A Survey of Reputation & Trust Management In P2P Systems

Σταθοπούλου Ευγενία
Γεωργούλας Κωνσταντίνος

06/02/06

0. Περίληψη

Τα peer-to-peer (P2P) συστήματα, στα οποία όλοι οι κόμβοι είναι ισότιμοι και λειτουργούν και σαν servers και σαν clients, αποκτούν όλο και περισσότερη προσοχή τόσο απο ερευνικής πλευράς όσο και απο χρηστικής. Η ερευνική πλευρά, με την οποία ασχολείται αυτή η εργασία, έχει ως σκοπό την εύρεση αξιόπιστων τεχνικών διαχείρισης ασφάλειας αυτών των συστημάτων. Στις περισσότερες εφαρμογές των P2P συστημάτων προσφέρεται στους χρήστες , *peers,* η ιδιότητα της ανωνυμίας με την οποία προστατεύονται απο άμεσες επιθέσεις πιθανών «κακών», *malicious,* κόμβων. Δυστυχώς, η ιδιότητα της ανωνυμίας αποτελεί τς περισσότερες φορές τροχοπέδι των «κακών» peers, οι οποίοι με την βοήθεια της, προστατέυονται οι ίδοι εφόσον δεν εκτίθεται η ταυτότητά τους στο δίκτυο, οπότε μπορούν να διαμοιράσουν επιβλαβή πληροφορία π.χ. Viruses, Trojan Horses, κ.α.. Για την αντιμετώπιση τέτοιων περιπτώσεων έχουν προταθεί αρκετά συστήματα διαχείρισης ασφάλειας τωνP2P συστημάτων, τα οποία στηρίζονται στη δημιουργία εμπιστοσύνης μεταξύ των κόμβων του δικτύου. Τα συστήματα αυτά εκμεταλλεύονται την εμπιστοσύνη που έχει δημιουργηθεί ανάμεσα σε δύο peers του δικτύου, η οποία προέρχεται είτε απο άμεση συναλλαγή των κόμβων, είτε από την φήμη που αποκτά ένας κόμβος μετά το πέρας επιτυχών συναλλαγών με άλλους κόμβους. Η εργασία αυτή παρουσιάζει μερικά από τα πιο σύγχρονα και πιο σημαντικά, κατά την γνώμη μας, συστήματα διαχείρισης εμπιστοσύνης και επιχειρεί μια αξιολόγηση τους, με βάση κάποια σημαντικά χαρακτηριστικά των P2P συστημάτων.

1. ΕΙΣΑΓΩΓΗ

Ένα peer-to-peer (*P2P*) δίκτυο είναι ένα δίκτυο υπολογιστών, το οποίο δεν έχει αυστηρά καθορισμένους κόμβους που παίζουν το ρόλο του server και του client. Στα P2P δίκτυα οι κόμβοι λειτουργούν και σαν clients και σαν servers. Αυτό έχει σαν αποτέλεσμα όλοι οι κόμβοι να θεωρούνται ισότιμοι στο δίκτυο.

Η δομή και η οργάνωση ενός P2P δικτύου δίνει τη δυνατότητα στους κόμβους να συνεργάζονται και να μοιράζουν τους πόρους τους με ευκολία και χωρίς περιορισμούς. Υπάρχουν διάφορες κατηγορίες εφαρμογών που υλοποιούνται σε ένα peer-to-peer δίκτυο και εκμεταλλεύονται την παραπάνω ιδιότητα. Κάποια παραδείγματα τέτοιων εφαρμογών είναι το file-sharing, ο distributed computation και το instant messaging. Με τον όρο file sharing εννοούμε το διαμοιρασμό/ ανταλλαγή αρχείων μεταξύ των κόμβων που ανήκουν στο σύστημα. Αντιπροσωπευτικές εφαρμογές file sharing αποτελούν το Gnutella, το KaZaA, το Napster κ.α. Στο distributed processing αντί για αρχεία οι κόμβοι διαμοιράζουν την υπολογιτική τους δύναμη (πόρους π.χ. δίσκο, μνήμη). Τέλος στο instant messaging οι χρήστες μπορούν να ανταλλάξουν εκτός από αρχεία, κείμενο, βίντεο και φωνητικά μηνύματα.

Οι παραπάνω P2P εφαρμογες μπορούν να χωριστούν σε δύο κατηγορίες:τις κεντρικοποιημένες *(centralized)* και τις μη-κεντρικοποιημένες *(decentralized)*. Η διαφορά μεταξύ κεντριοποιημένων και μη-κεντρικοποιημένων εφαρμογών έγκειται στο γεγονός ότι στις κεντρικοποιημένες, υπάρχει ένας ή περισσότεροι κεντρικοί κόμβοι (*servers*) με τους οποίους συνδέονται όλοι οι κόμβοι για να εξυπηρετηθούν. Οι servers αποθηκεύουν πληροφορία για όλους τους κόμβους του δικτύου και εξυπηρετούν τους υπόλοιπους κόμβους παρέχοντας τους πληροπφορία για το που θα βρουν το αντικείμενο (π.χ. αρχείο) που αναζητούν. Είναι προφανές ότι σε αυτούς τους κόμβους παρατηρείται μεγάλος φόρτος του δικτύου, εφόσον όλα τα μηνύματα καταλήγουν σε αυτούς. Στις μη-κεντρικοποιημένες εφαρμογές, απουσιάζει ένα κεντρικό σημείο στο οποίο καταλήγουν όλες οι αιτήσεις αλλά και από το οποίο ασκείται κεντρικός έλεγχος.

Κοινό χαρακτηριστικό όλων αυτών των εφαρμογών που υλοποιούνται σε ένα P2P δίκτυο είναι η *ανωνυμία* των κόμβων. Με τον όρο ανωνυμία εννοούμε την ιδιότητα του συστήματος να αποκρύπτει τα αναγνωριστικα χαρακτηριστικά των κόμβων κατα τη διάρκεια των συναλλαγών [10], [11]. Εκμεταλλευόμενοι αυτή την ανωνυμία, οι κακοί χρήστες προσπαθούν να προωθήσουν λογισμικό-αρχεία που παραπλανεί και θέτει σε κίνδυνο την ασφάλεια ενός κόμβου και κατ' επέκταση την ασφάλεια του συστήματος (viruses, Trojan horses, spam). Για να αντιμετωπιστεί το παραπάνω πρόβλημα είναι απαραίτητη η εισαγωγή της έννοιας της εμπιστοσύνης (*trust*). Το ποσοστό της εμπιστοσύνης που δείχνει ένας κόμβος σε ένα άλλο αντιπροσωπεύει/απεικονίζει το κατά πόσο η συναλλαγή τους θα είναι σωστή(π.χ. γίνεται download το σωστό αρχείο) και ολοκληρωμένη (π.χ. ο κόμβος παραμένει on-line μέχρι να

ολοκληρωθεί η συναλλαγή). Έτσι λοιπόν με βάση την εμπιστοσύνη που δείχνει ένας κόμβος σε κάποιον άλλο αποφασίζει αν θα πραγματοποιήσει μια συναλλαγη μαζί του ή όχι. Με τον τρόπο αυτό κόμβοι οι οποίοι παρουσιάζουν συμπεριφορά η οποίοα θ'ετει σε κίνδυνο το σύστημα αποκλείονται απ' αυτό, αφου χάνεται η εμπιστοσύνη προς αυτούς.

Σημαντικός παράγοντας για τον υπολογισμό της εμπιστοσύνης είναι η φήμη που έχει κόμβος στο δίκτυο. Η φήμη είναι η "άποψη που έχει ένας peer για κάποιον άλλο" και διαμορφώνεται/ενημερώνεται τόσο από τις προηγούμενες άμεσες συναλλαγές τους όσο και από την πληροφορία που παρέχεται από άλλους κόμβους του δικτύου και η οποία σχετίζεται με παλιότερες συναλλαγές των κόμβων αυτών με τον συγκεκριμένο peer.[5]

Η αναφορά αυτή έχει σαν σκοπό την παρουσίαση διαφόρων μηχανισμών διαχείρισης της εμπιστοσύνης (trust management). Στο κεφάλαιο *2* παρουσιάζεται ο διαχωρισμός των μηχανισμών σε δύο κατηγορίες: reputation-based trust management και social network-based trust management και περιγράφονται κάποια αντιπροσωπευτικά μοντέλα αυτών των κατηγοριών. Στο κεφάλαιο *3* γίνεται συγκριτική μελέτη των μοντέλων που παρουσιάστηκαν. Τέλος στο κεφάλαιο *4* παρατίθενται τα συμπεράσματα που προέκυψαν μέσω αυτής της μελέτης.

2. ΤΕΧΝΙΚΕΣ TRUST MANAGEMENT

Υπάρχουν αρκετές τεχνικές με σκοπό την διαχείρηση της αξιοπιστίας σε ένα P2P σύστημα, οι οποίες στηρίζονται στον υπολογισμό της φήμης των κόμβων (peers) που το αποτελούν. Οι τεχνικές αυτές μπορούν να κατηγοριοποιηθούν σε δυο βασικές κατηγορίες, σύμφωνα με το είδος της πληροφορίας που χρησιμοποιείται για τον υπολογισμό της φήμης.

Στην πρώτη κατηγορία λαμβάνεται υπόψην τόσο η υποκειμενική άποψη, τοπική πληροφορία, που έχει ο κόμβος ο οποίος κάνει την αξιολόγηση, όσο και η καθολική άποψη, άποψη όλων των κόμβων, του δικτύου για την φήμη του υπο-αξιολόγηση κόμβου. Οι τεχνικές που παρουσιάζονται παρακάτω γι'αυτή την κατηγορία είναι: *XREP*, *P-Grid*, *NICE* και *Framework using Currency*.

Στη δεύτερη κατηγορία λαμβάνονται υπόψη οι κοινωνικοί δεσμοί, δεσμοί εμπιστοσύνης, που έχουν αναπτυχθεί ανάμεσα στα μέλη του δικτύου. Οι δεσμοί αυτοί μπορεί να είναι δεσμοί φιλίας, συνεργασίας, αμοιβαίας υποστήριξης, ομοιότητας κ.α., οι οποίοι ουσιαστικά

αντιπροσωπεύουν δεσμούς εμπιστοσύνης μεταξύ των κόμβων, και αναπαριστούνται με την δημιουργία ενός κοινωνικού δικτύου [6]. Με βάση την πληροφορία που εξάγεται απο ένα τέτοιο κοινωνικό δίκτυο υπολογίζεται η αξιοπιστία ενός κόμβου. Αντιπρόσωποι αυτής της κατηγορίας, οι οποίοι και παρουσιάζονται παρακάτω είναι: *REGRET* και *NodeRanking*.

2.1 XREP

Το μοντέλο XREP, που παρουσιάζεται στο [1], προτείνει για τον υπολογισμό της αξιοπιστίας ενός εγγράφου, που πρόκειται να κάνει download ένας χρήστης ενός P2P συστήματος, το συνδυασμό της φήμης (reputation) τόσο του *servent* (αυτός που παρέχει το resource) όσο και του *resource* (εγγράφου) που πρόκειται να ληφθεί. Ονομάζουμε servent κάθε κόμβο του συστήματος, αφου σε ένα P2P σύστημα οι κόμβοι λειτουργούν τόσο σαν server όσο και σαν client.

Έτσι λοιπόν σε κάθε servent αποδίδεται ένα *servent_id* (αναγνωριστικό) το οποίο είναι μοναδικό και προσδιορίζει κάθε servent. Ομοίως σε κάθε έγγραφο αποδίδεται ένα *resource_id* το οποίο προκύπτει μέσω hash function στο περιεχόμενο του εγγράφου.

Η προσέγγιση και η αντιμετώπιση του θέματος του trust από το XREP γίνεται με τη βοήθεια ενός είδους ψηφοφορίας η οποία πραγματοποιείται από τους κόμβους του δικτύου. Στη ψηφοφορία αυτή κάθε κόμβος του δικτύου εκφράζει μέσω της ψήφου του την άποψη για ένα συγκεκριμένο έγγραφο αλλά και για τον servent που το κατέχει. Η άποψη κάθε κόμβου είναι απόρροια των συναλλαγών/συνεργασιών (*interactions*) που είχε ο κόμβος τόσο με τον servent για τον οποίο ερωτάται όσο και με το resource. Με τον τρόπο αυτό μπορεί ο κάθε κόμβος να μεταβιβάσει στους υπόλοιπους την εμπειρία του από τις συνδιαλλαγές με άλλους κόμβους η άλλα resources.

Για να επιτευχθεί το παραπάνω κάθε peer διατηρεί δυο repositories: το *resource repository* και το *servent repository*. Το resource repository είναι ένας πίνακας που περιέχει όλα τα resource_id των resources με τα οποία ο peer έχει προηγούμενη εμπειρία. Σε κάθε resource_id αντιστοιχίζεται ένας δυαδικός αριθμός ο οποίος μπορεί να είναι είτε θετικός είτε αρνητικός. Η τιμή αυτή δηλώνει τη θετική ή την αρνητική άποψη του κόμβου για το συγκεκριμένο resource. Αντίστοιχα, το servent repository είναι ένας πίνακας με τα servent_id των κόμβων που γνωρίζει ο peer και δίπλα σε κάθε τέτοιο id υπάρχουν δύο αριθμοί: *num_plus* και *num_minus*, οι οποίοι δηλώνουν αντίστοιχα πόσα ήταν τα επιτυχή και πόσα τα ανεπιτυχή download του peer από τον συγκεκριμένο servent. Με βάση αυτές τις τιμές αποδίδονται οι ψήφοι από τον peer όποτε του ζητηθεί η άποψη για ένα έγγραφο ή για ένα servent.

Το XREP πρωτόκολλο για να οδηγήσει στο σωστό υπολογισμό του trust ενός κόμβου λαμβάνοντας υπόψη όλα τα προηγούμενα στοιχεία που κρατά κάθε κόμβος, χωρίζεται σε πέντε φάσεις: *resource searching*, *resource selection* & *vote polling*, *vote evaluation*, *best servent che*ck και *resource downloading*.

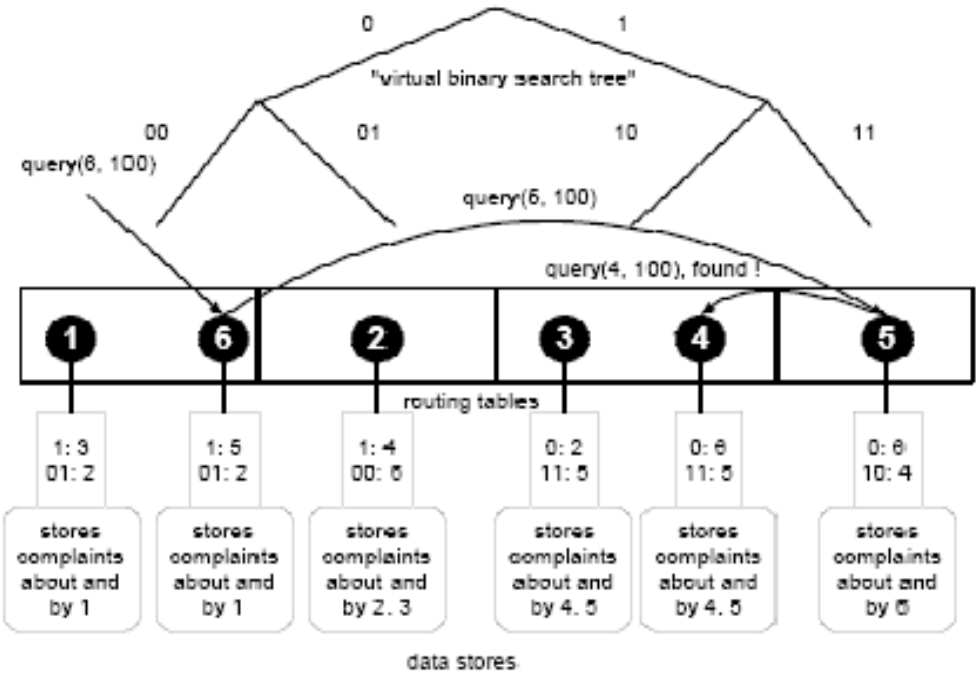
Στη πρώτη φάση ένας κόμβος στέλνει μια ερώτηση μέσω ενός *Query message* στους κόμβους του δικτύου και αυτό προωθείται με τη μέθοδο της πλημμύρας (*flooding*). Κάθε peer που διατηρεί έγγραφα με keyword ίδιο με αυτό της ερώτησης απαντά με ένα *Query Hit message* επιστρέφοντας το servent_id του, τα resource_id των εγγράφων που ικανοποιούν την ερώτηση και κάποια άλλα στοιχεία απαραίτητα για το download του εγγράφου (IP address & port number). Στη δεύτερη φάση υλοποίησης του XREP, ο κόμβος που έκανε την ερώτηση ζητά από τους υπόλοιπους peers του συστήματος να ψηφίσουν τόσο για το resource που θέλει να «κατεβάσει» όσο και για τους κόμβους οι οποίοι το κατέχουν. Έτσι λοιπόν στέλνει *Poll messages* στο δίκτυο ζητώντας τις ψήφους για ένα resource *r* αλλά και για τους servent $s_1, s_2, s_3, \ldots, s_n$ που το προσφέρουν. Σε κάθε Poll message υπάρχει pk_{poll} κλειδί που θα χρησιμοποιηθεί για την κρυπτογράφηση των απαντήσεων (ψήφων). Κάθε κόμβος που λαμβάνει μια Poll αίτηση, ελέγχει τα repositories του και απαντά στον peer με ένα *PollReply message* –κρυπτογραφημένο με το pk_{poll} κλειδί- στο οποίο περιέχονται οι ψήφοι και τα IP address & port number του κόμβου.

Στην τρίτη φάση ο κόμβος έχοντας λάβει όλες τις ψήφους πρέπει να λάβει μια απόφαση για πιο resource θα κάνει download. Για να γίνει όμως αυτό χρειάζεται πρώτα να γίνει επιβεβαίωση της αξιοπιστίας των ψήφων που έστειλαν οι διάφοροι peers. Έτσι λοιπόν, πρώτον αποκρυπτογραφεί τις ψήφους και εντοπιζει ποιοι κόμβοι έχουν πλαστογραφήσει και τους απορρίπτει. Δεύτερον, για να απομονώσει «κλίκες» από κακούς κόμβους, ομαδοποιεί τις ψήφους των κόμβων που έχουν το ίδιο net_id, υπολογίζει το μέσο όρο των ψήφων τους και τον λαμβάνει σαν την τελική ψηφο του cluster. Τρίτον, διαλέγει ένα σύνολο από κόμβους - ψηφοφόρους και τους ζητά να επιβεβαιώσουν την ψήφο τους. Στέλνει *True Vote message* και ο κάθε κόμβος απαντά με ένα *TrueVoteReply message*. Με βάση τις αξιόπιστες ψήφους στις οποίες έχει πλέον καταλήξει αποφασίζει πιο resource θα κάνει download.

Σε αυτό το σημείο θα πρέπει να αποφασιστεί από ποιον servent θα γίνει το download. Ο κόμβος με τη μεγαλύτερη φήμη ερωτάται αν κατέχει το συγκεκριμένο resource και αν η απάντηση είναι θετική ως τελευταίο βήμα πραγματοποιείται το download και ενημερώνονται τα repositories.

2.2 P-GRID

Στη συγκεκριμένη εργασία [2] παρουσιάζεται ένα ακόμη reputation-based πρωτόκολλο για τον υπολογισμό της αξιοπιστίας ενός κόμβου σε ένα P2P δίκτυο. Η reputation κάθε κόμβου προκύπτει από την ανάλυση των προηγούμενων συναλλάγων του με άλλους κόμβους του συστήματος. Έτσι λοιπόν θα μπορούσε κάθε peer να έχει μια εκτίμηση για τη φήμη ενός άλλου κόμβου αν ήταν σε θέση να βρεί στατιστικά στοιχεία για τις προηγούμενες συναλλαγές του κόμβου αυτού χρησιμοποιώντας μια μέθοδο εξόρυξης δεδομένων (*data mining*). Κάτι τέτοιο πετυχαίνεται με την τεχνική που προτείνεται χρησιμοποιώντας τη δομή του P-Grid, (*Σχήμα 1*), για την αποθήκευση των στατιστικών στοιχείων, που στη προκειμένη περίπτωση είναι complaints που εκφράζουν κάποιοι κόμβοι για τη συμπεριφορά κάποιου άλλου. Με τον όρο complaint εννοούμε μια εγγραφή δεδομένων που δηλώνει την αρνητική άποψη ενός κόμβου για τη συμπεριφορά ενός peer του συστήματος.



Σχήμα 1

Συγκεκριμένα η παραπάνω προσέγγιση προτείνει σαν τρόπο υπολογισμού της φήμης ενός peer p το γινόμενο $T_{(p)}$ των complaints που έχουν εκφράσει οι κόμβοι του δικτύου για τη συμπεριφορά του συγκεκριμένου peer επί τα complaints που έχει αναφέρει ο peer αυτός για όλους του υπόλοιπους κόμβους του δικτύου. Όσο πιο μεγάλο είναι το $T_{(p)}$, τόσο μικρότερη είναι και η αξιοπιστία του peer. Επειδή όμως η ανάκτηση των complaints που έχουν καταθέσει όλοι οι κόμβοι του συστήματος για ένα peer δεν είναι εύκολη υπόθεση και

περιορίζει πάρα πολύ τη scalability της μεθόδου κρίθηκε αναγκαία η αποθήκευση των complaints στη δομή του P-Grid.

Το P-Grid είναι ένα δυαδικό δέντρο του οποίου τα φύλλα είναι οι peers του δικτύου. Κάθε peer επομένως σχετίζεται με ένα συγκεκριμένο μονοπάτι του δέντρου. Σε κάθε κόμβο του δικτύου αποθηκεύεται ένα μέρος από το σύνολο των *complaints* που έχουν εκφράσει όλοι οι κόμβοι του P2P δικτύου. Η ανάθεση των complaints σε κόμβους δεν είναι καθόλου τυχαία. Τα complaints αποθηκεύονται στους κόμβούς των οποίων το path το οποίο τους αντιστοιχει, είναι prefix part του κλειδιου του κάθε complaint. Μάλιστα το κλειδί του complaint σχετίζεται με τον αριθμό του peer για τον οποίο εκδόθηκε. Επιπλέον κάθε κόμβος διατηρεί ένα routing table για να προωθεί ερωτήσεις που δέχεται σε άλλους κόμβους οι οποίοι είναι υπευθυνοι να απαντήσουν μιας και κρατουν τα κατάλληλα στοιχεία (complaints). Με τη βοήθεια δυο συναρτήσεων*: insert(a, k, u)* & *query(a, k)* μπορεί εύκολα κάθε κόμβος του συστήματος να εισάγει και να ανακτήσει ένα complaint για κάποιο peer του δικτύου.

Έτσι λοιπόν, όταν κάποιος θέλει να υπολογίσει την αξιοπιστία ενός peer του δικτύου το πρώτο που κάνει είναι να βρει όλα τα complaints που βρίσκονται αποθηκευμένα στο P-Grid. Αφού τα βρει θα είναι σε θέση να υπολογίσει την αξιοπιστία του συγκεκριμένου peer χρησιμοποιώντας τη συνάρτηση $T_{(p)}$ που αναφέρθηκε προηγουμένως. Για να μπορεί όμως αυτή η διαδικασία να οδηγήσει στο σωστό αποτέλεσμα χρειάζεται να ελεχθει η φερεγγυότητα των κόμβων που έχουν αποθηκευμένα τοπικά τα συγκεκριμένα complaints. Είναι απαραίτητο λοιπόν να γίνει ερώτηση γι' αυτούς τους κόμβους και να αναζητηθουν complaints που τους αφορούν. Αυτό όμως μπορεί να οδηγησει σε αναζήτηση ολόκληρου του δικτύου. Το φαινόμενο αυτό μπορεί να περιοριστεί λαμβάνοντας complaints από ένα μικρό σύνολο κόμβων r και ελέγχοντας αν κατέχουν ίδια δεδομένα για τον συγκεκριμένο κόμβο που ελεγχεται. Αν ισχύει κάτι τέτοιο δεν χρειάζεται να ερευνηθεί περαιτέρω η φερεγγυότητα του peer. Μετά από αυτό το βήμα μπορεί να γίνει χρήση της $T_{(p)}$ με τα complaints που ανακτήθηκαν από peers για τους οποίους είναι δεδομένη πλέον η αξιοπιστία τους.

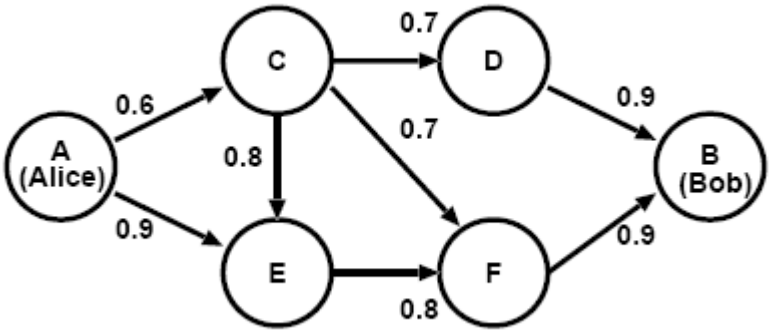
2.3 NICE

Στη συγκεκριμένη εργασία, [3], παρουσιάζεται μια τεχνική για την αποθήκευση πληροφορίας στους κόμβους η οποία βοηθά στον υπολογισμό της φήμης κάθε peer ενός δικτύου. Επίσης περιγράφεται και ο τρόπος με τον οποίο αξιοποιείται αυτή η πληροφορία από καθε κόμβο προκειμένου να λάβει μια απόφαση για την αξιοπιστία του peer με τον οποίο θα αλληλεπιδράσει. Όλα τα παραπάνω υλοποιούνται με τη βοήθεια του NICE. Το NICE είναι μια πλατφόρμα που χρησιμοποιείται για την υλοποίηση cooperative εφαρμογων. Cooperative

εφαρμογή ονομάζεται αυτή που αφιερώνει ένα υποσύνολο των πόρων της για χρήση από άλλους peers της εφαρμογής.

Η ιδιαιτερότητα αυτού του μοντέλου είναι ότι κάθε κόμβος κρατά λίγη πληροφορία και μάλιστα αυτή που έχει σχέση με το πόσο οι άλλοι κόμβοι του δικτύου τον εμπιστεύονται. Η πληροφορία αυτή είναι ένα σύνολο από cookies.*Cookie* είναι μια δήλωση υπογεγραμμένη από ένα κόμβο η οποία περιγράφει την ποιότητα μιας εξυπηρέτησης που έλαβε ο κόμβος αυτός από κάποιον άλλο κόμβο στο δίκτυο. Τα cookies εκδίδονται από αυτούς που εξυπηρετούνται και αποθηκεύονται σε αυτούς που παρείχαν την εξυπηρέτηση. Γίνεται λοιπόν αντιληπτό ότι κάθε κόμβος κρατά πληροφορία που είναι μόνο προς όφελος του και η οποία δηλώνει την αξιοπιστία των υπηρεσιών που προσφέρει. Αξίζει να σημειωθεί ότι επειδή οι κόμβοι για του οποίους εκδίδονται negative cookies δεν διατηρούν τοπικά αυτή την πληροφορία(αφού δεν τους οφελεί σε τίποτα), δημιουργείται η ανάγκη κάθε negative cookie να αποθηκεύεται τοπικά στον κόμβο από τον οποίο εκδόθηκε.

Για τον υπολογισμό της αξιοπιστίας των κόμβων προτείνεται η χρήση ενός κατευθυνόμενου γράφου *T* που λέγεται trust γράφος (*Σχήμα 2*). Στον γράφο αυτό κάθε κορυφή είναι ένας κόμβος του δικτύου και κάθε κατευθυνόμενη ακμή από ένα κόμβο A σε ένα κόμβο B, η τιμή της οποία δηλώνει πόσο ο A εμπιστεύεται τον B, γεγονός που εξαρτάται από τα cookies του A που κρατά ο B. Το μέτρο της εμπιστοσύνης αυτής προσδιορίζεται από την τιμή που υπάρχει στην κατευθυνόμενη αυτή ακμή. Αν όμως δεν υπάρχει άμεση σύνδεση μεταξύ δύο κόμβων τότε μπορεί να χρησιμοποιηθεί ένα μονοπάτι του γράφου για τον υπολογισμό της τιμής εμπιστοσύνης. Για την εύρεση του *strongest path* (ισχυρότερο μονοπατιού) απ' όλα τα δυνατά μονοπάτια ανάμεσα σε δύο κόμβους, επιλέγεται κάθε φορά η μετάβαση στον κόμβο με την μεγαλύτερη τιμή στην ακμή. Στο μονοπάτι αυτό αντιστοιχίζεται η μικρότερη τιμή ακμής που βρίσκεται στο μονοπάτι.



Σχήμα 2

Στο παραπάνω σχήμα με χρήση της τεχνικής του strongest path, ο κόμβος A θα επιλέξει το μονοπάτι AEFB και συγκεκριμένα την τιμή 0.8 για να εκτιμήσει την αξιοπιστία του κόμβου B.

Έτσι λοιπόν αν κάποια στιγμή ο Α θέλει κάποιους πόρους του Β θα πρέπει να του στείλει όλα τα cookies που κατέχει και έχουν την υπογραφή του Β. Αν όμως ο Α δεν έχει cookies του Β, δηλαδη δεν υπάρχει ακμή ΒΑ στο γράφο Τ, τότε ο Α ψάχνει να βρεί άλλους κόμβους του οποίους εμπιστεύεται και οι οποίοι έχουν cookies του Β. Μόλις τελειώσει η αναζήτηση, ο Α είναι σε θέση να παρουσιάσει στον Β ένα σύνολο από κατευθυνόμενα μονοπάτια τα οποία ξεκινούν από τον Β και καταλήγουν στον Α. Έπειτα ο Β μπορεί να χρησιμοποιήσει την τεχνική πουπροαναφέρθε και να υπολογίσει την αξιοπιστία του Α.

Τέλος σημαντική βελτίωση αυτού του μοντέλου είναι η χρήση preference lists που κρατά κάθε κόμβος του δικτύου. Οι κόμβοι που διατηρεί κάθε peer σε μια τέτοια λίστα είναι ένα σύνολο από κόμβους με τους οποίους δεν έχει καμιά συναναλλαγή αλλά τους θεωρεί κόμβους αρκετά αξιόπιστους. Στη λίστα ενός peer Α τοποθετούνται οι κόμβοι ενός μονοπατιού από τον Α στον Β οι οποίοι έχουν αρκετα μεγάλες trust values.

2.4 Framework using Currency

Στο [4] παρουσιάζεται ένα framework για την διαχείριση της φήμης των κόμβων των P2P δικτύων, όπου όλοι οι κόμβοι θεωρείται ότι συμπεριφέρονται εγωιστκά προσπαθώντας να αυξήσουν τη δική τους φήμη. Οι κόμβοι δημιουργούν κοινότητες εμπιστοσύνης, (*trusted communities*), στις οποίες όλοι οι κόμβοι εμπιστεύονται ο ένας τον άλλον και συνεργάζονται για την αντιμετώπιση τόσο της εγωιστικής συμπεριφόρας των άλλων κόμβων όσο της πιθανής «κακής» συμπεριφοράς των κόμβων που έχει ως σκοπό την ανατροπή της αξιοπιστίας και της σταθερότητας του δικτύου.Οι συναλλαγές μεταξύ των κόμβων του δικτύου πραγματοποιούνται μέσα στα κοινωνικά πλαίσια της χρηματικής ανταμοιβής για την παροχή κάποιας υπηρεσίας. Για τον λόγο αυτό εισάγεται ένα είδους εικονικού νομίσματος (*virtual currency*), με το οποίο υπολογίζεται ο πλούτος κάθε κόμβου άρα και το ποσοστό της φήμης του.

Κάθε φορά που ένας κόμβος παρέχει υπηρεσία ανταμοίβεται με κάποιο εικονικό χρηματικό ποσό (αύξηση της φήμης του), ένω αυτός που εξυπηρετήται επιβαρύνεται (μείωση της φήμης του) για την κατανάλωση πόρων.

Ανάλογα με την κατηγορία της υπηρεσίας που παρέχει ένας κόμβος (π.χ. download μουσικών αρχείων κάποιου καλλιτέχνη) δημιουργούνται κοινότητες εμπιστοσύνης έτσι ώστε να μην ανήκουν στην ίδια κοινότητα κόμβοι που παρέχουν την ίδια κατηγορία υπηρεσίας. Με αυτόν τον τρόπο αποφεύγεται το φαινόμενο της εγωιστικής συμπεριφοράς μέσα στις κοινότητες και η ανάπτυξη εμπιστοσύνης μεταξύ τω μελών της. Κάθε κόμβος ανήκει το πολύ σε μία

κοινότητα. Ο μέσος όρος των τιμών της φήμης όλων των μελών μιας κοινότητας απεικονίζει τη φήμη της κοινότητας ως προς τους κόμβους που δεν ανήκουν σε αυτή. Η τιμή της φήμης ενός κόμβου, άρα και της κοινότητάς του κυμαίνεται απο –1 έως 1. Η τιμή αυτή αυξάνεται ή μειώνεται, μετά από μια θετική ή αρνητική συναλλαγή αντίστοιχα, ανάλογα με την τιμή της φήμης του κόμβου που εξυπηρετείται. Η τιμή αυτή μειώνεται με τον χρόνο όταν δεν παρέχονται υπηρεσίες απο τους κόμβους. Άρα σκοπός κάθε κόμβου είναι η συχνή εξυπηρέτηση κόμβων με μεγάλη φήμη.

Κάθε κόμβος διατηρεί τρία σύνολα στα οποία κατατάσει τους κόμβους: ***Good***, κόμβοι για τους οποίους έχει καλή άποψη , ***Bad***, κόμβοι για τους οποίους έχει κακή άποψη, και ***φ***, κόμβοι που δεν γνωρίζει. Επιπλέον κρατάει τοπικά πληροφορία για τη φήμη των κοινοτήτων τις οποίες γνωρίζει καθώς επίσης και για τα υπόλοιπα μέλη της δικιάς του κοινότητας. Η τιμή της φήμης αντιπροσωπεύει την υποκειμενική άποψη του κόμβου για τις άλλες κοινότητες αλλά και τους "*συναδέλφους*" του.

Για να ενταχθεί ένας κόμβος σε μια κοινότητα θα πρέπει κανένα μέλος της να μην τον έχει κατατάξει στο σύνολο *Bad* και επιπλεόν να έχει μεγαλύτερη φήμη απο οποιονδήποτε άλλο κόμβο της κοινότητας. Η έξωση ενός κόμβου απο την κοινότητα πραγματοποιείται όταν μειωθεί η φήμη του αρκετά ώστε να πλήττει την κοινότητα. Η μείωση της φήμης μπορεί να οφείλεται είτε σε κακή εξυπηρέτηση είτε σε μη εξυπηρέτηση για μεγάλο χρονικό διάστημα.

Η ενημέρωση των κόμβων για μια επιτυχή ή μη συναλλαγή είναι συνυφασμένη με την εγωιστική συμπεριφορά των κόμβων. Η διάδοση μιας επιτυχούς παροχής υπηρεσιών από έναν κόμβο προωθείται απο τον κόμβο που παρείχε την υπηρεσία σε ένα μικρό σύνολο κόμβων (μέλη της ομάδας του και κάποιους γειτονές του και γνωστούς του). Όταν κάποιος κόμβος λάβει μήνυμα επιτυχούς εξυπηρέτησης αυξάνει την τιμή της φήμης του εξυπηρετητή ανάλογα με την τιμή της φήμης του εξυπηρετούμενου. Όταν τα μηνύματα αυτά φτάσουν σε κόμβους που δεν ανήκουν στη κοινότητα του εξυπηρετητή, αυτοί αυξάνουν τη φήμη της κοινότητας του εξυπηρετητή αλλά δεν προωθούν περαιτερω το μήνυμα εξαιτίας της εγωιστικής τους συμπεριφοράς.

Εν αντιθέσει, η διάδοση μιας αποτυχημένης εξυπηρέτησης προωθείται απο τον εξυπηρετούμενο σε όσο το δυνατόν περισσότερους κόμβους, ακολουθώντας τη μέθοδο της πλημμύρας. Στην περίπτωση που ένας κόμβος λάβει μήνυμα "παραπόνου" (*complaint*) θα πρέπει να μειωθούν οι τιμές της φήμης και των δυο κόμβων που εμπλέκονται στο μήνυμα (εξυπηρετητής-κατηγορούμενος, εξυπηρετούμενος-κατήγορος). Η φήμη του εξυπηρετητή μειώνεται ανάλογα με τη φήμη του εξυπηρετητή, και αντίστοιχα η φήμη του εξυπηρετητή ανάλογα με την φήμη του εξυπηρετούμενου. Με αυτόν τον τρόπο αντιμετωπίζεται το φαινόμενο της σκόπιμης "συκοφαντίας" ενός κόμβου από κάποιον άλλον, ο οποίος είτε είναι εγωιστής είτε είναι «κακός».

Φυσικά, όπως και σε κάθε κοινωνικό σύνολο, τα μέλη της ίδιας ομάδας υποστηρίζονται και μεροληπτούν. Εάν, λοιπόν, ο παραλήπτης ενός μηνύματος παραπόνου ανήκει στην ίδια κοινότητα με κάποιον απο τους εμπλεκόμενους κόμβους, μεροληπτεί υπέρ του "συναδέλφου" του, μειώνοντας ελάχιστα τη φήμη του, ενώ μειώνει αρκετά τη φήμη της κοινότητας στην οποία ανήκει ο άλλος κόμβος. Εάν ο παραλήπτης ανήκει στην ίδια κοινότητα και με τους δύο κόμβους μειώνει την τιμή της φήμης τους ελάχιστα, θεωρώντας το γεγονός ατυχές δίνοντας ευκαιρία στους "συναδέλφους" του. Στην περίπτωση που η σύγκρουση συμφερόντων (μήνυμα παραπόνου) πραγματοποιείται ανάμεσα σε δυο κοινότητες, σε καμία απο τις οποίες δεν ανήκει ο παραλήπτης, μειώνει η φήμη και των δύο κοινοτήτων . Σε αντίθετη περίπτωση, όπου η σύγκρουση συμφερόντων πραγματοποιείται ανάμεσα σε μέλη της ίδιας κοινότητας στην οποία δεν ανήκει ο ίδιος, δεν πραγματοποιείται καμία ενημέρωση στη τιμή της φήμης.

2.5 REGRET

Στο REGRET, που παρουσιάζεται στο [5], η έννοια της φήμης (reputation) θεωρείται ως το αποτέλεσμα του συνδυασμού διαφορετικών ειδών πληροφορίας οι οποίες μπορούν να εξαχθούν από την κοινωνική δομή του συνόλου των κόμβων (peers). Για τον υπολογισμό της φήμης εισάγονται τρεις διαστάσεις απεικόνισης της πληροφορίας που μπορεί να παρέχεται για κάποιον κόμβο: η *ατομική διάσταση* (*individual dimension*), η *κοινωνική διάσταση* (*social dimension*) και η *οντολογική διάσταση* (*ontological dimension*).

Αρχικά θεωρείται ότι οι κόμβοι είναι χωρισμένοι σε σύνολα, τα οποία μπορούν να παρέχουν υπηρεσίες. Η αξιολόγηση κάποιου κόμβου πραγματοποιείται στα πλαίσια της υπηρεσίας που παρείχε σε κάποιον άλλο κόμβο. Όσο πιο καλές υπηρεσίες παρέχει κάποιος κόμβος τόσο μεγαλύτερη φήμη έχει. Η αξιολόγηση και η τελική απόδοση της φήμης απεικονίζει την υποκειμενική άποψη του κόμβου που πραγματοποιεί την αξιολόγηση και αποθηκεύεται τοπικά σε αυτόν.

Στην περίπτωση που ένας κόμβος βασίζεται στην δική του, προσωπική άποψη, για κάποιον κόμβο, άποψη που είναι απόρροια προσωπικής συναλλαγής μεταξύ αυτών των κόμβων, τότε ο υπολογισμός της φήμης χρησιμοποιεί την ατομική διάσταση της φήμης.

Στην περίπτωση που κατά την αξιολόγηση ενός κόμβου, εκτός από την προσωπική του άποψη, ο κόμβος που κάνει την αξιολόγηση αποφασίσει να λάβει υπόψη του και την άποψη του συνόλου στο οποίο ανήκει, γίνεται χρήση της κοινωνικής διάστασης. Η άποψη του συνόλου απαρτίζεται από την άποψη που έχουν όλα τα μέλη του συνόλου για τον κόμβο αυτό καθώς επίσης και την άποψη όλων των μελών για το σύνολο στο οποίο ανήκει ο κόμβος. Με

αυτόν τον τρόπο η φήμη αποτιμάται ως ο συνδυασμός των τριών παραπάνω επιμέρους αξιολογήσεων, δίνοντας ίσως μεγαλύτερη βαρύτητα σε όποια άποψη θεωρείται πιο σημαντική.

Άλλη μία πολύ σημαντική διάσταση που υπεισέρχεται στον υπολογισμό της φήμης, είναι η οντολογική διάσταση, η οποία βασίζεται στην οντολογική δομή που έχει σχεδιάσει κάθε κόμβος που αξιολογεί. Έτσι λοιπόν κάθε κόμβος καταλήγει στο τελικό αποτέλεσμα για τη φήμη ενός άλλου κόμβου συνεκτιμώντας όλες τις τιμές φήμης που έχουν αποδοθεί για κάποια χαρακτηριστικά του κόμβου αυτού, δηλ. για διαφορετικού είδους υπηρεσίες που παρέχει ο κόμβος αυτός. Οι τιμές φήμης για τις διαφορεικού είδους υποηρεσίες του κόμβου προκύπτουν μέσω της κοινωνικής διάστασης των πληροφοριών. Η οντολογική διάσταση υπεισέρχεται έπειτα στη συνεκτίμηση όλων αυτών των τιμών φήμης. Η οντολογική δομή που έχει δημιουργήσει ο κόμβος-εκτιμητής είναι αυτή που θα καθορίσει το τελικό αποτέλεσμα, αφου αυτή θα καθορίσει το πως θα συνεκτιμηθούν οι διάφοτρες τιμές φήμης. Συγκεκριμένα το πόσο θα επηρρεάσει κάθε επιμέρους φήμη, την τελική φήμη εξαρτάται, και μάλιστα είναι ανάλογη, της βαρύτητας που δίνει ο κόμβος-εκτιμητής στις διαφορετικού είδους υπηρεσίες που παρέχει ο προς εκτίμηση κόμβος.

2.6 NODE RANKING

Στο [6] παρουσιάζεται ένας διαφορετικός τρόπος εύρεσης της φήμης, ο οποίος να δεν βασίζεται σε μηχανισμούς feedback ώστε να αποφευχθεί η ανάμειξη των χρηστών. Σε προηγούμενα μοντέλα, όπως το [5], κάθε κόμβος εμπιστεύεται κάποιον άλλον με βάση την τιμή της φήμης που του έχει αποδώσει ο ίδιος ή τα μέλη της ομάδας του. Μια εναλλακτική λύση που προτείνεται εδώ βασίζεται στην ανάλυση της τοποθεσίας του κάθε κόμβου μέσα στο κοινωνικό δίκτυο.

Το *κοινωνικό δίκτυο* (*social network*) είναι μια αναπαράσταση των σχέσεων μεταξύ των κόμβων που ανήκουν σε μια κοινότητα. Άρα μπορεί να δημιουργηθούν μέσα στην ίδια την κοινότητα, κοινωνικά δίκτυα βασιζόμενα σε σχέσεις: φιλίας, αμοιβαίας υποστήριξης, συνεργασίας, ομοιότητας κ.α. Τα κοινωνικά δίκτυα αναπαρίστανται από κατευθυνόμενους γράφους, στους οποίους οι κόμβοι με την μεγαλύτερη πείρα (άρα και φήμη) έχουν μεγαλύτερη συνδεσιμότητα και μπορούν εύκολα να αναγνωριστούν αλλά και να προσπελαστούν από τους υπόλοιπους κόμβους. Με αυτόν τον τρόπο δημιουργούνται γράφοι όμοιοι με τους power-low graphs, όπου υπάρχουν πολλοί κόμβοι οι οποίοι έχουν μικρή συνδεσιμότητα και λίγοι με μεγάλη συνδεσιμότητα.

Ο NodeRanking αλγόριθμος εκτιμά τη φήμη των κόμβων της κοινότητας με βάση το κοινωνικό δίκτυο. Κάθε κόμβος συσχετίζεται με ένα *βαθμό κύρους* (*degree of authority*). Κατά την αρχικοποίηση όλοι οι κόμβοι έχουν τον ίδιο βαθμό κύρους. Με την εκτέλεση του αλγορίθμου ο βαθμός κύρους κάθε κόμβου δίνεται ως συνάρτηση του συνολικού βαθμού κύρους του δικτύου και του βαθμού των κόμβων που δείχνουν σε αυτόν. Πιο συγκεκριμένα ο αλγόριθμος υπολογισμού της φήμης των κόμβων υλοποιείται ως εξής:

Ξεκινώντας από κάποιον τυχαίο κόμβο, και ακολουθώντας τη στρατηγική του *τυχαίου περιπατητή* (*random walker*), επιλέγεται κάποιος γείτονας του κόμβου, στον οποίο προωθείται ένα μέρος του κύρους που αυτός διαθέτει. Ο βαθμός του κύρους κάθε κόμβου λοιπόν, προκύπτει προσθέτοντας στο κύρος που έχει ήδη ανατεθεί στον κόμβο αυτό από τα προηγούμενα περάσματα των random walkers (δηλ. προηγούμενη εκτέλεση του αλγορίθμου), το ποσοστό κύρους που προωθείται σ' αυτόν από τους κόμβους που δείχνουν σε αυτόν μέσω ενός νέου random path. Η διαδικασία αυτή συνεχίζεται μέχρις ότου το ποσοστό κύρους που μεταβιβάζεται στον κόμβο μετά από κάθε random walk είναι πολύ μικρό. Μετά το τέλος εκτέλεσης του αλγορίθμου, η φήμη κάθε κόμβου αναπαρίσταται με βάση το βαθμό κύρους που του έχει ανατεθεί από τον αλγόριθμο.

3. *ΣΥΓΚΡΙΣΕΙΣ*

Στο κεφάλαιο αυτό πραγματοποιείται αξιολόγηση των συστημάτων που παρουσιάστηκαν στο προηγούμενο κεφάλαιο. Η αξιολόγηση αυτή γίνεται με βάση:

1) γενική κατηγοριοποίηση των συστημάτων σε *κεντρικοποιημένα* (***centralized***) και *μη-κεντρικοποιημένα* (***decentralized***),

2) γενικά χαρακτηριστικά που εξαρτώνται εν μέρει από την παραπάνω κατηγοριοποίηση, όπως το κόστος (***bandwidth cost***, ***storage cost***) , ***scalability*** (*κλιμάκωση*) και ***reliability*** (*αξιοπιστία*) του κάθε συστήματος, και

3) με χαρακτηριστικά που εμφανίζονται στα συστήματα για τον υπολογισμό της φήμης και της αξιοπιστίας ενός κόμβου, όπως ***οι τιμές της φήμης*** και τις ***τιμές της αξιοπιστίας*** που υποστηρίζει κάθε σύστημα. Στο τέλος του κεφαλαίου παρατίθεται ο συνοπτικός πίνακας σύγκρισης.

1) Από τα συστήματα που παρουσιάστηκαν, όλα εκτός του P-Grid και του NodeRanking, ανήκουν στην κατηγορία των μη-κεντρικοποιημένων συστημάτων. Το P-Grid δεν είναι

τελείως μη-κεντρικοποιημένο διότι η πληροφορία της φήμης ενός κόμβου, που προκύπτει μέσα απο την καταχώρηση παραπόνων, *complaints*¸ διαμοιράζεται στους κόμβους του δικτύου με την εφαρμογή μιας *hash function*. Με αυτό τον τρόπο, οι κόμβοι δεν έχουν τον πλήρη έλεγχο των δεδομένων που έχουν δημιουργήσει, αλλά ο έλεγχος αυτός μεταβιβάζεται στους κόμβους που είναι υπεύθυνοι για την αποθήκευσή τους μετά την εφαρμογή της hash function. Στο NodeRanking απαιτείται η ύπαρξη ενός κεντρικού κόμβου ο οποίος αρχικά δημιουργεί ένα κοινωνικό σύνολο με την βοήθεια της πληροφορίας, που εξάγεται από κάθε κόμβο, σχετικά με τους κοινωνικούς δεσμούς που υπάρχουν ανάμεσα σε αυτόν και κάποιον άλλο κόμβο. Στη συνέχεια ο κεντρικός κόμβος, κατά την εκτέλεση του αλγορίθμου, υπολογίζει και αποθηκεύει την τιμή του κύρους κάθε κόμβου με βάση την οποία ξαναδημιουργεί το κοινωνικό δίκτυο, μετά το πέρας του αλγορίθμου.

2) Το κόστος αποτιμάται ως προς τις έννοιες του ***bandwidth cost*** και ***storage cost***, οι οποίες αντιστοιχούν στο ποσοστό κατανάλωσης bandwidth του δικτύου και στις απαιτήσεις του αποθηκευτικού χώρου, αντίστοιχα, που απαιτεί η λειτουργία του κάθε συστήματος.

Συγκρίνοντας τα συστήματα σε σχέση με το bandwidth cost τους, συμπεραίνουμε ότι το XREP παρουσιάζει το μεγαλύτερο. Αυτό οφείλεται στην αποστολή *Poll queries*, για την εύρεση της φήμης τόσο ενός resource όσο και του servent, αλλά και των *TrueVote*, τα οποία αποστέλλονται για επιβεβαίωση των ψήφων των κόμβων. Επιπλέον ως προς το storage cost το XREP απαιτεί την αποθήκευση στα repositories των resources και των servent, εγγραφών που απεικονίζουν προηγούμενες άμεσες συναλλαγές μεταξύ των κόμβων. Άρα το αποθηκευτικό κόστος είναι μικρό.

Στο P-Grid τόσο το bandwidth όσο και το storage cost είναι αρκετά μικρά. Τα μηνύματα προωθούνται ανάλογα με την πληροφορία των routing tables των n κόμβων κάνοντας «άλματα» οπότε ο αριθμός των μηνυμάτων είναι της τάξης του $O(\log n)$. Επιπλέον εφόσον αποθηκεύονται μόνο complaints, δηλαδή αρνητική φήμη, ο αποθηκευτικός χώρος που απαιτείται γι' αυτά είναι μικρός.

Στο μοντέλο NICE, το bandwidth cost δεν είναι πολύ μεγάλο διότι, αν και ακολουθεί ένα είδος πλημμύρας για την εύρεση του *strongest path* , στον υπολογισμό εισάγεται η έννοια της πιθανότητας – μεγαλύτερη πιθανότητα ισοδυναμεί μεγαλύτερη εμπιστοσύνη- οπότε η επιλογή του επόμενου κόμβου γίνεται με βάση τη πιθανότητα αυτή. Όσον αφορά το storage cost για το NICE απαιτείται η αποθήκευση τόσο θετικής όσο και αρνητικής πληροφορίας ως αποτέλεσμα των άμεσων συναλλαγών μεταξύ των κόμβων, άρα το κόστος δεν είναι πολύ μεγάλο.

Για το Framework using Currency το bandwidth cost του κυρίως οφείλεται στην περίπτωση που δημιουργηθεί κάποιο παράπονο (complaint), πληροφορία η οποία προωθείται σε όλο το δίκτυο ακολουθώντας την στρατηγική της πλημμύρας. Στην

περίπτωση επιτυχούς συναλλαγής τα μηνύματα περιορίζονται μόνο σε ένα μικρό αριθμό γειτόνων του κόμβου. Άρα θα μπορούσαμε να συμπεράνουμε ότι το bandwidth cost είναι αρκετά μεγάλο μόνο στην περίπτωση complaint. Το storage cost είναι σχετικά μικρό γιατί κάθε κόμβος αποθηκεύει πληροφορία σχετικά με την φήμη των μελών της ομάδας του, και τη φήμη κάποιων άλλων ομάδων που γνωρίζει.

Στο REGRET αποθηκεύεται σε κάθε κόμβο μικρό ποσοστό πληροφορίας, η οποία αφορά θετικές και αρνητικές τιμές της φήμης που αντιστοιχίζονται σε έναν κόμβο τόσο από αυτόν όσο και από τα μέλη της ομάδας του. Επιπλέον το bandwidth cost περιορίζεται στο, σχετικά, μικρό αριθμό των μηνυμάτων που ανταλλάσσονται μεταξύ των μελών της ομάδας.

Τέλος, το NodeRanking είναι το δεύτερο σε σειρά μοντέλο το οποίο έχει μεγάλο bandwidth cost που παρατηρείται στον κεντρικό κόμβο του δικτύου, εφόσον σε αυτόν καταλήγουν όλα τα τελικά, μετά την εφαρμογή του αλγορίθμου, authorities των κόμβων για την ανακατασκευή του κοινωνικού δικτύου. Όσον αφορά το storage cost, από την στιγμή που κάθε κόμβος κρατάει μόνο πληροφορία για το authority των κόμβων τους οποίους εμπιστεύεται (κόμβους στους οποίους καταλήγει ακμή με πηγή αυτόν), είναι προφανές ότι είναι πολύ μικρό.

Το ***scalability*** κάθε συστήματος είναι άρρηκτα συνδεδεμένο με την παράμετρο του bandwidth και του storage cost. Όπως αναφέρθηκε προηγουμένως, το XREP έχει πολύ μεγάλο bandwidth cost γεγονός που σημαίνει ότι δεν θα μπορούσε εύκολα να εφαρμοστεί σε ένα δίκτυο με μεγάλο αριθμό κόμβων. Επιπλέον και ο NodeRanking αλγόριθμος λόγω του γεγονότος ότι απαιτείται για την εφαρμογή του ένας κεντρικός κόμβος στον οποίο παρατηρείται μεγάλη κατανάλωση bandwidth, δεν θα μπορούσε εύκολα να εφαρμοστεί σε ένα μεγάλο P2P δίκτυο κόμβων. Σε αυτή τη περίπτωση ίσως να ήταν αναγκαία η εισαγωγή περισσοτέρων κεντρικών κόμβων, ώστε το σύστημα να ανταποκρίνεται πιο γρήγορα. Για όλα τα άλλα συστήματα η επέκτασή τους σε δίκτυα με πολλούς κόμβους είναι εφικτή. Από αυτά τα συστήματα αυτό που παρουσιάζει το μεγαλύτερο scalability είναι το Framework using Currency, το οποίο και δημιουργήθηκε για να υποστηρίζεται από P2P δίκτυα εξ' αρχής.

Το ***reliability*** των συστημάτων, που παρουσιάστηκαν σε αυτή την εργασία, ορίζεται στα πλαίσια του κατά πόσο το κάθε σύστημα λειτουργεί σωστά στην περίπτωση που ένας ή μια ομάδα κόμβων με «κακές» προθέσεις προσπαθήσουν, εκμεταλλευόμενοι του τρόπου λειτουργίας του, να το ανατρέψουν και να επικρατήσουν αυτοί.

Ας υποθέσουμε ότι στο XREP μια ομάδα peers με κακές προθέσεις προσπαθεί να πείσει κάποιον peer να προτιμήσει ένα μέλος της ομάδας τους δίνοντας σε αυτό όλες τις ψήφους τους. Το XREP αντιμετωπίζει μια τέτοια περίπτωση με το να ομαδοποιεί τις ψήφους που προέρχονται από κοινό net_id και να θεωρεί μία ψήφο με τιμή το

μέσο όρο τους. Επιπλέον το XREP αντιμετωπίζει χαρακτηριστικά παραδείγματα επιθέσεων όπως το Pseudospoofing, ID steal και Shilling [1].

Στο P-Grid σύστημα, ας υποθέσουμε ότι ένας ή μια ομάδα peers με κακές προθέσεις παρέχουν στο κόμβο, που πραγματοποιεί μια ερώτηση αξιολόγησης για κάποιον άλλο, λανθασμένη πληροφορία (complaints που αντιστοιχούν σε αξιολόγηση άλλου κόμβου). Σε αυτή τη περίπτωση ο κόμβος, ο οποίος κάνει την αξιολόγηση, θα ζητήσει από το δίκτυο οποιοδήποτε αντίγραφο υπάρχει για τα complaints που έχουν καταχωρηθεί σε βάρος του κόμβου που θέλει να αξιολογήσει. Η διαφορά στην πληροφορία που του παρείχε ο «κακός» κόμβος, με αυτή που λαμβάνει από τα αντίγραφα θα οδηγήσει στην αποκάλυψη των προθέσεων του κακού κόμβου. Σε μια άλλη περίπτωση όπου μια ομάδα «κακών» χρηστών, χρησιμοποιώντας την ιδιότητα των complaints, δημιουργεί complaints για «καλούς» κόμβους, το σύστημα ανταποκρίνεται με παρόμοιο τρόπο. Ο κόμβος που ζητά πληροφορία για αξιολόγηση ενός άλλου κόμβου, ζητά να αξιολογηθούν οι κόμβοι που καταχώρησαν τα complaints, δηλαδή ζητά οποιαδήποτε καταχώρηση παραπόνου (complaint) έχει γίνει από τους κόμβους του δικτύου για τους κόμβους αυτούς. Άρα αν ο αριθμός των complaints που έχουν υποβάλλει οι «κακοί» κόμβοι συνδυασμένος με τον αριθμό των complaints που έχουν υποβάλλει οι άλλοι κόμβοι γι' αυτούς είναι μεγάλος, αποφασίζεται ότι μάλλον πρόκειται για «κακούς» κόμβους.
Σκοπός μιας ομάδας «κακών» κόμβων, στο NICE, είναι η εισαγωγή τους στα preference lists των άλλων κόμβων, δίνοντας μεταξύ τους μεγάλες τιμές εμπιστοσύνης. Ακόμα στη περίπτωση, όπου όλα ή τα περισσότερα μέλη μιας τέτοιας ομάδας καταφέρουν να εισχωρήσουν στις λίστες κάποιον «καλών» κόμβων, μετά την πρώτη αποτυχημένη συναλλαγή μαζί τους οι «καλοί» κόμβοι θα τους διαγράψουν από την λίστα τους και θα προσπαθήσουν να βρουν άλλους κόμβους στο δικτύου με τους οποίους θα μπορέσουν να συναλλαγούν. Αυτό βασίζεται στο γεγονός ότι, οι «κακοί» κόμβοι δεν μπορούν να σταματήσουν την επικοινωνία μεταξύ δύο οποιονδήποτε κόμβων. Άρα κάποια στιγμή ένας «καλός» κόμβος θα καταφέρει τελικά να επικοινωνήσει με έναν άλλο «καλό» κόμβο.

Στο Framework using Currency η αξιοπιστία του συστήματος είναι πολύ μεγαλύτερη απ' όλα τα άλλα συστήματα απέναντι σε οποιαδήποτε ομαδοποιημένη ή μη απόπειρα ανατροπής του. Ας υποθέσουμε ότι όλα τα μέλη της ομάδας αποφασίζουν να μειώσουν την φήμη ενός ή περισσοτέρων «δημοφιλών» (high reputated) κόμβων του δικτύου στέλνοντας πολλά complaints γι' αυτούς. Σύμφωνα με τρόπο λειτουργία του συστήματος, κάθε φορά που στέλνεται ένα complaint μειώνεται η φήμη του κάθε κόμβου που εμπλέκονται στο μήνυμα (καταγγέλων, κατηγορούμενος για αποτυχία) κατά ένα ποσό ανάλογο της φήμης που έχει ο άλλος κόμβος. Με αυτόν τον τρόπο όταν ο καταγγέλων - «κακός» peer- στείλει complaint για κάποιον «καλό» –άρα και δημοφιλή- κόμβο , από τον πρώτο αφαιρείται τόσο ποσοστό φήμης όσο έχει ο

δεύτερος. Άρα ο «κακός» κόμβος, όσο μεγάλη φήμη και να είχε αρχικά, να συνεχίσει να διαδίδει complaints θα αποκτήσει αρνητική φήμη, αφού η τιμή της θα μειώνεται συνεχώς ανάλογα με τους κόμβους που προσπαθεί να βλάψει.

Δυστυχώς το REGRET είναι σε θέση να αντιμετωπίσει μία ομάδα «κακών» κόμβων και να εξακολουθήσει να παρέχει αξιοπιστία μόνο στην περίπτωση όπου το πλήθος των «καλών» κόμβων υπερβαίνει σε αριθμό το πλήθος των «κακών» κόμβων. Σε αντίθετη περίπτωση, και όταν λαμβάνεται υπόψη η κοινωνική διάσταση της φήμης, δηλαδή όταν βασίζεται ένας κόμβος στην άποψη του συνόλου του, οι αποφάσεις που θα λαμβάνονται από αυτόν τον κόμβο όσον αφορά την εμπιστοσύνη του σε άλλους θα είναι λανθασμένες εφόσον θα στηρίζεται στις απόψεις «κακών» κόμβων.

Τέλος ο αλγόριθμος NodeRanking και το κοινωνικό δίκτυο που δημιουργείται με βάση αυτόν, δεν λαμβάνει καμία προφύλαξη απέναντι σε «κακούς» κόμβους οι οποίοι αλληλοϋποστηρίζονται (δείχνει ο ένας στον άλλον) και δημιουργούν μεγάλες ομάδες. Επιπλέον το NodeRanking λόγω της δομής του υστερεί σε έναν ακόμα τομέα όσον αφορά την αξιοπιστία, εφόσον υπάρχει ένας κεντρικός κόμβος με τον οποίον επικοινωνούν όλοι για την απόκτηση πληροφορίας σχετικά με το authority των κόμβων.

3) Ως ολοκλήρωση της σύγκρισης των συστημάτων, πραγματοποιείται ομαδοποίηση τους ανάλογα με τον τύπο και τις τιμές που παρέχει κάθε σύστημα στους κόμβους για την αξιολόγησή τους.

Στο σύστημα XREP δίνεται μόνο θετική ψήφος, στέλλοντας μήνυμα μόνο για τα resources τους servents που εμπιστεύεται ένας κόμβος, άρα η εμπιστοσύνη παίρνει μόνο θετικές τιμές. Ανάλογα στο P-Grid ένας κόμβος καταχωρεί complaints μόνο για τους κόμβους με τους οποίους είχε προηγούμενη αποτυχημένη συναλλαγή. Η εμπιστοσύνη μετά το τέλος του αλγορίθμου παίρνει διακριτές τιμές από το {-1,0,1}.

Στο NICE η αξιολόγηση κάποιου κόμβου πραγματοποιείται με την δημιουργία θετικών και αρνητικών cookies από κάποιον άλλο κόμβο με τον οποίον έχει προηγηθεί συναλλαγή. Η αποτίμηση της φήμης ενός κόμβους ως προς κάποιον άλλον, άρα και το ποσοστό της εμπιστοσύνης που δείχνει σε αυτόν ο κόμβος που τον αξιολόγησε, αντιστοιχίζεται με τιμές που λαμβάνονται από το διάστημα [0,1].

Στα συστήματα REGRET και Framework using Currency, κατά την αξιολόγηση δίνονται θετικές τιμές, απεικονίζοντας μια επιτυχημένη συναλλαγή, αλλά και αρνητικές τιμές, για μια αποτυχημένη συναλλαγή. Το ποσοστό της εμπιστοσύνης που έχει ένας κόμβος σε έναν άλλο λαμβάνει τιμές από το διάστημα [-1,1].

Τέλος στο NodeRanking το authority ενός κόμβου -πιο πιθανόν είναι να- λαμβάνει θετικές τιμές, δεδομένου ότι προκύπτει από την πρόσθεση της αρχικής τιμής, που δίνεται σε όλους τους κόμβους κατά την αρχική κατασκευή του κοινωνικού δικτύου, με ένα ποσοστό των authorities των κόμβων που καταλήγουν σε αυτόν. Το διάστημα από το οποίο λαμβάνει τιμές η εμπιστοσύνη (ανάλογα με το authority) δεν είναι γνωστό, πάντως είναι σίγουρα ένα υποσύνολο του [1,+∞) αν θεωρήσουμε ότι αρχικά το authority όλων των κόμβων είναι ίσο ή μεγαλύτερο του μηδενός.

Ως ένα επιπλέον αλλά πλέον σημαντικό σχόλιο θα πρέπει να σημειωθεί ότι <u>κανένα από τα παραπάνω μοντέλα δεν παρέχει ανωνυμία στους χρήστες του δικτύου</u>. Η ιδιότητα της ανωνυμίας αποτρέπει την επίτευξη εμπιστοσύνης μεταξύ των κόμβων-χρηστών, εφόσον, όπως είναι φυσικό, για να εμπιστευτεί κανείς κάποιον άλλο θα πρέπει είτε να τον γνωρίζει ο ίδιος είτε να υπάρχει κοινός γνωστός που τον εμπιστεύεται.

Συγκεντρωτικός πίνακας αποτελεσμάτων σύγκρισης

Μοντέλα / ***Συγρίσεις***	**XREP**	**P-Grid**	**NICE**	**Currency**	**REGRET**	**Node Ranking**
Τύπος της φήμης	Θετική	Αρνητική	Θετική και Αρνητική	Θετική και Αρνητική	Θετική και Αρνητική	Θετική
Τιμή του Trust	{0,1}	{-1,0,-1}	[0,1]	[-1,1]	[-1,1]	Πιθανόν [1,+∞)
Bandwidth cost	Μεγάλο	Μικρό	Μικρό	Μικρό	Μικρό	Μικρό
Storage cost	Αρκετό	Μικρό	Αρκετό	Αρκετό	Μικρό	Αρκετό
Scalability	Μικρό	Μεγάλο	Μεγάλο	Μεγάλο	Μεγάλο	Μικρό
Reliability	Μέτριο	Μέτριο	Μεγάλο	Μεγάλο	Μέτριο (εξαρτάται από το πλήθος των «κακών» κόμβων)	Μικρό
Μη – κεντρικ/μένη δομή	Ναι	Όχι τελείως	Ναι	Ναι	Ναι	Όχι
Ανωνυμία	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι

4. *ΣΥΜΠΕΡΑΣΜΑΤΑ*

Η εργασία αυτή είχε ως σκοπό την παρουσίαση και αξιολόγηση σημαντικών και σχετικά πρόσφατων συστημάτων διαχείρισης εμπιστοσύνης στα P2P συστήματα, ως παράμετρο της ασφάλειας που θα πρέπει να παρέχεται στους χρήστες τέτοιων συστημάτων, απέναντι σε χρήστες με κακές διαθέσεις. Τα συστήματα διαχείρισης εμπιστοσύνης εκμεταλλεύονται την φήμη που αποκτά ένας peer μέσα στο δίκτυο ως άμεση συνέπεια της αξιολόγησης των συναλλαγών που έχει πραγατοποιήσει.

Κατηγοριοποιήσαμε τα συστήματα με βάση την πληροφορία που εκμεταλλεύονται, σε δύο μεγάλες κατηγορίες. Στα reputation- based trust management systems, χρησιμοποιείται η φήμη που έχει αποκτήσει ένας κόμβος μέσα από τις συναλλαγές του. Η τελική απόφαση αν ένας κόμβος εμπιστευτεί κάποιον άλλον για να κάνει κάποια συναλλαγή, βασίζεται στην αξιολόγηση, *φήμη,* του κόμβου αυτού από τους υπόλοιπους κόμβους του δικτύου. Τα μοντέλα που παρουσιάστηκαν χρησιμοποιούν διάφορες τεχνικές, όπως ψηφοφορία των κόμβων του δικτύου για τον κόμβο που παρέχει κάποιο resource αλλά και του resource που παρέχεται, δημιουργία παραπόνων για μια αποτυχημένη συναλλαγή η οποία έχουν ως συνέπεια την μείωση της φήμης του κόμβου που την πραγματοποίησε, καθώς επίσης και την κατασκευή ενός εικονικού νομίσματος όπου ο πλούτος που αποκτά κάθε κόμβος αντιπροσωπεύει το ποσοστό της φήμης του, άρα και της εμπιστοσύνης που δείχνουν οι peers του δικτύου προς αυτόν για μια ολοκληρωμένη και σωστή συναλλαγή. Απ' όλα τα μοντέλα, αυτό που χρησιμοποιεί το εικονικό νόμισμα αποτελεί καλύτερη αντιμετώπιση του προβλήματος της διαχείρισης εμπιστοσύνης στα P2P συστήματα.

Στην δεύτερη κατηγορία, *social-based networks trust management systems*, τα μοντέλα εκμεταλλεύονται τους κοινωνικούς δεσμούς που δημιουργούνται μεταξύ των κόμβων του δικτύου. Οι δεσμοί αυτοί μπορεί να είναι δεσμοί φιλίας, αμοιβαίας υποστήριξης κ.α. μεταξύ των κόμβων, δημιουργόντας σύνολα, *groups*. Στην απόφαση που πρέπει να λάβει κάποιος κόμβος για το κατά πόσο μπορεί να εμπιστευτεί κάποιον άλλον για μια συναλλαγή, εκτός της υποκειμενικής του άποψης, σημαντικό ρόλο παίζει και η άποψη του συνόλου στο οποίο ανήκει ο κόμβος που κάνει την αξιολόγηση. Τα συστήματα αυτά, αν και προσπαθούν να εκεμταλλευτούν την ιδιότητα της δημιουργίας κοινωνικών δεσμών που αναπτύσσονται ανάμεσα στα μέλη κάθε συνόλου στο κόσμο, είναι ακόμα σε πρώιμο στάδιο σε ότι αφορά την διασφάλιση της εμπιστοσύνης, συνεπώς και της ασφάλειας, στα P2P συστήματα.

Όπως παρατηρήθηκε από την μελέτη των συστημάτων, η διατήρηση της ανωνυμίας ως ιδιότητας των P2P συστήματων αποτελεί ανατρεπτικό παράγοντα όσον αφορά στη δημιουργία δεσμών εμπιστοσύνης ανάμεσα στα μέλη ενός συνόλου. Με βάση το γεγονός ότι δεν μπορεί να υπάρχει εμπιστοσύνη μεταξύ δύο άγνωστων οντοτήτων, είναι προφανές ότι κανένα από τα μοντέλα που παρουσιάστηκαν δεν προσπαθούν να εισάγουν και να

διατηρήσουν την ιδιότητα της ανωνυμίας των χρηστών. Αν και γίνονται προσπάθειες εύρεσης τρόπων δημιουργίας εμπιστούνης με διατήρηση της ανωνυμίας των χρηστών [10], αυτές βρίσκονται ακόμα σε πολύ πρώιμο στάδιο και περιορίζονται σε θεωρητικό πλαίσιο. Θα πρέπει να σημειωθεί σε αυτό το σημείο, ότι τα παραδείγματα τεχνικών, που αναφέρονται στο [10], δανείζονται κάποιες απο τις τεχνικές που αναφέρονται στα μοντέλα που μελετήθηκαν, π.χ. αποτίμησης θετικής και αρνητικής φήμης των κόμβων, εισαγωγή *witnesses* (μαρτύρων) με βάση τους οποίους αποφασίζεται η φήμη ενός κόμβου, καθώς και δημιουργία ομάδων (*groups)* όπου όλοι οι κόμβοι που ανήκουν σε μια ομάδα θεωρείται ότι έχουν την ίδια φήμη.

Καταλήγοντας, παρατηρούμε ότι, δυστυχώς πάντα θα υπάρχουν χρήστες οι οποίοι θα εκμεταλλεύονται τις ιδιότητες των P2P συστημάτων και θα προσπαθούν να πλήξουν την αξιοπιστία των συστημάτων και των χρηστών τους. Συνεπώς, η δημιουργία εμπιστοσύνης μεταξύ των κόμβων ενός P2P συστήματος, αποτελεί, και θα συνεχίσει να αποτελεί, σημαντικό παράγοντα για την επίτευξη ασφάλειας στα συστήματα αυτά.

Αναφορές

[1] Ernesto Damiani, Sabrina De Capitani di Vimercati, Stefano Paraboschi, Pierangela Samarati and Fabio Violante. *A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Networks*. 9th ACM Conference on Computer and Communications Security, Washington DC. (2002)

[2] Karl Aberer and Zoran Despotovic. *Managing Trust in a Peer-2-Peer Information System*. Conference on Information and Knowledge Management, Atlanta, Georgia. (2001)

[3] Seungjoon Lee, Rob Sherwood and Bobby Bhattacharjee. *Cooperative peer groups in NICE*. IEEE Infocom, San Francisco, USA. (2003)

[4] Rohit Gupta and Arun K. Somani. *Cooperative Peer Groups in NICE*. 4th International Conference on Peer-to-Peer Computing, Zurich, Switzerland. (2004)

[5] Jordi Sabater and Carles Sierra. *REGRET: A Reputation Model for Gregarious Societies*. 4th Workshop on Deception, Fraud and Trust in Agent Societies, Montreal, Canada. (2001)

[6] Josep M. Pujol, Ramon Sanguesa and Jordi Delgado. *Extracting reputation in multi agent systems by means of social network topology*. First International Joint Conference on Autonomous Agents and Multi-Agent Systems, Bologna, Italy. (2002)

[8] http://www.irchelp.org/irchelp/security/

[9] http://spam.abuse.net/overview/whatisspam.shtml

[10] Roger Dingledine, Nick Mathewson and Paul Syverson. *Reputation in P2P Anonymity Systems*. Workshop on economics of p2p systems, Berkley CA. (2003)

[11] http://www.cc.gatech.edu/projects/disl/specialProjects/anonymity.htm