύπο:

$$t^{p_1}(s,\ d) \oplus t^{p_2}(s,\ d) = \frac{w(e_1^{p_1})}{w(e_1^{p_1})+w(e_1^{p_2})} t^{p_1}(s,\ d) + \frac{w(e_1^{p_2})}{w(e_1^{p_1})+w(e_1^{p_2})} t^{p_2}(s,\ d) \ ,$$

δηλαδή ένα σταθμισμένο άθροισμα μονοπατιών, όπου τα βάρη είναι εκείνα των πρώτων ακμών κάθε μονοπατιού, με τη διαφορά ότι τα μονοπάτια πρέπει να είναι ασύνδετα.

Όσων αφορά στις επιθέσεις που μπορεί το μοντέλο να αντιμετωπίσει, η χρήση των cookies δεν επιτρέπει σε κάποιον κόμβο να κάνει επίθεση αυτό-προώθησης. Όταν γίνεται μια συναλλαγή, μόνο ο κόμβος που τη ζήτησε μπορεί να την αξιολογήσει. Βέβαια μπορεί να δηλώσει ψευδώς ότι η ποιότητά της ήταν κακή και άρα να κακολογήσει τον άλλο κόμβο. Από την άλλη, μια επίθεση αντιφατικής συμπεριφοράς δεν μπορεί να επηρεάσει τη φήμη άλλων κόμβων, ενώ μια επίθεση on-off μπορεί να συμβεί προσθέτοντας όμως αρνητικά cookies στην ταυτότητά του, τόσα ώστε μπορεί να σταματήσει να θεωρείται αξιόπιστος και να μην μπορεί πλέον να πραγματοποιήσει συναλλαγές. Το NICE δυστυχώς δεν αποκλείει την περίπτωση κάποιος κόμβος να έχει πολλές ταυτότητες και να τις χρησιμοποιεί συγχρόνως, άρα δεν μπορεί να προφυλαχθεί από την επίθεση τύπου Sybil, αλλά επειδή οι συναλλαγές του στηρίζονται στα θετικά cookies, είναι δύσκολο να έχουν όλες οι ταυτότητές του θετικά cookies. Από την άλλη μπορεί η μια ταυτότητά του να ενισχύει με θετικά cookies την άλλη του ταυτότητα. Είναι προφανές ότι κάποιος κόμβος μπορεί να γλιτώνει από τα αρνητικά cookies που έχει συγκεντρώσει φεύγοντας από το δίκτυο και ξαναμπαίνοντας χρησιμοποιώντας νέα ταυτότητα, κάνοντας έτσι μια επίθεση αθώωσης, ενώ είναι δυνατό κακόβουλοι κόμβοι να συνεργάζονται μεταξύ τους πραγματοποιώντας μικρές συναλλαγές και δίνοντας θετικά cookies ο ένας στον άλλο.

4.3.9. Το μοντέλο των Abdul-Rahman και Hailes

Οι Abdul-Rahman και Hailes [41] παρουσίασαν ένα κατανεμημένο μοντέλο εμπιστοσύνης, το οποίο βασίζεται σε ένα πρωτόκολλο από κανόνες και σχέσεις συστάσεων. Οι συστάσεις για άγνωστους πράκτορες διαδίδονται μέσω αιτημάτων και απαντήσεων που τις περιέχουν, χρησιμοποιώντας ένα δίκτυο έμπιστων πρακτόρων, όπου τα μηνύματα προωθούνται από τον αρχικό πράκτορα που αιτείται μιας σύστασης προς τους πράκτορες που εμπιστεύεται και εκείνοι με τη σειρά τους στους πράκτορες που εκείνοι εμπιστεύονται, μέχρι να βρεθεί η ζητούμενη σύσταση και να αποσταλεί μέσω του ίδιου μονοπατιού στον πράκτορα που έστειλε την αίτηση. Όπως αναφέρουν οι συγγραφείς, το μοντέλο τους είναι κατάλληλο για εφαρμογή σε σχέσεις εμπιστοσύνης οι οποίες είναι προσωρινές, βραχυπρόθεσμες και δεν είναι πολύ επίσημες, όπως είναι οι εμπορικές συναλλαγές και όχι σε όσες βασίζονται σε νομικά συμβόλαια.

Το μοντέλο αυτό καλύπτει τέσσερεις στόχους. Καταρχήν υιοθετεί μια αποκεντρωμένη προσέγγιση της διαχείρισης της εμπιστοσύνης, όπου κάθε πράκτορας αποφασίζει για τον εαυτό

του βασιζόμενος στις δικές του πολιτικές, κάτι που βέβαια απαιτεί υπευθυνότητα και εμπειρία. Επιπλέον, το μοντέλο χρησιμοποιεί κατηγορίες εμπιστοσύνης για να αναπαραστήσει τις διαφορετικές πλευρές της εμπιστοσύνης στις οποίες αναφέρεται, καθώς και διαφορετικές τιμές για τα διαφορετικά επίπεδα εμπιστοσύνης σε καθεμία από αυτές τις κατηγορίες. Από την άλλη, οι κατηγορίες αυτές και οι τιμές εμπιστοσύνης βοηθούν στο να γίνονται οι δηλώσεις εμπιστοσύνης που υπάρχουν μέσα στις συστάσεις πιο σαφείς, μειώνοντας τις όποιες αμφιβολίες στην έννοια τους. Τέλος, το πρωτόκολλο συστάσεων που προτείνεται διευκολύνει την ανταλλαγή πληροφοριών που σχετίζονται με την εμπιστοσύνη, οι οποίες είναι υποκειμενικές και κρύβουν πάντα κάποιους παράγοντες, οι οποίοι οδήγησαν στις αποφάσεις για την εμπιστοσύνη ή τη δυσπιστία απέναντι στο ζητούμενο πράκτορα. Η επιλογή όμως από τους πράκτορες των πρακτόρων που εμπιστεύονται να τους παράσχουν συστάσεις, μετριάζει την αβεβαιότητα που κρύβουν οι προαναφερόμενοι κρυφοί παράγοντες, ενώ οι επαναλαμβανόμενες συναλλαγές μεταξύ τους βοηθούν στην αξιολόγηση της ποιότητας των παρεχόμενων συστάσεων με αυξανόμενη και μεγαλύτερη ακρίβεια.

Οι Theodorakopoulos και Baras παρουσίασαν μια τυποποίηση [51] για το μοντέλο των Abdul-Rahman και Hailes [41] σύμφωνα με την οποία η μετρική του βάρους που όρισαν στην εργασία τους είναι οι συνιστώμενες τιμές εμπιστοσύνης των χρηστών, οι οποίες παίρνουν τις διακριτές τιμές $\{-1, 0, 1, 2, 3, 4\}$, αναλόγως εάν πρόκειται για δυσπιστία (-1), άγνοια (0) ή αυξανόμενα επίπεδα εμπιστοσύνης $(1, 2, 3, 4)$. Έτσι, για τρεις τυχαίους κόμβους A, B και C ενός δικτύου και τα βάρη w των δεσμών μεταξύ τους, ο τελεστής της αλληλουχίας των Theodorakopoulos και Baras δίνει τον τύπο:

$$w(A,B) \otimes w(B,C) = \frac{w(A,B)}{4} \frac{w(B,C)}{4} .$$

Αντίστοιχα, ο τελεστής της σύνοψης δίνει τον τύπο:

$$t^{p_1}(s, d) \oplus t^{p_2}(s, d) = \frac{1}{2} t^{p_1}(s, d) + \frac{1}{2} t^{p_2}(s, d) .$$

Το βασικό πρόβλημα του μοντέλου αυτού είναι ότι κάθε πράκτορας πρέπει να διατηρεί πολύπλοκες και μεγάλες δομές δεδομένων, οι οποίες να αναπαριστούν τη σφαιρική γνώση που έχει για το δίκτυο στο οποίο βρίσκεται. Σε πραγματικές συνθήκες, η διατήρηση και ενημέρωση τέτοιων βάσεων δεδομένων μπορεί να είναι κοπιαστική και να απαιτεί πολύ χρόνο, ενώ δεν είναι ξεκάθαρο το πώς οι πράκτορες αποκτούν αρχικά τις τιμές εμπιστοσύνης. Από την άλλη, δεν ξέρουμε πώς θα λειτουργήσει το μοντέλο όταν ο αριθμός των πρακτόρων μεγαλώσει αρκετά [61].

Όπως αναφέρεται και στο μοντέλο, εάν ο κόμβος αποστολέας ενός αιτήματος σύστασης λάβει περισσότερες από μία συστάσεις για τον κόμβο που ζήτησε μέσω διαφορετικών μονοπατιών, τότε η τελική τιμή εμπιστοσύνης του κόμβου υπολογίζεται ως η μέση τιμή των επιμέρους τιμών εμπιστοσύνης από κάθε μονοπάτι. Κάτι τέτοιο όμως θέτει κάποια προβλήματα όπως παρατηρούν οι Li και Singhal [72]. Το μοντέλο, όπως αναφέρουν, δεν λαμβάνει υπόψη τυχόν ψευδείς συστάσεις, αλλά θεωρεί ότι όταν ένας πράκτορας διαθέτει μια καλή τιμή εμπιστοσύνης για να κάνει συστάσεις, αυτός δίνει πάντα αξιόπιστες συστάσεις, κάτι που μπορεί να μην είναι αλήθεια. Άρα το μοντέλο είναι μη ανθεκτικό σε επιθέσεις κακολόγησης και συνωμοσίας. Έτσι, μπορεί κάποιος κακόβουλος πράκτορας να συνωμοτήσει με άλλους κακόβουλους και να στείλει ο ένας στον άλλο ψευδείς συστάσεις, χάνοντας το ποιος ξεκίνησε αρχικά την επίθεση και καταλήγοντας με μια ψευδή σύσταση. Επιπλέον, το μοντέλο δεν παρέχει κάποιο μηχανισμό για την παρακολούθηση και την επαναξιολόγηση της εμπιστοσύνης των πρακτόρων, αλλά κάτι τέτοιο εξαρτάται από τον κάθε πράκτορα που έκανε μια σύσταση για κάποιον άλλο του οποίου η τιμή εμπιστοσύνης άλλαξε. Ο πράκτορας αυτός αναλαμβάνει να

ενημερώσει με νέα σύσταση τους πράκτορες που είχαν ζητήσει την αρχική σύσταση εμπιστοσύνης. Το μοντέλο επιτρέπει την ύπαρξη επιθέσεων αντιφατικής συμπεριφοράς, ώστε να επηρεάζονται οι τιμές εμπιστοσύνης σύστασης μεταξύ των υπόλοιπων πρακτόρων, όπως και επιθέσεις on-off με κάποιο κακόβουλο πράκτορα να στέλνει περιοδικά ψευδείς συστάσεις για άλλους πράκτορες. Τέλος, απουσιάζουν από το μοντέλο μηχανισμοί ελέγχου ταυτοτήτων και άρα το μοντέλο είναι ανοιχτό σε επιθέσεις τύπου Sybil και αθώωσης, ενώ δεν μπορεί να επηρεαστεί από επιθέσεις αυτό-προώθησης αφού οι συστάσεις για κάποιο πράκτορα αποστέλλονται από άλλους πράκτορες του δικτύου.

4.3.10. Το μοντέλο EigenTrust

Στο [42] περιγράφηκε ένα σύστημα φήμης για τη μείωση του αριθμού των πλαστών αρχείων κατά το διαμοιρασμό αρχείων σε δίκτυα ομότιμων κόμβων, σύμφωνα με το οποίο σε κάθε ισότιμο κόμβο εκχωρείται μια μοναδική τιμή καθολικής εμπιστοσύνης, η οποία βασίζεται στο ιστορικό του κόμβου για τα αρχεία που «ανέβασε». Έτσι οι ισότιμοι κόμβοι χρησιμοποιούν τις τιμές εμπιστοσύνης, προκειμένου να αποφασίσουν από ποιο κόμβο θα «κατεβάσουν» το αρχείο που επιθυμούν, αναγνωρίζοντας τους κακόβουλους κόμβους και σταδιακά απομονώνοντάς τους από το υπόλοιπο δίκτυο.

Οι συγγραφείς επιλέγουν να κανονικοποιήσουν τις τοπικές τιμές εμπιστοσύνης για κάθε ισότιμο κόμβο, προκειμένου να καταλήξουν στις καθολικές τιμές εμπιστοσύνης. Όπως όμως αναφέρουν και οι ίδιοι, οι κανονικοποιημένες αυτές τιμές δεν κάνουν διάκριση μεταξύ ενός κόμβου με τον οποίο ο ισότιμος κόμβος i δεν είχε καμία συναλλαγή και ενός κόμβου με τον οποίο είχε κακή εμπειρία. Επιπλέον, οι τιμές αυτές είναι σχετικές, δηλαδή όταν λέμε ότι $c_{ij} = c_{ik}$ σημαίνει ότι οι κόμβοι j και k έχουν την ίδια φήμη για έναν ισότιμο κόμβο i αλλά δεν ξέρουμε εάν η φήμη αυτή είναι μεγάλη ή μικρή. Παρ' όλ' αυτά, οι κανονικοποιημένες αυτές τιμές δίνουν καλά αποτελέσματα και επιτρέπουν τους περαιτέρω υπολογισμούς, χωρίς να απαιτείται η κανονικοποίηση των καθολικών τιμών εμπιστοσύνης σε κάθε επανάληψη του αλγορίθμου.

Οι Theodorakopoulos και Baras χρησιμοποίησαν το μοντέλο τους [51] για να τυποποιήσουν τα βάρη που χρησιμοποιούνται στην περίπτωση του EigenTrust, δηλαδή τις τοπικές τιμές εμπιστοσύνης, οι οποίες παίρνουν πραγματικές τιμές εντός του διαστήματος $[0,1]$. Τα βάρη κανονικοποιούνται όπως έχουμε αναφέρει για κάθε κόμβο ξεχωριστά. Τελικά, με την εφαρμογή του τελεστή αλληλουχίας, προκύπτει ο παρακάτω απλός τύπος πολλαπλασιασμού για τρεις τυχαίους κόμβους A, B και C ενός δικτύου και τα βάρη w των δεσμών μεταξύ τους:

$$w(A,B) \otimes w(B,C) = w(A,B)\ w(B,C)\ .$$

Αντίστοιχα, η εφαρμογή του τελεστή σύνοψης καταλήγει στην παρακάτω απλή πρόσθεση που είναι ίδια με του μοντέλου [31]:

$$t^{p_1}(s,d) \oplus t^{p_2}(s,d) = t^{p_1}(s,d) + t^{p_2}(s,d)\ .$$

Όπως αναφέρεται στο [42], η ύπαρξη κόμβων στο δίκτυο οι οποίοι είναι γνωστό ότι είναι αξιόπιστοι, είναι πολύ σημαντική για τη σύγκληση του αλγορίθμου EigenTrust και για την αντιμετώπιση ομάδων κακόβουλων κόμβων. Για το λόγο αυτό είναι βασικής σημασίας η επιλογή των κόμβων αυτών ώστε να μην ανήκουν σε κάποια από τις ομάδες αυτές, κάτι που θα έθετε σε κίνδυνο την ποιότητα του αλγορίθμου. Έτσι το σύστημα πρέπει να επιλέξει πολύ λίγους τέτοιους κόμβους και πιθανότατα μόνο τους δημιουργούς του δικτύου. Στην περίπτωση όμως των

κατανεμημένων δικτύων, οι κόμβοι αυτοί παραμένουν ανώνυμοι στους υπόλοιπους κόμβους του δικτύου, εξασφαλίζοντας την ομαλή λειτουργία του συστήματος.

Ο αλγόριθμος εφαρμόζεται με επιτυχία και σε κατανεμημένα δίκτυα, μην επιβαρύνοντας σημαντικά τους κόμβους με τον υπολογισμό των καθολικών τιμών εμπιστοσύνης, μιας και οι αλληλεπιδράσεις ενός κόμβου με τους υπόλοιπους κόμβους του δικτύου είναι περιορισμένες. Αλλά και τα μηνύματα που ανταλλάσσονται μεταξύ των ισότιμων κόμβων είναι μικρά, μιας και είναι επίσης περιορισμένα τα σύνολα των κόμβων από τους οποίους ένας κόμβος έχει «κατεβάσει» αρχεία, αλλά και οι άλλοι κόμβοι έχουν «κατεβάσει» από αυτόν. Στις περιπτώσεις όπου οι κόμβοι ενός δικτύου είναι πολύ δραστήριοι, μπορεί να περιοριστεί ο αριθμός των τοπικών τιμών εμπιστοσύνης τους οποίους μπορεί να διαδώσει κάθε κόμβος.

Με τον αλγόριθμο του ασφαλούς EigenTrust, επιτυγχάνεται ανωνυμία των κόμβων, μιας και ένας διαχειριστής βαθμολογίας δεν μπορεί να βρει την ταυτότητα του κόμβου για τον οποίο υπολογίζει την τιμή εμπιστοσύνης, εμποδίζοντας έτσι τους κακόβουλους κόμβους να αυξήσουν τη φήμη άλλων κακόβουλων κόμβων. Επιπλέον, εξασφαλίζεται η τυχαιότητα αφού κανένας κόμβος δεν μπορεί να επιλέξει το σημείο του κατακερματισμένου διαστήματος στο οποίο θα βρίσκεται και άρα να υπολογίσει ο ίδιος την τιμή εμπιστοσύνης του αλλοιώνοντας την. Τέλος, χρησιμοποιείται ο πλεονασμός προκειμένου η τιμή εμπιστοσύνης ενός κόμβου να υπολογίζεται από πολλούς διαχειριστές. Οι διαχειριστές αυτοί αναπαριστούν διαστήματα συντεταγμένων αλλά χρησιμοποιώντας αρκετές πολυδιάστατες συναρτήσεις κατακερματισμού, τα διαστήματα αυτά είναι αντίστοιχα πολλά και ένας κόμβος αναπαρίσταται ως σημείο σε καθένα από αυτά.

Η απόδοση του ασφαλούς EigenTrust δοκιμάστηκε σε τέσσερεις διαφορετικές καταστάσεις για τον περιορισμό των μη αυθεντικών αρχείων σε ένα δίκτυο. Αρχικά, στην περίπτωση όπου κακόβουλοι κόμβοι προσπαθούν να «ανεβάσουν» μη αυθεντικά αρχεία και εκχωρούν υψηλές τιμές εμπιστοσύνης σε άλλους κακόβουλους κόμβους με τους οποίους έρχονται σε επαφή στο δίκτυο, οι κακόβουλοι κόμβοι πράγματι λαμβάνουν υψηλές τοπικές τιμές εμπιστοσύνης, αλλά μόνο περιστασιακά και από άλλους επίσης κακόβουλους κόμβους, δεδομένου ότι οι κόμβοι πρέπει να ανταλλάξουν πρώτα κάποιο αρχείο. Οι κόμβοι όμως αυτοί έχουν χαμηλή τιμή εμπιστοσύνης και άρα σπάνια επιλέγονται ως πηγή για κατέβασμα κάποιου αρχείου, ελαχιστοποιώντας έτσι τα μη αυθεντικά αρχεία στο δίκτυο. Τελικά παρατηρείται ότι μόνο το 10% των αρχείων που μεταφορτώνονται στο δίκτυο είναι μη αυθεντικά, και αυτό γιατί ενίοτε γίνονται λάθη και από τους καλούς κόμβους, οι οποίοι ξεχνούν να σβήσουν κάποιο μη αυθεντικό αρχείο από τους φακέλους τους ή δημιουργούν και μοιράζονται κάποιο άλλο κατεστραμμένο.

Στη συνέχεια, μελετάται η περίπτωση κατά την οποία οι κακόβουλοι κόμβοι γνωρίζονται από πριν μεταξύ τους και αποδίδουν ντετερμινιστικά υψηλές τοπικές τιμές εμπιστοσύνης. Με την ενεργοποίηση του EigenTrust, ακόμα και αν η πλειοψηφία των κόμβων είναι κακόβουλοι, η ύπαρξη ομάδων κακόβουλων κόμβων δεν μπορεί να αυξήσει αποτελεσματικά τις καθολικές τιμές εμπιστοσύνης των κόμβων αυτών. Οι κόμβοι αυτοί έχουν χαμηλές τιμές εμπιστοσύνης και άρα σπάνια επιλέγονται ως πηγή κάποιου αρχείου. Μάλιστα, η ύπαρξη κόμβων που είναι γνωστό ότι είναι αξιόπιστοι, μπορεί να διασπάσει τέτοιες ομάδες κόμβων. Έτσι η επίθεση κακολόγησης, παρόλο που μπορεί να συμβεί, δεν έχει αποτέλεσμα. Βέβαια, προς αυτή την κατεύθυνση βοηθάει και η κανονικοποίηση των καθολικών τιμών εμπιστοσύνης.

Επόμενη περίπτωση που εξετάζεται είναι εκείνη όπου κακόβουλοι κόμβοι προσπαθούν να λάβουν υψηλές τοπικές τιμές εμπιστοσύνης από καλούς κόμβους, παρέχοντάς τους αυθεντικά αρχεία σε κάποιες από τις φορές που επιλέγονται. Έτσι δεν τους εκχωρείται μηδενική τιμή εμπιστοσύνης από όλους τους κόμβους, αφού σε κάποιους παρέχουν αυθεντικά αρχεία, πετυχαίνουν υψηλότερες καθολικές τιμές εμπιστοσύνης και τελικά ανεβάζουν περισσότερα αρχεία, κάποια από τα οποία παραμένουν μη αυθεντικά. Τελικά όμως, όπως φαίνεται από τις προσομοιώσεις, όταν τα αυθεντικά αρχεία που ανεβάζουν οι κακόβουλοι κόμβοι είναι λιγότερα από το 50% των συνολικών αρχείων, χάνουν στο τέλος όλες τις υψηλές τοπικές τιμές εμπιστοσύνης που τους δίνουν οι άλλοι κόμβοι αφού παρέχουν περισσότερα μη αυθεντικά αρχεία, ενώ μακροχρόνια τα μη αυθεντικά αρχεία τους δικτύου είναι περιορισμένα. Έτσι αποτυγχάνει και η επίθεση on-off. Η επίθεση αντιφατικής συμπεριφοράς δεν βρίσκει εφαρμογή

στο μοντέλο EigenTrust, μιας και δεν επηρεάζεται η φήμη των κόμβων όταν η επίθεση λάβει χώρα.

Στην τελευταία περίπτωση μελετάται η επίδραση ύπαρξης ενός συνόλου κακόβουλων κόμβων, οι οποίοι παρέχουν μόνο αυθεντικά αρχεία και χρησιμοποιούν τις υψηλές τιμές εμπιστοσύνης που κερδίζουν, για να εκχωρήσουν επίσης υψηλές τιμές εμπιστοσύνης σε άλλο σύνολο κακόβουλων κόμβων, οι οποίοι παρέχουν μόνο μη αυθεντικά αρχεία. Όπως δείχνει η προσομοίωση, η περίπτωση αυτή πετυχαίνει να έχει την ίδια επίδραση σε ανέβασμα μη αυθεντικών αρχείων από τους κακόβουλους κόμβους του δεύτερου συνόλου, όπως και η δεύτερη περίπτωση που εξετάστηκε, απαιτώντας όμως το ανέβασμα πολύ λιγότερων αυθεντικών αρχείων από την πρώτη ομάδα κακόβουλων κόμβων. Έτσι μια συνωμοσία μπορεί να έχει αποτέλεσμα στη λειτουργία του δικτύου. Παρόλο όμως που οι κόμβοι της πρώτης αυτής ομάδας δεν μπορούν να ανακαλυφθούν ποτέ – αφού παρέχουν μόνο αυθεντικά αρχεία, το σύστημα EigenTrust αποδίδει καλύτερα από ένα σύστημα που δε διαθέτει επιλογή πηγής «κατεβάσματος» αρχείων με βάση την εμπιστοσύνη.

Το σύστημα EigenTrust αντιμετωπίζει τέλος αποτελεσματικά την επίθεση Sybil, κατά την οποία ένας κακόβουλος κόμβος εκκινεί χιλιάδες άλλους κόμβους στο δίκτυο. Κατά τη διάρκεια της επίθεσης, καθένας από τους κόμβους αυτούς αποστέλλει ένα μη αυθεντικό αρχείο όταν επιλέγεται από κάποιο κόμβο και στη συνέχεια φεύγει από το δίκτυο, ενώ τη θέση του παίρνει κάποιος άλλος επίσης κακόβουλος κόμβος. Δεδομένου ότι οι κακόβουλοι κόμβοι είναι τόσοι πολλοί, οι καλοί κόμβοι δεν έχουν καμία πιθανότητα να ανεβάσουν τη φήμη τους. Η επίθεση όμως αυτή αντιμετωπίζεται, βάζοντας ένα κόστος για την είσοδο ενός νέου κόμβου στο δίκτυο, όπως είναι η επίλυση ενός γρίφου, ο οποίος δεν μπορεί να επιλυθεί από έναν υπολογιστή, βάζοντας έτσι φρένο στη δημιουργία κόμβων. Από την άλλη όμως, ένας κόμβος μπορεί να αποστείλει ένα μη αυθεντικό αρχείο, να βγει από το δίκτυο και άρα να γλιτώσει τη χαμηλή τιμή εμπιστοσύνης και να ξαναμπεί στο δίκτυο με άλλη ταυτότητα. Εάν βέβαια πρόκειται για υπολογιστή, κάτι τέτοιο δεν μπορεί και πάλι να συμβεί.

4.3.11. Το μοντέλο Poblano

Οι Chen και Yeager [43] πρότειναν ένα κατανεμημένο μοντέλο εμπιστοσύνης για εφαρμογές σε JXTA για δίκτυα ομότιμων κόμβων, το Poblano. Το μοντέλο επιτρέπει στους κόμβους να δημιουργούν κατανεμημένα και προσωποποιημένα δίκτυα εμπιστοσύνης, ενώ αναπαριστά σχέσεις εμπιστοσύνης τόσο μεταξύ κόμβων, όσο και μεταξύ κόμβων και codats. Παρέχει πρωτόκολλα διάδοσης της εμπιστοσύνης και αλγορίθμους ενημέρωσής της και είναι χρήσιμο για την εκτέλεση μιας κατευθυνόμενης αναζήτησης φήμης και το σχεδιασμό ενός συστήματος συστάσεων για λόγους ασφαλείας [73]. Όπως αναφέρεται στο [74], η αποσύζευξη της αξιοπιστίας του περιεχομένου και των ιδιοτήτων του κόμβου, καθώς και η εξάρτηση της αξιοπιστίας του κόμβου από τη σχετικότητα ή την αξιοπιστία του παρεχόμενου περιεχομένου καθιστούν το Poblano ελκυστικό. Επίσης, διευκολύνει την αναζήτηση με βάση τη φήμη και την εμπιστοσύνη και παρέχει ένα ευρύ φάσμα εμπιστοσύνης βασισμένο στα πιστοποιητικά. Η διάδοση όμως και η ανανέωση της επεξεργασμένης βεβαιότητας οδηγεί σε μεγάλη κυκλοφορία στο δίκτυο.

Το βασικό μειονέκτημα του μοντέλου Poblano αποτελεί η μη διαφοροποίηση μεταξύ της ικανότητας των χρηστών να παρέχουν υπηρεσίες και της ικανότητάς τους να αξιολογούν παρόχους υπηρεσιών και άρα η χρήση ενός περιορισμένου μονοδιάστατου ορισμού για την εμπιστοσύνη [49]. Ο Grandison [75] αναφέρει ότι οι εξισώσεις που χρησιμοποιεί το μοντέλο Poblano για τον υπολογισμό και την ενημέρωση των τιμών της εμπιστοσύνης είναι απλές και αυθαίρετες, θέτοντας υπό αμφισβήτηση την ακρίβεια και τη γενική εφαρμογή της φόρμουλας. Επιπλέον, σημειώνει ότι το μοντέλο φαίνεται να έχει σχεδιαστεί για την επίλυση προβλημάτων ανεύρεσης και αξιολόγησης των αποτελεσμάτων και των πηγών τους σε κατανεμημένα δίκτυα. Τέλος, επισημαίνει ότι το μοντέλο μπορεί να αντιμετωπίζει τα ίδια προβλήματα κλειδιού που αντιμετωπίζουν τα πιστοποιητικά δημοσίου κλειδιού, ενώ δε διαθέτει καμία διευκόλυνση στον

ορισμό περιορισμών, κάτι που περιορίζει την χρησιμότητά του στα περιβάλλοντα ηλεκτρονικού εμπορίου.

Το μοντέλο Poblano είναι δεν ανθεκτικό σε επιθέσεις αυτό-προώθησης, μιας και η τιμή CodatConfidence που διαθέτει ένας πάροχος υπηρεσιών αποστέλλεται μέσω μονοπατιών από τον ίδιο τον πάροχο προς τον κόμβο πηγή που τη ζήτησε. Βέβαια, ο υπολογισμός της τιμής PeerConfidence για τον πάροχο βασίζεται στις εκτιμήσεις του codat από τον ομότιμο κόμβο που αιτήθηκε της υπηρεσίας, αλλά αυτό θα γίνει αφού ο κόμβος πηγή αποφασίσει να ζητήσει το codat. Επιπλέον, το μοντέλο είναι ευάλωτο και σε επιθέσεις κακολόγησης αφού κάποιος κακόβουλος κόμβος μπορεί να στείλει ένα ψευδές PeerConfidence ως ανάδραση για κάποιον κόμβο σε κάποιον ομότιμο ο οποίος έχει υψηλή τιμή PeerConfidence για τον κακόβουλο κόμβο. Το αποτέλεσμα θα είναι η τελική τιμή PeerConfidence του υπό επίθεση κόμβου να μειωθεί. Κάτι τέτοιο θα μπορούσε να γίνει και σε συνδυασμό με μια επίθεση on-off, με τον κακόβουλο κόμβο να εκδηλώνει κακόβουλη συμπεριφορά περιοδικά, ώστε να μην μειώσει την τιμή PeerConfidence που έχουν οι υπόλοιποι κόμβοι για αυτόν. Αλλά και επιθέσεις συνωμοσίας μπορούν να υπάρξουν με κακόβουλους κόμβους να μεσολαβούν σε μονοπάτια μεταξύ κόμβων πηγής και παρόχων, οι οποίοι θα μπορούν να αλλάζουν τις τιμές CodatConfidence που αποστέλλονται και αν έχουν υψηλές τιμές PeerConfidence, τότε οι αποφάσεις των κόμβων πηγής για τη λήψη τελικά των codat μπορεί να είναι αρνητικές. Το μοντέλο από την άλλη είναι ανθεκτικό σε επιθέσεις αντιφατικής συμπεριφοράς, αφού τέτοιες επιθέσεις δεν μπορούν να επηρεάσουν τις τιμές PeerConfidence που έχουν έμπιστοι κόμβοι μεταξύ τους. Τέλος, επιθέσεις τύπου Sybil και αθώωσης δεν μπορούν να υπάρξουν, μιας και το ασφαλές πλαίσιο του μοντέλου απαιτεί αυθεντικοποίηση και εξουσιοδότηση.

4.3.12. Το μοντέλο των Wang και Vassileva

Το μοντέλο που πρότειναν οι Wang και Vassileva [44] προορίζεται για χρήση σε δίκτυα ομότιμων κόμβων, σε εφαρμογές διαμοιρασμού αρχείων και βασίζεται στη χρήση Μπεϋζιανών δικτύων. Στα δίκτυα αυτά εφαρμόζεται ένα φαινόμενο που έχει παρατηρηθεί στις πραγματικές κοινωνίες. Σύμφωνα με αυτό, οι άνθρωποι τείνουν να αλληλεπιδρούν συχνότερα με ανθρώπους οι οποίοι ανήκουν στο μικρόκοσμό τους, παρά με ανθρώπους έξω από αυτόν. Έτσι οι ομότιμοι κόμβοι τείνουν να ανταλλάσσουν αρχεία με άλλους ομότιμους της ίδιας «μικροκοινότητας», η οποία πολλές φορές περιέχει ομότιμους με τις ίδιες προτιμήσεις και απόψεις.

Το μοντέλο παρέχει έναν εύκολο τρόπο αναπαράστασης πολύπλοκων και αλληλοσχετιζόμενων σχέσεων, ενώ παράλληλα επιτρέπει την εύκολη εξαγωγή συμπερασμάτων όσον αφορά στη διαφοροποιημένη εμπιστοσύνη ενός ομότιμου στις διάφορες πλευρές της ικανότητας ενός άλλου ομότιμου. Επίσης, η χρήση των πινάκων δεσμευμένων πιθανοτήτων CPT από τους ομότιμους κόμβους, επιτρέπει τον άμεσο υπολογισμό της εμπιστοσύνης και οι ομότιμοι κόμβοι γλιτώνουν από την εύρεση τιμών εμπιστοσύνης για κάθε άποψη της ικανότητας ενός παρόχου ξεχωριστά ή νέων τιμών εμπιστοσύνης κάθε φορά που αλλάζουν οι συνθήκες μιας συναλλαγής.

Οι συγγραφείς συνέκριναν το μοντέλο τους με ένα άλλο, στο οποίο οι ομότιμοι δεν κάνουν χρήση Μπεϋζιανών δικτύων και άρα η εμπιστοσύνη που διαπραγματεύονται είναι γενικής μορφής και δεν διαφοροποιείται ανάλογα με τις ικανότητες ενός παρόχου. Το αποτέλεσμα της σύγκρισης έδειξε ότι το μοντέλο τους είχε λίγο καλύτερες επιδόσεις από το άλλο σύστημα ως προς το ποσοστό των επιτυχημένων συστάσεων και άρα οι ομότιμοι καταλήγουν να επιλέγουν τον πάροχο που ταιριάζει καλύτερα στις προτιμήσεις τους, ενώ έχει επίσης λίγο καλύτερες επιδόσεις από το άλλο σύστημα και ως προς το ποσοστό των επιτυχημένων συναλλαγών με τον πάροχο και άρα οι ομότιμοι καταλήγουν να έχουν καλύτερες επιδόσεις, αξιοποιώντας τις ανταλλασσόμενες συστάσεις των υπόλοιπων ομότιμων κόμβων.

Υπάρχουν όμως και ερευνητές που βλέπουν με δυσπιστία το μοντέλο. Οι Zheng et al. [76] αναφέρουν ότι η μαθηματική διατύπωση του μοντέλου για τον υπολογισμό της εμπιστοσύνης είναι στην καλύτερη περίπτωση διαισθητική και δεν περιέχει εξηγήσεις, ενώ τα Μπεϋζιανά δίκτυα που χρησιμοποιεί είναι πολύ απλοϊκά, σε σημείο να μην μπορούν να

αναπαραστήσουν πολύπλοκες σχέσεις. Επιπλέον, παρατηρούν ότι το μοντέλο αυτό μπορεί να χρησιμοποιηθεί σε δίκτυα μικρού μεγέθους, αφού η διατήρηση και σύγκριση πιο πολύπλοκων Μπεϋζιανών δικτύων για κάθε κόμβο θα ήταν υπολογιστικά δυσβάσταχτη.

Όσον αφορά στην ανθεκτικότητα του μοντέλου σε επιθέσεις, το μοντέλο εμφανίζεται αρκετά ευάλωτο. Καταρχήν, οι τιμές εμπιστοσύνης που έχει κάθε κόμβος για έναν πάροχο αρχείων διατηρούνται σε τοπικό επίπεδο και υπολογίζονται με βάση τις συναλλαγές των δύο κόμβων ή προέρχονται από συστάσεις άλλων κόμβων. Ο πάροχος δεν μπορεί να αυξήσει με κάποιο τρόπο τη φήμη του, άρα δεν μπορεί να πραγματοποιήσει επίθεση αυτό-προώθησης. Συγχρόνως, το μοντέλο υποθέτει ότι οι κόμβοι λένε πάντα την αλήθεια, κάτι που δεν ισχύει. Έτσι ένας κόμβος μπορεί να πραγματοποιήσει μια επίθεση κακολόγησης και να δώσει χαμηλές τιμές εμπιστοσύνης για κάποιους αξιόπιστους κόμβους και αντίθετα υψηλές τιμές για άλλους κακόβουλους κόμβους όταν αυτό του ζητηθεί. Από την άλλη όμως, η περιοδική ανταλλαγή και σύγκριση των Μπεϋζιανών δικτύων μεταξύ των ομότιμων κόμβων μπορεί να εντοπίσει κακόβουλους κόμβους, οι οποίοι κάνουν τέτοιες επιθέσεις και να μειωθούν οι τιμές εμπιστοσύνης που έχουν οι υπόλοιποι κόμβοι σε αυτούς. Θα μπορούσαν όμως οι κακόβουλοι κόμβοι να επιδεικνύουν τέτοια συμπεριφορά ανά περιόδους, εφαρμόζοντας επιθέσεις on-off, έτσι ώστε να μην γίνονται άμεσα αντιληπτοί. Ειδικά εάν συνωμοτούν πολλοί κακόβουλοι κόμβοι μεταξύ τους, μπορούν να πραγματοποιούν μεταφορές αρχείων μεταξύ τους και να δίνουν υψηλές τιμές εμπιστοσύνης ο ένας στον άλλο, αυξάνοντας έτσι τις πιθανότητες να αναθεωρηθούν οι πρότερες χαμηλές τιμές που τους έχουν δοθεί στο παρελθόν. Συγχρόνως, εάν κάποιος κόμβος στέλνει καλής ποιότητας αρχεία σε κάποιους κόμβους και κακής σε άλλους, μπορεί να επιτύχει επιθέσεις αντιφατικής συμπεριφοράς, μειώνοντας την εμπιστοσύνη που έχουν οι κόμβοι των δύο ομάδων στο να παρέχουν συστάσεις. Τέλος, το μοντέλο δεν προβλέπει μηχανισμούς για τον έλεγχο και τη διαχείριση των ταυτοτήτων των ομότιμων κόμβων και άρα μπορούμε να υποθέσουμε ότι είναι ευάλωτο σε επιθέσεις τύπου Sybil και αθώωσης.

4.3.13. Το μοντέλο των Sun et al.

Οι Sun et al. παρουσίασαν στην εργασία τους [29] ένα πλαίσιο για την αποτίμηση της εμπιστοσύνης σε κατανεμημένα δίκτυα. Ασχολήθηκαν με την έννοια της εμπιστοσύνης για τα δίκτυα υπολογιστών, ανέπτυξαν μετρικές εμπιστοσύνης με καθαρά φυσική σημασία, ανέπτυξαν αξιώματα για τις μαθηματικές ιδιότητες της εμπιστοσύνης και δημιούργησαν δύο μοντέλα υπολογισμού εμπιστοσύνης που βοηθούν στη διάδοσή της μέσω τρίτων. Στη συνέχεια παρουσίασαν ένα πλαίσιο αξιολόγησης και διαχείρισης της εμπιστοσύνης.

Οι Theodorakopoulos και Baras μελέτησαν το μοντέλο των Sun et al. και το τυποποίησαν χρησιμοποιώντας το αλγεβρικό πλαίσιο που παρουσίασαν οι ίδιοι [51]. Έτσι στην περίπτωση της πρώτης μετρικής, η τιμή εμπιστοσύνης μιας σχέσης εμπιστοσύνης αποτελεί το βάρος σύμφωνα με τους Theodorakopoulos και Baras, το οποίο ορίζει ουσιαστικά την πιθανότητα p_{AB} ο χρήστης B να είναι αξιόπιστος σύμφωνα με το χρήστη A. Το βάρος $w(A,B)$ δίνεται από τον παρακάτω τύπο ως συνάρτηση της εντροπίας της κατανομής Bernoulli:

$$w(A,B) = \begin{cases} 1 - H(p_{AB}), & \gamma\iota\alpha\ 0{,}5 \le p_{AB} \le 1 \\ H(p_{AB}) - 1, & \gamma\iota\alpha\ 0 \le p_{AB} \le 0{,}5 \end{cases}$$

Δεδομένου ότι $0 \le p_{AB} \le 1$, το βάρος w παίρνει τιμές εντός του διαστήματος [-1, 1]. Με την εφαρμογή του τελεστή αλληλουχίας των Theodorakopoulos και Baras προκύπτει ο παρακάτω απλός τύπος πολλαπλασιασμού για τρεις τυχαίους κόμβους A, B και C ενός δικτύου και τα βάρη w των σχέσεων εμπιστοσύνης μεταξύ τους:

$$w(A,B) \otimes w(B,C) = w(A,B)\ w(B,C)\ .$$

Αντίστοιχα, η εφαρμογή του τελεστή σύνοψης καταλήγει στον παρακάτω τύπο:

$$t^{p_1}(s,d) \oplus t^{p_2}(s,d) = \frac{w(e_1^{p_1})}{w(e_1^{p_1})+w(e_1^{p_2})}\, t^{p_1}(s,d) + \frac{w(e_1^{p_2})}{w(e_1^{p_1})+w(e_1^{p_2})}\, t^{p_2}(s,d)\ ,$$

δηλαδή ένα σταθμισμένο άθροισμα όπου το βάρος κάθε μονοπατιού είναι ανάλογο της τιμής εμπιστοσύνης της πρώτης του ακμής. Ο τύπος αυτός είναι ίδιος με εκείνον του μοντέλου [40].

Στην περίπτωση της δεύτερης μετρικής, το βάρος $w(A,B)$ που ορίζουν οι Theodorakopoulos και Baras είναι ζεύγη αριθμών της μορφής (p_{AB},σ_{AB}), όπου p_{AB} είναι ο μέσος της συνάρτησης κατανομής πιθανότητας Βήτα που χρησιμοποιούν οι Sun et al. και σ_{AB} η διακύμανσή της. Κάθε τέτοιο ζεύγος ορίζει τη βεβαιότητα που έχει ένας χρήστης A, σχετικά με την τιμή εμπιστοσύνης p_{AB}, δηλαδή πόσο σίγουρος είναι ο χρήστης A ότι το p_{AB} είναι μια ακριβής εκτίμηση της πιθανότητας ότι ο B είναι αξιόπιστος. Σε αυτή την περίπτωση, ο τελεστής αλληλουχίας των Theodorakopoulos και Baras δίνει τον παρακάτω τύπο για τρεις τυχαίους κόμβους A, B και C και τα αντίστοιχά τους βάρη w:

$$w(A,B) \otimes w(B,C) = (p_{AB},\sigma_{AB}) \otimes (p_{BC},\sigma_{BC}) = (p_{ABC},\sigma_{ABC})\ ,$$

όπου $p_{ABC} = p_{AB}p_{BC} + (1 - p_{AB})(1 - p_{BC})$ και $\sigma_{ABC} = p_{AB}\sigma_{BC} + \frac{1}{12}(1 - p_{AB}) + p_{AB}(1 - p_{AB})(2p_{BC} - 1)^2$.

Ο τελεστής σύνοψης δίνει τον παρακάτω τύπο μέσω ενός ενδιάμεσου μετασχηματισμού ο οποίος αναφέρεται στη συνέχεια:

$$t^{p_1}(s,d) \oplus t^{p_2}(s,d) = \left(p_{sd}^{p1}, \sigma_{sd}^{p1}\right) \oplus \left(p_{sd}^{p2}, \sigma_{sd}^{p2}\right).$$

Κάθε ζεύγος (p,σ) μετασχηματίζεται σε ένα ζεύγος (a,b). Στη συνέχεια, τα δύο ζεύγη (a_1,b_1) και (a_2,b_2) συνδυάζονται και σχηματίζουν ξανά ένα ζεύγος (p,σ), όπως φαίνεται παρακάτω:

$$(p,\sigma) \rightarrow (a,b) = \left(p\left(\frac{p(1-p)}{\sigma} - 1\right), (1-p)\left(\frac{p(1-p)}{\sigma} - 1\right)\right),$$

$$(a_1,b_1) \oplus (a_2,b_2) = (a_1 + a_2 - 1, b_1 + b_2 - 1)\ ,$$

$$(a,b) \rightarrow (p,\sigma) = \left(\frac{a}{a+b}, \frac{ab}{(a+b)^2(a+b+1)}\right).$$

Όπως παρατήρησαν οι Sun et al. μέσα από προσομοιώσεις επιθέσεων ασφαλείας, η διαχείριση της εμπιστοσύνης μπορεί να επαναφέρει την απόδοση ενός δικτύου το οποίο δέχεται επίθεση από κακόβουλους κόμβους, μιας και επιτρέπει τη διαδικασία επιλογής διαδρομής για την αποφυγή των λιγότερο αξιόπιστων κόμβων. Επιπλέον, εάν αυξηθεί ο χρόνος προσομοίωσης και δημιουργηθούν περισσότερες και ακριβέστερες εγγραφές εμπιστοσύνης, η

απόδοση του δικτύου μπορεί να γίνει ίση με εκείνη ενός δικτύου όπου δεν υπάρχουν κακόβουλοι κόμβοι.

Από την άλλη, φαίνεται ότι ο μηχανισμός συστάσεων βελτιώνει την ανίχνευση κακόβουλων κόμβων. Η επίθεση κακολόγησης οδηγεί σε μείωση της απόδοσης του δικτύου, δεδομένου ότι οι πληροφορίες έμμεσης εμπιστοσύνης μπορούν να είναι ανακριβείς, η μείωση όμως αυτή δεν είναι μεγάλη λόγω των παρακάτω αμυντικών μηχανισμών που διαθέτει το σύστημα διαχείρισης της εμπιστοσύνης. Καταρχήν, τα αρχεία εγγραφών της τιμής εμπιστοσύνης και σύστασης εμπιστοσύνης κάθε κόμβου διατηρούνται ξεχωριστά και μόνο οι κόμβοι που είχαν δώσει καλές συστάσεις στο παρελθόν μπορούν να έχουν υψηλή εμπιστοσύνη σύστασης. Από την άλλη, μόνο οι συστάσεις από τους κόμβους με θετικές τιμές εμπιστοσύνης μπορούν να συμμετέχουν στη διαδικασία διάδοσης της εμπιστοσύνης, ενώ τα τρία αξιώματα που υπέδειξαν οι συγγραφείς περιορίζουν τη δύναμη που έχουν οι κόμβοι με χαμηλή εμπιστοσύνη σύστασης να παρέχουν άλλες συστάσεις. Τέλος, η εμπιστοσύνη σύστασης αντιμετωπίζεται ως ένα επιπλέον μέγεθος στο μηχανισμό ανακάλυψης κακόβουλων κόμβων. Έτσι οι συστάσεις των κόμβων που έχουν χαμηλή εμπιστοσύνη σύστασης επηρεάζουν ελάχιστα τη λήψη μιας απόφασης από τους αξιόπιστους κόμβους και μπορούν να ανιχνευτούν ως κακόβουλες και να αποκλειστούν οι κόμβοι αυτοί από το δίκτυο. Επιπλέον, από τη στιγμή που δεν αποστέλλουν οι ίδιοι οι κόμβοι τιμές για την εμπιστοσύνη τους, αλλά στηρίζονται στις συστάσεις από άλλους κόμβους, μια επίθεση αυτό-προώθησης δεν μπορεί να υπάρξει.

Στην περίπτωση της επίθεσης on-off, οι συγγραφείς συστήνουν τη χρήση ενός προσαρμόσιμου σχήματος λήθης, το οποίο καταλήγει στις ελάχιστες τιμές εμπιστοσύνης για τους επιτιθέμενους κόμβους κατά τη διαχείριση της εμπιστοσύνης. Σύμφωνα με το σχήμα αυτό, χρησιμοποιείται ένας παράγοντας λήθης β, ο οποίος αποτελεί μια συνάρτηση της τρέχουσας τιμής εμπιστοσύνης και βοηθάει τις πιο πρόσφατες παρατηρήσεις να έχουν μεγαλύτερο βάρος από τις παλαιότερες. Ως αποτέλεσμα, η τιμή εμπιστοσύνης θα αλλάξει όταν ο κόμβος μετατραπεί σε κακόβουλο και θα μπορέσει να επανέλθει όταν αλλάξει πάλι η συμπεριφορά του και κάνει πολλές καλές πράξεις.

Τέλος, όταν δεν είναι εμφανείς οι τύποι επίθεσης που εφαρμόζονται, πρέπει να χρησιμοποιείται η εμπιστοσύνη σύστασης στον αλγόριθμο ανίχνευσης κακόβουλων κόμβων, λόγω των προφανών της πλεονεκτημάτων, με την εξαίρεση της επίθεσης αντιφατικής συμπεριφοράς, όπου η χρήση της μειώνει το ρυθμό ανίχνευσης των κόμβων αυτών. Άρα το σύστημα δεν είναι ανθεκτικό στην επίθεση αυτή.

Το πρόβλημα όμως με το σύστημα της σύστασης εμπιστοσύνης είναι ότι δεν ανακαλούν τους κακόβουλους κόμβους, οι οποίοι μπορούν να συνεχίσουν να έχουν κακόβουλη δραστηριότητα μέσα στο δίκτυο [71]. Επιπλέον, δεδομένου ότι οι τιμές εμπιστοσύνης των κόμβων διαμορφώνονται από τις συστάσεις των υπολοίπων κόμβων, το μοντέλο αυτό υποφέρει από επιθέσεις συνωμοσίας [66]. Τέλος, το σύστημα δε διαθέτει κάποιο μηχανισμό ελέγχου και διαχείρισης ταυτοτήτων, οπότε είναι ευάλωτο σε επιθέσεις τύπου Sybil και αθώωσης.

4.3.14. Το μοντέλο TrustMe

Οι Singh και Liu [46] παρουσίασαν ένα ασφαλές και ανώνυμο πρωτόκολλο για τη διατήρηση και προσπέλαση πληροφοριών εκτίμησης εμπιστοσύνης. Όπως αναφέρουν, η παροχή ασφαλούς, αξιόπιστης και υπεύθυνης διανομής και πρόσβασης σε εκτιμήσεις εμπιστοσύνης ομότιμων κόμβων απαιτούν εκτός από την αυθεντικοποίηση των μηνυμάτων, την εξασφάλιση της ανωνυμίας του αιτούμενου, καθώς και του παρόχου της εκτίμησης για την κατανεμημένη διαχείριση σχέσεων εμπιστοσύνης.

Έτσι, στο μοντέλο TrustMe διατηρείται η ανωνυμία και προφυλάσσονται από στοχευμένες επιθέσεις οι ομότιμοι οι οποίοι αποκτούν πρόσβαση στις εκτιμήσεις εμπιστοσύνης άλλων ομότιμων, καθώς και οι ομότιμοι οι οποίοι διατηρούν αποθηκευμένες τις εκτιμήσεις αυτές. Αφού το μοντέλο δεν επιτρέπει στους ομότιμους κόμβους να διατηρούν οι ίδιοι στοιχεία για τις εκτιμήσεις τους, οι επιθέσεις αυτό-προώθησης δεν μπορούν να υπάρξουν. Επιπλέον, με τη

χρήση μηχανισμών κρυπτογράφησης δημοσίου κλειδιού, εξασφαλίζεται ότι κάθε μήνυμα αποστέλλεται από τον σωστό ομότιμο και βοηθάει στην αναγνώριση των κακόβουλων κόμβων, οι οποίοι δημιουργούν μηνύματα με ψευδή στοιχεία. Ακόμα, χρησιμοποιώντας χρονικές σφραγίδες στα αποστελλόμενα μηνύματα, εξασφαλίζεται ότι ένα μήνυμα έχει ληφθεί μόνο μια φορά, αποφεύγοντας περιπτώσεις κακόβουλων κόμβων, οι οποίοι ξαναστέλνουν παλαιότερα μηνύματα. Έτσι, ένας κόμβος μπορεί να πάρει μια απόφαση αλληλεπίδρασης με κάποιον άλλον ομότιμο, λαμβάνοντας μηνύματα απάντησης από τους ομότιμους ΠΔΕ που διατηρούν αποθηκευμένη την τιμή εμπιστοσύνης του, απαιτώντας πολύ μικρούς συνολικούς χρόνους απόκρισης για όλες τις συναλλαγές. Το μοντέλο κάνει χρήση μηνυμάτων – αποδείξεων αλληλεπίδρασης, τα οποία χρησιμεύουν μεταξύ άλλων και στην αντιμετώπιση περιπτώσεων κατά τις οποίες συνεργαζόμενοι κακόβουλοι κόμβοι επιθυμούν να δώσουν ψευδώς αυξημένες τιμές εμπιστοσύνης ο ένας στον άλλο, άρα το μοντέλο αντιμετωπίζει επαρκώς επιθέσεις συνωμοσίας. Το μοντέλο TrustMe δε χρησιμοποιεί κάποια κεντρική έμπιστη αρχή, αλλά ο bootstrap server έχει τη μορφή της αρχής πιστοποίησης. Αυτός είναι που αποδίδει σε κάθε νέο κόμβο ένα αναγνωριστικό, το οποίο εμποδίζει επιθέσεις τύπου Sybil και αθώωσης.

Ο μηχανισμός επιλογής των ομότιμων ΠΔΕ είναι τυχαίος και άρα αρκετά ασφαλής. Από την άλλη, η τιμή εμπιστοσύνης κάθε ομότιμου κόμβου αποθηκεύεται σε περισσότερους από έναν ΠΔΕ κόμβους, αποφεύγοντας έτσι επιθέσεις κατά τις οποίες κάποιος ΠΔΕ κόμβος αποστέλλει ψευδείς τιμές εμπιστοσύνης για τον κόμβο που αντιπροσωπεύει, δηλαδή επιθέσεις κακολόγησης. Η συνολική τιμή εμπιστοσύνης του ομότιμου αυτού, με βάση την οποία θα αποφασίσει κάποιος άλλος να αλληλεπιδράσει μαζί του, θα προκύψει από την πλειοψηφία των τιμών που θα του δοθούν. Σε αυτή την περίπτωση, οι αξιόπιστοι ΠΔΕ ομότιμοι οι οποίοι βλέποντας τα μηνύματα των υπολοίπων ΠΔΕ κόμβων ανακαλύπτουν τον κακόβουλο ΠΔΕ, μπορούν να γνωστοποιήσουν την ύπαρξή του στον κόμβο που αιτείται την τιμή εμπιστοσύνης, περιλαμβάνοντας το αναγνωριστικό του στην απάντησή τους. Η ύπαρξη όμως ενός τέτοιου ομότιμου μπορεί να γίνει αντιληπτή και από τον ίδιο τον κόμβο που αιτείται την τιμή εμπιστοσύνης του κόμβου, μιας και η τιμή που θα αποστείλει ο κακόβουλος ΠΔΕ θα αποτελεί μειοψηφία. Η μειοψηφία αυτή εξασφαλίζεται από την τυχαιότητα της αρχικής επιλογής των ομότιμων ΠΔΕ από τον bootstrap server, η οποία κάνει ανέφικτη την ύπαρξη πολλών κακόβουλων και συνεργαζόμενων ομότιμων κόμβων, όπως γίνεται στις επιθέσεις συνωμοσίας. Ακόμα και αν κάποιος ΠΔΕ εκτελεί επιθέσεις on-off, μπορεί να γίνει αντιληπτός από τους υπόλοιπους ΠΔΕ όπως και πριν. Επιπλέον, οι επιθέσεις κακολόγησης αποφεύγονται επίσης με την κρυπτογράφηση των αποστελλόμενων μηνυμάτων από τους ΠΔΕ, έτσι ώστε να μην αποστέλλονται ψεύτικα μηνύματα από κακόβουλους κόμβους, οι οποίοι προσπαθούν να μειώσουν την τιμή εμπιστοσύνης άλλων ομότιμων. Αλλά και οι επιθέσεις αντιφατικής συμπεριφοράς δεν μπορούν να επηρεάσουν τη λειτουργία του μοντέλου, αφού δεν μπορούν να επηρεάσουν τις τιμές εμπιστοσύνης μεταξύ των ομότιμων κόμβων του δικτύου.

Από την άλλη, η διαδικασία της αναφοράς μιας νέας τιμής εμπιστοσύνης από έναν ομότιμο κόμβο, ο οποίος αλληλεπίδρασε με κάποιον, προς τους ομότιμους ΠΔΕ, οι οποίοι είναι υπεύθυνοι γι' αυτόν, αποτελεί μια εύκολη διαδικασία και αξιοποιεί την εμπειρία όλων των κόμβων, ακόμα και όταν αυτοί παύουν να ανήκουν στο δίκτυο, παρέχοντας έτσι έναν ισχυρότερο μηχανισμό εμπιστοσύνης. Ακόμα και στην περίπτωση που κάποιος ομότιμος επιχειρήσει να στείλει ψευδή αναφορά στους ΠΔΕ για κάποιον κόμβο με τον οποίο αλληλεπίδρασε, η καθολική τιμή εμπιστοσύνης που θα σχηματιστεί για τον υπό επίθεση ομότιμο κόμβο θα προκύψει από όλες τις ατομικές τιμές εμπιστοσύνης που έχουν αποσταλεί από τους ομότιμους οι οποίοι έχουν αλληλεπιδράσει με τον κόμβο αυτόν.

4.3.15. Το μοντέλο των Theodorakopoulos και Baras

Το μοντέλο που παρουσίασαν οι Theodorakopoulos και Baras στο [47] χρησιμοποιεί και αξιολογεί τις μαρτυρίες των χρηστών για την εμπιστοσύνη, μοντελοποιώντας τη διαδικασία αυτή ως πρόβλημα ελάχιστου μονοπατιού σε ένα κατευθυνόμενο γράφημα με βάρη και δείχνει πώς

δύο κόμβοι μπορούν να εγκαταστήσουν μια έμμεση σχέση εμπιστοσύνης, χωρίς προηγούμενη άμεση αλληλεπίδραση.

Η υπολογιστική πολυπλοκότητα του αλγορίθμου που παρουσίασαν οι Theodorakopoulos και Baras εξαρτάται από τον ημιδακτύλιο που χρησιμοποιείται και από την ακριβή τοπολογία του δικτύου. Η κρίσιμη παράμετρος της τοπολογίας είναι ο αριθμός των μονοπατιών από τον κόμβο πηγή προς τους υπόλοιπους κόμβους, κάνοντας τον αλγόριθμο αποδοτικότερο στα αραιά δίκτυα. Σε κάθε περίπτωση όμως, ο αλγόριθμος μπορεί να χρησιμοποιηθεί με κατανεμημένο τρόπο και ανταλλαγές τοπικών δεδομένων, όπως αναφέρουν οι συγγραφείς. Το μειονέκτημα βέβαια του αλγορίθμου εντοπίζεται στο γεγονός ότι οι συγγραφείς δεν διαφοροποιούν τον τύπο των ακμών που χρησιμοποιούνται στο γράφημά τους, ανάλογα με το αν πρόκειται για σύσταση για έναν κόμβο ή για αξιολόγηση της υπηρεσίας που προσφέρει ο κόμβος αυτός [49].

Στην προσομοίωση λειτουργίας του αλγορίθμου που παρουσίασαν, οι συγγραφείς υπέθεσαν ότι κάποιοι συγκεκριμένοι κόμβοι ήταν καλοί, ενώ οι υπόλοιποι ήταν κακοί. Σκοπός της προσομοίωσης ήταν τελικά ο προσδιορισμός των καλών κόμβων ως καλών και των κακών ως κακών. Οι καλοί κόμβοι προσάρμοζαν τις απόψεις τους για τους γειτονικούς τους κόμβους τυχαία. Αντίθετα, οι κακοί κόμβοι είχαν πάντα την καλύτερη άποψη για τους γειτονικούς τους κακόβουλους κόμβους $(1,1)$ και τη χειρότερη για τους γειτονικούς τους καλόβουλους κόμβους $(0,1)$. Όπως φαίνεται από τα αποτελέσματα, οι κόμβοι διαχωρίζονται τελικά σε καλούς και κακούς στους τελευταίους κύκλους της προσομοίωσης. Καθώς όμως το ποσοστό των κακόβουλων κόμβων έναντι των καλόβουλων στο δίκτυο αυξάνεται, ο διαχωρισμός πραγματοποιείται τελικά, αλλά ο αριθμός των διαχωριζόμενων κόμβων, δηλαδή εκείνων για τους οποίους έχουν συλλεχθεί αρκετά στοιχεία, μειώνεται και αυτό γιατί καθώς ανακαλύπτονται οι κακόβουλοι κόμβοι, μπλοκάρονται τα μονοπάτια στα οποία ανήκουν, αφού δεν έχουν πλέον το δικαίωμα να υποστηρίξουν κάποιον επόμενο κόμβο. Έτσι, οι επόμενοι αυτοί κόμβοι μπορούν να επικοινωνήσουν με τον κόμβο πηγή μέσω λιγότερων κάθε φορά μονοπατιών ή και να απομονωθούν πλήρως. Σε κάθε περίπτωση, η βεβαιότητα της άποψης του κόμβου πηγή για τους κόμβους αυτούς μειώνεται, οδηγώντας στην αδυναμία ταξινόμησής τους. Άρα φαίνεται ότι το μοντέλο είναι εκ πρώτης όψεως ανθεκτικό σε επιθέσεις κακολόγησης, αφού ένας κακόβουλος κόμβος ακόμα και αν δίνει καλή άποψη για κάποιον ο οποίος δεν είναι, θα υπάρξουν άλλοι κόμβοι από άλλα μονοπάτια που θα δώσουν την πραγματική άποψη για τον υπό επίθεση κόμβο. Όταν όμως στο δίκτυο υπάρχουν πολλοί κακόβουλοι κόμβοι, οι οποίοι συνωμοτούν μεταξύ τους και δίνουν πάντα καλές απόψεις ο ένας για τον άλλο και κακές για αξιόπιστους κόμβους, τότε είναι δυνατό να επιτύχουν στην επίθεσή τους, εάν ο αριθμός τους υπερβαίνει αυτό των αξιόπιστων κόμβων.

Ο αλγόριθμος αυτός δεν απαιτεί την παρουσία κάποιας κεντρικής υποδομής, ενώ οι χρήστες δεν χρειάζεται να έχουν προσωπική και άμεση εμπειρία με κάθε άλλο χρήστη στο δίκτυο προκειμένου να έχουν μια άποψη γι' αυτόν. Οι εμπειρίες ενδιάμεσων χρηστών μπορούν να χρησιμοποιηθούν προς όφελος εκείνων που δεν έχουν καμία άμεση ένδειξη για κάποιους κόμβους. Οι πληροφορίες που αποκτώνται σε κάθε κύκλο που τρέχει ο αλγόριθμος, αποθηκεύονται και μπορούν να χρησιμοποιηθούν για πολλές αποφάσεις εμπιστοσύνης. Στην περίπτωση που δεν υπάρχουν αρκετές ενδείξεις για κάποιο κόμβο, τότε δε διαμορφώνεται καμία άποψη. Έτσι, οι κακόβουλοι κόμβοι του δικτύου δεν μπορούν να ξεγελάσουν τους αξιόπιστους κόμβους για να δεχτούν άλλους κακόβουλους κόμβους ως επίσης αξιόπιστους. Επιπλέον, κανένας κόμβος δεν μπορεί να εκφέρει άποψη για τον εαυτό του και άρα το μοντέλο είναι ανθεκτικό απέναντι σε επιθέσεις αυτό-προώθησης. Αλλά και οι επιθέσεις on-off κάποιου κόμβου μπορούν να αντιμετωπιστούν, αφού όταν οι κακόβουλοι κόμβοι ενεργούν μόνοι τους, το μοντέλο καταφέρνει τελικά να τους αντιμετωπίζει, αφού λαμβάνονται υπόψη και οι απόψεις κόμβων από άλλα μονοπάτια. Δεδομένου ότι κάθε κόμβος σχηματίζει άποψη για κάποιον άλλο κόμβο βασιζόμενος στις δικές του εμπειρίες και μόνο όταν δεν έχει αλληλεπιδράσει με κάποιο κόμβο ζητάει την άποψη άλλων κόμβων, οι επιθέσεις αντιφατικής συμπεριφοράς δεν επηρεάζουν το μοντέλο των Theodorakopoulos και Baras. Το μοντέλο όμως δεν χρησιμοποιεί καμία τεχνική για τον έλεγχο ταυτοτήτων των κόμβων, οπότε επιθέσεις τύπου Sybil και αθώωσης μπορούν να συμβούν.

4.3.16. Το μοντέλο Regret

Οι Sabater και Sierra παρουσίασαν το μοντέλο Regret [48], ένα μοντέλο το οποίο βασίζεται στη φήμη για να προσδιορίσει την εμπιστοσύνη που πρέπει να έχει ένας πράκτορας σε έναν άλλο. Το μοντέλο αντιμετωπίζει τη φήμη ως έννοια με πολλές όψεις και μια ιεραρχική οντολογική δομή επιτρέπει την εξέταση πολλών όψεών της την ίδια στιγμή.

Εκτός από τις εμπειρίες που μπορεί να έχει ένας πράκτορας με άλλους μάρτυρες, το μοντέλο λαμβάνει υπόψη κατά τον υπολογισμό της φήμης του τις κοινωνικές του σχέσεις και το γεγονός ότι κάποιες από τις μαρτυρίες των υπόλοιπων πρακτόρων μπορεί να είναι ψευδείς ή συνδυασμένες, δίνοντας λανθασμένες τιμές φήμης για τον πράκτορα αυτόν. Επιπλέον, ο συνδυασμός συμπληρωματικών μεθόδων οι οποίες χρησιμοποιούν διαφορετικές πλευρές μιας συναλλαγής και τις κοινωνικές σχέσεις του πράκτορα, του δίνει τη δυνατότητα να υπολογίζει τιμές φήμης σε διάφορα στάδια της γνώσης του για την κοινωνία στην οποία βρίσκεται.

Όσον αφορά στις επιθέσεις που μελετήσαμε, κανένας πράκτορας δεν παρέχει ο ίδιος σε άλλους κάποια τιμή εμπιστοσύνης για τον εαυτό του, και άρα δεν μπορεί να πραγματοποιηθεί επίθεση αυτό-προώθησης. Από την άλλη, παρόλο που κάποιος κακόβουλος κόμβος μπορεί να στείλει ψευδείς τιμές εμπιστοσύνης για άλλους κόμβους, να υπονομεύσει την εμπιστοσύνη στην παροχή συστάσεων μεταξύ πρακτόρων ή να εμφανίσει περιοδική κακόβουλη συμπεριφορά, το μοντέλο Regret διαθέτει πολυσύνθετα συστήματα κατά τη σύνθεση της ατομικής φήμης ενός πράκτορα και της αξιοπιστίας της τιμής αυτής, χρησιμοποιώντας τον παράγοντα του αριθμού των αποτελεσμάτων που χρησιμοποιούνται για τον υπολογισμό της φήμης και την απόκλιση της φήμης αποτελέσματος. Αλλά και στην περίπτωση της σύνθεσης της κοινωνικής φήμης ενός πράκτορα λαμβάνει υπόψη το βαθμό σπουδαιότητας καθεμίας παρεχόμενης τιμής από κάποιο μάρτυρα, προσδιορίζοντας μια τιμή εμπιστοσύνης για το μάρτυρα αυτόν μέσω της κοινωνικής εμπιστοσύνης ή μέσω της φήμης εμπιστοσύνης αποτελέσματος της «εμπιστοσύνης» που αξίζει ο μάρτυρας, ή υπολογίζει τη φήμη γειτονιάς κάθε πράκτορα στόχου χρησιμοποιώντας τόσο τη φήμη όσο και την αξιοπιστία κάθε γείτονα. Κάτι τέτοιο καθιστά μη αποτελεσματική την επίθεση on-off. Ακόμα και σε μια επίθεση συνωμοσίας όπου οι κακόβουλοι πράκτορες θα συνεργάζονταν με σκοπό να μειώσουν τη φήμη κάποιων άλλων πρακτόρων, ο αλγόριθμος επιλογής των πρακτόρων που μετέχουν στον υπολογισμό της φήμης γειτονιάς είναι τέτοιος που είναι δύσκολο να βρεθούν ανάμεσα στους πράκτορες που θα αποστείλουν τιμές εμπιστοσύνης για το ζητούμενο πράκτορα. Γι' αυτό θεωρούμε ότι μια τέτοια επίθεση δεν είναι αποδοτική. Από την άλλη, οι πράκτορες που βρίσκονται να συνεργάζονται με άλλους κακόβουλους πράκτορες τυγχάνουν χαμηλής εκτίμησης και άρα είναι πιθανό μια επίθεση αντιφατικής συμπεριφοράς να επιτύχει στο σύστημα Regret, αλλά δεδομένου ότι κατά τον υπολογισμό της κοινωνικής φήμης λαμβάνονται υπόψη οι φήμες όλων των γειτόνων του πράκτορα, η επίθεση αυτή θα έχει μικρό αντίκτυπο. Τέλος, το μοντέλο δεν αναφέρει την ύπαρξη κάποιου συστήματος ελέγχου ταυτοτήτων των πρακτόρων κάτι που φαίνεται να το αφήνει ευάλωτο σε επιθέσεις τύπου Sybil και αθώωσης.

4.3.17. Το μοντέλο TwoHop

Το μοντέλο που προτείνουν οι Glynos et al. [49] εισάγει μια μετρική, η οποία περιγράφει την ποιότητα των παρεχόμενων υπηρεσιών, όπως τις βίωσαν οι γειτονικοί κόμβοι εκείνου του κόμβου που θέτει το αίτημα, χρησιμοποιώντας έτσι τις συλλογικές εμπειρίες τρίτων που έχουν τα ίδια ενδιαφέροντα. Η πρότασή τους δεν απαιτεί την ύπαρξη κάποιας κεντρικής δομής διαχείρισης και καλύπτει την ανάγκη που δημιουργεί η ραγδαία ανάπτυξη των δικτύων ομότιμων κόμβων, επιτρέποντας συγχρόνως τη δημιουργία ιεραρχιών εμπιστοσύνης, οι οποίες μπορούν να περιγράψουν τις αλληλεπιδράσεις των κόμβων μέσα σε ένα περιβάλλον δικτύωσης.

Όπως αποδεικνύουν, η πολυπλοκότητα του αλγορίθμου υπολογισμού της εμπιστοσύνης που χρησιμοποιεί το μοντέλο TwoHop είναι σχετικά μικρή και εξαρτάται από το μέγεθος των χαρτοφυλακίων των κόμβων οι οποίοι συμμετέχουν στο δίκτυο για μια συγκεκριμένη υπηρεσία, κάτι που τον κάνει εύκολα χρησιμοποιήσιμο στο διαδίκτυο. Πρόκειται

για ένα μοντέλο το οποίο αντιμετωπίζει αποτελεσματικά τους αναξιόπιστους κόμβους, εκείνους δηλαδή οι οποίοι δίνουν λάθος αξιολογήσεις σε υπηρεσίες παρόχων, αρκεί βέβαια οι πρώτοι να μην αποτελούν σημαντικό αριθμό έναντι του συνολικού των συμμετεχόντων στο δίκτυο. Οι συγγραφείς αναφέρουν ότι οι αναξιόπιστοι κόμβοι μπορούν να αντιμετωπιστούν σε μεγάλο βαθμό από τους υπόλοιπους κόμβους, χρησιμοποιώντας οι δεύτεροι τα βάρη εκτίμησής τους ως μέσο άμυνας απέναντί τους. Αλλά και στην περίπτωση που οι κακόβουλοι κόμβοι προσπαθήσουν να ενεργήσουν ως ομάδα, θα έχουν περιορισμένα αποτελέσματα στον υπολογισμό της εμπιστοσύνης ενός κόμβου εάν δράσουν ως αξιολογητές, ενώ εάν κάποιοι από την ομάδα αυτή βρεθούν να ανήκουν στο αρχικό χαρτοφυλάκιο εμπιστοσύνης, τότε θα δράσουν ως κριτές και άρα τα βάρη εμπιστοσύνης τους θα επηρεάσουν τα αποτελέσματα του υπολογισμού της εμπιστοσύνης. Για το λόγο αυτό οι συμμετέχοντες στο δίκτυο TwoHop μπορούν να απομακρύνουν τους κακόβουλους αυτούς κόμβους από το χαρτοφυλάκιο εμπιστοσύνης τους, όταν διαπιστώσουν την κακόβουλη συμπεριφορά τους.

Όπως αναφέρεται, το μοντέλο TwoHop είναι ευάλωτο σε επιθέσεις τύπου Sybil, και αυτό γιατί δεν ελέγχει τη δημιουργία νέων ταυτοτήτων και δε διαφοροποιεί τους χρήστες του με βάση την ταυτότητά τους. Αποδεικνύουν όμως ότι ακόμα και αν ένα μεγάλο ποσοστό των χρηστών του δικτύου προσπαθήσουν να επηρεάσουν το αποτέλεσμα του αλγορίθμου πιστοποιώντας ο ένας χρήστης τον άλλο, δεν το πετυχαίνουν. Τέλος, αναφέρουν ότι μπορούν να αντιμετωπίσουν επιθέσεις αθώωσης, όπου ο αναξιόπιστος κόμβος ο οποίος έχει πολλές χαμηλές αξιολογήσεις τελικά αποχωρεί από το δίκτυο για να ξαναμπεί σε αυτό με διαφορετική ταυτότητα. Το μοντέλο θέτει ως ελάχιστη τιμή για τις αξιολογήσεις, την τιμή που λαμβάνουν οι νέοι κόμβοι οι οποίοι εισέρχονται στο δίκτυο. Έτσι, ένας αναξιόπιστος κόμβος δε θα αποχωρήσει από το δίκτυο, αφού έτσι θα χάσει συγχρόνως όλες τις υπάρχουσες συνδέσεις του, οι οποίες θα του αποφέρουν μελλοντικά κέρδος. Όσον αφορά στις επιθέσεις αυτό-προώθησης, το μοντέλο TwoHop αγνοεί τις αξιολογήσεις που κάνουν οι ίδιοι οι κόμβοι για τους εαυτούς τους, πιστοποιώντας τις αξιολογήσεις μέσω ψηφιακών υπογραφών. Επίσης, το μοντέλο αναγνωρίζει, όπως είπαμε, τις ψευδείς αξιολογήσεις κακόβουλων κόμβων και μειώνει πολύ την τιμή εμπιστοσύνης τους ακόμα και αν αυτοί λάβουν κάποιες καλές αξιολογήσεις από άλλους κόμβους. Έτσι το μοντέλο αντιμετωπίζει αντιφατικές συμπεριφορές κακόβουλων κόμβων. Τέλος, αποδεικνύεται το μοντέλο εύρωστο και απέναντι σε επιθέσεις on-off, διατηρώντας και χρησιμοποιώντας τις κακές αξιολογήσεις που έχει λάβει κάποιος κόμβος κατά την κακόβουλη συμπεριφορά του περισσότερο χρόνο, μην επιτρέποντάς του να ανακτήσει την προηγούμενη τιμή εμπιστοσύνης του.

4.3.18. Το μοντέλο των Prasad et al.

Οι Prasad et al. [50] παρουσίασαν ένα δυναμικό σύστημα υπολογισμού φήμης, σύμφωνα με το οποίο η εμπιστοσύνη σε έναν ομότιμο κόμβο υπολογίζεται με βάση την αξιοπιστία του κόμβου που παρέχει την πληροφορία για τον κόμβο αυτό, την ικανοποίησή του από τις συναλλαγές του με αυτόν, το χρόνο κατά τον οποίο πραγματοποιήθηκαν οι συναλλαγές αυτές ώστε να δοθεί μεγαλύτερο βάρος στις πιο πρόσφατες, αλλά και την ομοιότητά του με τον κόμβο που αναζητά την τιμή της εμπιστοσύνης.

Το μοντέλο αυτό μπορεί να χρησιμοποιηθεί σε οποιαδήποτε εφαρμογή ηλεκτρονικού εμπορίου στην οποία παρέχονται αρχεία και υπηρεσίες μεταξύ παρόχων και καταναλωτών. Ο μηχανισμός του απευθύνεται γενικά σε κοινότητες και επιτρέπει την αντιστάθμιση της φήμης, βασιζόμενος στο είδος της κοινότητας στην οποία ανήκει ο συγκεκριμένος κόμβος.

Οι συγγραφείς έχουν μεριμνήσει για έναν μηχανισμό ο οποίος εντοπίζει και αποκλείει τυχόν αναδράσεις από κακόβουλους κόμβους, οι οποίοι είτε υπερβάλουν στις αναδράσεις τους προκειμένου να προωθήσουν ένα προϊόν, είτε τις υποβαθμίζουν δίνοντας και πάλι ψευδή τιμή ανάδρασης. Ο εντοπισμός τέτοιων κόμβων γίνεται όταν παρατηρούνται πολλές αλληλεπιδράσεις με συγκεκριμένους ομότιμους πωλητές, ενώ οι τιμές ανάδρασης που δίνουν για τους πωλητές αυτούς είναι χαμηλές. Στις περιπτώσεις αυτές, οι τιμές των αναδράσεων που προέρχονται από τους κόμβους αυτούς εξαιρούνται. Επιπλέον, χρησιμοποιείται ένας

διορθωτικός μηχανισμός στην περίπτωση που οι αναδράσεις κακόβουλων κόμβων είναι πολλές, έτσι ώστε να μην επηρεάσουν κατά πολύ τη φήμη κάποιου κόμβου. Έτσι το μοντέλο είναι ανθεκτικό σε επιθέσεις κακολόγησης.

Το μοντέλο αποφεύγει τις επιθέσεις αυτό-προώθησης κάποιου κακόβουλου κόμβου, αποκλείοντάς τον από τη διαδικασία υπολογισμού ή προώθησης της ανάδρασής του. Από την άλλη, το σύστημα εντοπισμού των κακόβουλων κόμβων που κάνουν επιθέσεις κακολόγησης όταν στέλνουν αναδράσεις για άλλους κόμβους, εντοπίζει τους κόμβους αυτούς όταν διατηρούν σταθερά κακόβουλη συμπεριφορά. Το μοντέλο όμως αποτυγχάνει να εντοπίσει τους κακόβουλους κόμβους, οι οποίοι στέλνουν ψευδείς αρνητικές αναδράσεις για κόμβους στόχους αλλά έχουν καλές αναδράσεις από πωλητές, οπότε θεωρούνται αξιόπιστοι συνιστώντες, κάτι που δεν εντοπίζεται από τον τύπο που υπολογίζει τη φήμη ενός κακόβουλου κόμβου σε σχέση με κάποιον άλλο συνιστώντα. Άρα είναι ευάλωτο σε επιθέσεις on-off. Όταν μάλιστα οι κόμβοι αυτοί συνεργάζονται με κόμβους πωλητές, οι οποίοι δίνουν πάντα θετική ανάδραση για τους πρώτους όταν τους το ζητείται, οι κακόβουλοι κόμβοι πετυχαίνουν και επιθέσεις συνωμοσίας. Από την άλλη, μια επίθεση αντιφατικής συμπεριφοράς από κάποιο κακόβουλο κόμβο θα εμπόδιζε τους κόμβους από το να σχηματίσουν κάποια άποψη για αυτόν. Σε καμία όμως περίπτωση δε θα επηρέαζε τη φήμη των υπόλοιπων κόμβων, αφού το μοντέλο δεν κάνει χρήση μηχανισμών ανταλλαγής και σύγκρισης φήμης. Τέλος, το μοντέλο δεν είναι ανθεκτικό σε επιθέσεις τύπου Sybil και αθώωσης, αφού δεν παρέχει μηχανισμούς ελέγχου και διαχείρισης ταυτοτήτων των ομότιμων κόμβων.

5. Συμπεράσματα

Το θέμα της εμπιστοσύνης στις μέρες μας έχει αναδειχθεί ιδιαίτερα λόγω της ανάγκης ύπαρξης ασφαλών συναλλαγών μεταξύ των οντοτήτων. Ειδικά η εξάπλωση της χρήσης του διαδικτύου και οι ποικίλες εφαρμογές που δημιουργούνται καθημερινά για το διαμοιρασμό αρχείων, την παροχή υπηρεσιών, τις ηλεκτρονικές αγοραπωλησίες και συναλλαγές, έχουν θέσει ως μείζον το ζήτημα της αξιοπιστίας των οντοτήτων και τις σχέσεις εμπιστοσύνης μεταξύ τους.

Με την παρούσα διατριβή, έγινε προσπάθεια να ερμηνευτεί η πολυδιάστατη έννοια της εμπιστοσύνης, χρησιμοποιώντας πολλούς τομείς της σύγχρονης επιστήμης. Αναλύθηκαν τα χαρακτηριστικά της και ο τρόπος που χρησιμοποιείται για να οδηγήσει τελικά δύο οντότητες σε συνεργασία. Ακολούθησε η μεταφορά της έννοιας στον τομέα των ηλεκτρονικών υπολογιστών και η χρήση της σε δίκτυα μέσω μοντέλων εμπιστοσύνης.

Στη συνέχεια παρουσιάστηκαν κάποια από τα σημαντικότερα μοντέλα εμπιστοσύνης που έχουν τυποποιήσει την έννοια της εμπιστοσύνης και έχουν μοντελοποιήσει τις διαδικασίες που ακολουθούνται για να διαπιστωθεί εάν μια οντότητα είναι καταρχήν αξιόπιστη και κατά δεύτερον, εάν μια συνεργασία με την οντότητα αυτή θα έχει τα επιθυμητά αποτελέσματα. Τα μοντέλα αυτά χρησιμοποιούν διάφορους μηχανισμούς και έχουν ιδιαίτερα χαρακτηριστικά, τα οποία τα κάνουν να ξεχωρίζουν από άλλα μοντέλα. Ο υπολογισμός της εμπιστοσύνης βάσει κοινών χαρακτηριστικών και προτιμήσεων, ο προσδιορισμός της φήμης με χρήση των τριών διαστάσεών της, η χρήση της εντροπίας ως μέτρο αβεβαιότητας και η εφαρμογή των Μπεϋζιανών δικτύων για την αναπαράσταση των σχέσεων μεταξύ των οντοτήτων, αποτελούν μερικά από τα χαρακτηριστικά αυτά.

Στην επόμενη ενότητα έγινε μια κριτική πάνω στα μοντέλα αυτά, βάσει τόσο των αποτελεσμάτων που παρουσίασαν οι ίδιοι οι ερευνητές από προσομοιώσεις των μοντέλων τους, όσο και από τα σχόλια άλλων ερευνητών. Η κριτική αυτή όμως έπρεπε να επεκταθεί και στις απειλές που αντιμετωπίζουν τα μοντέλα αυτά από κακόβουλους συμμετέχοντες. Για το λόγο αυτό περιγράφτηκαν οι γνωστότερες επιθέσεις που μπορούν να πραγματοποιήσουν κακόβουλες οντότητες και να απειλήσουν τη λειτουργία των μοντέλων εμπιστοσύνης, επηρεάζοντας κυρίως τις διαδικασίες προώθησης της εμπιστοσύνης μεταξύ των συμμετεχόντων. Από την ποιοτική αξιολόγηση των μοντέλων σε σχέση με τις επιθέσεις αυτές, προέκυψε ο πίνακας 3, ο οποίος παρατίθεται στο τέλος. Στον πίνακα αυτόν τα μοντέλα εμπιστοσύνης κατατάχθηκαν σε διαβαθμίσεις ανάλογα με την εκτιμώμενη ανθεκτικότητά τους στις επιθέσεις αυτές, σύμφωνα με τα χαρακτηριστικά και τις δικλείδες ασφαλείας που ενσωματώνουν. Χρησιμοποιήθηκαν τέσσερις διαβαθμίσεις, απόλυτη, μερική, ελάχιστη και μηδενική ανθεκτικότητα απέναντι στην εκάστοτε επίθεση. Στον πίνακα οι τέσσερις αυτές διαβαθμίσεις αναπαρίστανται με τη βοήθεια των τιμών 0, 1, 2 και 3 αντίστοιχα.

Όπως παρατηρούμε, τα περισσότερα μοντέλα αντιμετωπίζουν πλήρως την επίθεση της αυτό-προώθησης, μην επιτρέποντας σε μια οντότητα να εκφέρει άποψη για την τιμή εμπιστοσύνης που οι άλλες οντότητες πρέπει να της εκχωρήσουν. Μεγάλη επιτυχία σημειώνουν επίσης και ως προς την αντιμετώπιση της επίθεσης αντιφατικής συμπεριφοράς, μιας και οι οντότητες αρκούνται συνήθως στις παρατηρήσεις τους και στον καθορισμό των τιμών εμπιστοσύνης που πραγματοποιούν οι ίδιες για τις άλλες οντότητες και δεν μεταβάλλουν την εμπιστοσύνη που έχουν σε άλλες οντότητες να παρέχουν συστάσεις, όταν εκείνες έχουν διαφορετική άποψη για κάποια τρίτη οντότητα. Επιπλέον, τα περισσότερα μοντέλα αντιμετωπίζουν επαρκώς την επίθεση κακολόγησης, συνήθως εντοπίζοντας την κακόβουλη συμπεριφορά των επιτιθέμενων κόμβων και μειώνοντας την αξιοπιστία τους ως συνιστώντες.

Λίγο μεγαλύτερο πρόβλημα παρουσιάζουν σχεδόν όλα τα μοντέλα κατά την αντιμετώπιση επιθέσεων on-off και αυτό γιατί οι επιτιθέμενες οντότητες καταφέρνουν να ανακτούν την πρότερη καλή τους φήμη όταν σταματούν να έχουν κακόβουλη συμπεριφορά. Το μεγαλύτερο πρόβλημα των μοντέλων εμπιστοσύνης φαίνεται να είναι οι επιθέσεις συνωμοσίας. Σε αυτή την περίπτωση, οι κακόβουλες οντότητες σχηματίζουν ομάδες μεταξύ τους και εκτελούν συγχρόνως πολλά είδη άλλων επιθέσεων, μην επιτρέποντας στα μοντέλα εμπιστοσύνης να αντιμετωπίσουν αποτελεσματικά τέτοιες συντονισμένες ενέργειες.

Τέλος, τα περισσότερα μοντέλα εμφανίζονται ανοικτά απέναντι σε επιθέσεις τύπου Sybil και αθώωσης. Για το γεγονός αυτό όμως δεν ευθύνεται ο τρόπος διαχείρισης της εμπιστοσύνης που υιοθετεί κάθε μοντέλο, αλλά η απουσία μηχανισμών που θα πιστοποιούν και θα ελέγχουν τις ταυτότητες των οντοτήτων κατά την είσοδό τους στο εκάστοτε δίκτυο. Υπάρχουν βέβαια και μοντέλα εμπιστοσύνης, τα οποία προσφέρουν αντικίνητρα για τέτοιου είδους επιθέσεις, όπως η εκχώρηση της ελάχιστης τιμής εμπιστοσύνης που υπάρχει, όταν μια οντότητα εισέρχεται στο δίκτυο, έτσι ώστε να αποθαρρυνθεί να αποχωρήσει από αυτό προκειμένου να αυξήσει τη χαμηλή τιμή εμπιστοσύνης που έχει αποκτήσει.

Όπως φαίνεται και από τα μοντέλα εμπιστοσύνης που περιγράψαμε, η εμπιστοσύνη καθεαυτή δεν είναι μετρήσιμο μέγεθος, αλλά μπορεί να μετρηθεί η αξία που αποκομίζεται από αυτή. Μπορεί κάλλιστα να θεωρηθεί αγαθό, όπως είναι για παράδειγμα η ενημέρωση. Η γνώση της όμως, μπορεί να βοηθήσει οντότητες κατά την εξέταση μιας πιθανής κατάστασης συνεργασίας, όπου οι διαθέσιμες πληροφορίες μπορεί να είναι λιγοστές. Σε καμία όμως περίπτωση μια οντότητα δεν πρέπει να εμπιστευτεί μια άλλη οντότητα ότι θα ενεργήσει με έναν ορισμένο τρόπο, μόνο επειδή το λέει. Η εμπιστοσύνη πρέπει να πηγάζει από πρότερη εμπειρία μεταξύ των οντοτήτων ή τουλάχιστον η εμπειρία αυτή να προέρχεται από άλλες αξιόπιστες οντότητες. Από τις αξιολογήσεις των μοντέλων που περιγράψαμε προκύπτει ότι η απουσία εμφανών κυρώσεων για μια κακόβουλη συμπεριφορά ή αντίθετα, κινήτρων για μια αξιόπιστη συμπεριφορά, αφαιρεί το έναυσμα από μια οντότητα να συμπεριφέρεται αξιόπιστα. Η συνεργασία μπορεί να είναι αποδοτική, εάν όλοι οι συμμετέχοντες ενεργούν με έντιμο τρόπο.

Ακόμα όμως και αν κάποια οντότητα συμπεριφέρεται αξιόπιστα και έχει κερδίσει την εμπιστοσύνη των υπόλοιπων οντοτήτων του δικτύου, μπορεί να αλλάξει συμπεριφορά και να μετατραπεί σε κακόβουλη, πιθανόν γιατί άλλαξαν τα συμφέροντά της και τα οφέλη που θα αποκομίσει από μια τέτοια συμπεριφορά θα είναι μεγαλύτερα απ' ότι ήταν στην προηγούμενη κατάσταση, ή γιατί πολύ απλά η οντότητα αυτή ήταν από πάντα κακόβουλη, και περίμενε να ενεργήσει όταν έκρινε εκείνη ότι οι συνθήκες ήταν κατάλληλες. Έχοντας αυτό κατά νου μπορούμε να πούμε ότι τελικά, κανένα μοντέλο εμπιστοσύνης δεν μπορεί να εγγυηθεί ότι η εμπιστοσύνη που εκχωρείται στα μέλη του δικτύου στο οποίο εφαρμόζεται είναι και αυτή που πραγματικά τους αντιστοιχεί κάθε στιγμή. Παρ' όλ' αυτά, σε ένα εχθρικό περιβάλλον όπου η εμπιστοσύνη είναι μικρή, το κέρδος που θα προκύψει από μια επιτυχημένη συνεργασία και το οποίο υπερβαίνει κατά πολύ τη ζημία που θα προκύψει εάν η συνεργασία αυτή αποτύχει, θα είναι εκείνο που τελικά θα ωθήσει τις οντότητες να συνεργαστούν και προοδευτικά να αναπτύξουν σχέσεις εμπιστοσύνης μεταξύ τους.

Μοντέλα Επιθέσεων / Μοντέλα Εμπιστοσύνης	Αυτο-προώθηση	Κακολόγηση	Αντιφατική συμπεριφορά	On-off	Συνωμοσία	Sybil	Αθώωση
Marsh	0	0	0	2	0	3	3
Levien - Aiken	0	3	0	2	2	1	1
PGP	0	2	0	3	3	3	3
Maurer	0	1	0	1	1	3	3
Reiter - Stubblebine	0	1	0	1	1	0	0
Jøsang	1	2	0	2	2	3	3
eBay	0	1	2	2	3	0	0
NICE	0	2	0	1	3	2	3
Abdul-Rahman - Hailes	0	3	3	3	3	3	3
EigenTrust	0	1	0	1	2	0	1
Poblano	3	3	0	3	3	0	0
Wang - Vassileva	0	2	3	2	3	3	3
Sun et al.	0	1	2	0	2	3	3
TrustMe	0	0	0	0	0	0	0
Theodorakopoulos - Baras	0	0	0	0	2	3	3
Regret	0	1	1	1	1	3	3
TwoHop	0	0	0	0	0	1	0
Prasad et al.	0	3	0	3	2	3	3

Πίνακας 3: Ποιοτική αξιολόγηση των μοντέλων εμπιστοσύνης σε σχέση με την ανθεκτικότητά τους στις επιθέσεις

Βιβλιογραφία

1. Lewis, J. D. and Weigert, A. J. Trust as a social reality. Social Forces, 1985, 63(4): 967-985.
2. Golembiewski, R. T. and McConkie, M. The Centrality of Interpersonal Trust in Group Processes. In: Cooper, Cary L. (Ed), Theories of Group Processes, New York: Wiley, 1975, 7: 131–185.
3. Luhmann, N. Trust and Power. Chichester: Wiley, 1979.
4. Lagenspetz, O. Legitimacy and Trust. Philosophical Investigations, 1992, 15(1): 1–21.
5. Marsh, S. Formalising Trust as a Computational Concept. PhD Thesis, Department of Mathematics and Computer Science, University of Stirling, 1994.
6. Lewicki, R. J. and Bunker, B. B. Trust in relationships: A model of development and decline. In: B. B. Bunker & J. Z. Rubin (Eds), Conflict, cooperation and justice, San Francisco: Jossey-Bass, 1995, 133-173.
7. Garfinkel, H. Studies in ethnomethodology. Englewood Cliffs, NJ: Prentice-Hall, 1967.
8. Lewis, J. D. and Weigert, A. J. Social atomism, holism, and trust. The Sociological Quarterly, 1985, 216(4): 455-471.
9. Shapiro, S. P. The social control of impersonal trust. American Journal of Sociology, 1987, 93(3): 623-658.
10. Erikson, E. H. Identity: Youth and crisis. New York: W. W. Norton, 1968.
11. Deutsch, M. The resolution of conflict: Constructive and destructive processes. New Haven, CN: Yale University Press, 1973.
12. Holmes, J. G. Trust and the appraisal process in Close Relationships. In: Jones, W. H. & Perlman, D. (Eds), Advances in personal relationships, London: Jessica Kingsley, 1991, 2: 57-104.
13. Williamson, O. E. Calculativeness, trust, and economic organization. Journal of Law and Economics, 1993, 34: 453-502.
14. Bateson, P. The Biological Evolution of Cooperation and Trust. In Gambetta, Diego (Ed.), Trust: Making a breaking cooperative relations, Oxford: Blackwell, 1990, 2: 14–30.
15. Deutsch, M. Cooperation and Trust: Some Theoretical Notes. In: Jones, M. R. (Ed), Nebraska Symposium on Motivation, Nebraska University Press, 1962.
16. Hart, D. M., Anderson, S. D. and Cohen, P. R. Envelopes as a Vehicle for Improving the Efficiency of Plan Execution. Tech. rept. COINS 90-21, University of Massachusetts at Amherst, Department of Computing and Information Science, 1990.
17. Gambetta, D. Mafia: The Price of Distrust. In: Gambetta, Diego (Ed), Trust: Making a breaking cooperative relations, Oxford: Blackwell, 1990, 10: 158–176.
18. Boon, S. D. and Holmes, J. G. The dynamics of interpersonal trust: resolving uncertainty in the face of risk. In: Hinde, Robert A. & Groebel, Jo (Eds), Cooperation and Prosocial Behaviour, Cambridge University Press, 1991, 190–211.
19. Good, D. Individuals, Interpersonal Relations, and Trust. In: Gambetta, Diego (Ed), Trust: Making a breaking cooperative relations, Oxford: Blackwell, 1990, 3:31–48.
20. Marsh, S. Trust and Reliance in Multi-Agent Systems: A Preliminary Report. In: MAAMAW'92, 4th European Workshop on Modeling Autonomous Agents in a Multi-Agent World, Rome, 1992.
21. Yamamoto, Y. A Morality Based on Trust: Some Reflections on Japanese Morality. Philosophy East and West, 1990, XL(4): 451–469.
22. Dunn, J. The concept of 'trust' in the politics of John Locke. In: Rorty, Richard, Schneewind, J. B. & Skinner, Quentin (Eds), Philosophy in History, Cambridge University Press, 1984, 12: 279–301.

23. McKnight, D. H. and Chervany, N. L. The meanings of trust. MISRC Working Paper Series, Technical Report 94-04, arlson School of Management, University of Minnesota, 1996.
24. Fishbein, M. and Ajzen, I. Belief, attitude, intention and behavior: An introduction to theory and research. Reading, MA: Addison-Wesley, 1975.
25. Hertzberg, L. On the Attitude of Trust. Inquiry, 1988, 31(3): 307–322.
26. Shaw, M. E. Group Dynamics: The Psychology of Small Group Behaviour (3rd Edition). New York: McGraw-Hill, 1981.
27. Brown, R. Intergroup Conflict and Cooperation. In: Group Processes: Dynamics within and between groups, Oxford: Blackwell, 1988, 7: 192–220.
28. Argyle, M. Cooperation: The Basis of Sociability. London: Routledge, 1991.
29. Sun, Y., Han, Z., Yu, W., and Ray Liu, K. J. A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks, In Proceeding of the 27th Conference on Computer Communications (INFOCOM' 06), Barcelona, Spain, April 2006.
30. Gambetta, D. Can we Trust Trust? In: Gambetta, Diego (Ed), Trust: Making a breaking cooperative relations, Oxford: Blackwell, 1990, 13: 213–237.
31. Levien, R. and Aiken, A. Attack resistant trust metrics for public key certification. In 7th USENIX Security Symposium, San Antonio, Texas, January 1998.
32. Abdul-Rahman, A. The PGP Trust Model. EDI-Forum: The Journal of Electronic Commerce, 1997, 10(3): 27-31.
33. Zimmermann, P. The Official PGP User's Guide. MIT Press, 1995.
34. Maurer, U. Modelling a public-key infrastructure. Fourth European Symposium on Research in Computer Security (ESORICS 96), September 1996, 324-350.
35. Reiter, M. K. and Stubblebine, S. G. Authentication metric analysis and design. ACM Transactions on Information and System Security (TISSEC), 1999, 2: 138–158.
36. Jøsang, A. An algebra for assessing trust in certification chains. In Proceedings of the Network and Distributed Systems Security (NDSS'99) Symposium, 1999.
37. The Feedback Forum. eBay. http://pages.ebay.com/services/forum/feedback.html.
38. Sabater, J. and Sierra, C. Review on Computational Trust and Reputation Models. Artificial Intelligence Review, Springer, 2005, 24: 33–60.
39. Cornelli, F., Damiani, E., di Vimercati, S. D. C., Paraboschi, S., and Samarati, P. Implementing a reputation-aware gnutella servent. In International Workshop on Peer-to-Peer Computing, 2002.
40. Sherwood, R., Lee, S., and Bhattacharjee, B. Cooperative peer groups in NICE. Computer Networks Science Direct, 2005, 50(4): 523-44.
41. Abdul-Rahman, A. and Hailes, S. A Distributed Trust Model. In Proceedings of the New Security Paradigms Workshop, ACM Press, 1997, 48-60.
42. Kamvar, S. D., Schlosser, M. T., and Garcia-Molina, H. The EigenTrust algorithm for reputation management in p2p networks. Proc. WWW2003, 2003, 640–651.
43. Chen, R. and Yeager, W. Poblano: a Distributed Trust Model for Peer-to-Peer Networks. Technical Report, Sun Microsystems, Inc., 2003.
44. Wang, Y. and Vassileva, J. Bayesian network trust model in peer-to-peer networks. In Proceedings of the 2nd Int'l Workshop on Agents and Peer-to-Peer Computing, Berlin: Springer-Verlag, 2004, 23-34.
45. Heckerman, D. A Tutorial on Learning with Bayesian Networks. Microsoft Research report MSR-TR-95-06, 1995.
46. Singh, A. and Liu, L. TrustMe: Anonymous Management of Trust Relationships in Decentralized P2P Networks. In Proceedings of the 3rd IEEE Conf. Peer-to-Peer Computing, IEEE CS Press, 2003, 142-149.

47. Theodorakopoulos, G. and Baras, J. S. On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks. IEEE Journal on Selected Areas in Communications, February 2006, 24(2): 318-328.
48. Sabater, J. and Sierra, C. Reputation and social network analysis in multi-agent systems. In Proceedings of the first international joint conference on Autonomous agents and multiagent systems New York (AAMAS '02), NY: ACM Press, 2002, 475-482.
49. Glynos, D., Argyroudis, P. G., Douligeris, C. and O'Mahony, D. TwoHop: Metric-Based Trust Evaluation for Peer-to-Peer Collaboration Environments. In Proceedings of the Global Communications Conference New Orleans (GLOBECOM 2008), LA, IEEE, 2008, 1979-1984.
50. RVVSV Prasad, Vegi Srinivas, V. Valli Kumari, and KVSVN Raju. An Effective Calculation of Reputation in P2P Networks. Journal of Networks, Jul 2009, 4(5): 332-342.
51. Theodorakopoulos, G. and Baras, J.S. A Testbed for Comparing Trust Computation Algorithms. In Proceedings of the 25th Army Science Conference, 2006.
52. Hoffman, K., Zage, D. and Nita-Rotaru, C. A Survey of Attack and Defense Techniques for Reputation Systems. ACM Computing Surveys, December 2009, 42(1): 1-31.
53. Perrone, L. F. and Nelson, S. C. A Study of On-Off Attack Models for Wireless Ad Hoc Networks. First IEEE International Workshop on Operator-Assisted (Wireless Mesh) Community Networks (OpComm 2006). Berlin, Germany, 2006.
54. Sun, Y., Han, Z. and Liu, K. Defense of trust management vulnerabilities in distributed networks. IEEE Communications Magazine, 2008, 46(2): 112–119.
55. Douceur, J. R. The Sybil Attack. Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS), 2002.
56. Rotter, J. B. A new scale for the measurement of interpersonal trust. Journal of Personality, 1967, 35(4): 651-665.
57. Friedman, E. J. and Resnick, P. The social cost of cheap pseudonyms. Economics and Management Strategy, 2001, 10(2): 173–199.
58. Li Xiong, Ling Liu, PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. IEEE Transactions on Knowledge and Data Engineering, July 2004, 16(7): 843-857.
59. Chen Ding, Chen Yueguo, and Cheng Weiwei, A Survey Study on Trust Management in P2P Systems. Technical Report, National University of Singapore, Department of Computer Science, School of Computing, 2009.
60. Yu, B. and Singh, M. P. Detecting deception in reputation management. In Proceedings of the second international joint conference on Autonomous agents and multiagent systems, ACM Press, 2003, 73–80.
61. Aberer, K. and Despotovic, Z. Managing Trust in a Peer-2-Peer Information System. In Proceedings of the 10th International Conference on Information and Knowledge Management (2001 ACM CIKM), ACM Press, 2001, 310–317.
62. Abdul-Rahman, A. and Hailes, S. Supporting Trust in Virtual Communities. In Proceedings of 33rd Hawaii International Conference on System Sciences (HICSS 33), IEEE CS Press, 2000, 6: 6007.
63. Twigg, A. and Dimmock, N. Attack-Resistance of Computational Trust Models. Twelfth International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2003, 275.
64. Marchesini, J. and Smith, S. W. Modeling Public Key Infrastructures in the Real World. Public Key Infrastructure: EuroPKI 2005, Springer-Verlag LNCS, June 2005.
65. Ford Jr., L.R. and Fulkerson, D.R. Maximal Flow Through a Network. Canadian Journal of. Mathematics, 1956, 8: 399 404.

66. Fung, C., Zhang, J., Aib, I. and Boutaba, R. Robust and scalable trust management for collaborative intrusion detection. In Proceedings of the 11th IFIP/IEEE International Symposium on Integrated Network Management (IM), 2009.
67. Dellarocas, C. The digitalization of Word-Of-Mouth: Promise and Challenges of Online Reputation Mechanisms. Management Science, 2003.
68. Resnick, P. and Zeckhauser, R. Trust among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System. Working paper for the NBER Workshop on Empirical Studies of Electronic commerce, 2000.
69. Golbeck, J. A. Computing and applying trust in web-based social networks. Dissertation Submitted to the Faculty of the Graduate School of the University of Maryland, College Park in partial fulfillment of the requirements for the degree of Doctor of Philosophy, 2005.
70. Resnick, P., Zeckhauser, R., Friedman, E. and Kuwabara, K. Reputation Systems: Facilitating Trust in Internet Interactions. Communications of the ACM, 2006, 43(12): 45-48.
71. Jun-Won Ho, Distributed Detection of Node Capture Attacks in Wireless Sensor Networks. In: Smart Wireless Sensor Networks, Hoang Duc Chinh and Yen Kheng Tan (Eds), Croatia: InTech, 2010, 345-360.
72. Huaizhi Li, Mukesh Singhal, Trust Management in Distributed Systems. IEEE Computer, Feb. 2007, 40(2): 45-53.
73. Vishwas Patil and Shyamasundar, R. K. Trust management for e-transactions. Sadhana, April/June 2005, 30(2-3): 141–158.
74. Weiler, N. Security in Peer-to-Peer Networks, Zürcher Hochschule Winterthur, 2004.
75. Tyrone Grandison, Trust Management Tools. In: Trust in E-Services: Technologies, Practices and Challenges, Song, R., Korba L. and Yee, G. (Eds), Idea Group Publishing, Hershey, USA, 2007, 208.
76. Xiaoqing Zheng, Zhaohui Wu, Huajun Chen, and Mao, Y. A Scalable Probabilistic Approach to Trust Evaluation. In Fourth International Conference on Trust Management (iTrust'06), Pisa, Italy, 2006, 423-438.