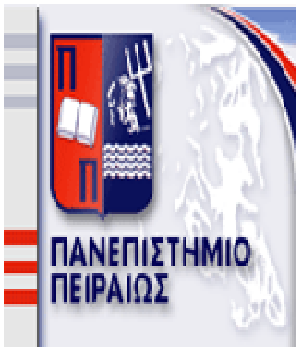


ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ
ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΚΑΤΕΥΘΥΝΣΗ : "ΨΗΦΙΑΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ & ΔΙΚΤΥΑ"

Διπλωματική Εργασία

Μελέτη των Μηχανισμών ασφάλειας που εφαρμόζονται σε Peer to Peer συστήματα

Ονοματεπώνυμο : Ασπασία Χ. Ζαλαχώρη

Επιβλέπων:Χρήστος Ξενάκης

ΠΕΙΡΑΙΑΣ

ΦΕΒΡΟΥΑΡΙΟΣ 2009

Ευχαριστίες

Θερμές ευχαριστίες εκφράζω στον Επίκουρο Καθηγητή κ. Χρήστο Ξενάκη για την επίβλεψη και τη βοήθεια που μου παρείχε για την ολοκλήρωση της διπλωματικής μου.
Τέλος εκφράζω την ευγνωμοσύνη μου στους γονείς μου, τα αδέλφια μου, τους φίλους μου για την υποστήριξη και βοήθειά τους σε όλη τη διάρκεια των μεταπτυχιακών σπουδών μου.

Περιεχόμενα

Πρόλογος

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια του Προγράμματος Μεταπτυχιακών Σπουδών του τμήματος Διδακτικής της Τεχνολογίας και Ψηφιακών συστημάτων του Πανεπιστημίου Πειραιώς (Κατεύθυνση Ψηφιακές Επικοινωνίες και Δίκτυα), σε συνεργασία με τον λέκτορα του τμήματος κ. Χρήστο Ξενάκη. Το αντικείμενο ουσιαστικά εμπίπτει στη μέλετη των peer to peer συστημάτων και στην ανάπτυξη μηχανισμών ασφάλειας.

Φεβρουάριος 2009

Η συγραφέας
Ασπασία Χ.Ζαλαχώρη

Εισαγωγή

Κατανεμημένα συστήματα που στηρίζονται στην ομότιμη και εθελοντική συμπεριφορά των κόμβων που τα απαρτίζουν έγιναν ευρέως γνωστά ως peer-to-peer συστήματα. Το δίκτυο που σχηματίζουν είναι χτισμένο πάνω στην υπάρχουσα υποδομή του διαδικτύου και παρέχουν κοινή χρήση πόρων (αποθηκευτικό χώρο, υπολογιστική ισχύς, κλπ.) ή διαμοιράζουν δεδομένα. Η μη απαίτηση για κεντρικό εξυπηρέτη, η δυνατότητα απευθείας επικοινωνίας μεταξύ των κόμβων (υπολογιστών που μετέχουν), η scalability, η αυτοδιοργάνωση, η αυτονομία και η ανωνυμία και δυναμικότητα (peers join and leave) είναι χαρακτηριστικά που κάνουν τα συστήματα αυτά δημοφιλή, και ελκυστικά ακόμη και στον εμπορικό κόσμο.

Στην παρούσα εργασία το ενδιαφέρον εστιάζεται στους μηχανισμούς ασφάλειας που εφαρμόζονται έτσι ώστε τα συστήματα να είναι αποδοτικότερα.
Το πρόβλημα της ασφάλειας στα δίκτυα υπολογιστών γενικά και στο Διαδίκτυο συγκεκριμένα έχει απασχολήσει έντονα όλους όσων τα συμφέροντα διακυβεύονται σε μεγάλο βαθμό και έχει κινητοποιήσει τόσο την επιστημονική κοινότητα όσο και εταιρίες ανάπτυξης λογισμικού και δικτυακών υποδομών προς την κατεύθυνση της πληρέστερης κατανόησης και επίλυσής του.

Είναι κοινώς αποδεκτό ότι το βασικότερο βήμα για την επίλυση ενός προβλήματος είναι η όσο το δυνατόν πληρέστερη κατανόησή του, δηλαδή η οριοθέτηση του ίδιου του γενικού προβλήματος και των εκφάνσεων και παραλλαγών του. Στα πλαίσια αυτής της εργασίας πραγματοποιηται μια απόπειρα καταγραφής, ταξινόμησης και ομαδοποίησης των peer to peer συστημάτων και των επιθέσεων που δέχονται καθώς και στρατηγικές αντιμετώπισης των των περιστατικών προσβολής της ασφάλειας των peer to peer συστημάτων.

Ακολουθεί ο ορισμός ενός peer-to-peer συστήματος όπως δίνεται από τους Ανδρουτσέλλης-Θεοτόκης-Σπινέλλης:
“Peer-to-peer συστήματα είναι κατανεμημένα συστήματα που αποτελούνται από διασυνδεδεμένους κόμβους, ικανούς να αυτοδιοργανώνονται σε τοπολογίες δικτύου με

σκοπό την κοινή χρήση πόρων όπως περιεχόμενα, κύκλους μηχανής, χώρο αποθήκευσης, και εύρος, ικανά να προσαρμόζονται στις αποτυχίες και στις παροδικές μετακινήσεις κόμβων ενώ διατηρούν προσβάσιμη συνδετικότητα και εκτελούνται χωρίς την απαίτηση για μεσολάβηση ή υποστήριξη ενός καθολικού κεντρικού εξυπηρέτη ή αρχής".

ΚΕΦΑΛΑΙΟ 1

1. Τεχνολογία ομότιμων οντοτήτων (Peer to Peer)

Πριν δημιουργηθεί ο όρος Peer-to-Peer και εφαρμοστεί στην πράξη, οι χρήστες του Internet αλληλεπιδρούσαν μεταξύ τους μεν αλλά με δύσχρηστους και αργούς τρόπους όπως πχ με τα mail και μέσω ομάδων συζητήσεων (Usenet, newsgroups). Μπορούσαν να στείλουν ο ένας στον άλλο αρχεία χωρίς να γίνεται έλεγχος των συναλλαγών αυτών από κάποιον κεντρικό φορέα. Δεν μπορούσαν όμως να συζητήσουν σε πραγματικό χρόνο πάνω σε αυτά, να τα οργανώσουν σε κατηγορίες ή να σημειώνουν σχόλια πάνω σε αυτά. Η εισαγωγή αυτού του τρόπου αλληλεπίδρασης στο διαδίκτυο θα βελτίωνε τον τρόπο με τον οποίο οι χρήστες επικοινωνούσαν μεταξύ τους.

Αν και ο όρος αυτός υπάρχει εδώ και λίγο καιρό ο τρόπος λειτουργίας του και η αρχιτεκτονική του υπάρχουν εδώ και πολλά χρόνια. Στην πραγματικότητα η αρχιτεκτονική αυτή είναι η παλαιότερη στον κόσμο των επικοινωνιών. Τα τηλέφωνα και το τηλεφωνικό δίκτυο είναι Peer to Peer. Το ίδιο ισχύει και για την αρχική υλοποίηση του Usenet και για το IP routing. Το τελευταίο μάλιστα ακόμα και τώρα είναι Peer to Peer αν και δημιουργήθηκαν πολύ μεγαλύτερα σημεία πρόσβασης σε σχέση με τα υπόλοιπα. Το Internet στην αρχική του μορφή, δηλ. στην μορφή που είχε μέχρι και την δεκαετία του 1980 ήταν και αυτό Peer to Peer αφού κάθε τελικός κόμβος στο δίκτυο ήταν και Client και Server σε αντίθεση με το ιεραρχικό μοντέλο που επικρατεί στην δημοφιλέστερη σημερινή εφαρμογή (www).

Ένα δίκτυο ομότιμων οντοτήτων (peer-to-peer ή P2P) είναι ένα δίκτυο που στηρίζεται στην υπολογιστική ισχύ των δύο άκρων μιας σύνδεσης παρά στο ίδιο το δίκτυο. Δίκτυα P2P χρησιμοποιούνται για διαμοιρασμό οποιασδήποτε πληροφορίας σε ψηφιακή μορφή. Σε ένα αμιγές δίκτυο P2P μεταφοράς αρχείων δεν υπάρχουν οι έννοιες των πελατών και των εξυπηρετητών, αλλά μόνο των «peers» ή «ομότιμων κόμβων» που δρουν ταυτόχρονα ως πελάτες και ως εξυπηρετητές προς τους υπόλοιπους κόμβους του δικτύου ανταλλάσσοντας πληροφορίες επί ίσοις όροις. Αυτό το μοντέλο διαφέρει από το

μοντέλο πελάτη-εξυπηρετητή, όπου η επικοινωνία γίνεται μέσω ενός κεντρικού εξυπηρετητή.

Οι τεχνολογίες peer to peer επιτρέπουν το διαμοιρασμό των δικτυακών πόρων και υπηρεσιών, όπως είναι η πληροφορία, τα αρχεία, οι κύκλοι επεξεργασίας και ο χώρος αποθήκευσης, μέσω απευθείας επικοινωνίας μεταξύ των συστημάτων (χωρίς απαραίτητα τη χρήση κεντρικών servers). Σε αντίθεση με τα δίκτυα client - server τα peer to peer δίκτυα υπόσχονται βελτιωμένη επεκτασιμότητα, χαμηλότερα κόστη ιδιοκτησίας, μεγαλύτερη ανέχεια σε σφάλματα και αποκεντρωμένο συντονισμό των υποχρησιμοποιούμενων ή περιορισμένων πόρων. Τα χαρακτηριστικά αυτά σε συνδυασμό με την ανάπτυξη του Internet δημιούργησαν νέα πεδία εφαρμογών για peer to peer δίκτυα. Σαν αποτέλεσμα τα τελευταία χρόνια ο αριθμός των peer to peer εφαρμογών αυξήθηκε σε πολύ μεγάλο βαθμό. Παράλληλα αυξήθηκαν και οι συζητήσεις σχετικά με την απόδοση και τα όρια τους, όπως επίσης με τις οικονομικές, κοινωνικές και νομικές επιπτώσεις αυτών των εφαρμογών.

1.1 Αρχιτεκτονική πελάτη-εξυπηρετητή (client - server)

Οι περισσότερες υπηρεσίες διαδικτύου διανέμονται χρησιμοποιώντας την παραδοσιακή αρχιτεκτονική πελάτη - εξυπηρετητή. Σε αυτήν την αρχιτεκτονική υπάρχουν δύο διακριτοί ρόλοι, οι πελάτες που ζητούν υπηρεσίες και οι εξυπηρετητές που προσφέρουν υπηρεσίες. Οι μεν πελάτες είναι εκείνοι που ξεκινούν την διαδικασία όταν επιθυμούν μια υπηρεσία και συνδέονται με έναν εξυπηρετητή χρησιμοποιώντας ένα συγκεκριμένο πρωτόκολλο επικοινωνίας για να αποκτήσουν πρόσβαση σε έναν συγκεκριμένο πόρο. Το μεγαλύτερο μέρος της επεξεργασίας στην προσφορά μιας υπηρεσίας λαμβάνει χώρα συνήθως στον εξυπηρετητή.

Οι πιο δημοφιλείς εφαρμογές διαδικτύου, συμπεριλαμβανομένου του παγκόσμιου ιστού, όπως το Telnet, και το ηλεκτρονικό ταχυδρομείο, χρησιμοποιούν αυτό το πρότυπο υπηρεσίας. Ένα τυπικό παράδειγμα μεταφοράς αρχείων με αυτήν την τεχνική είναι το πρωτόκολλο μεταφοράς αρχείων (FTP). Ένας πελάτης φορτώνει ένα αρχείο στον FTP εξυπηρετητή, έπειτα πολλοί πελάτες το μεταφορτώνουν από αυτόν, χωρίς να είναι

αναγκαία η απευθείας σύνδεση των χρηστών που μεταφορτώνουν και αυτών που φορτώνουν.

Πλεονεκτήματα

Το πλεονέκτημα αυτής της αρχιτεκτονικής είναι ότι απαιτεί τη λιγότερη υπολογιστική δύναμη από την πλευρά πελατών. Ειρωνικά, οι περισσότεροι χρήστες έχουν επιδιώξει να αναβαθμίσουν τους ηλεκτρονικούς υπολογιστές τους σε επίπεδα που είναι παράλογα ανώτερα για τις δημοφιλέστερες εφαρμογές διαδικτύου, όπως η περιαγωγή στον παγκόσμιο ιστό, ανάκτηση του ηλεκτρονικού ταχυδρομείου και η μεταφορά αρχείων.

Μειονεκτήματα

Δυστυχώς, αυτή η αρχιτεκτονική έχει ένα σημαντικό μειονέκτημα. Δεδομένου ότι ο αριθμός πελατών αυξάνεται, οι απαιτήσεις φορτίων και εύρους ζώνης στον εξυπηρετητή αυξάνονται επίσης, αποτρέποντας τελικά τον εξυπηρετητή από το να χειριστεί πρόσθετους πελάτες. Για να αντεπεξέλθουν στην αυξανόμενη ζήτηση για τις υπηρεσίες τους, οι εταιρείες, προσπαθούν να μοιράσουν την κίνηση προς τους εξυπηρετητές τους χρησιμοποιώντας πολύπλοκες τεχνικές εξισορρόπησης φορτίου (load balancing) και ανανεώνοντας τους υπάρχοντες πόρους τους (αναβάθμιση συσκευών, εύρος ζώνης).

Ο πελάτης στην αρχιτεκτονική πελάτης - εξυπηρετητής περιορίζεται σε έναν παθητικό ρόλο, ικανό να απαιτεί υπηρεσίες από τους εξυπηρετητές αλλά ανίκανο να προσφέρει υπηρεσίες σε άλλους πελάτες. Εάν όμως όλες οι μηχανές στο δίκτυο έτρεχαν και ως εξυπηρετητές και ως πελάτες, θα διαμόρφωναν την αρχή ενός στοιχειώδους P2P δικτύου.

1.2 Τεχνολογία peer-to-peer

Αν αναλογιστούμε τον ανεκμετάλλευτο αποθηκευτικό χώρο, το αναξιοποίητο εύρος ζώνης και τη σπαταλημένη επεξεργαστική ισχύ, καταλαβαίνουμε ότι υπάρχει ένα τεράστιο αναξιοποίητο δυναμικό στα «άκρα» του διαδικτύου. Η τεχνολογία P2P είναι το κλειδί στην πραγματοποίηση αυτής της δυνατότητας, παρέχοντας στις μεμονωμένες μηχανές ένα μηχανισμό για προσφορά υπηρεσιών από τη μία στην άλλη. Αντίθετα από την αρχιτεκτονική πελατών - εξυπηρετητών τα δίκτυα P2P δεν στηρίζονται σε έναν

κεντρικό υπολογιστή για την παροχή πρόσβασης σε υπηρεσίες και λειτουργούν συνήθως έξω από το σύστημα ονόματος περιοχών (DNS). Τα δίκτυα P2P αποφεύγουν τη συγκεντρωμένη οργάνωση της αρχιτεκτονικής πελάτη - εξυπηρετητή και υιοθετούν άντ' αυτού μια επίπεδη, ιδιαίτερα διασυνδεόμενη αρχιτεκτονική. Επιτρέποντας περιοδικά συνδεδεμένους υπολογιστές να βρουν ο ένας τον άλλον, η τεχνολογία P2P επιτρέπει σε αυτές τις μηχανές να ενεργήσουν και ως πελάτες και εξυπηρετητές, να καθορίζουν τις υπηρεσίες που προσφέρουν στο P2P δίκτυο και να συμμετέχουν σε αυτές τις υπηρεσίες με κάποιο ορισμένο από εφαρμογή τρόπο. Έτσι οι αποφάσεις λαμβάνονται με αποκεντρωμένο τρόπο.

Τα προαναφερόμενα αποτελούν μία απόπειρα περιγραφής των χαρακτηριστικών που ορίζουν μία εφαρμογή Peer to Peer, καθώς πρόκειται για έναν αρκετά πολυμορφικό όρο. Σε αυτό συμβάλλει και το γεγονός ότι δεν έχουν ακόμη καθορισθεί πρότυπα για τέτοιου είδους εφαρμογές. Ήδη όμως γίνονται σοβαρές προσπάθειες προς αυτή την κατεύθυνση, αφού είναι πλέον εμφανή τα πλεονεκτήματα της τεχνολογίας P2P.

Πλεονεκτήματα

Τα κύρια πλεονεκτήματα των δικτύων P2P είναι τα εξής:

- Μοιράζουν τα καθήκοντα προσφοράς υπηρεσιών μεταξύ όλων των ομότιμων οντοτήτων (peers) στο δίκτυο, πράγμα που αποβάλλει τις διακοπές παροχής υπηρεσιών λόγω βλάβης του κεντρικού εξυπηρετητή. Έτσι παρέχεται μια πιο εξελικτική λύση για την προσφορά των υπηρεσιών.

- Τα δίκτυα P2P εκμεταλλεύονται το διαθέσιμο εύρος ζώνης σε ολόκληρο το δίκτυο με τη χρησιμοποίηση ποικίλων καναλιών επικοινωνίας και με την πλήρωση του εύρους ζώνης στα άκρα του δικτύου. Αντίθετα από τις παραδοσιακές επικοινωνίες πελάτης - εξυπηρετητής, στις οποίες οι συγκεκριμένες διαδρομές στους δημοφιλείς προορισμούς μπορούν να υπερφορτωθούν, η τεχνολογία P2P επιτρέπει την επικοινωνία μέσω ποικίλων διαδρομών δικτύου, μειώνοντας τη συμφόρηση δικτύων.

- Η τεχνολογία P2P έχει την ικανότητα της προσφοράς πόρων με υψηλή διαθεσιμότητα και με πολύ χαμηλότερο κόστος, μεγιστοποιώντας τη χρήση των πόρων από κάθε ισότιμη οντότητα που συνδέεται με το P2P δίκτυο. Ενώ οι

αρχιτεκτονικές πελάτη – εξυπηρετητή στηρίζονται στην προσθήκη δαπανηρού εύρους ζώνης και εξοπλισμού και για να διατηρήσουν μια δυνατή λύση, η τεχνολογία P2P μπορεί να προσφέρει ένα παρόμοιο επίπεδο ευρωστίας με τη εξάπλωση των δικτύων και των πόρων μέσω του P2P δικτύου.

Μειονεκτήματα

Δυστυχώς η τεχνολογία P2P πάσχει και αυτή από μερικά μειονεκτήματα λόγω της φύσης της δομής ενός P2P δικτύου.

- Η διανεμημένη μορφή καναλιών επικοινωνιών στα P2P δίκτυα οδηγεί σε αιτήσεις για υπηρεσίες μη ντετερμινιστικής φύσης. Παραδείγματος χάριν, οι πελάτες που ζητούν ακριβώς τον ίδιο πόρο από το P2P δίκτυο, μπορεί να συνδεθούν με τις εξ ολοκλήρου διαφορετικές μηχανές μέσω διαφορετικών διαδρομών επικοινωνίας, με διαφορετικά αποτελέσματα.

- Αιτήματα που στέλνονται μέσω ενός P2P δικτύου μπορεί να μην οδηγήσουν σε μια άμεση απάντηση και, σε μερικές περιπτώσεις, να μην οδηγήσουν σε οποιαδήποτε απάντηση.

- Οι πόροι σε ένα P2P δίκτυο μπορούν να εξαφανιστούν κατά περιόδους καθώς αυτοί που φιλοξενούν εκείνους τους πόρους αποσυνδέονται από το δίκτυο, κάτι που έρχεται σε αντιπαράθεση με τις ως τώρα πρακτικές στο διαδίκτυο, όπου οι υπηρεσίες που παρέχονται έχουν τους πόρους τους συνεχώς διαθέσιμους.

Εντούτοις, η τεχνολογία P2P μπορεί να υπερνικήσει όλους αυτούς τους περιορισμούς. Αν και οι πόροι θα εξαφανίζονται κατά περιόδους, μια P2P εφαρμογή μπορεί να εφαρμόσει τη λειτουργία της αντανάκλασης (mirror) για τους δημοφιλέστερους πόρους σε περισσότερες του ενός ισότιμες οντότητες, ελαχιστοποιώντας έτσι αιτήσεις για πρόσβαση στον πόρο της και αυξάνοντας ταυτόχρονα την προσφορά του συγκεκριμένου πόρου. Έτσι μεγαλύτεροι αριθμοί διασυνδεόμενων ισότιμων οντοτήτων μειώνουν την πιθανότητα ότι ένα αίτημα για μια υπηρεσία θα μείνει αναπάντητο. Εν ολίγοις, η ίδια η δομή ενός P2P δικτύου που προκαλεί το πρόβλημα μπορεί να χρησιμοποιηθεί και για να το λύσει.

1.3 Αρχιτεκτονική

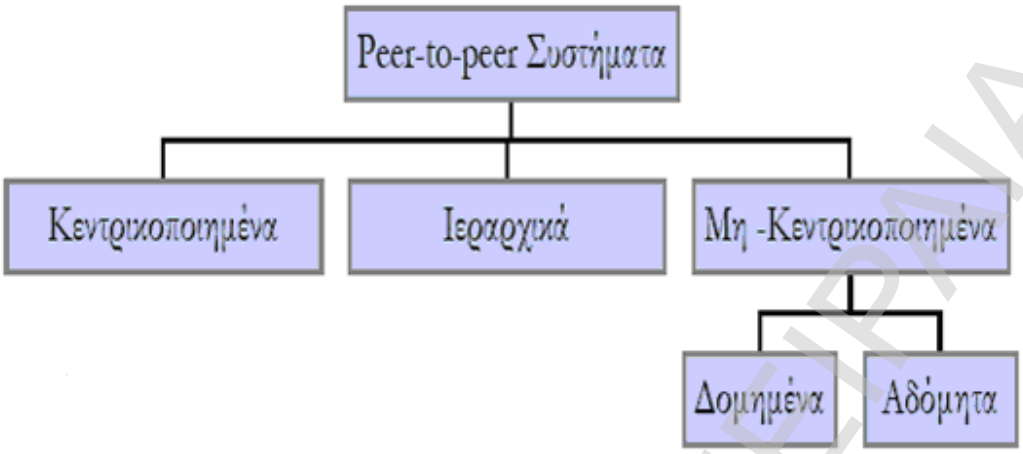
Οι κόμβοι, (πρόκειται για προσωπικούς υπολογιστές, σταθμούς εργασίας, κλπ.) που μετέχουν σε ένα peer-to-peer σύστημα σχηματίζουν ένα δίκτυο επικάλυψης (overlay network) πάνω από την υπάρχουσα υποδομή του διαδικτύου. Διασυνδέονται, επικοινωνούν και ανταλλάσσουν πληροφορίες μεταξύ τους σε τοπολογίες ανεξάρτητα από το δίκτυο υποδομής (IP network) διατηρώντας την αυτονομία τους. Η αρχιτεκτονική του δικτύου επηρεάζει τον μηχανισμό δρομολόγησης μηνυμάτων αναζήτησης, την απόδοση, την ικανότητα κλιμάκωσης, την προσαρμοστικότητα -ανοχή σε σφάλματα, κλπ. και στοχεύει στην υποστήριξη λειτουργιών όπως διαμοιρασμό αρχείων (file sharing), κατανεμημένο υπολογισμό (distributed computing), επικοινωνία – συνεργασία μεταξύ των χρηστών (collaboration network).
Υπάρχουν διάφορες αρχιτεκτονικές για τον σχηματισμό του overlay δικτύου:

1.3.1 Κεντρικοποιημένα peer-to-peer συστήματα

Στις κεντρικοποιημένες αρχιτεκτονικές υπάρχει ένας κεντρικός εξυπηρέτης (Directory Server) στον οποίο απευθύνουν οι κόμβοι τις ερωτήσεις τους για να πληροφορηθούν που βρίσκονται οι επιθυμητές πληροφορίες (π.χ Napster). Μια τέτοια αρχιτεκτονική αν και είναι αρκετά αποδοτική, δεν έχει την ιδιότητα της κλιμάκωσης ενώ έχει ενιαίο σημείο της αποτυχίας (bottleneck).

1.3.2 Ιεραρχικά

Οι κόμβοι οργανώνονται σε ιεραρχική δομή όπως γίνεται με τους DNS στο διαδίκτυο. Στα ιεραρχικά peer-to-peer συστήματα εισάγεται ή έννοια των “super-peers” (FastTrack). Η δομή τους μπορεί να είναι κεντρικοποιημένη ή μη.



Σχήμα 1.1: P2P Αρχιτεκτονική

1.3.3 Μη Κεντρικοποιημένα peer-to-peer συστήματα

Μια άλλη κατηγορία αρχιτεκτονικών είναι οι μη – κεντρικοποιημένες όπου οι κόμβοι συγκροτούν το overlay δίκτυο είτε δομημένα ακολουθώντας κανόνες για τον σχηματισμό του δικτύου, είτε αδόμητα όπου δεν υπάρχει ούτε κεντρικό directory ούτε ακριβείς οδηγίες για τον σχηματισμό τοπολογίας του δικτύου και την τοποθέτηση των περιεχομένων.

Δομημένα

Στα δομημένα peer-to-peer συστήματα οι κόμβοι οργανώνονται σε δομημένο γράφο για το σχηματισμό του overlay δικτύου. Στα δεδομένα αντιστοιχίζεται ένα κλειδί και η τοποθέτηση τους στους κόμβους γίνεται με προκαθορισμένο τρόπο έτσι ώστε να διευκολύνεται η αναζήτησή τους και να επιτυγχάνεται η κλιμάκωση. Η τοποθέτηση των αρχείων στα χαλαρά δομημένα συστήματα (Freenet) βασίζεται στην εκτίμηση (on hints) για το που μπορεί να βρεθεί η αναζητούμενη πληροφορία. Στα αυστηρά δομημένα συστήματα τόσο η δόμηση του overlay δικτύου όσο και η τοποθέτηση των αρχείων είναι σαφώς καθορισμένη.

Ο εντοπισμός ενός αντικειμένου (δεδομένου) από μια εφαρμογή στα δομημένα συστήματα γίνεται σε μικρό αριθμό βημάτων (network hops), υπό την απαίτηση βέβαια να διατηρείται ένας μικρός πίνακας δρομολόγησης σε κάθε κόμβο.
Παραδείγματα τέτοιων συστημάτων αποτελούν τα: Content Addressable Network (CAN), Chord , Tapestry, Pastry, Kademlia και Viceroy.

Αδόμητα

Στα συστήματα αυτά δεν υπάρχει καμιά δομή στο overlay δίκτυο και τα περιεχόμενα τοποθετούνται σε κόμβους στο δίκτυο χωρίς γνώση της τοπολογίας ή άλλης συσχέτισης με αυτό. Τα μη δομημένα συστήματα είναι κατάλληλα σε περιπτώσεις όπου μεγάλο πλήθος κόμβων μετέχει παροδικά στο δίκτυο χωρίς όμως αποδοτικούς μηχανισμούς αναζήτησης, κλιμάκωσης, διαθεσιμότητας. Υποστηρίζουν καλύτερα πολύπλοκες ερωτήσεις σε σχέση με τα δομημένα.

Αδόμητα peer-to-peer δίκτυα είναι: Napster, Gnutella, FastTrack, KaZaA, BitTorrent, κ.α.

Ακόμα μία κατηγοριοποίηση που μπορεί να κάνει κάποιος είναι οι εφαρμογές τύπου διανομής αρχείων (file sharing) για την ανταλλαγή αρχείων μεταξύ κόμβων, όπως είναι το Napster και το BitTorrent, και οι εφαρμογές κατανεμημένης επεξεργασίας (distributed computing) για τη συνεισφορά της αναξιοποίητης επεξεργαστικής ισχύος πολλών υπολογιστών με σκοπό την επίλυση ενός εξαιρετικά δύσκολου προβλήματος, το οποίο τυπικά θα απαιτούσε τη χρήση υπερυπολογιστή, όπως το SETI@Home.
Στις περισσότερες περιπτώσεις, οι ομότιμοι κόμβοι συνδέονται ο ένας με τον άλλο μέσω του διαδικτύου χρησιμοποιώντας είτε το TCP είτε το HTTP πρωτόκολλο.

1.4 Χαρακτηριστικά peer to peer δικτύων

Όπως ήδη αναφέρθηκε τα κύρια χαρακτηριστικά των δικτύων peer to peer είναι ο διαμοιρασμός των δικτυακών πόρων και υπηρεσιών, η αποκέντρωση και η αυτονομία.

Διαμοιρασμός δικτυακών πόρων και υπηρεσιών (sharing of distributed resources and services)

Σε ένα peer to peer δίκτυο κάθε κόμβος μπορεί να λειτουργήσει και σαν client και σαν server δηλαδή σαν παροχέας και καταναλωτής αντίστοιχα πόρων και υπηρεσιών όπως πληροφορία,αρχεία, bandwidth, κύκλοι επεξεργασίας και αποθήκευση. Έτσι καθώς προστίθενται νέοι κόμβοι και η ζήτηση στο σύστημα αυξάνεται, αυξάνεται επίσης και η χωρητικότητά του.

Αποκέντρωση (decentralization)

Στα peer to peer δίκτυα δεν υπάρχει κάποιο κεντρικό σημείο που να οργανώνει το δίκτυο ή τη χρήση των πόρων και των επικοινωνιών ανάμεσα στους κόμβους του δικτύου. Αυτό σημαίνει ότι κανένας κόμβος δεν έχει κεντρικό έλεγχο πάνω στους υπόλοιπους. Με αυτήν την έννοια η επικοινωνία μεταξύ των κόμβων γίνεται απευθείας.

Γίνεται διάκριση μεταξύ των “καθαρών” και των υβριδικών peer to peer δικτύων. Στα “καθαρά” peer to peer συστήματα οι κόμβοι μοιράζονται ίσα δικαιώματα και λειτουργίες. Στα υβριδικά συστήματα ένα σύνολο επιλεγμένων λειτουργιών όπως το indexing και η επικύρωση εκχωρείται σε ένα υποσύνολο κόμβων που υιοθετούν τον ρόλο μιας οντότητας συντονισμού.

Αυτονομία (autonomy)

Κάθε κόμβος ενός peer to peer δικτύου μπορεί αυτόνομα να αποφασίσει πότε και σε ποιο βαθμό θα κάνει τους πόρους του διαθέσιμους στους υπόλοιπους κόμβους.

Τα παραπάνω χαρακτηριστικά δημιουργούν μια σειρά πλεονεκτημάτων για τα peer to peer δίκτυα όπως μειωμένα κόστη ιδιοκτησίας, επεκτασιμότητα και υποστήριξη ad hoc δικτύων.

Μειωμένο κόστος ιδιοκτησίας

Τα έξοδα απόκτησης και λειτουργίας των υποδομών μπορούν να μειωθούν με τη χρησιμοποίηση των ήδη υπαρχουσών υποδομών και τη μείωση του κόστους διαχείρισης

και χρήσης. Για παράδειγμα με τη χρήση peer to peer δικτύων για αποθήκευση δεδομένων δεν υπάρχει η ανάγκη διατήρησης κεντρικού server για την αποθήκευση ολόκληρου του όγκου των δεδομένων.

Επεκτασιμότητα

Στα peer to peer δίκτυα η εξάρτηση από κεντρικά σημεία είναι μειωμένη. Για το λόγο αυτό και εξαιτίας του χωρικού διαμοιρασμού της πληροφορίας και της δημιουργίας αντιγράφων η πιθανότητα συμφόρησης (bottleneck) είναι μικρότερη. Τα υβριδικά συστήματα διαμοιρασμού αρχείων έχουν πλεονεκτήματα επεκτασιμότητας σε σχέση με τις client/server προ-σεγγίσεις. Αυτό οφείλεται στην απευθείας ανταλλαγή αρχείων μεταξύ των κόμβων χωρίς τη βοήθεια κάποιου server.

Ad hoc δίκτυα

Με τον όρο ad hoc εννοούμε περιβάλλοντα στα οποία τα μέλη τους έρχονται και φεύγουν βασισμένα ίσως στην φυσική τους θέση ή στα ενδιαφέροντά τους εκείνη τη στιγμή. Τα peer to peer δίκτυα είναι ιδανικά για ad hoc δικτυώσεις των κόμβων καθώς ανέχονται διακοπές στις συνδέσεις.

Τα πλεονεκτήματα αυτά, βέβαια, αντισταθμίζονται από μια σειρά μειονεκτημάτων. Οι μηχανισμοί ασφαλείας όπως η επικύρωση και η εξουσιοδότηση μπορούν να υλοποιηθούν ευκολότερα στα δίκτυα με κεντρικό server. Επίσης η διαθεσιμότητα των πόρων και των υπηρεσιών σε μικρά δίκτυα δεν μπορεί πάντα να εγγυηθεί λόγω των διακοπών των συνδέσεων.

Για παράδειγμα, στα δίκτυα διαμοιρασμού αρχείων απαιτείται η δημιουργία μεγάλου αριθμού αντιγράφων ώστε να εγγυηθεί το επιθυμητό επίπεδο διαθεσιμότητας. Το γεγονός αυτό, βέβαια, έχει σαν αποτέλεσμα την αύξηση του απαιτούμενου αποθηκευτικού χώρου.

Λόγω της ευρύτατης διάδοσής τους (κυρίως στον τομές του File Sharing) έχει γίνει προφανές ότι με την αποκεντρωμένη δομή τους τα δίκτυα p2p μπορούν να οδηγήσουν σε επαναστατικές εφαρμογές και να χρησιμοποιηθούν σε περιπτώσεις όπου η ιεραρχική προσέγγιση είναι απλά αδύνατη.

ΚΕΦΑΛΑΙΟ 2

2. Αδόμητα δίκτυα Peer to Peer

Σε αυτή την κατηγορία οι κόμβοι οργανώνονται σε τυχαίους γράφους, με επίπεδες τοπολογίες (flat topologies) με όλους τους κόμβους να είναι ίσοι μεταξύ τους, ή με ιεραρχικές τοπολογίες (Hierarchical topologies) όπου ένα μικρό σύνολο κόμβων (υπερκόμβοι, superpeers) χαρακτηρίζονται από αυξημένες αρμοδιότητες και δυνατότητες.

Σε αυτά τα δίκτυα δεν υπάρχει στενή σχέση μεταξύ της τοπολογίας και των σημείων (κόμβων) όπου αποθηκεύεται η πληροφορία. Η αναζήτηση και ο εντοπισμός των αντικειμένων επιτυγχάνεται κυρίως με τεχνικές flooding και random walks. Έτσι, οι αιτήσεις ανάκτησης αντικειμένων πλημμυρίζουν το δίκτυο, με κάθε κόμβο να εξυπηρετεί την αίτηση με βάση την πληροφορία που έχει αποθηκευμένη και στην συνέχεια να την προωθηθεί σε επόμενους κόμβους. Η συγκεκριμένη τεχνική δεν θεωρείται ιδιαίτερα αποδοτική, μιας και αιτήσεις αναζήτησης πληροφορίας που είναι ελάχιστα κατανεμημένη στο δίκτυο, θα πρέπει να ταξιδέψουν σε όλο το δίκτυο μέχρι να καταφέρουν να την εντοπίσουν.

2.1 Gnutella

Η Gnutella είναι ένα από τα πιο δημοφιλή peer-to-peer δίκτυα για διαμοιρασμό αρχείων (file sharing). Είναι ένα κατανεμημένο πρωτόκολλο αναζήτησης και εντοπισμού αντικειμένων σε μία επίπεδη τοπολογία. Κάθε κόμβος στο δίκτυο που εκμεταλλεύεται το πρωτόκολλο Gnutella μπορεί να είναι είτε απλός χρήστης είτε εξυπηρετητής την ίδια στιγμή. Χαρακτηριστικό τους είναι ότι δεν υπάρχει κεντρικός έλεγχος ούτε αναφορικά με την τοπολογία που σχηματίζουν οι κόμβοι αλλά ούτε και σχετικά με το που αποθηκεύονται τα αντικείμενα. Οι κόμβοι σχηματίζουν το δίκτυο ακολουθώντας ορισμένους χαλαρούς κανόνες και αφού πρώτα γνωρίζουν για την ύπαρξη ενός τουλάχιστον κόμβου μέλους του δικτύου.

Η λειτουργία του στηρίζεται σε ένα μικρό πρόγραμμα (μόλις 100Κ) που οι κόμβοι εγκαθιστούν για να έχουν την δυνατότητα δικτύωσης και που ουσιαστικά αποτελεί το πρωτόκολλο βάση του οποίου γίνεται η ανταλλαγή των δεδομένων από κόμβο σε κόμβο (από PC σε PC).

Η λειτουργία του Gnutella έχει ως εξής: Το δίκτυο απαρτίζεται από κόμβους (χρήστες) που έχουν εγκαταστήσει το λογισμικό του client και συνδέονται μεταξύ τους χωρίς συγκεκριμένη δομή. Αρχικά, για να συνδεθεί κανείς στο δίκτυο, αρκεί να εντοπίσει έναν κόμβο που συμμετέχει ήδη στο Gnutella. Εκείνος τον ενημερώνει με μια λίστα (την δική του) από άλλους κόμβους που μετέχουν στο δίκτυο. Ο κόμβος στέλνει τις ερωτήσεις του για αναζήτηση σε όλους τους ενεργά συνδεδεμένους κόμβους – συνήθως μέχρι πέντε – με εκείνον (flooding). Η ερώτηση εφόσον δεν απαντηθεί, προωθείται σε γειτονικούς κόμβους. Αν το επιθυμητό αρχείο εντοπισθεί σε περισσότερους κόμβους, τότε ο αιτών κόμβος μπορεί να κατεβάσει το αρχείο σε τμήματα από διαφορετικούς κόμβους, απευθείας. Όταν ο κόμβος αποσυνδέεται η λίστα των κόμβων που ήταν ενεργά συνδεδεμένοι σε αυτόν αποθηκεύεται τοπικά για μελλοντική χρήση.

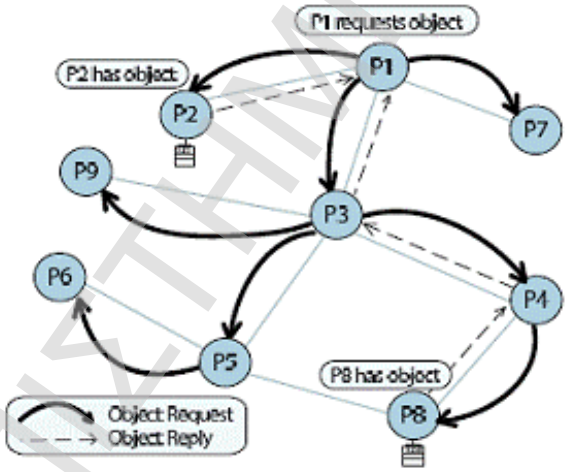
Η Gnutella λειτουργεί σαν ένα πρωτόκολλο ερωτήσεων. Για να το πετύχει αυτό χρησιμοποιεί πακέτα μηνυμάτων πέντε διαφορετικών τύπων (έκδοση 0.4).

- ping: για τον εντοπισμό κόμβων στο δίκτυο
- pong: απάντηση στο μήνυμα ping
- query: αναζήτηση αρχείου
- query hit: απάντηση στο ερώτημα της αναζήτησης
- push: κατέβασμα (download) του αιτούμενου αρχείου

Για τον περιορισμό των μηνυμάτων που προκύπτουν από την δρομολόγηση των ερωτήσεων με την μέθοδο της πλημμύρας και τον τερματισμό της αναζήτησης χρησιμοποιείται ένα πεδίο στο μήνυμα που στέλνεται, το πεδίο Time – To – Live (TTL). Κάθε φορά που στέλνεται ένα μήνυμα από έναν κόμβο η τιμή του πεδίου μειώνεται κατά ένα. Ένας κόμβος που λαμβάνει την ερώτηση την προωθεί αν το πεδίο TTL έχει τιμή μεγαλύτερη του 0 και δεν έχει ξαναδεί το μήνυμα.

Ο μηχανισμός δρομολόγησης δημιουργεί υπερφόρτωση του δικτύου με μηνύματα και σπαταλά τους δικτυακούς πόρους.
Δεν προσφέρει κανένα είδος ανωνυμία μιας και τα μηνύματα στο δίκτυο περιέχουν τις IP διευθύνσεις των κόμβων που έχουν κάποιο αντικείμενο, οπότε κάποιος χρήστης μπορεί να γνωρίζει ποιος κατέχει τι. Τελευταίες εκδόσεις του Gnutella περιλαμβάνουν την έννοια των υπερκόμβων (superpeers) που διευκολύνουν στην δρομολόγηση των αιτήσεων στο δίκτυο.

Παρά τα αρνητικά στοιχεία του Gnutella που σχετίζονται κυρίως με το θέμα της κλιμάκωσης και του τρόπου που εκτελείται η αναζήτηση, έχουν κατά καιρούς προταθεί εργασίες που μπορούν να βελτιώσουν την απόδοση του δραματικά.



Σχήμα 2.1 :Αναζήτηση αντικειμένων στο δίκτυο Gnutella

2.2 Freenet

Το δίκτυο Freenet (1999) αναπτύχθηκε με σκοπό την αποθήκευση και τον διαμοιρασμό αρχείων. Κάθε αρχείο διαχειρίζεται από το δίκτυο χρησιμοποιώντας ένα κλειδί που κατασκευάζεται με βάση το περιεχόμενο του αρχείου και πληροφορία που δίνει ο ίδιος ο χρήστης. Το Freenet αποτελεί χαρακτηριστικό παράδειγμα αδόμητου δικτύου ομοτίμων εταίρων, όπου τα αντικείμενα (αρχεία σε αυτή την περίπτωση) και οι κόμβοι στους οποίους τελικά θα αποθηκευθούν δεν καθορίζονται με κάποιο γενικό κανόνα.

Το δίκτυο Freenet προσφέρει κλιμάκωση, ανοχή σε λάθη, ενώ παράλληλα επικεντρώνεται σε θέματα που σχετίζονται με τη βιωσιμότητα των αντικειμένων στο δίκτυο καθώς και την ανωνυμία τόσο των χρηστών που αρχικά προσέφεραν κάποιο αρχείο όσο και αυτών που το κατέχουν και το διαμοιράζουν .

Τα αρχεία στο Freenet χαρακτηρίζονται από το αναγνωριστικό τους που προκύπτει με τη χρήση της SHA1 συνάρτησης κατακερματισμού. Κατά την αναζήτηση αρχείων, ο χρήστης στέλνει στο δίκτυο μία αίτηση με το αναγνωριστικό του αρχείου. ΄Οταν ένας κόμβος λάβει μια τέτοια αίτηση, ελέγχει τον τοπικό αποθηκευτικό του χώρο για την ύπαρξη του αρχείου και αν αυτό βρίσκεται εκεί το επιστρέφει στον χρήστη που έκανε την αίτηση, ακολουθώντας το αντίστροφο μονοπάτι που ακολούθησε η αίτηση αναζήτησης.

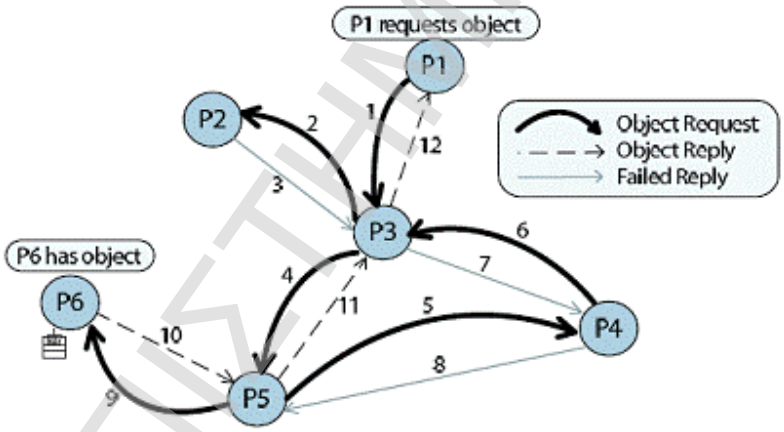
Διαφορετικά, προωθεί την αίτηση σε έναν από τους κόμβους που βρίσκονται στον πίνακα δρομολόγησης του. Ο πίνακας δρομολόγησης αποτελείται από τις διευθύνσεις των γειτονικών κόμβων ενώ παράλληλα κρατείται και πληροφορία σχετικά με τα αρχεία που έχουν αποθηκευμένα. Η επιλογή του επόμενου κόμβου που θα αποσταλεί η αίτηση βασίζεται στο αναγνωριστικό του αρχείου και τα αναγνωριστικά των κόμβων στον πίνακα δρομολόγησης, επιλέγοντας αυτόν που ταιριάζει περισσότερο. ΄Οταν τελικά το αρχείο εντοπιστεί, και κατά την αποστολή του, όλοι οι ενδιάμεσοι κόμβοι στο μονοπάτι που ακολουθεί το αρχείο προς τον τελικό κόμβο, αποθηκεύουν στον πίνακα δρομολόγησης τους πληροφορία σχετικά με το συγκεκριμένο αρχείο ώστε να διευκολυνθούν μελλοντικές αναζητήσεις.

Κάθε αίτηση στο Freenet συνοδεύεται από ένα αναγνωριστικό ώστε να αποφευχθούν οι κυκλικές διαδρομές στο δίκτυο. Επίσης, συνοδεύεται και από έναν μετρητή TTL (Time To

Live) που μειώνεται σε κάθε επιτυχημένη προώθηση της αίτησης, ώστε τελικά να κρατηθεί η κίνηση στο δίκτυο (που αφορά την αναζήτηση) σε χαμηλά επίπεδα.

Η εισαγωγή νέων αρχείων στο σύστημα γίνεται με τη δημοσίευση του αναγνωριστικού του, στους υπόλοιπους ακολουθώντας παρόμοια τεχνική με αυτή της αναζήτησης αρχείων, όπου κάθε κόμβος ενημερώνει τον πίνακα δρομολόγησης του με την προέλευση του αρχείου.

Η ανωνυμία των χρηστών επιτυγχάνεται με το να θεωρείται ο κάθε κόμβος που έχει πληροφορία για ένα αρχείο, σαν ο κόμβος που κατέχει το αρχείο. Έτσι είναι αδύνατο να γνωρίζει κανείς ποιος πραγματικά είναι ο κάτοχος (που πρώτος εισήγαγε το αρχείο στο δίκτυο). Επίσης, κάθε κόμβος που λαμβάνει μια αίτηση αναζήτησης δεν γνωρίζει αν ο κόμβος που του έστειλε την αίτηση είναι αυτός που ενδιαφέρεται για το αρχείο, ή κάποιος ενδιάμεσος στο μονοπάτι αναζήτησης.



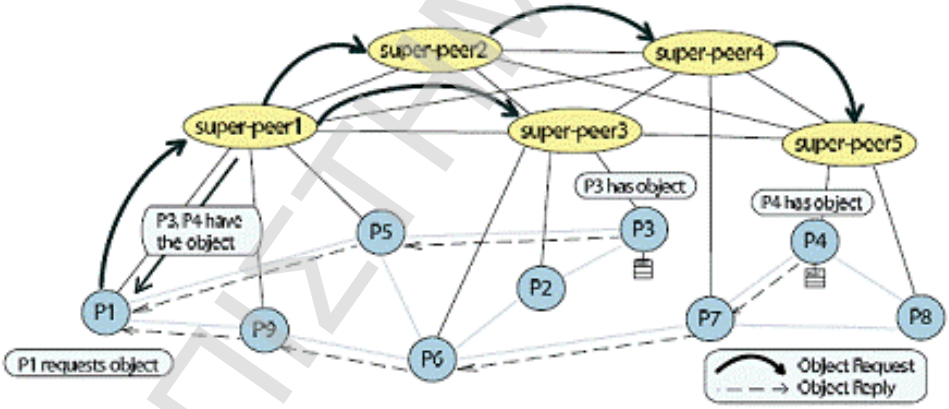
Σχήμα 2.2 Αναζήτηση αντικειμένων στο δίκτυο Freenet

2.3 Kazaa

Το Kazaa βασίζεται στο δίκτυο Fasttrack που πρωτοεμφανίστηκε το 2001. Αποτελεί κλασσικό παράδειγμα ιεραρχικής αρχιτεκτονικής. Στα *Ιεραρχικά* δίκτυα peer to peer υπάρχει η έννοια της ιεραρχίας με ορισμένους κόμβους να έχουν αυξημένες αρμοδιότητες αλλά και πόρους (αυξημένο εύρος ζώνης, αποθηκευτικό χώρο,

υπολογιστική ισχύ) και με την πλειονότητα των χρηστών να είναι συνδεδεμένοι με αυτούς και να διαμοιράζονται πληροφορία. Οι υπερκόμβοι (superpeers) οργανώνονται σε ένα δίκτυο p2p, όπου ο κάθε υπερκόμβος εξυπηρετεί ένα σύνολο των χρηστών που είναι συνδεδεμένοι με το δίκτυο, και χρησιμοποιούνται για να διευκολύνουν την αναζήτηση αντικειμένων.

Οι απλοί χρήστες μεταφέρουν πληροφορία σχετικά με τα αντικείμενα που κατέχουν στους υπερκόμβους (στα πρότυπα λειτουργίας του Napster). Όλες οι αιτήσεις αναζήτησης, επίσης μεταφέρονται στους υπερ-κόμβους, οι οποίοι εκτελούν αναζήτηση στα πρότυπα του Gnutella στο δίκτυο που σχηματίζουν μεταξύ τους, ώστε να εντοπίσουν το σύνολο των χρηστών που κατέχουν ένα συγκεκριμένο αντικείμενο. Αυτή η πληροφορία επιστρέφεται στον χρήστη που εκτέλεσε την αναζήτηση που στη συνέχεια συνδέεται με τους υπόλοιπους χρήστες, ώστε τελικά να ανακτηθεί το αντικείμενο.



Σχήμα 2.2: Αναζήτηση στο Kazaa

2.4 BitTorrent

Το BitTorrent είναι ένα νέο πρωτόκολλο διαμοιρασμού και διανομής δεδομένων στο internet που δημιούργησε το 2002 ο Bram Cohen. Η πρώτη του εμφάνιση έγινε στο

CodeCon ενώ από τότε έχει γίνει ιδιαίτερα διάσημο τόσο για νόμιμη όσο και για παράνομη μεταφόρτωση (downloading).

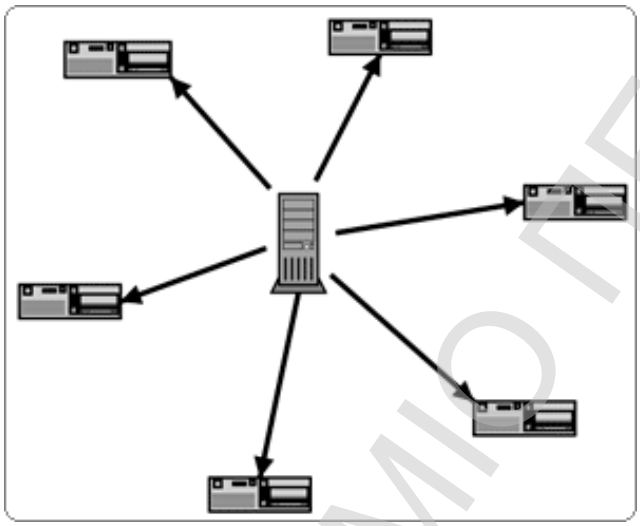
Η βασική αρχή λειτουργίας του βασίζεται στο γεγονός ότι όταν ένας πελάτης της υπηρεσίας κατεβάζει δεδομένα, ταυτόχρονα τα διαθέτει και σε άλλους πελάτες της υπηρεσίας. Όλοι οι πελάτες της υπηρεσίας που κατεβάζουν τα ίδια δεδομένα σχηματίζουν ένα δίκτυο και γνωρίζουν ο ένας την ύπαρξη του άλλου μεσώ ενός ανιχνευτή (tracker) στον οποίο συνδέονται περιοδικά και οποίος τους αποστέλλει τη λίστα με του πελάτες. Στο σχηματιζόμενο δίκτυο κάποιοι έχουν διαθέσιμο το σύνολο των δεδομένων που διανέμεται και έχουν το ρόλο μόνο του διανομέα (seed). Ο εξυπηρετητής ανίχνευσης είναι ο κεντρικός κόμβος ενός συστήματος διανομής που βασίζεται στο πρωτόκολλο BitTorrent. Ένας πελάτης που επιθυμεί να κατεβάσει κάποιο διαθέσιμο στο σύστημα αρχείο δεδομένων συνδέεται σε αυτόν και λαμβάνει τη λίστα των πελατών που κατεβάζουν το ίδιο αρχείο και έτσι ο νέος πελάτης εισάγεται στο δίκτυο διανομής.
Στο υπό εξέταση μοντέλο διανομής δεδομένων η αχρησιμοποίητη χωρητικότητα της δικτυακής σύνδεσης από τον κόμβο προς τα έξω τώρα αξιοποιείται με τον τρόπο που διανέμονται τα δεδομένα στο δίκτυο, μειώνοντας σημαντικά τον φόρτο του κεντρικού εξυπηρετητή. Οι πελάτες συμμετέχουν στην διανομή των δεδομένων και με αυτό τον τρόπο μπορεί να ικανοποιηθεί ο ίδιος αριθμός χρηστών με πολύ λιγότερες απαιτήσεις σε χωρητικότητα δικτύου από ένα κεντρικό σημείο.

Το σύστημα διανομής αρχείων BitTorrent χρησιμοποιεί τη λογική «μία σου και μία μου» (tit-for-tat) ως μέθοδο αναζήτησης με αποδοτικότητα κατά Παρέτο (Pareto efficiency). Επιτυγχάνει ένα υψηλό επίπεδο ευρωστίας και χρησιμοποίησης πόρων συγκρινόμενο με οποιαδήποτε αυτήν την περίοδο γνωστή τεχνική.

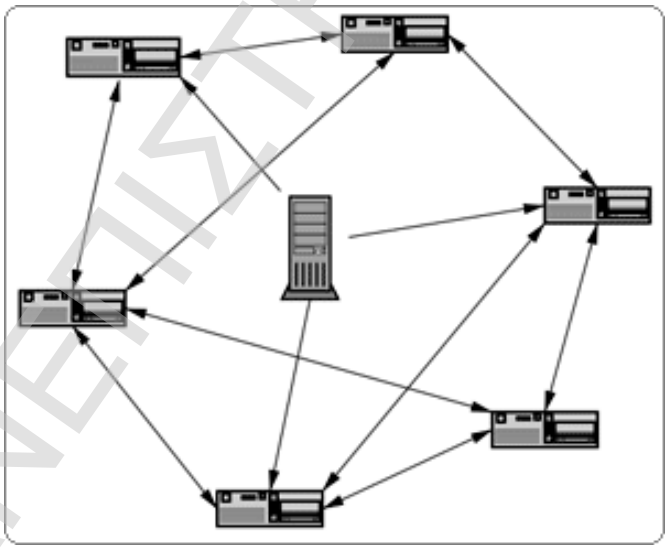
Μια εφαρμογή που χρησιμοποιεί το πρωτόκολλο BitTorrent για τη διανομή δεδομένων επιτρέποντας την δραστική μείωση των δικτυακών απαιτήσεων χωρίς αντίστοιχη μείωση των υποστηριζόμενων χρηστών είναι και η ανοιχτού κώδικα εφαρμογή Aelitis Azureus.

Για να αρχίσει μια εφαρμογή BitTorrent, ένα στατικό αρχείο με την επέκταση *.torrt* τίθεται σε έναν συνηθισμένο κεντρικό υπολογιστή δικτύου. Το *.torrent* περιέχει κάποιες πληροφορίες για το αρχείο όπως το μήκος του, το όνομα, τη σύνοψη SHA1 του περιεχομένου του και τη URL διεύθυνση του ανιχνευτή (tracker). Οι ανιχνευτές βοηθούν

τους χρήστες που ενδιαφέρονται για το συγκεκριμένο αρχείο να βρεθούν μεταξύ τους. Μιλούν ένα πολύ απλό πρωτόκολλο τοποθετημένο σε στρώσεις πάνω από το HTTP ή HTTPS, στο οποίο κάθε κόμβος στέλνει τις πληροφορίες για το αρχείο που μεταφορτώνει, τη θύρα στην οποία ακούει και παρόμοιες πληροφορίες, ενώ ο ανιχνευτής αποκρίνεται με έναν κατάλογο κόμβων που μεταφορτώνουν το ίδιο αρχείο. Ο κάθε κόμβος χρησιμοποιεί έπειτα αυτές τις πληροφορίες για να συνδεθεί με τους υπόλοιπους.



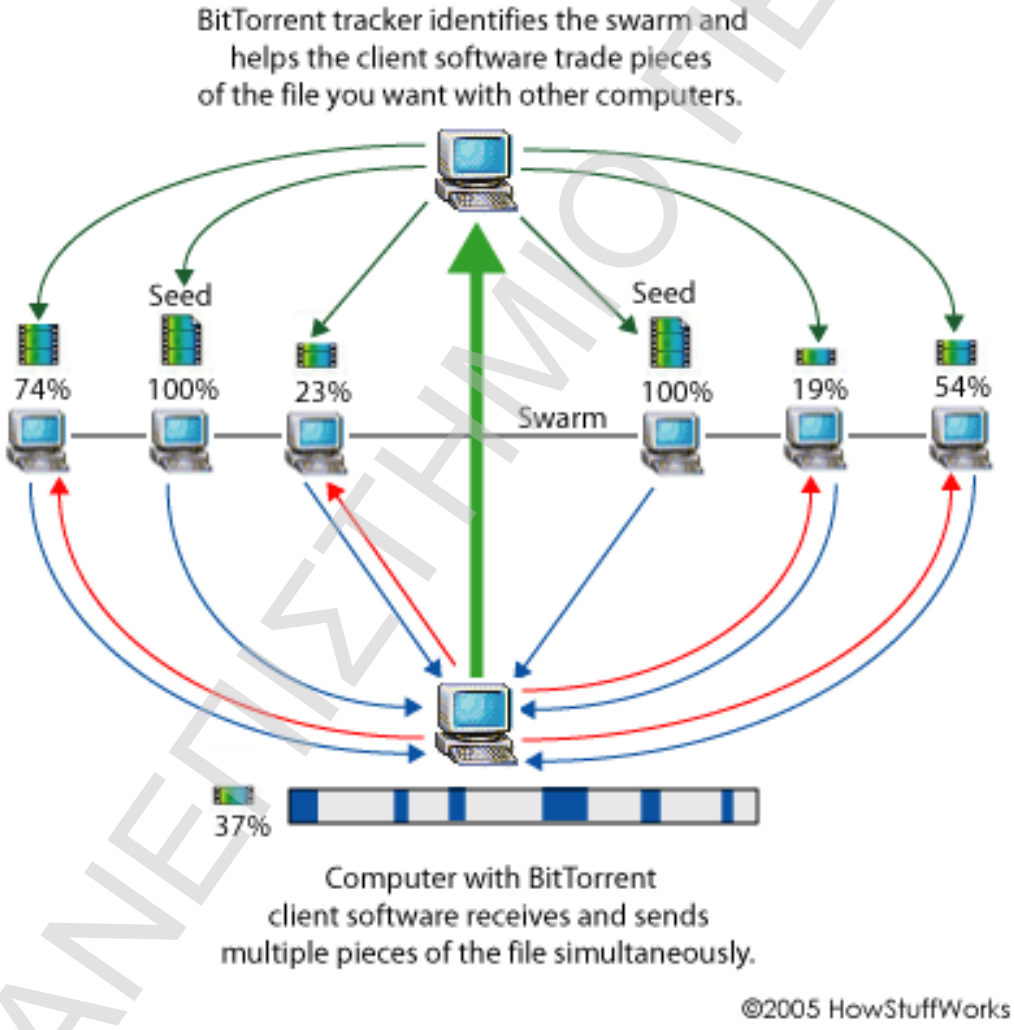
Σχήμα 2.3: Ο κλασικός τρόπος μεταφοράς αρχείων



Σχήμα 2.4: Μεταφορά αρχείων με BitTorrent

Για να καθίσταται δυνατή η λειτουργία του πρωτοκόλλου πρέπει τουλάχιστον ένας κόμβος που συμβαίνει να έχει το πλήρες αρχείο ήδη, γνωστός ως διανομέας (seed), να είναι συνδεδεμένος.

Οι απαιτήσεις εύρους ζώνης του ιχνηλάτη και του κεντρικού υπολογιστή δικτύου είναι πολύ χαμηλές, ενώ ο διανομέας πρέπει να στείλει τουλάχιστον ένα πλήρες αντίγραφο του αρχικού αρχείου.



Σχήμα 2.5: Λειτουργία BitTorrent

ΚΕΦΑΛΑΙΟ 3

3. Δομημένα δίκτυα Peer to Peer

Στα δομημένα δίκτυα ομοτίμων εταίρων, υπάρχει η έννοια της δομής με βάση την οποία δημιουργείται η τοπολογία και η συνεκτικότητα του δικτύου, η οποία διασφαλίζεται με τη βοήθεια προηγμένων κατανεμημένων δομών δεικτοδότησης, όπως για παράδειγμα των Κατανεμημένων Πινάκων Κατακερματισμού (DHT Distributed Hash Table).

Σε ένα DHT κάθε κόμβος έχει ένα μοναδικό αναγνωριστικό nodeID το οποίο έχει επιλεχθεί τυχαία από ένα πολύ μεγάλο χώρο διευθύνσεων. Κάθε αντικείμενο (για παράδειγμα κάποιο έγγραφο, ένα αρχείο μουσικής κτλ.) αντιστοιχίζεται με ένα κλειδί που αποτελεί ένα μοναδικό αναγνωριστικό για το αντικείμενο, που και αυτό έχει επιλεχθεί από τον ίδιο χώρο διευθύνσεων που χρησιμοποιείται για τα αναγνωριστικά των κόμβων. Η βασική ιδέα είναι η αποθήκευση των αντικείμενων στους κόμβους των οποίων το αναγνωριστικό είναι ίδιο ή αριθμητικά πολύ κοντά στο κλειδί του αντικειμένου. ΄Ετσι, κατά την αναζήτηση, αρκεί να επισκεφθούμε τον κόμβο με αναγνωριστικό ίσο με αυτό του αντικειμένου.

Τα περισσότερα DHTs εγγυώνται τη δρομολόγηση ενός μηνύματος στον κατάλληλο κόμβο (με βάση το αναγνωριστικό του) σε O(log(N)) βήματα (hops) σε ένα δίκτυο με N κόμβους (αυτή η διαδικασία συνήθωςαποκαλείται DHT lookup()). Επίσης η ποσότητα πληροφορίας που διατηρείται σε κάθε κόμβο και σχετίζεται με την δρομολόγηση (πίνακας δρομολόγησης, λίστες γειτονικών κόμβων κτλ.) είναι λογαριθμική συνάρτηση του αριθμού των κόμβων N.

Σε αυτή τη κατηγορία ανήκουν τα πιο γνωστά δίκτυα ομοτίμων εταίρων, όπως το CAN, CHORD, Pastry, Tapestry, Bamboo, SkipNet και άλλα.

3.1 Pastry

Το p2p δίκτυο Pastry, όπως επίσης και το Tapestry αλλά και το Bamboo, στηρίζονται στον αλγόριθμο δρομολόγησης και εντοπισμού αντικειμένων που πρώτος πρότεινε ο Plaxton το 1997. Ο Plaxton παρουσιάζει στην εργασία μία κατανεμημένη δομή δεδομένων (που είναι επίσης γνωστή και ως Plaxton Mesh) που χρησιμοποιείται για την αποδοτική δρομολόγηση μηνυμάτων και εντοπισμό αντικειμένων που είναι αποθηκευμένα σε δίκτυο αποτελούμενο από χιλιάδες κόμβους, χρησιμοποιώντας σταθερού μεγέθους πίνακες δρομολόγησης.

Σχεδιασμός του Pastry

Το σύστημα Pastry είναι ένα αυτο-διοργανούμνεο υπερκείμενο δίκτυο κόμβων όπου κάθε κόμβος δρομολογεί αιτήσεις πελατών και αλληλεπιδρά με τοπικά στιγμιότυπα μιας ή περισσοτέρων εφαρμογών. Οποιοσδήποτε υπολογιστής είναι συνδεδεμένος στο Διαδίκτυο και τρέχει λογισμικό κόμβου Pastry μπορεί να δράσει σαν κόμβος Pastry και υπόκειται μόνο στις πολιτικές ασφαλείας της εφαρμογής.

Σε κάθε κόμβο στο peer-to-peer υπερκείμενο δίκτυο Pastry ανατίθεται ένα αναγνωριστικό των 128 bits (*nodeId*). Το nodeId χρησιμοποιείται για να προσδιορίσει τη θέση του κόμβου σε έναν κυκλικό χώρο των nodeIds που κυμαίνεται από το 0 έως το 2^{128-1}. Το nodeId ανατίθεται τυχαία όταν ένας κόμβος προσχωρεί στο σύστημα. Τα nodeIds παράγονται έτσι ώστε το προκύπτον σύνολο των nodeIds να είναι ομοιόμορφα κατανεμημένο στο χώρο των nodeIds. Για παράδειγμα, τα nodeIds θα μπορούσαν να παράγονται υπολογίζοντας τον κρυπτογραφημένο κατακερματισμό του δημοσίου κλειδιού ενός κόμβου ή της IP διεύθυνσής του. Σαν αποτέλεσμα της τυχαίας ανάθεσης των nodeIds, με πολύ μεγάλη πιθανότητα, οι κόμβοι με διπλανά nodeIds διαφοροποιούνται σε γεωγραφική θέση, σε ιδιοκτήτη και σε δικαιοδοσία.

Εάν έχουμε ένα δίκτυο με N κόμβους, το Pastry μπορεί να δρομολογήσει στον αριθμητικά πλησιέστερο κόμβο σε δεδομένο κλειδί σε λιγότερα από $\log_{2^b} N$ βήματα υπό κανονικές συνθήκες (b είναι μια παράμετρος ρύθμισης με τυπική τιμή 4). Παρόλες τις ταυτόχρονες αποτυχίες κόμβων η τελική παράδοση είναι εγγυημένη, εάν δεν «πέσουν»

ταυτόχρονα |L| / 2 κόμβοι με διπλανά nodeIds (|L| είναι μια παράμετρος ρύθμισης με τυπική τιμή 16 ή 32).

Για να εξυπηρετηθεί η δρομολόγηση, τα nodeIds και τα κλειδιά θεωρούνται ακολουθίες ψηφίων με βάση 2^b. Το Pastry δρομολογεί μηνύματα στον κόμβο του οποίου το nodeId είναι αριθμητικά κοντύτερα στο δεδομένο κλειδί. Αυτό επιτυγχάνεται ως εξής: σε κάθε βήμα δρομολόγησης, ένας κόμβος προωθεί κανονικά το μήνυμα σε έναν κόμβο του οποίου το nodeId μοιράζεται με το κλειδί ένα πρόθεμα το οποίο είναι τουλάχιστον ένα ψηφίο (ή b bits) μακρύτερο από το πρόθεμα που μοιράζεται το κλειδί με τον τοπικό κόμβο. Εάν δεν υπάρχει τέτοιος κόμβος, το μήνυμα προωθείται στον κόμβο του οποίου το nodeId μοιράζεται ένα πρόθεμα με το κλειδί τόσο μακρύ όσο και ο τοπικός κόμβος, αλλά είναι αριθμητικά κοντύτερα στο κλειδί από ότι το nodeId του τοπικού κόμβου. Για να υποστηριχθεί αυτή η διαδικασία δρομολόγησης, κάθε κόμβος διατηρεί κάποια πληροφορία δρομολόγησης

Πληροφορία ανά κόμβο στο Pastry

Κάθε κόμβος Pastry διατηρεί έναν πίνακα δρομολόγησης (*routing table*), ένα σύνολο γειτονιάς (*neighborhood set*) και ένα σύνολο φύλλων (*leaf set*).

- Ο πίνακας δρομολόγησης R ενός κόμβου οργανώνεται σε $\log_2 b$ Ν γραμμές με $2^b - 1$ εγγραφές η κάθε μία. Κάθε μία από τις $2^b - 1$ εγγραφές στη γραμμή n του πίνακα δρομολόγησης αναφέρεται στον κόμβο με nodeId που μοιράζεται τα πρώτα n ψηφία με το nodeId του τοπικού κόμβου, αλλά το n+1 –ιοστό ψηφίο του έχει μία από τις $2^b - 1$ πιθανές τιμές (εκτός από το n+1 –ιοστό ψηφίο του τοπικού κόμβου).

Κάθε εγγραφή στον πίνακα δρομολόγησης περιέχει την IP διεύθυνση ενός κόμβου του οποίου το nodeId έχει το κατάλληλο πρόθεμα. Στην πράξη, επιλέγεται ένας κόμβος που είναι κοντά στον τοπικό κόμβο σύμφωνα με ένα μέτρο εγγύτητας. Αυτή η επιλογή παρέχει καλές ιδιότητες τοπικότητας. Εάν κανένας κόμβος δεν είναι γνωστός με το κατάλληλο nodeId, τότε η είσοδος του πίνακα δρομολόγησης παραμένει άδεια. Η ομοιόμορφη κατανομή των nodeIds εξασφαλίζει έναν κανονικό πληθυσμό μέσα στον χώρο των nodeIds. Έτσι, κατά μέσο όρο μόνο $\log_2 b$ N γραμμές είναι κατειλημμένες στον πίνακα δρομολόγησης.

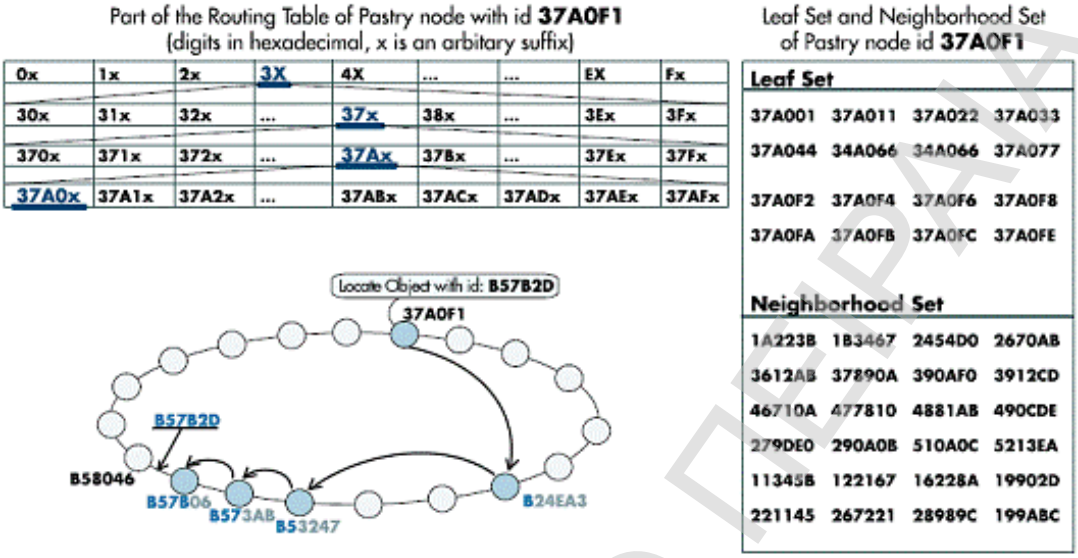
Η επιλογή του b περιλαμβάνει επιλογή ανάμεσα στο μέγεθος του κατειλημμένου ποσοστού του πίνακα δρομολόγησης (περίπου $\log_{2^b} N$ $(2X^b - 1)$ εγγραφές) και στο μέγιστο αριθμό των βημάτων που απαιτούνται για τη δρομολόγηση ανάμεσα σε δύο οποιουσδήποτε κόμβους ($\log_{2^b} N$). Με b = 4 και 10^6 κόμβους, ο πίνακας δρομολόγησης περιέχει περίπου 75 εγγραφές και ο αναμενόμενος αριθμός των βημάτων για δρομολόγηση είναι 4, ενώ με 10^9 κόμβους ο πίνακας δρομολόγησης περιέχει περίπου 105 εγγραφές και ο αναμενόμενος αριθμός των βημάτων για δρομολόγηση είναι 7.

- Το σύνολο γειτονιάς M περιέχει τα nodeIds και τις IP διευθύνσεις των |M| κόμβων που είναι κοντύτερα (σύμφωνα με το μέτρο εγγύτητας) στον τοπικό κόμβο. Το σύνολο γειτονιάς δε χρησιμοποιείται κανονικά στα μηνύματα δρομολόγησης. Είναι χρήσιμο για τη διατήρηση των ιδιοτήτων τοπικότητας.

- Το σύνολο φύλλων L είναι το σύνολο των κόμβων με τα |L| / 2 αριθμητικά αμέσως μεγαλύτερα nodeIds, και τα |L| / 2 αριθμητικά αμέσως μικρότερα nodeIds σε σχέση πάντα με το nodeId του τοπικού κόμβου. Το σύνολο φύλλων χρησιμοποιείται κατά τη δρομολόγηση μηνυμάτων. Τυπικές τιμές του |L| και του |M| είναι 2^b ή $2 X 2^b$.

Δρομολόγηση στο Pastry

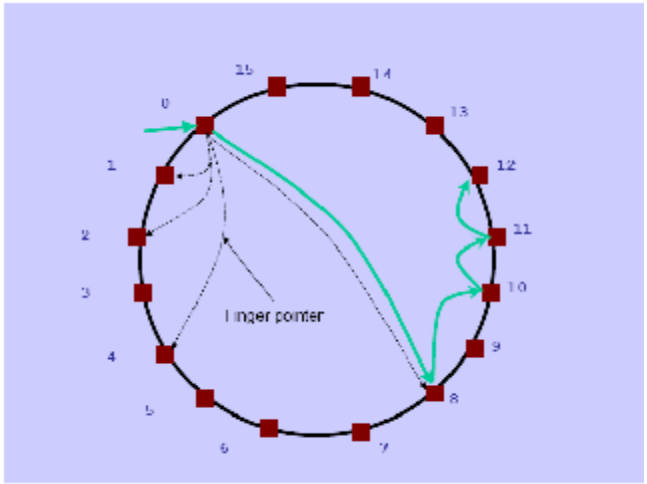
Όταν ένας κόμβος έχει ένα μήνυμα για αποστολή, πρώτα ελέγχει να δει εάν το κλειδί πέφτει στην περιοχή των nodeIds που καλύπτεται από το σύνολο φύλλων του. Εάν αυτό ισχύει, το μήνυμα προωθείται αμέσως στον κόμβο-προορισμό που θα είναι ο κόμβος στο σύνολο φύλλων με nodeId πλησιέστερα στο κλειδί (πιθανότατα ο τοπικός κόμβος).
Εάν το κλειδί δεν ανήκει στην παραπάνω περιοχή, τότε χρησιμοποιείται ο πίνακας δρομολόγησης και το μήνυμα προωθείται σε έναν κόμβο που μοιράζεται κοινό πρόθεμα με το κλειδί τουλάχιστον κατά ένα ψηφίο περισσότερο.



Σχήμα 3.1 : Αναζήτηση στο Pastry

3.2 Chord

Το Chord είναι ένα κατανεμημένο πρωτόκολλο για τον εντοπισμό δεδομένων σε ένα peer-to-peer σύστημα που αναπτύχθηκε από ομάδα του MIT και παρουσιάσθηκε το 2001 (Sigcomm conference). Βασίζεται στη λειτουργία: δεδομένου ενός κλειδιού, αυτό αντιστοιχίζεται σε έναν κόμβο, όπου αποθηκεύεται το ζεύγος κλειδί/τιμή. Πρόκειται για ένα σύστημα απλό στην κατασκευή του, ανεκτικό στις αλλαγές του peer-to-peer δικτύου και εγγυάται την εύρεση



Σχήμα 3.2:Το σύστημα Chord όπου φαίνονται τα Fingers του κόμβου 0

των δεδομένων σε χρόνο O(logN) όπου N το πλήθος των κόμβων στο δίκτυο.

Το Chord μπορεί να λειτουργήσει σε ένα δυναμικό περιβάλλον όπου οι κόμβοι εισέρχονται και αποχωρούν από το σύστημα αυθαίρετα με την απαίτηση όμως κάθε κόμβος να αποθηκεύει τμήμα της πληροφορία για επιτυχή δρομολόγηση.
Τόσο οι κόμβοι όσο και τα δεδομένα που έχουν μοναδικό m-bit (160 bits) αναγνωριστικό (ID) οργανώνονται σε έναν εικονικό δακτύλιο. Το ID του κόμβου κατακερματίζεται από την IP του, και το ID του αντικειμένου (δεδομένο) κατακερματίζεται από το όνομά του και έτσι προκύπτει η θέση τους πάνω στο δακτύλιο (δακτύλιος των 0 έως 2^m-1 θέσεων).

Οι κόμβοι κατέχουν πληροφορία για τον προηγούμενο και τον επόμενο κόμβο στο δακτύλιο. Ο κάθε κόμβος είναι υπεύθυνος για τα αντικείμενα που είναι μεταξύ του προηγούμενου κόμβου και του ίδιου.

Οι βασικές λειτουργίες που μπορούν να πραγματοποιηθούν σε ένα τέτοιο σύστημα είναι η εισαγωγή νέου κόμβου (join), η αποθήκευση και ανάκτηση δεδομένου (store & retrieve) και η αποχώρηση ενός κόμβου (leave).

Εισαγωγή κόμβου (Join)

Όταν ένας κόμβος n επιθυμεί να εισέλθει στο σύστημα κατακερματίζει την IP διεύθυνσή του για να προκύψει το αναγνωριστικό του και με κάποια διαδικασία (εξωτερικό μηχανισμό) μαθαίνει το αναγνωριστικό ενός κόμβου n' που ήδη ανήκει στο Chord. Ο νέος κόμβος χρησιμοποιεί τον n' κόμβο για να προσθέσει τον εαυτό του στο δίκτυο Chord και να αρχικοποιήσει την κατάσταση του που περιλαμβάνει και την μεταφορά κλειδιών από τον επόμενό του κόμβο, αν αυτά αντιστοιχίζονται τώρα σε αυτόν (ο κόμβος n είναι τώρα ο επόμενος τους). Η τελευταία διαδικασία απαιτεί το πολύ O(1/N) μετακινήσεις κλειδιών.

Αποχώρηση κόμβου (leave)

Όταν ένας κόμβος αποχωρεί από το σύστημα, τότε τα κλειδιά που είχε στην ευθύνη του αντιστοιχίζονται στον επόμενό του κόμβο. Η διαδικασία της ενημέρωσης καθώς οι κόμβοι έρχονται και φεύγουν από το σύστημα απαιτεί $O(\log^2 N)$ μηνύματα.

Εισαγωγή Δεδομένων

Ο κόμβος που επιθυμεί να αποθηκεύσει ένα αντικείμενο στο σύστημα εφαρμόζει μια συνάρτηση κατακερματισμού στο όνομα του αντικείμένου και προκύπτει το αναγνωριστικό του. Το νέο αντικείμενο αντιστοιχίζεται (και αποθηκεύεται) στον κόμβο που έχει ID ίσο με το ID του, αν υπάρχει ή του αμέσως επόμενου αν δεν υπάρχει.

Για την ανάκτηση του αντικειμένου χρησιμοποιείται παρόμοια διαδικασία. Εφαρμόζεται η συνάρτηση κατακερματισμού και προκύπτει η θέση του αντικειμένου και δρομολογείται η ανάκτησή του.

Η μόνη πληροφορία που είναι απαραίτητη στο σύστημα Chord για επιτυχή δρομολόγηση είναι η γνώση του επομένου. Όμως ένα τέτοιο σχήμα δεν διατηρεί την ιδιότητα της κλιμάκωσης. Για το λόγο αυτό κάθε κόμβος διατηρεί ένα τμήμα πληροφορίας για τους άλλους κόμβους βελτιώνοντας έτσι την απόδοση του αλγορίθμου. Η πληροφορία που διατηρεί ο κάθε κόμβος είναι ένας πίνακας m εγγραφών, finger table, και περιέχει τους κόμβους που βρίσκονται σε απόσταση $2^0, 2^1, 2^2, , \ldots, 2^{m-1}$ από αυτόν. Οι ερωτήσεις τώρα δρομολογούνται μέσω του finger table και η αναζήτηση ολοκληρώνεται σε O(logN) το πολύ hops.

Μία διαστρωματωμένη εφαρμογή Chord

Χρησιμοποιώντας ένα επιπλέον στρώμα μετάφρασης ονομάτων υψηλού επιπέδου σε αναγνωριστικά Chord, το Chord μπορεί να χρησιμοποιηθεί σαν μία ισχυρή υπηρεσία αναζήτησης. Έτσι, πάνω σε ένα στρώμα Chord μπορεί να τοποθετηθεί ένα στρώμα DHASH (Distributed HASH table) και μία peer-to-peer εφαρμογή αποθήκευσης. Παρακάτω φαίνεται η κατανομή της λειτουργικότητας σε μια εφαρμογή αποθήκευσης.

Στρώμα	Λειτουργικότητα
Chord	Αντιστοιχίζει αναγνωριστικά σε κόμβους - διαδόχους
DHASH	Συσχετίζει τιμές με αναγνωριστικά
Εφαρμογή	Παρέχει ένα interface συστήματος αρχείων

Αξιοπιστία και απόδοση

Το στρώμα DHASH εκμεταλλεύεται στοιχεία του Chord, για να πετύχει μεγαλύτερη αξιοπιστία και απόδοση. Για να εξασφαλίσει ότι οι αναζητήσεις θα πετύχουν ακόμα και στην περίπτωση απρόοπτων αποτυχιών κόμβων, το DHASH αποθηκεύει την τιμή που

αντιστοιχεί σε ένα δεδομένο κλειδί όχι μόνο στον άμεσο διάδοχο αυτού του κλειδιού, αλλά και στους επόμενους r διαδόχους.

Η στενή σύνδεση ανάμεσα στην προσέγγιση του DHASH για την αντιγραφή και του Chord (και τα δύο χρησιμοποιούν τη γνώση των άμεσων διαδόχων ενός κόμβου) είναι ενδεικτική της αλληλεπίδρασης ανάμεσα στο Chord και στα υψηλότερα στρώματα.
Για τη βελτίωση της απόδοσης αναζήτησης του DHASH χρησιμοποιείται η εξής ιδιότητα του αλγορίθμου αναζήτησης του Chord: οι διαδρομές προς αναζήτηση ενός συγκεκριμένου διαδόχου (ξεκινώντας από διαφορετικούς κόμβους) μέσα στο δακτύλιο του Chord είναι πολύ πιθανό να επικαλύπτονται. Αυτές οι επικαλύψεις είναι πιο πιθανό να συμβούν κοντά στο στόχο της αναζήτησης, όπου κάθε βήμα του αλγόριθμου αναζήτησης κάνει ένα μικρότερο ‘βήμα’ στο χώρο των αναγνωριστικών. Εκεί δίνεται η δυνατότητα για προσωρινή αποθήκευση δεδομένων. Σε κάθε επιτυχημένη λειτουργία αναζήτησης του ζεύγους (k, v), η τιμή-στόχος, v, αποθηκεύεται σε κάθε κόμβο στη διαδρομή των κόμβων που διασχίζεται για την εύρεση του διαδόχου του k (πρόκειται για το μονοπάτι που επιστρέφεται από τη συνάρτηση διαδόχου του Chord).

Οι επόμενες αναζητήσεις αποτιμούν τη συνάρτηση διαδόχου βήμα προς βήμα χρησιμοποιώντας τη μέθοδο *next_hop* και ρωτούν κάθε ενδιάμεσο κόμβο για την τιμή v. Η αναζήτηση τερματίζεται γρήγορα, εάν ένας από αυτούς τους κόμβους μπορεί να επιστρέψει τη νωρίτερα αποθηκευμένη τιμή v.

Συνεπώς, οι τιμές «σκορπίζονται» στο δακτύλιο του Chord κοντά στους αντίστοιχους κόμβους διαδόχους. Επειδή η ανάκτηση ενός αρχείου οδηγεί και στην προσωρινή αποθήκευσή του, τα δημοφιλή αρχεία είναι ευρύτερα αποθηκευμένα (cached) από ότι τα μη δημοφιλή. Αυτή είναι μια επιθυμητή παρενέργεια του σχεδιασμού της προσωρινής αποθήκευσης. Η προσωρινή αποθήκευση μειώνει το μήκος διαδρομής που απαιτείται για την εύρεση μιας τιμής, επομένως και τον αριθμό των μηνυμάτων ανά αναζήτηση. Και μια τέτοια μείωση είναι ιδιαίτερα σημαντική δεδομένου ότι η καθυστέρηση επικοινωνίας μεταξύ κόμβων αποτελεί μία σοβαρή στένωση επίδοσης για το σύστημα.

Επιθέσεις άρνησης υπηρεσίας

Η κατανεμημένη φύση του Chord το βοηθά να αντισταθεί σε αρκετές αλλά όχι σε όλες τις επιθέσεις DoS. Επί παραδείγματι, το Chord «αντέχει» επιθέσεις που βγάζουν εκτός λειτουργίας κάποιες γραμμές δικτύου, αφού κόμβοι που βρίσκονται κοντά στο χώρο των αναγνωριστικών είναι απίθανο να εμφανίζουν δικτυακή τοπικότητα. Για τον εμποδισμό και των άλλων επιθέσεων DoS χρειάζονται επιπλέον χειρισμοί.

Ένα σύστημα αποθήκευσης βασισμένο στο Chord μπορεί να δεχτεί επίθεση με την εισαγωγή πολύ μεγάλης ποσότητας άχρηστων δεδομένων στο σύστημα, καθώς θα αποκλειστούν από την αποθήκευση τα «νόμιμα» αρχεία. Παρατηρώντας ότι η πυκνότητα των κόμβων κοντά σε έναν οποιονδήποτε κόμβο δίνει μια εκτίμηση του αριθμού των κόμβων στο σύστημα το Chord μπορεί να προστατευτεί μερικώς από αυτήν την επίθεση περιορίζοντας τον αριθμό των αρχείων που μπορεί να αποθηκεύσει ένα κόμβος του συστήματος. Παίρνεται μια τοπική απόφαση για την αναλογία των αρχείων στο σύστημα βασισμένη στον αριθμό των κόμβων του συστήματος. Κατ' αυτόν τον τρόπο, κάθε χρήστης του συστήματος αναγκάζεται να τηρήσει αυτήν την αναλογία.

Κόμβοι που μπορούν μόνοι τους να διαλέξουν αναγνωριστικό μπορούν να διαγράψουν κάποιο κομμάτι πληροφορίας από το σύστημα θέτοντας τον εαυτό τους διάδοχο της πληροφορίας και μετά αποτυγχάνοντας να την αποθηκεύσουν, όταν αυτό τους ζητείται. Αυτή η επίθεση μπορεί να εμποδιστεί απαιτώντας κάποια αντιστοιχία του αναγνωριστικού ενός κόμβου με την κατακερματισμένη IP διεύθυνσή του.

Οι κακόβουλοι κόμβοι μπορεί να αρνούνται να εκτελέσουν ορθά το πρωτόκολλο Chord με αποτέλεσμα να παρουσιάζουν αυθαίρετη και ασυνεπής συμπεριφορά. Ένας κόμβος που δεν εμφανίζει τη σωστή συμπεριφορά μπορεί να ανιχνευτεί επαληθεύοντας τις απαντήσεις του με άλλων κόμβων που θεωρείται ότι είναι συνεργάσιμοι. Για παράδειγμα, εάν ένας κόμβος l αναφέρει ότι διάδοχός του είναι ο s, ερωτάται ο s ποιος είναι ο προηγούμενός του κόμβος. Η απάντηση που αναμένεται είναι προφανώς ο l. Μια ομάδα τέτοιων κόμβων, όπως ο s, μπορεί να συνεργαστεί για τη συγκρότηση ενός δικτύου Chord με «έμπιστους» κόμβους. Δεν υπάρχει κατανεμημένη λύση στο παραπάνω πρόβλημα, αλλά θεωρώντας ότι οι κόμβοι αρχικοποίησης είναι «έμπιστοι» αποφεύγεται μια τέτοια επίθεση.

Αυθεντικότητα

Ένα σύστημα αρχείων βασιζόμενο στο Chord μπορεί να παρέχει εγγυήσεις αυθεντικότητας με χρήση μηχανισμών του εξυπηρετητή SFS Read-Only (SFSRO). Με τον όρο αυθεντικότητα εννοείται η επιβεβαίωση της ακεραιότητας του αρχείου. Στον SFSRO τα blocks του συστήματος αρχείων ονομάζονται σύμφωνα με τον κρυπτογραφημένο κατακερματισμό των περιεχομένων τους. Αυτό το αναγνωριστικό δεν μπορεί από τη φύση του να πλαστογραφηθεί. Για την ονομασία συστημάτων αρχείων χρησιμοποιούνται ονόματα διαδρομών (pathnames) που πιστοποιούνται μόνα τους: το block που περιέχει τον αρχικό δείκτη (root inode) ενός συστήματος αρχείων ονομάζεται σύμφωνα με το δημόσιο κλειδί του εκδότη και υπογράφεται από αυτό το δημόσιο κλειδί.

Το στρώμα DHASH μπορεί να επαληθεύσει ότι ο αρχικός δείκτης έχει υπογραφεί με το κλειδί με το οποίο έχει εισαχθεί. Έτσι, εμποδίζονται οι μη-εξουσιοδοτημένες ανανεώσεις σε ένα σύστημα αρχείων.

Τέλος, η ονομασία των συστημάτων αρχείων με δημόσιο κλειδί δεν παράγει ανθρωπίνως κατανοητά ονόματα αρχείων. Ωστόσο αυτό δεν αποτελεί σοβαρό μειονέκτημα σε ένα περιβάλλον hypertext, ή σε ένα περιβάλλον με δείκτες και συμβολικές συνδέσεις.

Προβλήματα του Chord

Οι εφαρμογές που έχουν δομηθεί πάνω στο Chord αντιμετωπίζουν έναν αριθμό προβλημάτων, όπως τα παρακάτω:

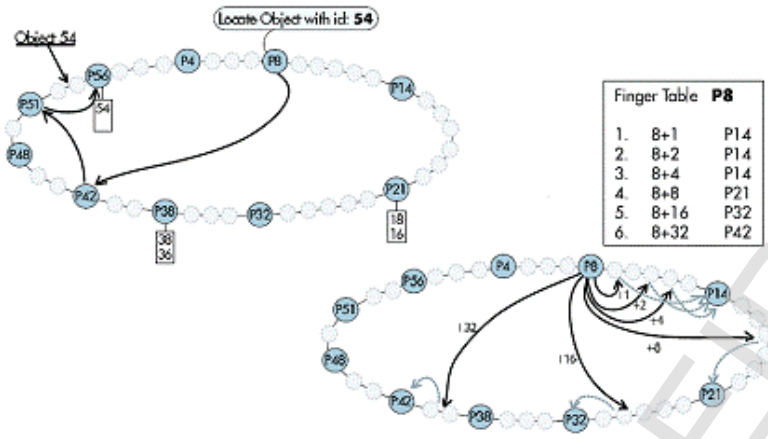
- Ο παραπάνω σχεδιασμός ηθελημένα διαχωρίζει ερωτήσεις ανωνυμίας από τη διαδικασία του εντοπισμού. Η ανώνυμη δημοσίευση και το ανώνυμο διάβασμα είναι δύσκολο να προστεθούν σε ένα σύστημα Chord δεδομένης της ισχυρής αντιστοίχησης μεταξύ ενός αρχείου και του κόμβου που είναι υπεύθυνος για την εξυπηρέτηση αυτού του αρχείου. Με ένα υπερκείμενο δίκτυο mix-network πάνω στο Chord θα μπορούσε να υποστηριχτεί η ανώνυμη δημοσίευση και το ανώνυμο διάβασμα.

- Η δόμηση ενός καταλόγου με όλα τα αρχεία που είναι αποθηκευμένα στο Chord είναι μια στρωτή και απλή διαδικασία: ένας δείκτης μπορεί να επισκέπτεται κάθε κόμβο στο σύστημα ακολουθώντας τους δείκτες στους διαδόχους. Ωστόσο, η αποθήκευση ενός δείκτη και η εξυπηρέτηση ερωτήσεων χωρίς την καταφυγή σε μια γενική αρχή παραμένει ένα ανοικτό θέμα. Εναλλακτικά, θα μπορούσε το σύστημα Chord να δίνεται σε έναν WWW gateway και να εξυπηρετείται από τις υπάρχουσες υπηρεσίες καταλόγου.

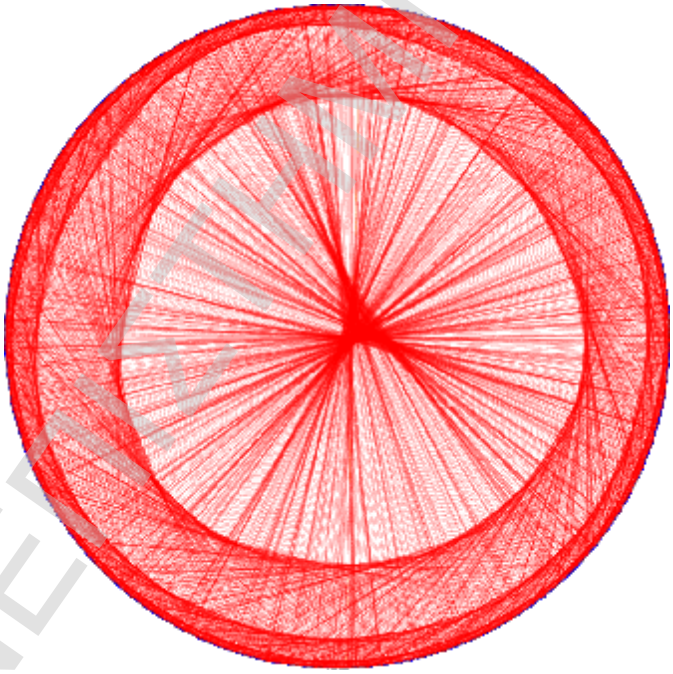
- Η κατεύθυνση αιτήσεων σε εξυπηρετητές κοντινούς στη δικτυακή τοπολογία είναι σημαντικό για τη μείωση των καθυστερήσεων των αιτήσεων. Για να γίνει αυτό πρέπει να μετρηθεί η απόδοση των εξυπηρετητών στο σύστημα. Ωστόσο, επειδή το Chord διανέμει επιθετικά αρχεία σε άσχετους μεταξύ τους εξυπηρετητές σε ένα μεγάλο δίκτυο δεν είναι πολύ πιθανό να συναντήσουμε τον ίδιο εξυπηρετητή πολλαπλές φορές. Αυτό δυσκολεύει αρκετά τη διατήρηση τεχνικών μέτρησης για την απόδοση των εξυπηρετητών.

Συμπερασματικά

Η επίδοση και η αξιοπιστία των συστημάτων peer-to-peer περιορίζεται από μη ελαστικές αρχιτεκτονικές που επιχειρούν να βρουν λύση σε πολλά προβλήματα. Χρησιμοποιώντας το βασικό στρώμα Chord για το διαχωρισμό των προβλημάτων της κατανομής δεδομένων, της αυθεντικότητας και της ανωνυμίας, τα συστήματα peer-to-peer μπορούν να αποφασίσουν πού να συμβιβαστούν και σαν αποτέλεσμα προσφέρουν καλύτερη επίδοση, μεγαλύτερη αξιοπιστία και ακεραιότητα.



Σχήμα 3.3: Αναζήτηση στο Chord



Σχήμα 3.4: Chord δίκτυο με 1000 κόμβους

3.3 CAN

Το μεγαλύτερο πλεονέκτημα για ένα σύστημα peer-to-peer είναι η ευκολία κλιμάκωσής του. Η διαδικασία peer-to-peer μεταφοράς ενός αρχείου είναι από τη φύση της κλιμακούμενη, αλλά η πραγματική δυσκολία έγκειται στην εύρεση του κόμβου που διαθέτει το αρχείο**.** Δίκτυα Διευθυνσιοδότησης σύμφωνα με το Περιεχόμενο (Content-Addressable Networks - CANs) είναι τα δίκτυα που χρησιμοποιούν ένα σχήμα δεικτοδότησης για την αντιστοίχηση ονομάτων αρχείων σε θέση στο σύστημα.

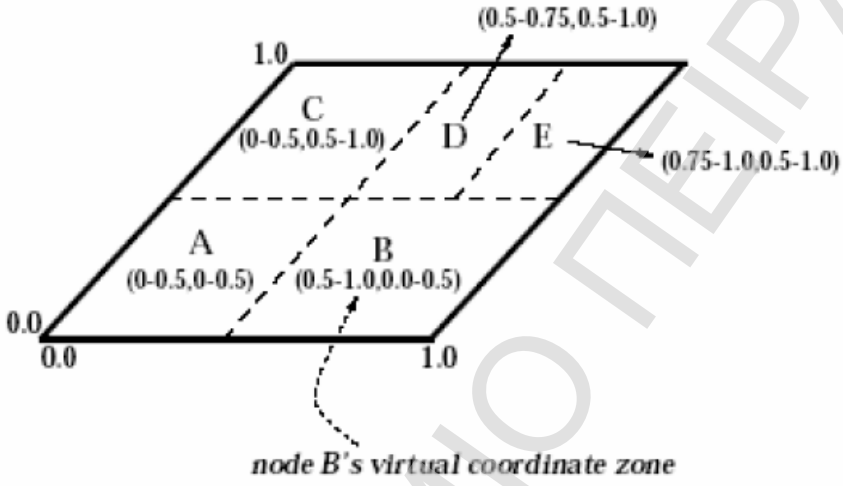
Τα CANs, εκτός από τα συστήματα peer-to-peer, βρίσκουν εφαρμογή και σε συστήματα οργάνωσης αποθήκευσης μεγάλης κλίμακας, όπως το OceanStore, το Farsite και το Publius. Και αυτά τα συστήματα απαιτούν αποδοτική εισαγωγή και ανάκτηση περιεχομένου σε μία μεγάλη κατανεμημένη υποδομή αποθήκευσης και έτσι ένας εύκολα κλιμακούμενος μηχανισμός δεικτοδότησης είναι απαραίτητος.

Μια άλλη πιθανή εφαρμογή των CANs θα μπορούσε να είναι η κατασκευή υπηρεσιών ανάλυσης ονόματος (name resolution) ευρείας κλίμακας, οι οποίες, σε αντίθεση με το DNS, θα αποσυνδέουν το σχήμα της ονοματοδοσίας από τη διαδικασία της ανάλυσης ονόματος και έτσι θα επιτρέπουν τη χρήση αυθαίρετων και ανεξάρτητων από τη θέση σχημάτων ονοματοδοσίας.
Γενικά, σκοπός των CANs (και ειδικότερα της αφαιρετικής δομής ενός πίνακα κατακερματισμού) είναι να χρησιμοποιηθούν σαν σχεδιαστικό εργαλείο από τους σχεδιαστές Διαδικτύου για την ανάπτυξη νέων εφαρμογών και μοντέλων επικοινωνίας.

Ένα CAN αποτελεί κλειδί. Αυτός ο CAN σχεδιασμός είναι εντελώς κατανεμημένος (δεν απαιτείται καμιάς μορφής κεντρικός έλεγχος, συνεργασία ή ρύθμιση), κλιμακούμενος (οι κόμβοι διατηρούν μονάχα μια μικρή ποσότητα της πληροφορίας ελέγχου, η οποία είναι ανεξάρτητη από τον αριθμό των κόμβων στο σύστημα) και ανεκτικός σε σφάλματα (οι κόμβοι μπορούν να συνεχίζουν τη δρομολόγηση παρά τις αποτυχίες). Επίσης, δε χρησιμοποιεί καμιά μορφή ιεραρχικής δομής ονοματοδοσίας (όπως το DNS ή η IP δρομολόγηση), για να πετύχει καλή κλιμάκωση και μπορεί να υλοποιηθεί εξολοκλήρου σε επίπεδο εφαρμογής.

Ένας συγκεκριμένος CAN σχεδιασμός

Το κυριότερο στοιχείο αυτής της σχεδίασης είναι ένας εικονικός d-διάστατος καρτεσιανός χώρος συντεταγμένων. Σε κάθε χρονική στιγμή ολόκληρος ο χώρος κατανέμεται δυναμικά ανάμεσα σε όλους τους κόμβους του συστήματος, έτσι ώστε κάθε κόμβος να έχει τη δική του ζώνη μέσα στο χώρο.



Εικόνα 3.5: Διδιάστατος [o,1]*[0,1] χώρος συντεταγμένων κατανεμημένος ανάμεσα σε 5 κόμβους

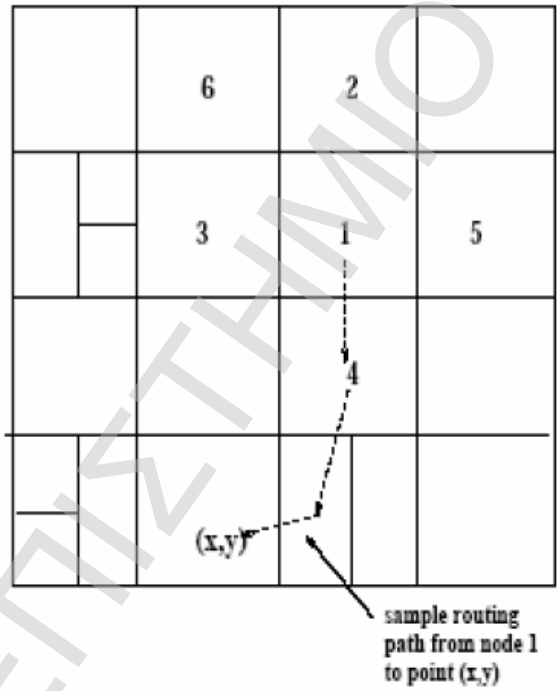
Αυτός ο εικονικός χώρος συντεταγμένων χρησιμοποιείται, για να αποθηκεύσει ζεύγη (κλειδί, τιμή). Για την αποθήκευση του ζεύγους (K1,V1), το κλειδί K1 αντιστοιχίζεται συγκεκριμένα σε ένα σημείο P του χώρου με τη χρήση μιας ομοιόμορφης συνάρτησης κατακερματισμού. Το ζεύγος (K1,V1) θα αποθηκευτεί στον κόμβο, ο οποίος κατέχει τη ζώνη, στην οποία «πέφτει» το σημείο P. Για την ανάκτηση του αντικειμένου με κλειδί K1, ο εκάστοτε κόμβος μπορεί να εφαρμόσει την ίδια συνάρτηση κατακερματισμού, για να αντιστοιχίσει το κλειδί K1 στο σημείο P και μετά να ανακτήσει την αντίστοιχη τιμή από το P. Εάν το σημείο P δεν ανήκει στον κόμβο που κάνει την αναζήτηση ή στους γείτονές του, η αίτηση πρέπει να δρομολογηθεί μέσω της CAN υποδομής μέχρι να φτάσει στον κόμβο με τη ζώνη που περιέχει το P. Συνεπώς, η αποδοτική δρομολόγηση είναι ένα κρίσιμο κομμάτι του CAN.

Οι κόμβοι στο CAN αυτο-διοργανώνονται σε ένα υπερκείμενο δίκτυο, το οποίο αναπαριστά τον εικονικό χώρο συντεταγμένων. Κάθε κόμβος μαθαίνει και διατηρεί τις IP

διευθύνσεις των κόμβων που κατέχουν τις ζώνες, οι οποίες γειτονεύουν στο χώρο των συντεταγμένων με τη δική του ζώνη. Αυτό το σύνολο των άμεσων γειτόνων στο χώρο ουσιαστικά είναι ένας πίνακας δρομολόγησης που επιτρέπει τη δρομολόγηση ανάμεσα σε δύο αυθαίρετα σημεία στο χώρο.

Δρομολόγηση στο CAN

Όπως αναφέρθηκε και παραπάνω, ένας κόμβος CAN διατηρεί έναν πίνακα δρομολόγησης με τις IP διευθύνσεις και εικονικές ζώνες όλων των άμεσων γειτόνων του στο χώρο των συντεταγμένων. Σε έναν d-διάστατο χώρο δύο κόμβοι είναι γειτονικοί, εάν τα διαστήματα των συντεταγμένων τους δεν επικαλύπτονται για d - 1 διαστάσεις και συνορεύουν κατά μήκος μίας μόνο διάστασης. Έτσι, στην Εικόνα 3 ο κόμβος 5 είναι γείτονας του κόμβου 1, ενώ ο κόμβος 6 δεν είναι γείτονας του κόμβου 1.



Εικόνα 3.6 : Παράδειγμα διδιάστατου χώρου.
Το σύνολο των γειτόνων του κόμβου 1 είναι {2,3,4,5}

Αυτή η πληροφορία είναι αρκετή για τη δρομολόγηση ανάμεσα σε δύο αυθαίρετα σημεία στο χώρο των συντεταγμένων, εφόσον ένα μήνυμα CAN περιλαμβάνει τις συντεταγμένες του προορισμού του. Χρησιμοποιώντας τις συντεταγμένες των γειτόνων του, ένας κόμβος δρομολογεί ένα μήνυμα προς τον προορισμό του προωθώντας το στο γείτονα με

τις πλησιέστερες συντεταγμένες στις συντεταγμένες του προορισμού. Για ένα χώρο d διαστάσεων χωρισμένο σε n ίσες ζώνες, το μέσο μήκος μονοπατιού δρομολόγησης είναι $(d / 4)(n^{1/d})$ βήματα και κάθε κόμβος διατηρεί 2d γείτονες.

Συνεπώς, σε έναν τέτοιο χώρο μπορούμε να αυξήσουμε τον αριθμό των κόμβων (άρα και των ζωνών) χωρίς να αυξάνουμε την πληροφορία ανά κόμβο, ενώ το μέσο μήκος μονοπατιού θα αυξάνει με πολυπλοκότητα $O(n^{1/d})$.

Επιπλέον, υπάρχουν προφανέστατα πολλά διαφορετικά μονοπάτια ανάμεσα σε δύο σημεία στο χώρο, πράγμα που σημαίνει ότι, εάν ο γείτονας ενός κόμβου είναι «νεκρός», ο κόμβος μπορεί αυτόματα να δρομολογήσει την αίτησή του κατά μήκος της επόμενης καλύτερης διαδρομής. Εάν, ωστόσο, ένας κόμβος χάσει όλους τους γείτονές του προς μία συγκεκριμένη κατεύθυνση και οι διορθωτικοί μηχανισμοί που περιγράφονται αργότερα δεν καταφέρουν να γεμίσουν το κενό που δημιουργείται στο χώρο των συντεταγμένων, τότε η «άπληστη» προώθηση μπορεί να αποτύχει προσωρινά. Σε αυτήν την περίπτωση, ο κόμβος μπορεί να χρησιμοποιήσει μια επεκτεινόμενη αναζήτηση δακτυλίου (με ελεγχόμενη πλημμύρα στο unicast υπερκείμενο πλέγμα CAN), για να εντοπίσει έναν κόμβο που είναι πλησιέστερα στον προορισμό από τον εαυτό του. Έπειτα, το μήνυμα προωθείται σε αυτόν τον κόμβο και επαναφέρεται η «άπληστη» προώθηση.

Δόμηση του CAN

Όλοι οι κόμβοι σε ένα CAN κατέχουν τη δική τους ζώνη. Για να επιτραπεί σε ένα CAN να αυξήσει τον αριθμό των κόμβων του, κάθε καινούριος κόμβος που προσχωρεί στο σύστημα θα πρέπει να αποκτήσει τη δικιά του ζώνη στο χώρο των συντεταγμένων. Αυτό μπορεί να γίνει, εφόσον ένας ήδη υπάρχων κόμβος χωρίσει στη μέση τη δική του ζώνη και παραχωρήσει τη μισή στον καινούριο κόμβο.
Συγκεκριμένα, η διαδικασία ολοκληρώνεται σε τρία βήματα:

- Ο νέος κόμβος βρίσκει έναν ήδη υπάρχοντα κόμβο στο CAN :

Ένας νέος κόμβος CAN πρώτα ανακαλύπτει την IP διεύθυνση ενός οποιουδήποτε κόμβου στο σύστημα. Η λειτουργία του CAN δεν εξαρτάται από τον τρόπο που γίνεται αυτό. Υποθέτουμε ότι ένα CAN έχει ένα DNS όνομα δικτύου, το οποίο αναλύεται στην IP

διεύθυνση ενός ή περισσοτέρων κόμβων αρχικοποίησης (bootstrap nodes) του CAN. Ένας κόμβος αρχικοποίησης διατηρεί μια μερική λίστα των κόμβων CAN που πιστεύει ότι ανήκουν στο σύστημα. Για να προσχωρήσει στο CAN, ο νέος κόμβος αναζητά το όνομα δικτύου του CAN στο DNS, για να αποκτήσει την IP διεύθυνση ενός κόμβου αρχικοποίησης. Στη συνέχεια, ο κόμβος αρχικοποίησης δίνει τις IP διευθύνσεις μερικών τυχαία επιλεγόμενων κόμβων του συστήματος.

- Με χρήση των μηχανισμών δρομολόγησης CAN βρίσκει έναν κόμβο, του οποίου η ζώνη θα μοιραστεί :

Ο νέος κόμβος επιλέγει τυχαία ένα σημείο P στο χώρο και στέλνει μία JOIN αίτηση με προορισμό το σημείο P. Αυτό το μήνυμα στέλνεται στο CAN μέσω οποιουδήποτε υπάρχοντος κόμβου CAN και προωθείται σύμφωνα με τους μηχανισμούς δρομολόγησης CAN στον κόμβο που είναι υπεύθυνος για το P. Αυτός ο κόμβος χωρίζει τη ζώνη του στα δύο και αναθέτει το ένα κομμάτι στον καινούριο κόμβο. Αυτός ο χωρισμός γίνεται υποθέτοντας μια συγκεκριμένη ταξινόμηση των διαστάσεων για την επιλογή της διάστασης που θα χωριστεί, έτσι ώστε οι ζώνες να μπορούν να ενωθούν, όταν κόμβοι αποχωρούν από το σύστημα. Έτσι, σε ένα διδιάστατο χώρο μια ζώνη πρώτα θα χωριζόταν κατά την X διάσταση, μετά κατά την Y κ.ο.κ. Τα ζεύγη (κλειδί, τιμή) της μισής ζώνης που παραχωρείται μεταφέρονται στον καινούριο κόμβο.

- Οι γείτονες της ζώνης που μοιράστηκε ενημερώνονται, ώστε να συμπεριληφθεί στη δρομολόγηση ο νέος κόμβος :

Αφού έχει αποκτήσει τη ζώνη του, ο νέος κόμβος μαθαίνει τις IP διευθύνσεις των γειτόνων του από τον κόμβο που του παραχώρησε τη μισή ζώνη του. Προφανώς, και αυτός ο κόμβος ανήκει στο σύνολο των γειτόνων του νέου κόμβου και πρέπει και αυτός να ανανεώσει τη λίστα των γειτόνων του και να διαγράψει αυτούς που δεν ανήκουν πλέον σε αυτή. Τέλος, οι γείτονες του νέου και του παλιού κόμβου πρέπει να ενημερωθούν για την αλλαγή στο χώρο των συντεταγμένων.

Κάθε κόμβος στο σύστημα στέλνει ένα άμεσο μήνυμα ενημέρωσης στους γείτονές του, ακολουθούμενο από περιοδικές ανανεώσεις, με περιεχόμενο τη ζώνη που του έχει ανατεθεί τη δεδομένη χρονική στιγμή. Αυτές οι "soft-state style" ενημερώσεις

εξασφαλίζουν ότι όλοι οι γείτονες θα μάθουν γρήγορα τις τυχόν αλλαγές και θα ενημερώσουν ανάλογα το σύνολο των γειτόνων τους.

Η πρόσθεση καινούριων κόμβων επηρεάζει μόνο ένα μικρό αριθμό κόμβων σε μια μικρή περιοχή του χώρου των συντεταγμένων. Ο αριθμός των γειτόνων ενός κόμβου εξαρτάται μόνο από τις διαστάσεις του χώρου και είναι ανεξάρτητος του συνολικού αριθμού των κόμβων στο σύστημα. Έτσι, η εισαγωγή ενός κόμβου επηρεάζει μόνο O(*αριθμός διαστάσεων*) υπάρχοντες κόμβους, πράγμα πολύ σημαντικό για ένα CAN με πάρα πολλούς κόμβους.

Αποχώρηση κόμβου, ανάκαμψη και διατήρηση του CAN

Όταν κόμβοι αποχωρούν από ένα CAN, είναι απαραίτητο να διασφαλίζεται ότι οι ζώνες που είχαν καταλάβει θα περάσουν υπό την επίβλεψη των κόμβων που παραμένουν. Αυτό γίνεται με την παραχώρηση της ζώνης και της βάσης δεδομένων (κλειδί, τιμή) που συνδέεται με αυτήν σε κάποιον από τους γείτονες του αποχωρούντος κόμβου. Εάν η ζώνη ενός γείτονα μπορεί να ενωθεί με τη ζώνη του αποχωρούντος κόμβου παράγοντας μία έγκυρη ζώνη, τότε γίνεται η ένωση. Εάν αυτό δεν είναι δυνατό, τότε η ζώνη παραχωρείται στο γείτονα με τη μικρότερη ζώνη, ο οποίος προσωρινά θα μεταχειρίζεται δύο ζώνες.

Το CAN πρέπει επίσης να παραμένει σταθερό παρά τις αποτυχίες κόμβων ή δικτύου (όταν ένας ή περισσότεροι κόμβοι χάνουν συνδεσιμότητα). Αυτό ρυθμίζεται με έναν άμεσο αλγόριθμο απόκτησης ελέγχου, ο οποίος διασφαλίζει ότι ένας γείτονας του νεκρού κόμβου θα αναλάβει τη ζώνη του. Ωστόσο, σε αυτήν την περίπτωση τα ζεύγη (κλειδί, τιμή) του νεκρού κόμβου χάνονται μέχρι να ανανεωθεί η κατάσταση από τους κόμβους που κρατούν τα δεδομένα.

Υπό κανονικές συνθήκες ένας κόμβος στέλνει περιοδικά μηνύματα ανανέωσης σε κάθε έναν από τους γείτονές του περικλείοντας τις συντεταγμένες της ζώνης του και τη λίστα των γειτόνων του με τις συντεταγμένες των ζωνών τους. Μία παρατεταμένη απουσία ενός τέτοιου μηνύματος από ένα γείτονα ερμηνεύεται ως αποτυχία κόμβου.

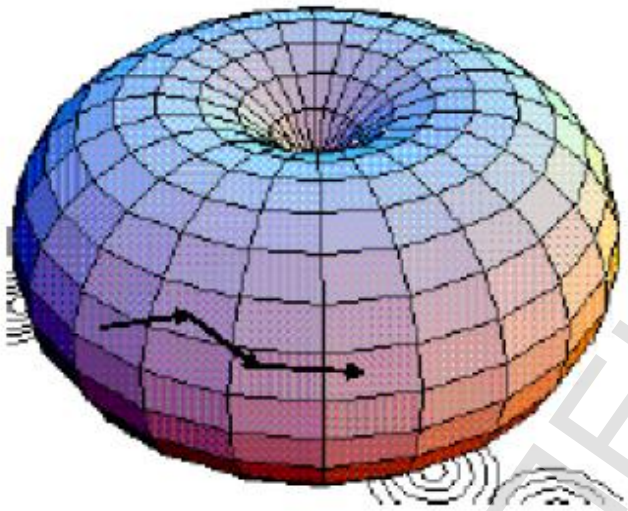
Μόλις ένας κόμβος αποφασίσει ότι ένας γείτονας του είναι νεκρός, ξεκινά το μηχανισμό κατάληψης μαζί με ένα χρονιστή απόκτησης ελέγχου. Κάθε γείτονας του νεκρού κόμβου

θα δράσει ανάλογα, με τον χρονιστή ενεργοποιημένο σε αναλογία με το μέγεθος της ζώνης του. Όταν ο χρονιστής αποπνέει, ο κόμβος στέλνει ένα μήνυμα TAKEOVER μαζί με το μέγεθος της ζώνης του σε όλους τους γείτονες του νεκρού κόμβου.

Λαμβάνοντας ένα μήνυμα TAKEOVER, κάθε κόμβος ακυρώνει τον χρονιστή του, εάν το μέγεθος της ζώνης στο μήνυμα είναι μικρότερο από το μέγεθος της δικής του ζώνης. Διαφορετικά, απαντά με το δικό του μήνυμα TAKEOVER. Με αυτόν τον τρόπο, επιλέγεται ο γείτονας-κόμβος που είναι ζωντανός και έχει τη μικρότερη ζώνη σε μέγεθος. Στην περίπτωση που «πέσουν» ταυτόχρονα πολλοί διπλανοί κόμβοι, είναι δυνατό να ανιχνευτεί η αποτυχία, εάν λιγότεροι από τους μισούς γείτονες του νεκρού κόμβου είναι ακόμα προσιτοί. Εάν ένας κόμβος αναλάβει μια άλλη ζώνη υπό αυτές τις συνθήκες, μπορεί το CAN να γίνει ασυνεπές. Σε αυτήν την περίπτωση, πριν πυροδοτηθεί ο μηχανισμός διόρθωσης, ο κόμβος ξεκινά μια επεκτεινόμενη αναζήτηση δακτυλίου για κόμβους που βρίσκονται πέρα από την περιοχή αποτυχίας και έτσι αποκτά ξανά την απαραίτητη πληροφορία για τους γειτονικούς κόμβους και μπορεί να εκκινήσει πάλι την κατάληψη με ασφάλεια.

Τέλος, και η κανονική διαδικασία αποχώρησης και ο άμεσος αλγόριθμος κατάληψης μπορούν να καταλήξουν σε έναν κόμβο που κρατά περισσότερες από μία ζώνες. Για να αποφευχθεί περαιτέρω τεμαχισμός του χώρου, ένας παρασκηνιακός αλγόριθμος συναρμολόγησης ζωνών τρέχει, για να διασφαλίσει ότι το CAN θα τείνει πάλι σε μία ζώνη ανά κόμβο.

Ανάμεσα στα προβλήματα που αντιμετωπίζει το CAN είναι η αντοχή του σε επιθέσεις DoS. Αυτό το πρόβλημα είναι ιδιαίτερα δύσκολο στην αντιμετώπιση, γιατί ένας κακόβουλος κόμβος μπορεί να συμπεριφέρεται και σαν πελάτης και σαν εξυπηρετητής. Έτσι, η έρευνα για ασφαλή CAN ακόμα συνεχίζεται. Επιπλέον, γίνεται προσπάθεια, ώστε να επεκταθούν οι CAN αλγόριθμοι και να χειρίζονται και μεταβαλλόμενο περιεχόμενο.



Σχήμα 3.7: Ο d-διάστατος χώρος CAN, Πηγή 2002, K. Aberer, EPFL-SSC, Laboratoire

3.3 Kademlia

Το Kademlia είναι ένα peer-to-peer σύστημα αποθήκευσης και αναζήτησης ζευγών (κλειδί, τιμή). Βασικό χαρακτηριστικό του είναι ότι ελαχιστοποιεί τον αριθμό των μηνυμάτων ρύθμισης που πρέπει να στείλουν οι κόμβοι, για να μάθουν όσα χρειάζεται να ξέρουν για τους άλλους κόμβους. Οι πληροφορίες ρύθμισης εξαπλώνονται αυτόματα, καθώς διεξάγονται οι αναζητήσεις κλειδιών.

Επιπλέον, οι κόμβοι έχουν την απαραίτητη γνώση και ευελιξία, ώστε να δρομολογούν ερωτήσεις μέσω διαδρομών χαμηλής καθυστέρησης. Το Kademlia χρησιμοποιεί παράλληλα ασύγχρονα ερωτήματα, για να αποφύγει καθυστερήσεις λήξης χρόνου από νεκρούς κόμβους και ο αλγόριθμος με τον οποίο ενημερώνονται οι κόμβοι για την κατάσταση των άλλων κόμβων στο σύστημα είναι ανθεκτικός απέναντι στη βασική επίθεση DoS.

Τα κλειδιά στο Kademlia είναι λέξεις των 160 bits (π.χ. ο SHA-1 κατακερματισμός μεγαλύτερων δεδομένων). Κάθε ένας από τους συμμετέχοντες στο σύστημα υπολογιστές έχει ένα node ID σε έναν χώρο κλειδιών των 160 bits. Τα ζεύγη (κλειδί,

τιμή) αποθηκεύονται σε κόμβους με IDs «κοντά» στο κλειδί. Τέλος, ο αλγόριθμος δρομολόγησης βασίζεται στα node IDs και επιτρέπει τον εντοπισμό των εξυπηρετητών κοντά σε ένα κλειδί-προορισμό από κάθε κόμβο.

Ένα από τα καινοτόμα στοιχεία του Kademlia είναι η XOR τεχνική μέτρησης της απόστασης ανάμεσα σε δύο σημεία στο χώρο των κλειδιών. Η XOR τεχνική είναι συμμετρική και επιτρέπει στους κόμβους του Kademlia να λαμβάνουν ερωτήσεις αναζήτησης από ακριβώς την ίδια κατανομή κόμβων που περιέχεται στους πίνακες δρομολόγησης τους. Ένας κόμβος Kademlia μπορεί να στείλει ερώτηση σε οποιονδήποτε κόμβο εντός ενός διαστήματος και έτσι μπορεί να επιλέξει διαδρομές ανάλογα με την καθυστέρηση ή ακόμα και να στείλει παράλληλα ασύγχρονες ερωτήσεις.
Για τον εντοπισμό κόμβων κοντά σε ένα συγκεκριμένο ID το Kademlia χρησιμοποιεί έναν απλό αλγόριθμο δρομολόγησης από την αρχή μέχρι το τέλος (άλλα συστήματα χρησιμοποιούν έναν αλγόριθμο για να πλησιάσουν το ID-στόχο και έναν άλλο για τα τελευταία λίγα βήματα).

Περιγραφή συστήματος Kademlia

Κάθε κόμβος Kademlia έχει ένα node ID των 160 bits. Κάθε μήνυμα που μεταδίδεται από έναν κόμβο περιλαμβάνει και το node ID του, επιτρέποντας κατ' αυτόν τον τρόπο στον παραλήπτη να καταγράψει την ύπαρξη του αποστολέα.
Τα κλειδιά είναι και αυτά αναγνωριστικά των 160 bits. Για τη δημοσίευση και την εύρεση ζευγών (κλειδί, τιμή) το Kademlia χρησιμοποιεί μια δική του έννοια για την απόσταση ανάμεσα σε δύο αναγνωριστικά. Δεδομένου δύο αναγνωριστικών των 160 εκφρασμένο σαν ακέραιο, d (x, y) = x XOR y.

Το XOR είναι μονοκατευθυντικό. Για κάθε δεδομένο σημείο x και απόσταση Δ > 0, υπάρχει ένα και μόνο σημείο y, για το οποίο ισχύει d (x, y) = Δ. Η μονοκατευθυντικότητα εξασφαλίζει ότι όλες οι αναζητήσεις για το ίδιο κλειδί θα συγκλίνουν στην ίδια διαδρομή ανεξάρτητα του κόμβου που την ξεκίνησε. Έτσι, η προσωρινή αποθήκευση ζευγών (κλειδί, τιμή) κατά μήκος της διαδρομής αναζήτησης μπορεί να ανακουφίσει τα δημοφιλή ζεύγη. Τέλος, η XOR τοπολογία είναι συμμετρική (x, y: d (x, y) = d (y, x)). □

Πληροφορία ανά κόμβο

Οι κόμβοι Kademlia αποθηκεύουν πληροφορίες επικοινωνίας με του άλλους κόμβους, για να δρομολογούν μηνύματα-ερωτήσεις. Για κάθε $0 \leq i < 160$, κάθε κόμβος διατηρεί μια λίστα από τριπλέτες του τύπου (IP διεύθυνση, UDP πόρτα, node ID) για κόμβους με απόσταση 2^i και 2^{i+1} από τον εαυτό του. Αυτές οι λίστες καλούνται *k-κάδοι* (k-buckets). Κάθε k-κάδος κρατείται ταξινομημένος σύμφωνα με το χρόνο τελευταίας συνάντησης. Στην κεφαλή της λίστας βρίσκεται ο κόμβος που «ακούστηκε» νωρίτερα και στην ουρά ο κόμβος που «ακούστηκε» πιο πρόσφατα. Για μικρές τιμές του i, οι k-κάδοι θα είναι γενικά άδειοι, αφού δε θα υπάρχουν οι αντίστοιχοι κόμβοι. Για μεγάλες τιμές του i, οι λίστες μπορούν να φτάσουν μέχρι και μέγεθος k, όπου k είναι η παράμετρος αντιγραφής του συστήματος. Το k επιλέγεται έτσι ώστε οποιοιδήποτε k κόμβοι να μην βρίσκονται μεταξύ τους σε περισσότερο από μία ώρα απόσταση.

Όταν ένας κόμβος Kademlia λαμβάνει ένα μήνυμα (αίτηση ή απάντηση) από έναν άλλο κόμβο, ενημερώνει τον αντίστοιχο k-κάδο με το node ID του αποστολέα. Εάν τα στοιχεία του κόμβου αποστολέα υπάρχουν ήδη στον k-κάδο του παραλήπτη, τότε ο παραλήπτης μεταφέρει την τριπλέτα στην ουρά της λίστας. Εάν δεν υπάρχουν και ο k-κάδος έχει λιγότερες από k στοιχεία, τότε ο παραλήπτης απλά εισάγει τον αποστολέα στην ουρά της λίστας. Αν πάλι ο k-κάδος είναι γεμάτος, τότε ο παραλήπτης κάνει ping στον τελευταίο κόμβο από τον οποίο «άκουσε», για να αποφασίσει τι θα κάνει. Εάν αυτός ο κόμβος δεν απαντήσει, διαγράφεται από τον κάδο και εισάγεται στην ουρά της λίστας ο νέος αποστολέας. Διαφορετικά, μεταφέρεται στην ουρά της λίστας και ο νέος αποστολέας απορρίπτεται από τον κάδο.

Οι k-κάδοι υλοποιούν αποδοτικά μια τεχνική απόρριψης του κόμβου που συναντήθηκε λιγότερο πρόσφατα χωρίς να απομακρύνουν ζωντανούς κόμβους. Αυτή η προτίμηση για παλιές επαφές πηγάζει από μία ανάλυση, κατά την οποία, όσο περισσότερο είναι ζωντανός ένας κόμβος, τόσο περισσότερο πιθανό είναι να παραμείνει ζωντανός για άλλη μια ώρα. Έτσι, κρατώντας τις παλιότερες επαφές στους κάδους οι k-κάδοι μεγιστοποιούν την πιθανότητα να περιέχουν κόμβους που θα παραμένουν συνδεδεμένοι.

Ένα δεύτερο πλεονέκτημα των k-κάδων είναι ότι παρέχουν ασφάλεια απέναντι σε συγκεκριμένες επιθέσεις DoS. Κανείς δεν μπορεί να εξαφανίσει την πληροφορία δρομολόγησης που φυλάει ένας κόμβος πλημμυρίζοντας το σύστημα με νέουςκόμβους,

γιατί οι νέοι κακόβουλοι κόμβοι θα εισαχθούν στους k-κάδους μόνο όταν αποχωρήσουν από το σύστημα οι παλιοί κόμβοι.

Πρωτόκολλο Kademlia

Το πρωτόκολλο Kademlia περιλαμβάνει τέσσερις απομακρυσμένες κλήσεις διαδικασίας (Remote Procedure Calls – RPCs): PING, STORE, FIND_NODE και FIND_VALUE.

Η *PING* RPC επιχειρεί να μάθει εάν ένας κόμβος είναι συνδεδεμένος. Η *STORE* δίνει την εντολή σε έναν κόμβο να αποθηκεύσει ένα ζεύγος (κλειδί, τιμή), για να ανακτηθεί αργότερα.

Η *FIND_NODE* παίρνει ένα ID των 160 bits σαν όρισμα. Ο παραλήπτης της RPC επιστρέφει μια τριπλέτα (διεύθυνση IP, UDP πόρτα, node ID) για τους k κόμβους που γνωρίζει ότι είναι κοντύτερα στον στόχο-ID. Αυτή η τριπλέτα μπορεί να προέρχεται από έναν και μόνο κάδο, ή μπορεί να προέρχεται από πολλούς κάδους, εάν ο κοντινότερος k-κάδος δεν είναι γεμάτος. Σε κάθε περίπτωση, ο παραλήπτης RPC πρέπει να στείλει k τεμάχια, εκτός εάν υπάρχουν λιγότεροι από k κόμβοι σε όλους συνολικά τους κάδους του, οπότε και στέλνει πληροφορία μόνο για τους κόμβους που γνωρίζει.

Η *FIND_VALUE* συμπεριφέρεται σαν την FIND_NODE –επιστρέφει και αυτή τριπλέτες- με μία εξαίρεση. Εάν ο παραλήπτης RPC έχει λάβει κλήση STORE για το κλειδί, απλά επιστρέφει την αποθηκευμένη τιμή.

Σε όλα τα RPCs, ο παραλήπτης πρέπει να συμπεριλάβει ένα τυχαίο RPC ID των 160 bits, το οποίο παρέχει κάποια αντίσταση σε απόπειρες πλαστογραφίας. Τα PINGs μπορούν επίσης να γίνουν piggy-backed σε απαντήσεις RPC, έτσι ώστε ο παραλήπτης RPC να λάβει μια επιπλέον επιβεβαίωση της διεύθυνσης δικτύου του αποστολέα.
Η πιο σημαντική εργασία για έναν κόμβο Kademlia είναι ο εντοπισμός των k κοντινότερων κόμβων σε ένα δεδομένο ID. Αυτή η εργασία καλείται *αναζήτηση κόμβου*. Το Kademlia εφαρμόζει έναν αναδρομικό αλγόριθμο για τις αναζητήσεις κόμβων. Ο κόμβος – εκκινητής της αναζήτησης – (τον ονομάζουμε *αρχικό*) διαλέγει α κόμβους από τον κοντινότερο μη-άδειο k-κάδο του. Εάν ο κάδος έχει λιγότερα από *α* στοιχεία, παίρνει απλά του κοντινότερους *α* κόμβους που γνωρίζει. Ο αρχικός στέλνει στη συνέχεια

παράλληλα και ασύγχρονα FIND_NODE RPCs στους *α* κόμβους που έχει επιλέξει. Το *α* είναι μια παράμετρος ταυτοχρονισμού του συστήματος.

Συμπερασματικά
Λόγω της πρωτότυπης τοπολογίας που βασίζεται στο XOR μέτρο απόστασης, το Kademlia είναι ένα σύστημα peer-to-peer που συνδυάζει συνέπεια, απόδοση, δρομολόγηση με ελαχιστοποιημένη καθυστέρηση και συμμετρική, μονοκατευθυντική τοπολογία. Επιπλέον, εισάγει μία παράμετρο ταυτοχρονισμού, α, που επιτρέπει την επιλογή ανάμεσα σε εύρος ζώνης για την ασύγχρονη επιλογή του βήματος με την ελάχιστη καθυστέρηση και σε ανάκαμψη από αποτυχίες ανεξαρτήτως χρόνου. Τέλος, το Kademlia είναι το πρώτο σύστημα peer-to-peer το οποίο εκμεταλλεύεται το γεγονός ότι οι αποτυχίες κόμβων είναι αντίστροφα σχετιζόμενες με το χρονικό διάστημα που οι ίδιοι κόμβοι είναι ζωντανοί.

3.4 Tapestry

Το Tapestry είναι μια επεκτάσιμη υποδομή, η οποία παρέχει αποκεντρωμένο εντοπισμό και δρομολόγηση ενός αντικειμένου (Decentralized Object Location and Routing – DOLR). Το DOLR interface εστιάζει στη δρομολόγηση μηνυμάτων σε τελικά σημεία, όπως είναι οι κόμβοι και τα αντίγραφα αντικειμένων. Το DOLR παρέχει εικονικούς πόρους, αφού τα τελικά σημεία παίρνουν ονόματα αναγνωριστικών κωδικοποιώντας μηδενική πληροφορία για τη φυσική τους θέση. Με αυτήν την υλοποίηση επιτρέπεται η παράδοση μηνυμάτων σε κινητά τελικά σημεία ή αντίγραφα τελικών σημείων κατά την παρουσία αστάθειας στην υποκείμενη υποδομή. Σαν αποτέλεσμα, ένα δίκτυο DOLR παρέχει μια απλή πλατφόρμα πάνω στην οποία μπορούν να υλοποιηθούν κατανεμημένες εφαρμογές, ενώ μπορεί να αγνοηθεί η δυναμικότητα του δικτύου. Ήδη το Tapestry έχει κάνει δυνατή την ανάπτυξη εφαρμογών αποθήκευσης μεγάλης κλίμακας όπως το OceanStore και συστημάτων multicast διανομής όπως το Bayeux.

Το Tapestry χρησιμοποιεί προσαρμοστικούς αλγόριθμους, για να επιδείξει αντοχή σε λάθη, καθώς αλλάζει το σώμα μελών του δικτύου και γίνονται δικτυακά λάθη. Η αρχιτεκτονική του είναι τμηματική και περιλαμβάνει μια εκτεταμένη λειτουργικότητα "upcall" γύρω από έναν απλό, υψηλής απόδοσης δρομολογητή. Αυτό το API επιτρέπει

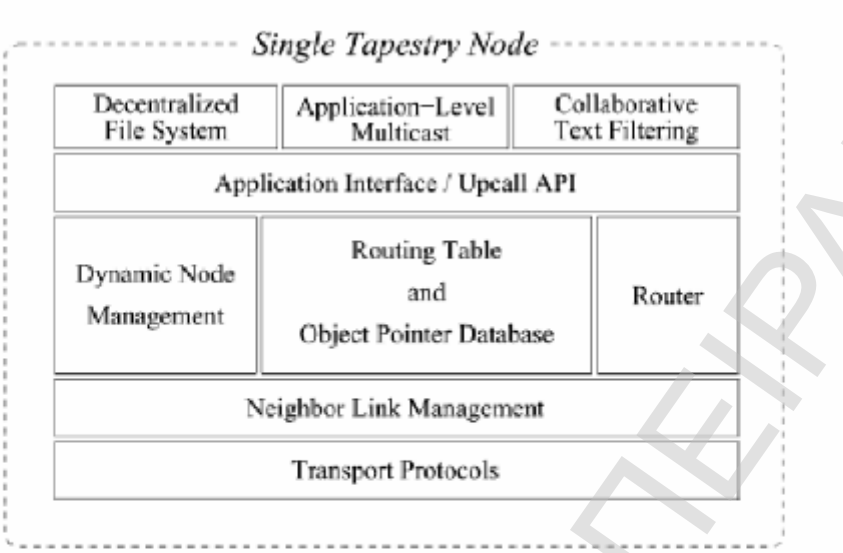
στους προγραμματιστές να αναπτύξουν και να επεκτείνουν την υπερκείμενη λειτουργικότητα, όταν η βασική λειτουργικότητα DOLR είναι ανεπαρκής για την εφαρμογή τους.

Το Tapestry επιτρέπει στις εφαρμογές να τοποθετούν αντικείμενα ανάλογα με τις ανάγκες τους και δε ρυθμίζει, όπως άλλα συστήματα peer-to-peer, τον αριθμό και τη θέση των αντιγράφων των αντικειμένων μέσω ενός DHT interface. Το Tapestry «δημοσιεύει» δείκτες θέσης μέσα στο δίκτυο, για να διευκολυνθεί η δρομολόγηση στα αντικείμενα που έχουν μικρή διασπορά στο δίκτυο. Αυτή η τεχνική δίνει στο Tapestry ιδιότητες τοπικότητας: οι ερωτήσεις για κοντινά αντικείμενα ικανοποιούνται γενικά σε χρόνο ανάλογο της απόστασης ανάμεσα στην πηγή της ερώτησης και στο πλησιέστερο αντίγραφο του αντικειμένου.

Το Tapestry είναι υλοποιημένο σε Java και υπό κανονικές συνθήκες το σχετικό κόστος καθυστέρησης (relative delay penalty – RPD) για τον εντοπισμό δύο κινητών τελικών σημείων είναι το πολύ δύο σε μία μεγάλη περιοχή. Σύμφωνα με τις προσομοιώσεις, οι λειτουργίες του Tapestry είναι επιτυχείς σχεδόν κατά το 100% του χρόνου, ενώ υπό συνεχείς δικτυακές αλλαγές και υπό μαζικές αποτυχίες ή προσχωρήσεις παρουσιάζουν μικρές περιόδους υποβαθμισμένης επίδοσης (όσο διαρκεί η αυτο-διόρθωση). Αυτά τα αποτελέσματα καταστούν το Tapestry ικανό να λειτουργήσει σαν μία υπηρεσία μακράς διαρκείας σε δυναμικά και επιρρεπή σε λάθη δίκτυα όπως το Διαδίκτυο.

Αρχιτεκτονική και υλοποίηση ενός κόμβου Tapestry

Στην παρακάτω εικόνα απεικονίζεται η λειτουργική διαστρωμάτωση ενός κόμβου Tapestry. Στην κορυφή φαίνονται οι εφαρμογές που έρχονται σε επαφή με το υπόλοιπο σύστημα μέσω του Tapestry API. Κάτω από αυτό βρίσκονται τα στρώματα δρομολόγησης (*router*) και δυναμικής διαχείρισης κόμβων (*dynamic node management*). Το πρώτο επεξεργάζεται μηνύματα δρομολόγησης και θέσης, ενώ το δεύτερο χειρίζεται την άφιξη και την αναχώρηση κόμβων στο δίκτυο. Αυτά τα δύο στρώματα επικοινωνούν μέσω του πίνακα δρομολόγησης. Στη βάση βρίσκονται τα στρώματα μεταφοράς (*transport*) και γειτονικών συνδέσεων (*neighbor links*), τα οποία μαζί παρέχουν ένα στρώμα ανταλλαγής μηνυμάτων μεταξύ των κόμβων.



Εικόνα 3.8: Αρχιτεκτονική επιμέρους τμημάτων του Tapestry. Τα μηνύματα κατευθύνονται προς τα πάνω από τα στρώματα φυσικού δικτύου και προς τα κάτω από τα στρώματα εφαρμογών. Κρίσιμο στρώμα για την επικοινωνία είναι αυτό του δρομολογητή.

Στρώμα μεταφοράς (Transport layer)

Το στρώμα μεταφοράς παρέχει την αφαίρεση των καναλιών επικοινωνίας ανάμεσα σε έναν υπερκείμενο κόμβο και σε έναν άλλο. Αντιστοιχεί στο στρώμα 4 της OSI αρχιτεκτονικής. Χρησιμοποιώντας τις δυνατότητες του εκάστοτε λειτουργικού συστήματος είναι δυνατές πολλές υλοποιήσεις καναλιών. Αυτή τη στιγμή υποστηρίζονται δύο υλοποιήσεις (TCP/IP και (UDP)/IP).

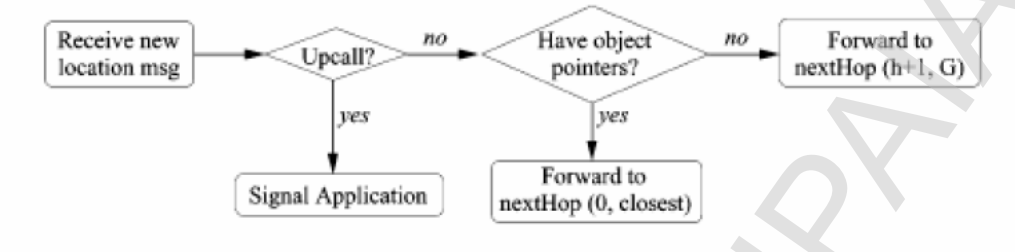
Στρώμα γειτονικών συνδέσεων (Neighbor link layer)

Πάνω από το στρώμα μεταφοράς είναι το στρώμα γειτονικών συνδέσεων. Παρέχει ασφαλείς αλλά αναξιόπιστες υπηρεσίες δεδομενογραφήματος στα παραπάνω στρώματα συμπεριλαμβανομένου του τεμαχισμού και της συναρμολόγησης μεγάλων μηνυμάτων. Την πρώτη φορά που ένα υψηλότερο στρώμα επιθυμεί να επικοινωνήσει με έναν άλλο κόμβο πρέπει να δώσει στο στρώμα γειτονικών συνδέσεων τη φυσική διεύθυνση (IP διεύθυνση και πόρτα) του προορισμού. Εάν επιθυμείται ένα ασφαλές κανάλι, πρέπει να δώσει επίσης ένα δημόσιο κλειδί για τον απομακρυσμένο κόμβο. Το στρώμα γειτονικών συνδέσεων χρησιμοποιεί αυτή την πληροφορία, για να εγκαταστήσει μια σύνδεση με τον απομακρυσμένο κόμβο.

Οι συνδέσεις ανοίγονται υπό αίτηση ανώτερων επιπέδων του Tapestry. Για να αποφευχθεί η κατάχρηση πόρων του λειτουργικού συστήματος που δεν αφθονούν, όπως οι δείκτες σε αρχεία, το στρώμα γειτονικών συνδέσεων μπορεί να κλείνει περιοδικά μερικές συνδέσεις. Οι κλεισμένες συνδέσεις ανοίγονται υπό αίτηση.
Μια σημαντική λειτουργία αυτού του στρώματος είναι η συνεχής παρακολούθηση των συνδέσεων και η προσαρμογή. Παρέχει ανίχνευση λαθών μέσω soft-state μηνυμάτων *keep-alive* και εκτιμήσεις καθυστέρησης και ποσοστού απωλειών. Το στρώμα γειτονικών συνδέσεων ενημερώνει τα υψηλότερα στρώματα όποτε τα χαρακτηριστικά ενός συνδέσμου αλλάζουν σημαντικά.

Αυτό το στρώμα βελτιστοποιεί επίσης την επεξεργασία μηνυμάτων, καθώς αναλαμβάνει το parsing των επικεφαλίδων των μηνυμάτων και το deserialising μόνο του περιεχομένου των μηνυμάτων, όταν χρειάζεται. Τέλος, η πιστοποίηση κόμβου και οι κώδικες πιστοποίησης μηνυμάτων (message authentication codes – MACs) μπορούν να ενσωματωθούν σε αυτό το στρώμα για επιπλέον ασφάλεια.

Στρώμα δρομολογητή (Router layer)
Ενώ το στρώμα γειτονικών συνδέσεων παρέχεις βασικές δικτυακές υπηρεσίες, το στρώμα δρομολογητή παρέχει μία λειτουργικότητα μοναδική στο Tapestry. Σε αυτό το στρώμα περιλαμβάνονται ο πίνακας δρομολόγησης και οι δείκτες τοπικών αντικειμένων.
Όπως έχει ήδη αναφερθεί, το δίκτυο δρομολόγησης είναι μια λίστα από σύμφωνα με το πρόθεμα ταξινομημένους γείτονες, που αποθηκεύονται στον πίνακα δρομολόγησης. Ο δρομολογητής εξετάζει το GUID προορισμού των μηνυμάτων που λαμβάνει και καθορίζει το επόμενο βήμα τους χρησιμοποιώντας τον πίνακα και τους δείκτες τοπικών αντικειμένων. Τα μηνύματα περνάνε στη συνέχεια στο στρώμα γειτονικών συνδέσεων για παράδοση.
Στην Εικόνα 3.9 βλέπουμε το διάγραμμα ροής της διαδικασίας εντοπισμού ενός αντικειμένου. Τα μηνύματα φτάνουν από το στρώμα γειτονικών συνδέσεων στα αριστερά. Κάποια από τα μηνύματα πυροδοτούν περαιτέρω upcalls και βάζουν αμέσως σε λειτουργία τους χειριστές των upcalls. Διαφορετικά, οι δείκτες στα τοπικά αντικείμενα ελέγχονται μήπως υπάρξει ταίριασμα με το GUID που αναζητείται. Εάν πράγματι βρεθούν δύο GUIDs που να ταυτίζονται, το μήνυμα προωθείται στον κοντινότερο κόμβο από το σύνολο των δεικτών που ταιριάζουν με το αναζητούμενο GUID. Αλλιώς, το μήνυμα προωθείται στο επόμενο βήμα προς τη ρίζα



Εικόνα 3.9: Διάγραμμα ροής επεξεργασίας μηνυμάτων

Πρέπει να σημειώσουμε ότι ο πίνακας δρομολόγησης και η βάση δεδομένων των δεικτών προς αντικείμενα μεταβάλλονται συνεχώς από το στρώμα δυναμικής διαχείρισης κόμβων και το στρώμα γειτονικών συνδέσεων. Για παράδειγμα, λόγω συνεχών αλλαγών στις καθυστερήσεις συνδέσεων, το στρώμα γειτονικών συνδέσεων μπορεί να αναδιατάξει τις προτιμήσεις που έχουν ανατεθεί στους γείτονες που καταλαμβάνουν την ίδια εγγραφή στον πίνακα δρομολόγησης. Ομοίως, το στρώμα δυναμικής διαχείρισης κόμβων μπορεί να προσθέσει ή να αφαιρέσει δείκτες προς αντικείμενα μετά την άφιξη ή αναχώρηση γειτόνων.

Tapestry και εφαρμογές

Έχοντας εξετάσει την υλοποίηση και τη συμπεριφορά του Tapestry, καταλήγουμε στο ότι το Tapestry παρέχει ένα σταθερό interface υπό μια ποικιλία συνθηκών δικτύου. Μένει να δούμε πως το Tapestry μπορεί να σταθεί απέναντι στις προκλήσεις που αντιμετωπίζουν οι μεγάλης κλίμακας εφαρμογές.

Με την αυξανόμενη χρησιμοποίηση του Διαδικτύου, οι μηχανικοί εφαρμογών έχουν αρχίσει να εστιάζουν σε εφαρμογές μεγάλης κλίμακας που εκμεταλλεύονται κοινούς πόρους του δικτύου. Παραδείγματα αποτελούν το multicast επιπέδου εφαρμογής, τα συστήματα αποθήκευσης μεγάλης κλίμακας, και τα συστήματα ανακατεύθυνσης κίνησης για ανθεκτικότητα και ασφάλεια. Αυτές οι εφαρμογές μοιράζονται νέες προκλήσεις, όταν πλέον μιλάμε για μεγάλες περιοχές εφαρμογής: θα είναι πιο δύσκολο για τους χρήστες να εντοπίζουν κοντινούς πόρους, καθώς μεγαλώνει το δίκτυο, και η εξάρτηση από περισσότερα κατανεμημένα επιμέρους τμήματα σημαίνει μικρότερος μέσος χρόνος μεταξύ αποτυχιών (mean time between failures – MTBF) για το σύστημα. Επί

παραδείγματι, ένας χρήστης ενός συστήματος ανταλλαγής αρχείων θέλει να εντοπίσει και να ανακτήσει ένα κοντινό αντίγραφο ενός αρχείου αποφεύγοντας αποτυχίες εξυπηρετητή ή δικτύου.

Ασφάλεια

Η ασφάλεια είναι επίσης ένα σημαντικό θέμα. Η επίθεση Sybil είναι μια επίθεση όπου ένας χρήστης παίρνει έναν μεγάλο αριθμό από IDs, για να αυξήσει τις επιθέσεις συνωμοσίας (collusion attacks). Το Tapestry αντιμετωπίζει την παραπάνω επίθεση χρησιμοποιώντας μία έμπιστη υποδομή δημόσιου κλειδιού (public-key infrastructure – PKI) για την ανάθεση των nodeIDs. Για να μειωθεί η ζημιά από ελεγχόμενους κόμβους, οι κόμβοι του Tapestry μπορούν να δουλεύουν σε ζευγάρια δρομολογώντας μηνύματα μεταξύ τους μέσω γειτόνων και επαληθεύοντας στη συνέχεια τη διαδρομή που ακολουθήθηκε. Τέλος, το Tapestry υποστηρίζει τη χρήση MACs, για να διατηρήσει την ακεραιότητα της υπερκείμενης κίνησης.

Το Tapestry, εκτός του ότι υποστηρίζει αποδοτική δρομολόγηση των μηνυμάτων σε ονομαζόμενα αντικείμενα ή τελικά σημεία στο δίκτυο, αυξομειώνεται λογαριθμικά με το μέγεθος του δικτύου σε πληροφορία δρομολόγησης ανά κόμβο και σε αναμενόμενο αριθμό υπερκείμενων βημάτων σε μία διαδρομή. Επιπλέον, εμφανίζει ανθεκτικότητα σε αποτυχίες εξυπηρετητών και αποτυχίες δικτύου επιτρέποντας στα μηνύματα να δρομολογούνται γύρω τους σε εφεδρικές διαδρομές. Οι εφαρμογές μπορούν να πετύχουν πρόσθετη αντοχή αντιγράφοντας δεδομένα σε πολλαπλούς εξυπηρετητές και περιμένοντας από το Tapestry να κατευθύνει αιτήσεις πελατών σε κοντινά αντίγραφα.
Μια ποικιλία από διαφορετικές εφαρμογές έχουν σχεδιαστεί, υλοποιηθεί και λειτουργήσει πάνω στο Tapestry. Το OceanStore είναι μία μεγάλης κλίμακας υπηρεσία αποθήκευσης υψηλής διαθεσιμότητας, η οποία έχει δοκιμαστεί στο PlanetLab Testbed. Οι εξυπηρετητές OceanStore χρησιμοποιούν το Tapestry, για να διασκορπίσουν αποδοτικά κωδικοποιημένα τμήματα αρχείων (blocks). Οι πελάτες μπορούν να εντοπίσουν γρήγορα και να ανακτήσουν κοντινά τμήματα αρχείων από το ID τους ανεξάρτητα από αποτυχίες εξυπηρετητών ή αποτυχίες δικτύου. Άλλες εφαρμογές είναι το Mnemosyne, ένα σύστημα αρχείων, το Bayeux, ένα αποδοτικό αυτο-διοργανούμενο σύστημα multicast επιπέδου εφαρμογής, και το SpamWatch, ένα αποκεντρωμένο σύστημα που φιλτράρει το "spamming" και χρησιμοποιεί μία μηχανή αναζήτησης ομοιότητας υλοποιημένη στο Tapestry.

Συμπερασματικά

Η αρχιτεκτονική εντοπισμού και δρομολόγησης του Tapestry είναι μία αυτο-διοργανούμενη, κλιμακούμενη σε μέγεθος και εύρωστη υποδομή ευρείας κλίμακας που δρομολογεί αποτελεσματικά αιτήσεις περιεχομένου υπό την παρουσία υψηλού φορτίου και λαθών δικτύου ή κόμβων. Ένα υπερκείμενο δίκτυο Tapestry μπορεί να δομηθεί αποτελεσματικά, για να υποστηρίξει δυναμικά δίκτυα χρησιμοποιώντας κατανεμημένους αλγορίθμους. Ενώ το Tapestry είναι παρόμοιο με την κατανεμημένη τεχνική αναζήτησης Plaxton, έχει πρόσθετους μηχανισμούς που εκμεταλλεύονται την soft-state πληροφορία και παρέχουν αυτόματη οργάνωση, ευρωστία, κλιμάκωση σε μέγεθος, δυναμική προσαρμογή, και ικανοποιητική υποβάθμιση/ μείωση της απόδοσης παρουσία αποτυχιών και υψηλού φορτίου.

Το Tapestry αποτελεί την πλέον κατάλληλη λύση για δυναμικά, ευρείας κλίμακας συστήματα ονοματοδοσίας αντικειμένου και δρομολόγησης μηνυμάτων, όταν αυτά τα συστήματα πρέπει να παραδώσουν μηνύματα στο πλησιέστερο αντίγραφο των αντικειμένων ή των υπηρεσιών με έναν τρόπο ανεξάρτητο θέσης, χρησιμοποιώντας μόνο τις από σημείο σε σημείο συνδέσεις και χωρίς συγκεντρωμένες υπηρεσίες. Το Tapestry το πετυχαίνει αυτό χρησιμοποιώντας την τυχαιότητα, για να επιτύχει και την κατανομή φορτίου και την τοπικότητα της δρομολόγησης.

ΚΕΦΑΛΑΙΟ 4

Τα peer to peer συστήματα εμφανίζουν μια ιδιαίτερη πρόκληση για την παροχή των διαφόρων επιπέδων ασφάλειας -διαθεσιμότητα, μυστικότητα, εμπιστευτικότητα, ακεραιότητα, και αυθεντικότητα που απαιτείται συχνά, λόγω της ανοικτής και αυτόνομης φύσης τους. Οι κόμβοι δικτύων πρέπει να θεωρηθούν untrusted συμβαλλόμενα μέρη, και καμία υπόθεση δεν μπορεί να γίνει σχετικά με τη συμπεριφορά τους.
Εστιάζουμε ιδιαίτερα στην ασφαλή αποθήκευση, την ασφαλή δρομολόγηση, τον έλεγχο πρόσβασης, την επικύρωση, και τη διαχείριση ταυτότητας.

4.1 Γενικές επιθέσεις και Υπερασπίσεις

Man-in-the-middle attack (MITM) είναι μια κοινή παραβίαση ασφάλειας. Ο επιτιθέμενος παρεμποδίζει μια νόμιμη επικοινωνία μεταξύ δύο μερών, τα οποία είναι φιλικά μεταξύ τους. Στη συνέχεια, ο κακόβουλος host ελέγχει τη ροή επικοινωνίας και μπορεί να αποσπάσει ή να αλλάξει πληροφορίες που στέλνονται από έναν από τους αρχικούς συμμετέχοντες. Man-in-the-middle επιθέσεις εφαρμόζονται ιδιαίτερα σε πρωτόκολλα όπου η ανταλλαγή κλειδιών γίνεται χωρίς επικύρωση (authentication).

Οι man-in-the-middle επιθέσεις έχουν δύο κοινές μορφές. Ο επιτιθέμενος είτε κρυφακούει (eavesdropping), είτε αλλοιώνει κατάλληλα το μήνυμα. Με eavesdropping (κρυφακοή), ένας επιτιθέμενος ακούει απλά ένα σύνολο μεταδόσεων σε και από διαφορετικούς hosts ακόμα κι αν ο υπολογιστής του επιτιθεμένου δεν είναι συμβαλλόμενο μέρος στη συνδιάλεξη. Πολλοί σχετίζουν αυτόν τον τύπο επίθεσης με διαρροή, κατά την οποία ευαίσθητες πληροφορίες μπορούν να αποκαλυφθούν σε έναν τρίτο, χωρίς αυτό να είναι εν γνώση των νόμιμων χρηστών.Οι επιθέσεις κατά τις οποίες προκαλείται αλλοίωση του μηνύματος βασίζονται στην ικανότητα του επιτιθέμενου να κρυφακούει. Ο επιτιθέμενος παίρνει αυτή την μη εξουσιοδοτημένη απόκριση, ένα ρεύμα δεδομένων (data stream), αλλάζοντας τα περιεχόμενα ώστε να ικανοποιούν έναν ορισμένο σκοπό - πιθανόν χρησιμοποιώντας ψευδή διεύθυνση IP, αλλάζοντας την διεύθυνση MAC για να μιμηθεί κάποιο άλλο host ή κάνοντας κάποια άλλη τροποποίηση.Επειδή με αυτό τον τρόπο δεν γίνεται αντιληπτός από τον αρχικό

αποστολέα ή τον παραλήπτη, ένας επιτιθέμενος μπορεί ξεγελάσει το θύμα, ώστε να του αποκαλύψει εμπιστευτικές πληροφορίες. Ο επιτιθέμενος υποκρίνεται πως είναι ο αρχικός αποστολέας, τον οποίο πιθανώς εμπιστεύεται ο παραλήπτης.

Υπερασπίσεις

Χωρίς μια κεντρική εμπιστη αρχή στα P2P στα δίκτυα, δεν είναι δυνατό να ανιχνευθεί μια Man-in-the-middle attack. Οι κόμβοι δεν έχουν πληροφορίες για τους γείτονές τους και δεν έχουν ικανό τρόπο να τον προσδιορίσουν με βεβαιότητα.

Διάδοση Σκουληκιών

Τα σκουλήκια αποτελούν ήδη μιας από τις μεγαλύτερες απειλές στο Διαδίκτυο. Ένα σκουλήκι (worm) είναι ένα μικρό κομμάτι προγράμματος που χρησιμοποιεί τα δίκτυα των υπολογιστών και τις τρύπες ασφαλείας για να αναπαράγει τον εαυτό του. Ένα αντίγραφο του προγράμματος σαρώνει το δίκτυο με σκοπό να εντοπίσει ένα άλλο μηχάνημα που να έχει μια συγκεκριμένη τρύπα ασφαλείας (security hole). Αντιγράφει τον εαυτό του στο καινούργιο μηχάνημα χρησιμοποιώντας αυτήν την τρύπα ασφαλείας και μετά ξεκινάει την αναπαραγωγή του από εκεί κοκ.

Διάδοση σκουληκιών μέσω P2P εφαρμογών θα ήταν καταστρεπτική και είναι μια από τις πολύ σοβαρές απειλές.Υπάρχουν διάφοροι παράγοντες που καθιστούν τα P2P δίκτυα ελκυστικά για τα σκουλήκια:

- τα P2P δίκτυα αποτελούνται από υπολογιστές που τρέχουν όλοι το ίδιο λογισμικό με αποτέλεσμα να είναι δυνατό με την ανέρευση ενός κενού ασφαλειας να επιτεθουν σε ολόκληρο το δίκτυο.

- οι P2P κόμβοι τείνουν να διασυνδέονται με πολλούς διαφορετικούς γειτονικούς κόμβους, οπότε το σκουλήκι που τρέχει στη P2P εφαρμογή δεν χάνει χρόνο για να βρεί άλλα θύματα.

- Οι P2P εφαρμογές εγκαθίστανται κυρίως σε προσωπικούς υπολογιστές και όχι σε servers με αποτέλεσμα ο επιτιθέμενος να έχει πρόσβαση σε ευαίσθητα αρχεία όπως αριθμοί πιστωτικών καρτών, κωδικοί πρόσβασης ή βιβλία διευθύνσεων.

Υπερασπίσεις

Πρίν εξετάστεί οποιαδήποτε τεχνική αντιμετώπιση είναι βασικό και μεγάλης σημασίας να υπάρξει ευαισθητοποίηση των P2P χρήστων έτσι ώστε να παρέχον τη μεγαλύτερη δυνατή ασφάλεια στους προσωπικούς τους υπολογιστές με ενημερωμένα ανιτιικά και firewalls.

Επιθέσεις DDoS

Οι Κατανεμημένες επιθέσεις Άρνησης Υπηρεσίας (Distributed Denial of Service attacks – DDoS attacks) αποτελούν μία μεγάλη απειλή γενικά για το Διαδίκτυο. Μέχρι τώρα δεν υπάρχει απόλυτα αποτελεσματικός μηχανισμός άμυνας σε επιθέσεις DDoS μεγάλης κλίμακας. Αν και υπάρχουν διάφορα αμυντικά συστήματα για επιθέσεις DDoS, στην πλειοψηφία τους αποδίδουν μόνο για συγκεκριμένα σενάρια με αποτέλεσμα οι επιτιθέμενοι που ξεφεύγουν από αυτά τα σενάρια να αποφεύγουν τα παραπάνω αμυντικά συστήματα. Το κλειδί για την επιτυχημένη αντιμετώπιση των επιθέσεων DDoS είναι η ευρεία εφαρμογή των μέτρων αντιμετώπισης σε περισσότερα του ενός δίκτυα. Ωστόσο αυτή δεν μπορεί σε καμία περίπτωση να θεωρηθεί κάτι εύκολο, ή ακόμα και εφικτό, γιατί εξαρτάται από την αγορά. Μέχρι τώρα καμία τεχνολογία δεν έχει καταφέρει να μονοπωλήσει την αγορά, συνεπώς είναι μάλλον απίθανο κάτι τέτοιο να συμβεί με ένα και μόνο σύστημα αντιμετώπισης επιθέσεων DDoS.

Βασικά στοιχεία μιας επίθεσης DDoS

Επίθεση DDoS έχουμε, όταν ένας αριθμός από ελεγχόμενα μηχανήματα (agents) παράγουν μεγάλο όγκο κίνησης προς το θύμα με στόχο να καταβάλλουν τους πόρους του. Είναι προφανές, λοιπόν, ότι στις επιθέσεις DDoS περιλαμβάνονται περισσότεροι από ένας επιτιθέμενοι και πιθανώς περισσότερα από ένα μηχανήματα-στόχος. Αυτές οι επιθέσεις καταλήγουν να είναι ιδιαίτερα «αποτελεσματικές» χρησιμοποιώντας την κατανεμημένη υποδομή του Διαδικτύου. Κατευθύνοντας πολλαπλές "επιθετικές" ροές κίνησης προς μία περιοχή δικτύου είναι δυνατό οι συνδέσεις, ακόμα και αν είναι υψηλής

χωρητικότητας, να κατακλυστούν και να σταματήσουν να είναι διαθέσιμες για κανονική κίνηση.

Συγκεκριμένα, μια επίθεση DDoS εξαπολύεται με τα ακόλουθα βήματα:

-βήμα 1°: οι επιτιθέμενοι διεισδύουν σε ένα αριθμό μηχανημάτων και εγκαθιστούν κώδικα ελέγχου μικρού μεγέθους και αντίκτυπου στην κανονική λειτουργία ("footprint" κώδικας). Αυτά τα μηχανήματα είναι πλέον οι masters πρώτου επιπέδου.

-βήμα 2°: οι masters πρώτου επιπέδου οργανώνουν την υποδομή της επίθεσης. Μετά από μια διαδικασία διερεύνησης (scanning) διαφόρων μηχανημάτων (από προσωπικούς υπολογιστές μέχρι μεγάλα συστήματα) για γνωστές αδυναμίες αναγνωρίζουν τα τρωτά μηχανήματα και εγκαθιστούν σε αυτά τον κώδικα που θα παράγει την επίθεση. Αυτά τα μηχανήματα ελέγχονται από τον επιτιθέμενο και ονομάζονται agents της επίθεσης, ενώ όσο τα κακόβουλα προγράμματά τους δεν είναι σε δράση ονομάζονται "zombies" ή "bots".

-βήμα 3°: μετά από εντολή του επιτιθέμενου οι agents εξαπολύουν την επίθεση ενεργοποιώντας μεγάλη ροή πακέτων προς το δίκτυο-θύμα. Αυτές οι ροές πακέτων μπορεί μεμονωμένες και κοντά στην πηγή τους να είναι σχετικά μικρές, αλλά αθροιζόμενες κοντά στο δίκτυο-θύμα καταλήγουν να καταλάβουν σημαντικό τμήμα του διαθέσιμου δικτυακού εύρους (bandwidth). Στην Εικόνα 1 φαίνονται τα πολλαπλά επίπεδα της επίθεσης.

Τα εργαλεία που μπορούν να εκκινήσουν επιθέσεις DDoS καλούνται rootkits. Είναι έτοιμα πακέτα εργαλείων hacking που αυτοματοποιούν τις εργασίες της επίθεσης και εγκατάστασης κώδικα στους agents, αφού πρώτα ανιχνευθούν τα τρωτά μηχανήματα- που θα εξυπηρετήσουν τη διάδοση του λογισμικού επίθεσης. Οι κακόβουλες ροές πακέτων που ξεκινούν από τους agents για το δίκτυο-θύμα μπορεί να είναι οποιοδήποτε είδος κίνησης (TCP, UDP, ICMP κ.λπ.) καθώς και συνδυασμοί τους.

Δυσκολίες στην αντιμετώπιση

Για να εξαπολύσει κανείς μια τέτοιου είδους επίθεση δε χρειάζεται ιδιαίτερες γνώσεις ή ικανότητες και εάν μάλιστα το θύμα δεν είναι εφοδιασμένο με αποδοτικούς αμυντικούς μηχανισμούς, θα «υποφέρει» όσο χρονικό διάστημα διαρκεί η επίθεση. Επιπλέον, οι επιτιθέμενοι δεν φοβούνται το ενδεχόμενο εντοπισμού, μιας και είναι πολύ δύσκολο να

ανιχνευτεί η επίθεση με βήματα προς τα πίσω - η διαδικασία αναφέρεται ως "Back-tracing" - που θα οδηγήσει στον εντοπισμό των agents, ενώ είναι ακόμα πιο δύσκολο να εντοπιστούν αυτοί που μόλυναν τους agents.
Ορισμένα χαρακτηριστικά των επιθέσεων DDoS που εμποδίζουν την επιτυχημένη αντιμετώπισή τους είναι:

- Φαινομενικά «νόμιμα» πακέτα: τα πακέτα των επιθέσεων μπορεί να είναι ίδια με τα «νόμιμα» πακέτα, αφού ο επιτιθέμενος στοχεύει στο να προκαλέσει πρόβλημα με τον όγκο των πακέτων και όχι το περιεχόμενό τους. Έτσι, το σύστημα ανίχνευσης επιθέσεων δεν μπορεί να διαχωρίσει τα πακέτα σε «κακόβουλα» και «νόμιμα» βασιζόμενο σε μεμονωμένα πακέτα, αλλά θα πρέπει να κρατά στατιστικά, για να συσχετίσει πακέτα και να ανιχνεύσει ανωμαλίες.

- Αυξημένος όγκος κίνησης: τα αθροιζόμενα μονοπάτια επίθεσης σχηματίζουν τόσο μεγάλη ροή που μπορεί να καταρρεύσει μέχρι και το σύστημα ανίχνευσης επιθέσεων, ενώ οι δικτυακοί τόποι που βρίσκονται πάνω στη διαδρομή της επίθεσης θα συνεχίσουν να «υποφέρουν».

- IP spoofing: οι επιτιθέμενοι συνήθως βάζουν ψεύτικη διεύθυνση στο πεδίο IP source των πακέτων της επίθεσης. Κατ' αυτόν τον τρόπο «κρύβονται» οι agents και δυσχεραίνεται ο εντοπισμός τους.

- Έλεγχος και ευελιξία: ο έλεγχος της επίθεσης από τον επιτιθέμενο έχει πολλαπλά επίπεδα, ξεκινώντας από έναν μικρό αριθμό από masters που αυξάνονται σταδιακά με την πρόσθεση των agents και μπορούν τελικώς να εξαπλωθούν σε ευρεία κλίμακα. Συγχρόνως, ο επιτιθέμενος μπορεί να εναλλάσσει τους στόχους της επίθεσης και τις πηγές της κίνησης, να ενεργοποιεί και απενεργοποιεί τμήματα της κίνησης και να μεταβάλλει τα χαρακτηριστικά των ροών σύμφωνα με τις αντιδράσεις των δικτύων που αντιλαμβάνονται με κάποιον τρόπο την επίθεση. Τέλος, στα πολλαπλά επίπεδα της επίθεσης μπορούν να προστεθούν επιπλέον επίπεδα κατά την παράδοσή της. Για παράδειγμα, αντί να στέλνονται τα πακέτα απευθείας από τα υπονομευόμενα μηχανήματα, τα τελευταία στέλνουν νόμιμες αιτήσεις σε εξυπηρετητές Διαδικτύου με διεύθυνση επιστροφής το θύμα.

Τέλος, πρέπει να σημειώσουμε ότι και τα συμβατικά IDS (Intrusion Detection Systems) αποτυγχάνουν στην αντιμετώπιση των επιθέσεων DDoS. Τα IDSs μπορούν να αναγνωρίσουν έγκαιρα μια επίθεση, αλλά δεν έχουν τη δυνατότητα διάσχισης ενός δικτυακού τόπου (domain) και κλιμακούμενης σε μέγεθος αντίδρασης. Επιπλέον, δεν υπάρχει η αναγκαία υποδομή για την ανταλλαγή αιτήσεων και απαντήσεων με άλλους δικτυακούς τόπους. Ωστόσο, ακόμα και αν κάτι τέτοιο ήταν διαθέσιμο, μία τέτοια συναλλαγή θα επέφερε πολλά ζητήματα ασφαλείας και το IDS θα έπρεπε επίσης να γνωρίζει την τοπολογία και τα interfaces των απομακρυσμένων μηχανημάτων στα άλλους δικτυακούς τόπους, για να εκδώσει τις κατάλληλες εντολές.

Τακτικές αντιμετώπισης

Σκοπός ενός αμυντικού συστήματος DDoS είναι να μειώσει την αρνητική επίδραση της επίθεσης στο θύμα και να συνεχιστεί η καλή εξυπηρέτηση των «νόμιμων» πελατών του θύματος και της «φυσιολογικής» κίνησης κατά τη διάρκεια της επίθεσης. Για να επιτευχθεί αυτό μπορεί να προσεγγίσει κανείς το θέμα της άμυνας σε επιθέσεις DDoS από τρεις πλευρές: 1) παρεμπόδιση της επίθεσης, 2) εφοδιασμός του θύματος με εργαλεία-μεθόδους, ώστε να επιβιώσει από την επίθεση, 3) ανίχνευση και αντιμετώπιση της επίθεσης.

- Για την παρεμπόδιση της επίθεσης είναι αναγκαίο να δοθεί προσοχή στα τρωτά σημεία, τα οποία εκμεταλλεύονται οι επιτιθέμενοι, για να εξαπολύσουν την επίθεση. Παρόλο που μια τέτοια προσέγγιση έχει ελπίδες να συνεισφέρει σημαντικά στην ασφάλεια Διαδικτύου, θα χρειαστεί πολύ χρόνος να αποκτήσει τέτοια πληρότητα και εξάπλωση, ώστε να εμποδίσει τις επιθέσεις DDoS.

- Για την επιβίωση του θύματος κατά την επίθεση πρέπει να αυξηθούν οι πόροι του θύματος αρκετά, ώστε να μπορεί να εξυπηρετεί και «νόμιμη» και κακόβουλη κίνηση. Κάτι τέτοιο θα μπορούσε γενικά να φέρει αποτέλεσμα σε υπηρεσίες, όπως στατικές σελίδες Web, αλλά δε θα μπορούσε να αποτελέσει γενικευμένη λύση, καθώς ο επιτιθέμενος μπορεί να αυξάνει συνεχώς τους κατανεμημένους πόρους του (αύξηση των agents), ενώ το θύμα δε θα έχει ποτέ τα ίδια περιθώρια.

- Για την ανίχνευση και αντιμετώπιση της επίθεσης απαιτείται η υλοποίηση ενός μηχανισμού με δυνατότητα ανίχνευσης της πλειοψηφίας των απειλητικών επιθέσεων, μείωσης της ροής σε λογικά επίπεδα ανεξάρτητα από τον όγκο ή την κατανομή της κίνησης, και διαφοροποίησης της φυσιολογικής από την κακόβουλη κίνηση, ώστε να εξασφαλίζεται η καλή εξυπηρέτηση της νόμιμης κίνησης. Η παράπλευρη ζημιά κατά την αντιμετώπιση της επίθεσης πρέπει να είναι μικρότερη από τη ζημιά που θα προκαλούσε η παντελής έλλειψη μηχανισμού αντιμετώπισης.

Συγκεκριμένα για την αντιμετώπιση μιας επίθεσης DDoS, είναι αναγκαία η συνεργασία μεταξύ των δικτυακών τόπων (sites), αφού η φύση της επίθεσης εμποδίζει την αποτελεσματική αντιμετώπισή της από ένα μεμονωμένο δικτυακό τόπο. Όπως έχει ήδη αναφερθεί, το IP spoofing, η εξάπλωση της επίθεσης σε πολλά επιτιθέμενα δίκτυα και η αδυναμία ενός δικτύου να διαμορφώσει τον όγκο της εισερχόμενης κίνησης (traffic shaping) καθιστούν μη αποτελεσματικές τις προσπάθειες ενός και μόνο δικτυακού τόπου να αντιμετωπίσει την επίθεση.

Η συνεργασία ανάμεσα στους δικτυακούς τόπους μπορεί να λάβει χώρα με τις ακόλουθες ενέργειες:
(α) καθορισμός των χαρακτηριστικών της επίθεσης (χρησιμοποιούμενο πρωτόκολλο, πόρτες κ.α.) σε κάθε σημείο κατά μήκος της διαδρομής της επίθεσης, έτσι ώστε να μπορούν να τεθούν σε λειτουργία τα κατάλληλα φίλτρα αντιμετώπισης,
(β) διάδοση αυτών των χαρακτηριστικών σε όλα τα δίκτυα που βρίσκονται πάνω στο μονοπάτι της επίθεσης και επικοινωνία ανάμεσα στο θύμα και στα δίκτυα προέλευσης της κίνησης για έλεγχο της αποτελεσματικότητας των φίλτρων (προσαρμογή τους στα εναλλασσόμενα μοτίβα επιθέσεων).

Ωστόσο μια τέτοια συνεργατική προσέγγιση έχει να αντιμετωπίσει ένα σημαντικό πρόβλημα. Η αποτελεσματικότητά της εξαρτάται έντονα από τη διαθεσιμότητα και προθυμία των υπεύθυνων των δικτύων προέλευσης της κίνησης, καθώς και από τις πολιτικές λειτουργίας τους. Επιπλέον, δεν προβλέπει μέτρα για την ανακούφιση από τη συμφόρηση, η οποία εξακολουθεί να πλήττει το δίκτυο-θύμα και τα δίκτυα που

βρίσκονται πλησιέστερα σε αυτό στο μονοπάτι της επίθεσης. Συνεπώς, χρειάζονται επιπρόσθετα μέτρα, για να μειωθεί το κόστος σε εύρος δικτύου.

Προτεινόμενες λύσεις

Κατά την προσπάθεια αντιμετώπισης των επιθέσεων DDoS έχουν αναπτυχθεί τρεις βασικές μεθοδολογίες – προσεγγίσεις: *ανίχνευση*, *traceback* (ανακάλυψη πηγής και διαδρομής επίθεσης) και *αντίδραση*. Η διαδικασία της ανίχνευσης μπορεί να γίνεται στο δίκτυο-θύμα με παρακολούθηση της συμφόρησης και ανάλυση της κίνησης ή των απορριφθέντων πακέτων, ή στο μονοπάτι της επίθεσης με συνδυασμό διαφόρων αναφορών από τα δίκτυα που πλήττονται. Το traceback μπορεί να διεξαχθεί με συνεργασία της υποδομής Διαδικτύου ή με απλή κίνηση προς τα πίσω χωρίς προηγούμενη παρατήρηση. Γενικά, μπορεί να γίνει μια εξαιρετικά δύσκολη διαδικασία, εάν η επίθεση χρησιμοποιεί IP spoofing.

Τέλος, η αντίδραση μπορεί να είναι προληπτική ή άμεση κατά την επίθεση. Οι άμεσες προσπάθειες αντίδρασης μπορούν να αφορούν ένα και μόνο δικτυακό τόπο ή να αποτελούν κομμάτι μιας συνολικής κατανεμημένης υποδομής με κοινό στόχο την αντιμετώπιση της επίθεσης DDoS.
Στη συνέχεια ακολουθούν λίγα λόγια για τέσσερις προτεινόμενες λύσεις, οι οποίες αντιμετωπίζουν μερικώς τις επιθέσεις DDoS, αλλά παρουσιάζουν μειονεκτήματα:

- Υπερκείμενο Δίκτυο CenterTrack : αυτό το υπερκείμενο δίκτυο έχει ως σκοπό την ανίχνευση των ροών της επίθεσης. Εγκαθίσταται τούνελ από το δρομολογητή συνόρου του δικτυακού τόπου ως ένα συγκεκριμένο σημείο στο δίκτυο και όταν το θύμα δέχεται επίθεση, η κίνηση δρομολογείται σε αυτό μέσω του υπερκείμενου δικτύου. Έτσι, είναι εφικτό να γίνει ανά βήμα traceback στους δρομολογητές συνόρου, από τους οποίους περνάει η κίνηση της επίθεσης. Αυτή η τεχνική από τη μία χρειάζεται διαγνωστικά στοιχεία μόνο στους δρομολογητές συνόρου, από την άλλη η εγκατάσταση των τούνελ απαιτεί την κατανάλωση πόρων και αυξάνει την πολυπλοκότητα διαχείρισης. Προφανώς, χρησιμοποιείται η μεθοδολογία του traceback.

- Pushback πρωτόκολλο: το ειδικό αυτό πρωτόκολλο αποτελεί μια προσπάθεια προτυποποίησης της επικοινωνίας ανάμεσα σε δρομολογητές που συνεργάζονται. Σκοπός είναι ο έλεγχος των υψηλού εύρους δικτύου ροών κίνησης μιας επίθεσης DDoS. Οι δρομολογητές επικοινωνούν μεταξύ τους δεδομένα για τυχόν κακόβουλη κίνηση και κινητοποιούνται για να τη σταματήσουν χρησιμοποιώντας εξειδικευμένα φίλτρα. Κατά αυτόν τον τρόπο ακολουθούν τις επιμέρους ροές προς την πηγή τους και ελέγχουν σε διάφορα σημεία την κατανομή του εύρους δικτύου. Μειονέκτημα αποτελεί και πάλι η κατανάλωση πόρων για την επεξεργασία των επικοινωνούντων μηνυμάτων σε όλους τους δρομολογητές προς την πηγή. Η μεθοδολογία-προσέγγιση που χρησιμοποιείται είναι το traceback και η αντίδραση.

- Panoptis: ο Panoptis είναι ένα εργαλείο ανοιχτού λογισμικού για τη μέτρηση αλλαγών στα μοτίβα ροής κίνησης στους δρομολογητές συνόρου. Συγκεκριμένα, συσχετίζει πρόσφατα πακέτα με δεδομένα από μετρήσεις κίνησης, για να συμπεράνει ποιο interface ενός δρομολογητή συνόρου εμπλέκεται σε επίθεση. Κατόπιν, με την εφαρμογή κατάλληλων φίλτρων στα interfaces που πλήττονται μπορεί να αντιμετωπιστεί η επίθεση. Αυτή η λύση παρουσιάζει καλή κλιμάκωση, αλλά είναι απαραίτητη μία μεγάλη ποσότητα ιστορικών δεδομένων προκειμένου να γίνει η συσχέτιση και μάλιστα πρέπει όλη η επεξεργασία να γίνεται τοπικά, για να μην καταναλωθεί και άλλο εύρος δικτύου για τη μεταφορά των δεδομένων. Ο Panoptis ανήκει στη μεθοδολογία της ανίχνευσης και της αντίδρασης.

- Υποδομή Cooperative Intrusion Traceback and Response (CITRA): η υποδομή CITRA βασίζεται στην οργάνωση διαφόρων κοινοτήτων σε γειτονιές. Κάθε κοινότητα εκτελεί ανίχνευση εισβολής χαμηλού επιπέδου και περιορίζεται σε συγκεκριμένα όρια. Με την ανίχνευση μίας επίθεσης από μία κοινότητα, η τελευταία διανέμει αναφορές επίθεσης στους γείτονές της, οι οποίοι μπορούν να ανακαλύψουν το μονοπάτι της επίθεσης και να αντιδράσουν. Η CITRA χρησιμοποιεί εντολές αντίδρασης ανεξάρτητες μηχανήματος, και η διαδικασία των αναφορών και ο συντονισμός γίνεται κεντρικά. Τέλος, χρησιμοποιείται το πρωτόκολλο IDIP (Intruder Detection and Isolation Protocol) και η μεθοδολογία ανήκει στην κατηγορία της ανίχνευσης και της αντίδρασης.

Συστήματα IDS

Με τον όρο IDS (Intrusion Detection Systems) αναφερόμαστε σε ειδικά σχεδιασμένες εφαρμογές που παρακολουθούν την υπό εξέταση δικτυακή συσκευή ή και ολόκληρο το δίκτυο παθητικά και ανιχνεύουν προβλήματα που ενδεχομένως να είναι απόρροια επιθέσεων ενάντια σε αυτό. Στην πρώτη περίπτωση, όπου δηλαδή μας ενδιαφέρει μια συγκεκριμένη συσκευή (network router ή server) και παρακολουθούμε αποκλειστικά τα χαρακτηριστικά λειτουργίας της (χρησιμοποίηση του επεξεργαστή, διαθεσιμότητα όρων, system logs) αναφερόμαστε σε hosted based προσέγγιση.

Η τεχνική αυτή πολλές φορές μπορεί να αποβεί ανεπαρκής λόγω απώλειας των logs ή απόκρυψης αυτών από ποιον εισβολέα, είτε να μην δώσει τα αναμενόμενα αποτελέσματα λόγω υπερφόρτωσης του συστήματος από φυσικά αίτια. Η δεύτερη προσέγγιση συστημάτων ανίχνευσης επιθέσεων βασίζεται στην παρακολούθηση του δικτύου παθητικά από ένα μηχάνημα που είναι τοποθετημένο στο ίδιο κομβικό σημείο με το σύνορο του δικτύου. Αυτό γίνεται εφικτό με την τοποθέτησή του στη θύρα Monitoring του Network Switch ή σε ένα Hub έτσι ώστε να μπορεί να «βλέπει» όλη την εισερχόμενη και εξερχόμενη κίνηση. Οι συσκευές αυτές είναι ουσιαστικά Sniffers που είτε αποθηκεύουν την κίνηση για μελέτη σε δευτερεύοντα χρόνο είτε πραγματοποιούν μετρήσεις σε πραγματικό χρόνο για την κατάσταση του δικτύου.

4.2 Επιθέσεις σε δομημένα συστήματα P2P

Η πρώτη μεγάλη κατηγορία επιθέσεων είναι αυτή των λεγόμενων routing attacks. Όπως έχει ήδη αναφερθεί η σωστή δρομολόγηση σε αυτά τα συστήματα είναι ζωτικής σημασίας λόγω του τρόπου λειτουργίας και σχεδιασμού τους. Παρόλα αυτά είναι και ένας από τους βασικότερους τομείς στους οποίους κάποιος κακόβουλος κόμβος προσπαθεί να σαμποτάρει. Αν σκεφτούμε και το γεγονός ότι ένα πραγματικό τέτοιο σύστημα μπορεί να στηθεί στο internet, βλέπουμε κατευθείαν ότι ο αριθμός των πιθανών επιτιθέμενων κόμβων είναι μεγάλος και ότι η πρώτη επίθεση που πιθανώς θα επιχειρείται θα είναι επάνω στη δρομολόγηση. Από εκεί και πέρα τα routing attacks είναι

πολλών ειδών και διαφορετικά μεταξύ τους. Τα πιο σημαντικά τα οποία και θα εξετάσουμε είναι το lookup attack, το routing update attack και το partition attack.

Incorrect lookup attack

Η συγκεκριμένη επίθεση συνίσταται στο γεγονός ότι ο επιτιθέμενος προσπαθεί να προωθήσει τα lookups τα οποία περνούν από αυτόν σε κόμβους οι οποίοι είτε δεν είναι οι σωστοί, είτε δεν υπάρχουν. Σε ένα σύστημα ένας τέτοιος κόμβος προσπαθεί να εμφανίζει κατά τα άλλα φυσιολογική συμπεριφορά ώστε να μη γίνεται εύκολα αντιληπτός και εκδιωχθεί από αυτό.

Incorrect routing updates attack

Σε ένα DHT σύστημα κάθε κόμβος δημιουργεί και ενημερώνει τους πίνακες δρομολόγησης που διατηρεί με το να συμβουλεύεται τους υπόλοιπους κόμβους. Σε αυτό το είδος επίθεσης οι επιτιθέμενοι προσπαθούν να προκαλέσουν βλάβες στους πίνακες αυτούς είτε με το να αλλοιώνουν τα updates που περνούν από αυτούς, είτε με το να δημιουργούν οι ίδιοι updates εντελώς λανθασμένα.

Partition attack

Το partition είναι μια επίθεση κατά την οποία επιτιθέμενοι κόμβοι δημιουργούν ένα παράλληλο δίκτυο το οποίο τρέχει τα ίδια πρωτόκολλα με το πραγματικό. Ένας από τους κόμβους αυτούς ανήκει και στο πραγματικό δίκτυο υποκλέπτοντας δεδομένα. Στόχος των επιτιθέμενων είναι να προσπαθήσουν να εισάγουν στο παράλληλο δίκτυο καινούριους κόμβους χωρίς αυτοί να το αντιληφθούν προκειμένου να υποκλέπτουν τα δεδομένα τους και να τους διαχειρίζονται με όποιο τρόπο θέλουν. Οι κόμβοι που ίσως και τυχαία να εισαχθούν σε αυτό το δίκτυο έχουν την εντύπωση ότι συμμετέχουν στο πραγματικό δίκτυο.

.

Η δεύτερη κατηγορία επιθέσεων την οποία εξετάσαμε είναι η λεγόμενη ***Storage and Retrieval Attack***. Σε αυτό το είδος επίθεσης οι κόμβοι που την επιχειρούν, ενώ συμμετέχουν στο σύστημα κανονικά και καθίστανται υπεύθυνοι για κάποια κλειδιά (δεδομένα), όταν αυτά ζητηθούν από κάποιους κόμβους που τα αναζητούν, αυτοί αρνούνται να τους εξυπηρετήσουν και εμφανίζονται ότι δεν τα έχουν. Δηλαδή ενώ ενημερώνουν το σύστημα ότι όντως τα κλειδιά τα οποία τους ζητήθηκε να αποθηκεύσουν τα αποθήκευσαν σωστά, αυτό δεν συμβαίνει και είτε δεν τα αποθηκεύουν

καθόλου, είτε εκμεταλλεύονται τις πληροφορίες αυτές με άλλο τρόπο εκτός του συστήματος. Η συγκεκριμένη επίθεση ανήκει στις DoS (Denial of Service) επιθέσεις. Ο συνήθης τρόπος αντιμετώπισης αυτού του είδους των επιθέσεων είναι η εφαρμογή replication στα DHT συστήματα

Η τρίτη κατηγορία επιθέσεων χαρακτηρίζεται ως ***Miscellaneous Attacks.*** Αυτή η κατηγορία είναι πιο γενική και συμπεριλαμβάνει ένα σύνολο επιθέσεων διαφόρων ειδών τις οποίες θα δούμε αμέσως παρακάτω.

Inconsistent Behavior

Σε αυτή την κατηγορία επίθεσης ο κόμβος εμφανίζει σε ένα μέρος του δικτύου ομαλή συμπεριφορά, ενώ στο υπόλοιπο εμφανίζει ασυνέπειες. Οι κόμβοι στους οποίους επιλέγει να εμφανίζει αυτή την ασυνεπή συμπεριφορά είναι συνήθως μακρινοί κόμβοι προκειμένου να είναι πιο δύσκολη η ανίχνευση του. Αν εφάρμοζε το ίδιο σε κοντινούς κόμβους το πιθανότερο θα ήταν το σύστημα να τον αντιληφθεί και να τον εκδιώξει από τους routing tables.

Overload of Targeted nodes

Η επίθεση αυτή σαν στόχο έχει να επιβαρύνει πολύ κάποιους συγκεκριμένους κόμβους του δικτύου ώστε να προκαλέσει πτώση του διαθέσιμου bandwidth του θύματος ή και να καταφέρει να τον βγάλει εκτός δικτύου λόγω υπερφόρτωσης – υπερχείλισης.

Rapid Joins and Leaves.

Με την επίθεση αυτή κάποιος κακόβουλος χρήστης προσπαθεί να επιβαρύνει το σύστημα με την επαναλαμβανόμενη είσοδο και έξοδο από το σύστημα. Η επιβάρυνση αυτή είναι η κατανάλωση του bandwidth λόγω των συνεχόμενων μηνυμάτων που ανταλλάσσονται και της επαναλαμβανόμενης εκτέλεσης της διαδικασίας του stabilize.

Unsolicited messages

Εδώ έχουμε μια man in the middle attack, όπου ο επιτιθέμενος «μπαίνει» ανάμεσα σε δύο κόμβους χωρίς να τον αντιληφθούν και υποκλέπτει τα πακέτα που στέλνει ο ένας στον άλλο. Στη συνέχεια αλλοιώνει αυτά τα πακέτα προκειμένου να σαμποτάρει την επικοινωνία μεταξύ των δύο κόμβων.

4.3 Ασφαλής Αποθήκευση

Η αποθήκευση αποτελεί ένα ευαίσθητο σημείο των peer to peer συστημάτων. Κάθε χρήστης θέλει τα δεδομένα του να είναι διαθέσιμα ανά πάσα στιγμή και ανεξαρτήτως συνθηκών του δικτύου να μπορεί να τα προσπελάσει. Τα δεδομένα που αποθηκεύονται στο σύστημα μπορεί να περιέχουν ασφαλή πρόσβαση σε αυτά ώστε μόνο εξουσιοδοτημένοι χρήστες να μπορούν να τα προσπελαυνουν.

Οι επιθέσεις που έχουν παρατηρηθεί στον τομέα της αποθήκευσης σε δίαφορα p2p συστήματα αφορούν την πρόσβαση μη εξουσιοδοτημένων χρηστών σε δεδομένα. Τα κίνητρα των κακόβουλων κόμβων είναι η πρόσβαση σε ευαίσθητα δεδομένα και η περαιτέρω επεξεργασία τους. Μια ακόμη επίθεση σχετίζεται με την άρνηση αποθήκευσης δεδομένων ή διαμοιρασμού αυτών που κατέχει ένας κακόβουλος κόμβος. Έτσι ένας κόμβος ο οποίος κατέχει είτε αρνείται να αποθηκεύσει δεδομένα κερδίζει σε χώρο αποθήκευσης καθώς και σε εισερχόμενη κίνηση.

Συγκεκριμένα, όσον αφορά τη μη εξουσιοδοτημένη πρόσβαση σε δεδομένα οι κακόβουλοι κόμβοι επεξεργάζονται κάθε μήνυμα που αποθηκεύεται ή που περνάει από αυτούς. Στο κάποια σύστηματα αποθήκευσης όπως πχ στο PAST κάτι τέτοιο είναι εξαιρετικά δύσκολο να συμβεί καθώς όλα τα μηνύματα που διακινούνται στο δίκτυο είναι κρυπτογραφημένα.

Όσον αφορά τις επιθέσεις άρνησης διαμοιρασμού δεδομένων, ένας κόμβος που κατέχει δεδομένα και αρνείται να τα διαμοιράσει μπορεί να κερδίσει σε εισερχόμενη κίνηση, κάτι το οποίο μπορεί να επηρεάσει το balance του δικτύου.

Επίσης και η άρνηση αποθήκευσης από ένα σύνολο κακόβουλων κόμβων μπορεί να επηρεάσει το balance του δικτύου καθώς τα δεδομένα θα ποθηκευτούν σε τρίτους κόμβους. Έτσι εαν οι κακόβουλοι κόμβοι αυξηθούν σημαντικά μπορεί να παρατηρηθεί αυξημένη κίνηση προς τους κόμβους οι οποίοι συμπεριφέρονται σύμφωνα με το πρωτόκολλο.
Σχετικά με την άρνηση αποθήκευσης δεδομένων υπάρχουν δύο τρόποι να υλοποιηθεί.

Στον πρώτο ο κακόβουλος κόμβος αρνείται να αποθηκεύσει δεδομένα στέλνοντας αρνητική απάντηση. Στο δεύτερο τρόπο αρνείται να αποθηκεύσει τα δεδομένα χωρίς να ειδοποιήσει ότι δεν τα αποθήκευσε.

Διάφοροι *κρυπτογραφικοί αλγόριθμοι και πρωτόκολλα* υιοθετούνται για να παρέχουν ασφάλεια για το περιεχόμενο που δημοσιεύεται και που αποθηκεύεται στα p2p δίκτυα.

Στοιχεία αυτοεπιβεβαίωσης (Self- Certifying Data)

Το στοιχείο αυτοεπιβεβαίωσης είναι στοιχείο του οποίου η ακεραιότητα μπορεί να ελεγχθεί από τον κόμβο που το ανακτά. Ένας κόμβος που εισαγάγει ένα αρχείο στο δίκτυο υπολογίζει κρυπτογραφικό hash του περιεχομένου ενός αρχείου, βασισμένο σε μια γνωστή συνάρτηση κατακερματισμού, για να παραγάγει το κλειδί αρχείων. Όταν ένας κόμβος ανακτά το αρχείο χρησιμοποιώντας το κλειδί του, υπολογίζει την ίδια hash λειτουργία για να ελέγξει την ακεραιότητα των στοιχείων.

Υπάρχει η απαίτηση για την κοινή γνώση της hashing λειτουργίας από όλους τους κόμβους στο δίκτυο. Η ανωτέρω προσέγγιση υιοθετείται από το σύστημα CFS ενώ χρησιμοποιεί μια παρόμοια προσέγγιση.

Διασπορά πληροφοριών (Information Dispersal)

Ο αλγόριθμος διασποράς πληροφοριών από Rabin χρησιμοποιείται ευρέως. Τα Publius, Mnemosyne και FreeHaven χρησιμιοποιούν τον αλγόριθμο για τις πληροφορίες που δημοσιεύονται στο δίκτυο. Τα αρχεία κωδικοποιούνται σε μ blocks, έτσι ώστε οποιοδήποτε ν είναι επαρκές για να συγκεντρώσει εκ νέου τα αρχικά στοιχεία (μ < ν). Αυτό δίνει ανθεκτικότητα "ανάλογη" προς έναν παράγοντα πλεονασμού ίση με το μυστικό σχέδιο διανομής MN Shamir.

Αυτός που εκδίδει το περιεχόμενο κρυπτογραφεί ένα αρχείο με ένα κλειδί K, κατόπιν χωρίζει το K σε l κομμάτια , έτσι ώστε οποιοδήποτε κ από αυτά να μπορεί αναπαραγάγει το K, αλλά το κ-1 να μη δίνει καμιά πληροφορία για το K. Κάθε server κρυπτογραφεί έπειτα ένα από τα βασικά κομμάτια με το φραγμό αρχείων. Για να γίνει το αρχείο απρόσιτο, τουλάχιστον (l-k-1) servers που περιέχουν το κλειδί πρέπει να τερματιστούν.

Ανώνυμες κρυπτογραφημένες αναμεταδόσεις (Anonymous Cryptographic Relays)
Ένας μηχανισμός βασισμένος στον εκδότη, αποστολέα, storer, και client επικοινωνία μέσω της ανώνυμης σύνδεσης είναι υιοθετημένος από το PAST. Ο εκδότης επιλέγει διάφορους αποστολείς και στέλνει σε αυτους, μέσω μιας ανώνυμης σύνδεσης, κρυπτογραφημένα τμήματα ενός αρχείου. Οι αποστολείς, στη συνέχεια, επιλέγουν άλλους κόμβους για να ενεργήσουν ως storers των τμημάτων και να διαβιβάσουν τα τμήματα αυτά (πάλι μέσω ανώνυμη σύνδεσης). Εφόσον ολά τα τμήματα αρχειών αποθηκεύονται ο εκδότης τα καταστρέφει και αναγγέλλει το όνομα αρχείων, από κοινού στον κατάλογο των αποστολέων που χρησημοποιήθηκαν.

Προκειμένου να ανακτηθεί το περιεχόμενο, ένας πελάτης θα έρθει σε επαφή με τους αποστολείς, στη συνέχεια οι αποστολείς θα έρθουν σε επαφή με τους τυχαίους servers οι οποίοι θα λειτουργήσουν σαν αποκωδικοποιητές για τις διευθύνσεις των storers που διατηρούν τα τμήματα των αρχείων. Οι αποστολείς έπειτα θα έρθουν σε επαφή με storers που ζητούν τα τμήματα. Οι Storers θα αποκρυπτογραφήσουν τα τμήματα και θα τα στείλουν πίσω στον πελάτη. Η διαδικασία επαναλαμβάνεται έως ότου συλλεγχθούν αρκετά τμήματα για να αναδημιουργήσουν το έγγραφο. Οι αποστολείς είναι ορατοί σε έναν πιθανό επιτιθέμενο, αλλά είναι λιγότερο πιθανό να υποστούν επίθεση δεδομένου ότι δεν αποθηκεύουν το περιεχόμενο, ούτε τις διευθύνσεις των κόμβων όπου αποθηκεύεται το περιχόμενο.

Έξυπνες κάρτες
Η χρήση των έξυπνων επιτρέπει στους κόμβους να αποδείξουν σε άλλους κόμβους οτι αυτοί λειτουργούν στο πλαίσιο δικαιοδοσίας τους.Υποστηρίζεται, εντούτοις, ότι αυτό μπορεί να μην είναι πρακτικό να διανεμηθούν έξυπνες κάρτες σε έναν πολύ μεγάλο αριθμό κόμβων, και ότι ο κίνδυνος των κλειδιών έξυπνων καρτών που συμβιβάζονται από τους κόμβους του δικτύου είναι ιδιαίτερος.

Distributed Steganographic File Systems
Το κύριο χαρακτηριστικό σε ένα τέτοιο σύστημα αρχείων είναι ότι τα κρυπτογραφημένα blocks είναι όμοια με ένα τυχαίο υπόστρωμα, έτσι ώστε η παρουσία τους μην μπορεί να ανιχνευθεί. Το σύστημα είναι προετοιμασμένο έτσι ώστε πρώτα να γράψει τα τυχαία στοιχεία σε όλα τα blocks και έπειτα τα αρχεία αποθηκεύονται κρυπτογραφώντας τα blocks και τοποθετώντας τα σε ψευδο-τυχαία επιλεγμένες θέσεις.

Κωδικοποίηση εξάλειψης (Erasure Coding)

Με την κωδικοποίηση εξάλειψης, τα δεδομένα είναι χωρισμένα σε blocks και είναι εξαπλωμένα σε πολλούς servers. Μόνο ένα μέρος απαιτείται για να αναδημιουργήθεί η αρχική πληροφορία. Τα δεδομένα και τα σχετιζόμενα blocks ονομάζονται με ένα μοναδικό προσδιοριστικό. Αυτό παρέχει την ακεραιότητα στοιχείων, εξασφαλίζοντας ότι ένα ανακτημένο αρχείο δεν έχει αλλοιωθεί, δεδομένου ότι ένα αλλοιωμένο αρχείο θα παρήγε ένα διαφορετικό προσδιοριστικό. Τα blocks είναι διασκορπισμένα με τέτοιο τρόπο ώστε να αποφευχθούν πιθανές συσχετισμένες αποτυχίες, επιλέγοντας τους κόμβους σε διαφορετικές γεωγραφικές θέσεις ή διοικητικές περιοχές, ή βασισμένοι στα πρότυπα των ιστορικών μετρήσεων. Ένα "εσωτερικό δαχτυλίδι" των κεντρικών υπολογιστών οργανώνεται για κάθε αντικείμενο για να παρέχει τις versioning ικανότητες. Ο ρόλος του δαχτυλιδιού είναι να διατηρηθεί μια χαρτογράφηση από το αρχικό προσδιοριστικό του αντικειμένου, στο προσδιοριστικό της πιό πρόσφατης έκδοσης του αντικειμένου. Έτσι η χαρτογράφηση από ένα ενεργό (αρχικό) προσδιοριστικό, στο πιό πρόσφατο προσδιοριστικό, είναι ανεκτική σε λάθη. Το εσωτερικό δαχτυλίδι είναι επίσης αρμόδιο για την επαλήθευση των νόμιμων συγγραφέων του αντικειμένου και τη διατήρηση μιας ιστορίας των updates του αντικειμένου, παρέχοντας κατά συνέπεια ένα καθολικό αναστρέψιμο μηχανισμό, συνεισφέροντας έτσι στην ακεραιότητα με την αποθήκευση προηγούμενων εκδόσεων των αντικειμένων.

4.4 Ασφαλής δρομολόγηση (Secure Routing)

Ο στόχος της ασφαλούς δρομολόγησης είναι να επιλυθεί το πρόβλημα των κακόβουλων κόμβων που προσπαθούν να αλλοιώσουν, να διαγράψουν, να αρνηθούν την πρόσβαση, ή να παρέχουν τα πολυδιατηρημένα αντίγραφα των αντιγράφων αντικειμένου που μεταφέρονται μεταξύ των κόμβων. Οι ασφαλείς αρχές δρομολόγησης που προτείνονται αντιμετωπίζουν τα προβλήματα:

(1) εξασφαλιση της ανάθεση IDs στους κόμβους.

(2) εξασφάληση της συντήρησης των πινάκων δρομολόγησης.

(3) εξασφάληση της αποστολής μηνυμάτων.

Αυτές οι αρχές σε συνδυασμό με άλλες υπάρχουσες τεχνικές ασφάλειας μπορούν να παράγουν γερές εφαρμογές.

Οι επιθέσεις σε επίπεδο δρομολόγησης έχουν ως στόχο να προκαλέσουν εσφαλμένη λειτουργία του δικτύου με το να οδηγούν πακέτα σε απώλεια ή κόμβους σε κατάρρευση. Αυτό μπορεί να γίνει με διάφορους τρόπους, από τους οποίους μερικοί εξηγούνται αναλυτικότερα παρακάτω.

Η πιο κλασική επίθεση σε κόμβο είναι η denial of service (DOS) attack και μια παραλλαγή της, η distributed denial of servise (dDos). Η υλοποίηση της γίνεται ως εξής: Ένας κακόβουλος κόμβος στέλνει συνέχεια πολλά πακέτα σε ένα συγκεκριμένο κόμβο του δικτύου, με σκοπό να γεμίσει το χώρο αποθήκευσης εισερχόμενων μηνυμάτων του. Αυτό έχει ως αποτέλεσμα την απόρριψη όσων νέων πακέτων καταφθάνουν στον κόμβο (μεταξύ των οποίων υπάρχουν φυσικά και χρήσιμα), αφού δεν μπορούν να εξυπηρετηθούν. Η επίθεση αυτή οδηγεί σε μόνιμη απώλεια πακέτων, ή σε κάποια ευνοικότερη περίπτωση στην αναδρομολόγηση των χαμένων πακέτων (με χρήση ελέγχων για timeouts), γεγονός που αυξάνει αρκετά τη συνολική κίνηση και καθυστέρηση του δικτύου.

Στην dDOS επίθεση η μόνη διαφορά είναι ότι αντί για ένα κακόβουλο κόμβο, συμμετέχουν πολλοί οι οποίοι συγχρονίζονται ώστε όλοι μαζί να στείλουν πακέτα σε αυτόν. Με αυτό τον τρόπο ο χώρος εισερχόμενων μηνυμάτων γεμίζει γρηγορότερα.

Ένα άλλο είδος επίθεσης που προκαλεί πολλά προβλήματα στη δρομολόγηση είναι αυτό κατά το οποίο ένας κακόβουλος κόμβος τη στιγμή που λειτουργεί ως ενδιάμεσος σταθμός στη μετάδοση ενός πακέτου και όχι ως τελικός παραλήπτης, δεν προωθεί το πακέτο σωστά. Συγκεκριμένα. μπορεί να δράσει με 2 διαφορετικούς τρόπους. Ο πιο επιζήμιος είναι να μην προωθήσει καθόλου (no routing attack), επίθεση ιδιαίτερα καταστροφική στην περίπτωση UDP πακέτων, καθώς σε αυτά δεν υπάρχει κανένας έλεγχος και καμία εγγύηση για το αν το πακέτο θα παραδοθεί σωστά. Στην περίπτωση πακέτων TCP, η επίθεση αυτή, στην καλύτερη περίπτωση οδηγεί σε αυξημένη καθυστέρηση και άσκοπη κατανάλωσητου bandwidth τουδικτύου.

Μια λιγότερο επιζήμια παραλλαγή αυτής της επίθεσης είναι αυτή στην οποία ο κακόβουλος κόμβος προωθεί το πακέτο που λαμβάνει, αλλά όχι στον σωστό κόμβο (false routing attack) 2. Αντιθέτως, το στέλνει σε κάποιον άλλο κόμβο, άλλοτε με τυχαία

επιλογή και όταν υπάρχει η δυνατότητα, η επιλογή δεν είναι τυχαία αλλά γίνεται με κάποιο κριτήριο (συνήθως εκτίμηση της απόστασης από τον τελικό παραλήπτη). Η επίθεση αυτή δεν οδηγεί σε τόσο μεγάλη απώλεια πακέτων, αφού σχεδόν όλα τα πακέτα κάποια στιγμή θα παραδοθούν στο σωστό κόμβο, έστω από ενα εναλλακτικό μονοπάτι στο οποίο δρομολογούνται. Επικεντρώνεται κυρίως στην αύξηση της κίνησης του δικτύου ενώ το μεγάλο της πλεονέκτημα είναι οτι δεν γίνεται τόσο εύκολα αντιληπτή παρά μόνο σε ορισμένες περιπτώσεις.

4.5 Έλεγχος πρόσβασης, επικύρωση και διαχείρισης ταυτότητας

Τα ζητήματα του ελέγχου πρόσβασης, της επικύρωσης, και της διαχείρισης ταυτότητας συχνά αγνοούνται στα p2p συστήματα. Μέσα σε ένα κατανεμημένο περιβάλλον, είναι δυνατό η ίδια φυσική οντότητα να εμφανιστεί κάτω από διαφορετικές ταυτότητες, ιδιαίτερα στα συστήματα με προσωρινούς πληθυσμούς κόμβων. Αυτό θέτει μια απειλή ασφάλειας, ειδικά στα p2p συστήματα που χρησιμοποιούν την διατήρηση αντιγράφων και τη διατήρηση κομματιασμένων αρχείων σε πολλούς κόμβος για επίτευξη ασφάλειας και διαθεσιμότητας και, επομένως, στηρίζονται στην ύπαρξη των ανεξάρτητων κόμβων με διαφορετικές ταυτότητες.

Αυτό το πρόβλημα ονομάζεται "επίθεση Sybil" και καταλήγουμε στο συμπέρασμα ότι αν υπάρχει μια κεντρική αρχή πιστοποίησης ή προσδιορισμού τα p2p συστήματα θα είναι ευαίσθητα σε αυτό το είδος επίθεσης.

Η μόνη προτεινόμενη εναλλακτική λύση είναι η χρήση απαιτητικών σε πόρους προσδιορισμών, οι οποίοι υποθέτουν ότι οι πόροι του επιτιθεμένου είναι περιορισμένοι. Σε διάφορα συστήματα, η έλλειψη επικύρωσης ξεπερνιέται με τη διανομή κλειδιών απαραίτητων για την πρόσβαση στο περιεχόμενο ενός υποσυνόλου προνομιούχων χρηστών. Οι κατάλογοι ελέγχου πρόσβασης μπορούν επίσης να οριστούν στα αντικείμενα από τους αρχικούς συντάκτες τους μέσω της χρήσης των υπογεγραμμένων πιστοποιητικών.

Όλες οι τροποποιήσεις περιεχομένου σχετικά με ένα αντικείμενο ελέγχονται έπειτα σύμφωνα με τον κατάλογο πρόσβασης και οι αναρμόδιοι αγνοούνται.

Τέλος, υποστηρίζεται ότι ο έλεγχος πρόσβασης συσχετίζεται πολύ με τη διαχείριση πνευματικής ιδιοκτησίας και τα ψηφιακά ζητήματα δικαιωμάτων.

4.6 Ανωνυμία

Η ανωνυμία είναι βασικό κομμάτι στο οποίο εστιάζουν πολλά συστήματα διανομής απευθυνόμενοα στη μυστικότητα και την εμπιστευτικότητα.
Στα συστήματα διανομής η ανωνυμία μπορεί να αναφερεται :
—στον συντάκτη (ή εκδότη) του περιεχομένου,
—στη ταυτότητας ενός κόμβου που αποθηκεύει το περιεχόμενο,
—στη ταυτότητας και τις λεπτομερειες του ίδιου του περιεχομένου, και
—στις λεπτομερειες μιας ερώτησης για την ανάκτηση του περιεχομένου.
Αυτό το τμήμα περιγράφει τις κύριες προσεγγίσεις που υιοθετούνται αυτήν την περίοδο για την παροχή της ανωνυμίας.

Disassociation of Content Source and Requestor

Το Freenet είναι ένα p2p σύστημα κατανομής περιεχομένου κατεξοχήν προσανατολισμένο στην παροχή ανωνυμίας στους χρήστες καθιστώντας αδύνατο να προσδιοριστεί η πραγματική προέλευση ή ο προορισμός ενός αρχείου που περνά μέσω του δικτύου του, και δύσκολο για ένα διαχειριστή κόμβων να καθορίσει ή να θεωρηθεί αρμόδιο για το πραγματικό περιεχόμενο του κόμβου τους.

Η ανωνυμία των χρηστών επιτυγχάνεται με το να θεωρείται ο κάθε κόμβος που έχει πληροφορία για ένα αρχείο, σαν ο κόμβος που κατέχει το αρχείο. ΄Ετσι είναι αδύνατο να γνωρίζει κανείς ποιος πραγματικά είναι ο κάτοχος (που πρώτος εισήγαγε το αρχείο στο δίκτυο).
Επίσης, κάθε κόμβος που λαμβάνει μια αίτηση αναζήτησης δεν γνωρίζει αν ο κόμβος που του έστειλε την αίτηση είναι αυτός που ενδιαφέρεται για το αρχείο, ή κάποιος ενδιάμεσος στο μονοπάτι αναζήτησης.

Anonymous Connections Layers

Τα συστήματα διανομής που επιδιώκουν να παρέχουν ανωνυμία υιοθετούν συχνά τις υποδομές για την παροχή των ανώνυμων στρωμάτων σύνδεσης, όπως onion routing, mix networks.

Το σύστημα Tarzan είναι μια εντελώς αποκεντρωμένη anonymizing υποδομή στρώματος δικτύων που χτίζει ανώνυμες σήραγγες IP μεταξύ ενός μεγάλου αριθμού κόμβων. Με τη χρηση της υποδομής Tarzan, ένας πελάτης μπορεί να επικοινωνήσει με έναν κεντρικό υπολογιστή χωρίς οποιοσδήποτε να είναι σε θέση να καθορίσει την ταυτότητά τους.

Το σύστημα Tarzan είναι ένα πλήρως αποκεντρωμένο στώμα δικτύου και από τους πελάτες και από τους κεντρικούς υπολογιστές, και περιλαμβάνει ακολουθίες mix relays που επιλέγονται από μια μεγάλη ομάδα εθελοντικών κόμβων που συμμετέχουν. Τα πακέτα καθοδηγούνται μέσω μιας σήραγγας από τυχαία επιλεγμένους κόμβους Tarzan που χρησιμοποιούν κρυπτογράφηση, παρόμοια με onion-routing.

Οι δύο άκρες της σήραγγας είναι ένας κόμβος Tarzan, που τρέχει μια εφαρμογή πελατών, και ένας κόμβος Tarzan, που τρέχει έναν μεταφραστή διευθύνσεων δικτύου. Το τελευταίο διαβιβάζει την κυκλοφορία στον τελευταίο προορισμό που είναι ένας Internet server. Μια προτεινόμενη πολιτική για να μειωθεί ο κίνδυνος επίθεσης του συστήματος είναι οι εμπλεκόμενοι κόμβοι να έχουν διαφορετικές αρμοδιότητες ή να ανήκουν σε διαφορετικές οργανώσεις, ακόμα κι αν η απόδοση θυσιάζεται. Αντίστοιχο τέτοιο σύστημα είναι και το Crowds.

4.7 Το πρόβλημα της μόλυνσης

Σε αυτή την Ενότητα ορίζεται το πρόβλημα της μόλυνσης στα P2P συστήματα και ο τρόπος με τον οποίο μπορούμε να το επιλύσουμε σε αυτά χρησιμοποιώντας τεχνικές φήμης. Παρουσιάζονται επίσης κάποια υπάρχοντα συστήματα που προτάθηκαν για την αντιμετώπιση του συγκεκριμένου προβλήματος και βασίζονται σε τέτοιες τεχνικές.

Μόλυνση σε P2P συστήματα

Στα file sharing συστήματα όπως το Gnutella και το KaZaA, για την ανταλλαγή αρχείων τα μέλη επικοινωνούν κατευθείαν μεταξύ τους. Λόγω του γεγονότος ότι οι κοινότητες των χρηστών σχηματίζονται δυναμικά, τα μέλη, ως επί των πλείστον, είναι άγνωστα μεταξύ τους και υπάρχει αυξημένο ρίσκο κατά την διάρκεια της συναλλαγής τους, καθώς λόγω του ότι τέτοιου είδους συστήματα παρέχουν ανωνυμία αποκρύπτονται τα αναγνωριστικά χαρακτηριστικά των κόμβων κατά τη διάρκεια των συναλλαγών, γεγονός που εκμεταλλεύονται κακόβουλοι χρήστες, οι οποίοι διαμοιράζουν πλήθος μολυσμένων αρχείων (polluted/decoy files) στο δίκτυο χωρίς καμία ευθύνη. Τα μολυσμένα αρχεία είναι αρχεία τα οποία έχουν τροποποιηθεί έτσι ώστε να μην μπορούν να χρησιμοποιηθούν. Το περιεχόμενο ενός μολυσμένου αρχείου μπορεί να είναι σκουπίδια, διαφήμιση ή στην χειρότερη περίπτωση κάποιος ιός, ο οποίος πιθανόν να καταστρέψει δεδομένα και προγράμματα στο σκληρό δίσκο του peer που το κατεβάζει.

Η εισαγωγή τέτοιων decoy files σε ένα σύστημα P2P ονομάζεται μόλυνση (pollution). Αυτοί που έχουν «πλημμυρίσει» τα P2P συστήματα με decoy files, εκτός από μεμονωμένους κακόβουλους χρήστες, είναι κυρίως οι δισκογραφικές εταιρείες, οι οποίες το έχουν βρει ως ένα τρόπο να προστατέψουν την πνευματική τους ιδιοκτησία. Η εισαγωγή decoy files σε ένα P2P file sharing σύστημα μειώνει την διαθεσιμότητα των σωστών (αυθεντικών) αρχείων και «εκνευρίζει» τους χρήστες με αποτέλεσμα να μειώνει πιθανότατα και τη χρήση των P2P συστημάτων. Κάποιες φορές το αποτέλεσμα είναι τα μολυσμένα αρχεία να υπερβαίνουν κατά πολύ το πλήθος των αυθεντικών αρχείων.

4.8 P2P Reputation-based trust management systems

Για την αντιμετώπιση του προβλήματος αναπτύχθηκαν συστήματα *trust management systems* που αξιολογούν τον βαθμό εμπιστοσύνης που έχει κάθε μέλος της κοινότητας για κάποιο άλλο. Η εμπιστοσύνη (*trust*) που δείχνει ένας κόμβος σε έναν άλλο αντιπροσωπεύει το κατά πόσο πιστεύει ότι η συναλλαγή τους θα είναι σωστή και ολοκληρωμένη. Η εμπιστοσύνη σε κάποιον μπορεί να έχει διάφορες οπτικές γωνίες.

Ένας peer μπορεί να εμπιστεύεται κάποιον άλλον επειδή έχει π.χ. καλή ποιότητα στα αρχεία με μουσική, ενώ κάποιος άλλος να μην τον εμπιστεύεται επειδή δεν έχει καλή ταχύτητα για download. Τα περισσότερα trust management συστήματα που έχουν αναπτυχθεί για τον υπολογισμό της εμπιστοσύνης βασίζονται στην φήμη (*reputation*), στην άποψη δηλαδή που έχει ένας peer για κάποιον άλλον και η οποία διαμορφώνεται και ενημερώνεται τόσο από τις προηγούμενες άμεσες συναλλαγές τους, όσο και από την γνώμη που εκφράζεται από άλλους κόμβους του δικτύου, η οποία σχετίζεται με παλιότερες συναλλαγές των κόμβων αυτών με τον συγκεκριμένο peer.

Στα reputation-based συστήματα, λοιπόν, η εκτίμηση της εμπιστοσύνης εξαρτάται τόσο από την υποκειμενική άποψη που έχει ο κόμβος ο οποίος κάνει την αξιολόγηση, όσο και η καθολική άποψη, άποψη όλων των κόμβων του δικτύου, για τον κόμβο που αξιολογείται. Φήμη μπορεί να οριστεί, εκτός για τους peers που διαθέτουν τα αρχεία στο δίκτυο, και για το ίδιο το αρχείο. Η φήμη διαχέεται στο δίκτυο με διάφορες τεχνικές, όπως ψηφοφορία κόμβων, αποστολή παραπόνων ή δημιουργία εικονικών νομισμάτων.

Τα reputation-based συστήματα επιτρέπουν στους peers να αξιολογούν ο ένας τον άλλον. Αυτά τα συστήματα μπορούν να χρησιμοποιηθούν για να μειώσουν τη μόλυνση στα P2P συστήματα, εντοπίζοντας κακόβουλους peers, οι οποίοι είναι υπεύθυνοι για την εισαγωγή μολυσμένων αρχείων στο σύστημα, και απομονώνοντας τους. Σε ένα ιδανικό σύστημα φήμης, οι κακόβουλοι peers αποκτούν με τον καιρό πολύ χαμηλή φήμη και έτσι οι υπόλοιποι peers αποφεύγουν να κατεβάζουν αρχεία από αυτούς. Αυτό έχει ως αποτέλεσμα την ελαχιστοποίηση των μη αυθεντικών (*inauthentic)* αρχείων που διαδίδουν κακόβουλοι χρήστες σε ένα P2P file sharing system.

4.8.1 Υπάρχοντα P2P Reputation-based systems

Σε αυτή την ενότητα αναφέρουμε μερικά από τα υπάρχοντα P2P reputation συστήματα επικεντρώνοντας ιδιαίτερα σε θέματα που έχουν να κάνουν με την αποθήκευση και την ακεραιότητα της reputation πληροφορίας σε αυτά τα συστήματα. Σε ένα ιδανικό reputation-based σύστημα η reputation πληροφορία πρέπει να είναι αποθηκευμένη με κατανεμημένο τρόπο, η ανάκτησή της να είναι εύκολη και να έχει μεγάλη διαθεσιμότητα.

Όσον αφορά το θέμα της ακεραιότητας της reputation πληροφορίας είναι πιο δύσκολο να αντιμετωπιστεί σε ένα αποκεντρικοποιημένο σύστημα όπως είναι τα P2P συστήματα και συνήθως για την διασφάλισή της χρησιμοποιούνται τεχνικές κρυπτογράφησης.

Στο P2Prep κάθε peer διατηρεί και διαμοιράζεται την φήμη για άλλους peers, αποθηκεύοντας τοπικά την προηγούμενη εμπειρία του με άλλους peers, η οποία βασίζεται στις συναλλαγές τους και ανανεώνεται σε κάθε συναλλαγή τους. Ο διαμοιρασμός της reputation πληροφορίας βασίζεται σε έναν κατανεμημένο αλγόριθμο ψηφοφορίας. Πριν ξεκινήσει ένας peer να κατεβάζει ένα αρχείο μπορεί να ενημερωθεί για την αξιοπιστία του peer από τον οποίο προτίθεται να κατεβάσει το αρχείο με μια διαδικασία ψηφοφορίας μεταξύ των peers.

Το πρωτόκολλο χρησιμοποιώντας κρυπτογραφία δημοσίου κλειδιού (public-key cryptography) κρυπτογραφεί την ψήφο ενός κόμβου, εξασφαλίζοντας ότι αυτή δεν μπορεί να τροποποιηθεί από ενδιάμεσους πιθανόν κακόβουλους peers. Αυτό σε συνδυασμό με το ότι η reputation πληροφορία δεν διατηρείται στον ίδιο κόμβο στον οποίο αναφέρεται έχει ως αποτέλεσμα να παρέχεται ακεραιότητα της reputation πληροφορίας.

Μία επέκταση του P2Prep είναι το XRep, το οποίο εκτός από την φήμη για τους peers διατηρεί και φήμη για τα ίδια τα αρχεία.

Στο TrustMe η αποθήκευση και διατήρηση της reputation πληροφορίας κάθε peer του συστήματος ανατίθεται σε άλλους peers, οι οποίοι ονομάζονται trust hosts (THA) του peer, για τους οποίους το πρωτόκολλο παρέχει ανωνυμία και ούτε ο ίδιος ο peer γνωρίζει ποιοι είναι οι THA peers του.

Το πρωτόκολλο TrustMe χρησιμοποιεί public-key κρυπτογράφηση και παρέχει αμοιβαία ανωνυμία και για τον trust host (THA), αλλά και για τον querying peer, ο οποίος αναζητεί την trust value κάποιου peer. Ο querying peer μπορεί να εξακριβώσει ότι η απάντηση που θα λάβει προέρχεται από έναν THA peer. Επίσης σε περίπτωση που ο querying peer λάβει διαφορετικά trust values από διαφορετικούς THA peers ενός peer λαμβάνει υπόψη του την γνώμη της πλειοψηφίας των THA peers και ο THA peer που έστειλε το λανθασμένο trust value τιμωρείται με την εισαγωγή του σε μαύρη λίστα.

Το JXTA είναι μια πρόταση για μια ομοιόμορφη διεπαφή στα συστήματα ομότιμων βάσεων και για τη διευκόλυνση της διαλειτουργικότητας των συστημάτων αυτών. Το JXTA καθορίζει μια αρχιτεκτονική λογισμικού δικτύου ομότιμων, τριών στρωμάτων, μία ομάδα πρωτοκόλλων βασισμένων σε XML και ενός συνόλου από αφαιρέσεις και έννοιες, όπως οι ομάδες ομότιμων, οι σωλήνες, και οι διαφημίσεις. Με τον τρόπο αυτό παρέχει μια ομοιόμορφη πλατφόρμα για τις εφαρμογές που χρησιμοποιούν την τεχνολογία P2P και καθιστά εφικτή την αλληλεπίδραση συστημάτων P2P.

Με αυτό τον τρόπο εξασφαλίζεται ότι ένας peer ο οποίος αναζητεί την trust value κάποιου άλλου peer θα λάβει σωστή trust value ακόμα και υπό την παρουσία κακόβουλων χρηστών.

Το EigenTrust αναθέτει σε κάθε peer μία μοναδική καθολική trust value, η οποία αντικατοπτρίζει την εμπειρία όλων των peers του συστήματος με τον συγκεκριμένο peer. Κάθε peer αποθηκεύει μια local trust value για κάθε peer με τον οποίο έχει αλληλεπιδράσει. Κάθε φορά που ένας χρήστης κατεβάζει ένα *authentic* αρχείο από έναν peer αυξάνει το local trust value που έχει για αυτόν τον peer, ενώ αν κατεβάζει ένα *inauthentic* αρχείο από έναν peer μειώνει το local trust value που έχει για αυτόν τον peer.

Η global trust value κάθε peer βρίσκεται συναθροίζοντας όλες τις local trust values όλων των peers για τον συγκεκριμένο peer. Η global trust value χρησιμοποιείται για την απομόνωση των κακόβουλων χρηστών, καθώς οι peers του συστήματος κατεβάζουν αρχεία από peers με μεγάλο global trust value, και αποτελεί και κίνητρο για τους peers να διαμοιράζονται τα αυθεντικά αρχεία τους, καθώς το σύστημα ανταμείβει τους peers με μεγάλο global trust value.

Στην κατανεμημένη έκδοση του αλγορίθμου κάθε peer διατηρεί την global trust τιμή του τοπικά. Το πρόβλημα που δημιουργείται σε αυτή την περίπτωση είναι ότι κακόβουλοι χρήστες μπορεί να αναφέρουν σκόπιμα λανθασμένες trust values για τους εαυτούς τους.

Η λύση που προτείνεται είναι για έναν peer να υπολογίζουν την global trust τιμή του άλλοι peers. Για το λόγο αυτό ορίζονται κάποιοι score managers για κάθε peer που υπολογίζουν το trust value για αυτόν τον peer. Για την ανάθεση των score managers και

την αποθήκευση της reputation πληροφορίας χρησιμοποιείται ένα DHT, όπως το CAN ή το Chord. Οι score managers κάθε peer ορίζονται κάνοντας hash ένα μοναδικό ID του peer, όπως είναι η IP διεύθυνσή του, σε ένα σημείο του DHT hash space. Ο peer που καλύπτει αυτή την περιοχή του DHT space ορίζεται ως score manager αυτού του peer. Αν ένας κόμβος θέλει να μάθει την global trust τιμή ενός peer γνωρίζοντας το μοναδικό ID αυτού του peer μπορεί να εντοπίσει τους score managers του και να τους ρωτήσει.

Η ακεραιότητα της reputation πληροφορίας εξαρτάται από την αξιοπιστία των peers που υπολογίζουν και αποθηκεύουν τις global trust values. Ωστόσο η τυχαία επιλογή των score managers για κάθε peer και το γεγονός ότι σε περίπτωση που διαφέρουν οι global trust τιμές που στέλνουν οι score managers για έναν συγκεκριμένο peer λαμβάνεται ως η σωστή η τιμή που αναφέρει η πλειοψηφία των score managers έχει ως αποτέλεσμα να μειώνεται η πιθανότητα παραποίησης των trust values από κακόβουλους score managers.

Συνήθως υπάρχουν και κάποιοι peers στο σύστημα που θεωρούνται έμπιστοι εκ των προτέρων (pre-trusted peers) και είναι σημαντικοί για τον αλγόριθμο καθώς εγγυούνται την σύγκλιση του αλγορίθμου και σπάνε τις ομάδες κακόβουλων χρηστών που γνωρίζονται μεταξύ τους και δίνουν ο ένας στον άλλον μεγάλα local trust values με στόχο να αποκτήσουν μεγάλα global trust values.

Η προσέγγιση η οποία χρησιμοποιείται στο EigenTrust έχει κάποια μειονεκτήματα

- **ü** εφαρμόζεται μόνο σε δομημένα P2P δίκτυα
- **ü** το σύστημα λόγω της χρήσης του DHT είναι ευπαθές σε DHT-threats
- **ü** δεν παρέχεται ανωνυμία για τους score managers και έτσι ένας κακόβουλος χρήστης μπορεί να αναγνωρίσει ποιοι score managers του αναφέρουν χαμηλές trust values για αυτόν και να τους επιτεθεί
- **ü** δεν εξασφαλίζεται ότι η αναφορά που στέλνει ένας score manager με την trust value ενός κόμβου δεν θα τροποποιηθεί από ενδιάμεσους κακόβουλους χρήστες
- **ü** η επιλογή των σχεδιαστών του συστήματος ως pre-trusted peers και η τυχαία κατανομή τους έχει ως αποτέλεσμα όχι και τόσο δίκαιες τιμές για τις trust values που ανατίθενται σε κάποιους peers

Κεφάλαιο 5

Όπως προκύπτει οι περισσότερες P2P λύσεις συμφωνούν με κάποια μορφή.
Δυστυχώς όμως, οι τρέχουσες εφαρμογές P2P τείνουν να χρησιμοποιήσουν τα πρωτόκολλα που είναι ιδιόκτητα και κάθε δίκτυο διαμορφώνει μια κλειστή κοινότητα, απολύτως ανεξάρτητη από τα άλλα δίκτυα.

Μέχρι τώρα, ο ενθουσιασμός της διερεύνησης των δυνατοτήτων της P2P τεχνολογίας έχει επισκιάσει τη σημασία της διαλειτουργικότητας και της επαναχρησιμοποίησης λογισμικού. Για να εξελίχθεί η τεχνολογία P2P σε μια ώριμη πλατφόρμα λύσης, χρειάζεται μια κοινή γλώσσας επικοινωνίας για να επιτραπεί στις οντότητες που συμμετέχουν να επικοινωνούν και να εκτελέσουν τις βασικές αρχές της P2P δικτύωσης.

Κατανοώντας αυτήν την ανάγκη για μια κοινή γλώσσα, η Sun Microsystems διαμόρφωσε το πρόγραμμα JXTA. Στον πυρήνα του, το JXTA είναι απλά ένα σύνολο από προδιαγραφές πρωτοκόλλων, και αυτό είναι που το καθιστά τόσο ισχυρό. Έτσι κάποιος που θέλει να παραγάγει μια νέα P2P εφαρμογή δεν συναντά πλέον τη δυσκολία κατάλληλου σχεδιασμού πρωτοκόλλων για να χειριστεί τις βασικές λειτουργίες της P2P επικοινωνίας.

Το όνομα JXTA προέρχεται από την Αγγλική λέξη juxtapose που σημαίνει αντιπαραθέτω. Με την επιλογή αυτού του ονόματος, η ομάδα ανάπτυξης στη Sun αναγνώρισε ότι οι P2P λύσεις θα υπήρχαν πάντα παράλληλα με τις τρέχουσες λύσεις πελατών - κεντρικών υπολογιστών παρά να τις αντικαταστήσουν εντελώς.

5.1 Η πλατφόρμα του JXTA

Το JXTA (JuXTApose) είναι ένα σύνολο από έξι ανοιχτά, γενικευμένα P2P πρωτόκολλα που επιτρέπουν σε οποιεσδήποτε συσκευές σε ένα δίκτυο να επικοινωνούν και να

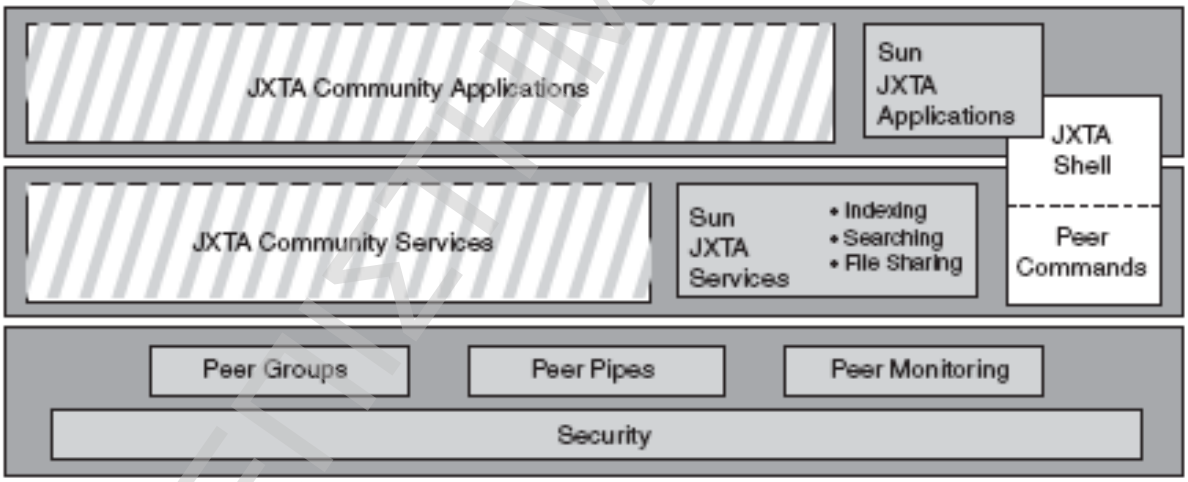
συνεργάζονται σαν ισότιμες οντότητες. Μάλιστα τα πρωτόκολλα αυτά είναι ανεξάρτητα από τη γλώσσα υλοποίησης. Στόχος του JXTA είναι να δώσει μια πλατφόρμα με τις βασικές λειτουργίες πάνω στις οποίες μπορεί να χτιστεί ένα P2P δίκτυο. Φυσικά αναφερόμαστε σε ένα νοητό δίκτυο υπερκείμενο στην υπάρχουσα τοπολογία.

Συνοπτικά, τα πρωτόκολλα του JXTA προτυποποιούν τον τρόπο με τον οποίο οι ισότιμες οντότητες:

- Ανακαλύπτουν άλλες οντότητες.
- Οργανώνονται σε ομάδες.
- Διαφημίζουν και ανακαλύπτουν υπηρεσίες.
- Επικοινωνούν μεταξύ τους.
- Ελέγχουν η μία την άλλη.

Να τονιστεί ότι σημεία κλειδιά του JXTA θεωρούνται:

- η χρήση της XML ως θεμέλιο.
- η απουσία κεντρικής αρχής διευθυνσιοδότησης και ονοματοδοσίας.



Εικόνα 5.1 :Αρχιτεκτονική JXTA

Κεντρική ορολογία στο JXTA

Ένα δίκτυο που βασίζεται στο JXTA αποτελείται από δια-συνδεδεμένους κόμβους, τους λεγόμενους peers. Κάθε peer λειτουργεί ανεξάρτητα από τους υπόλοιπους και

χαρακτηρίζεται από ένα μοναδικό peer ID. Επιπλέον οι peers μπορούν να οργανώνονται από μόνοι τους σε ομάδες.

Το peer group είναι ένα σύνολο κόμβων, οι οποίοι έχουν συμφωνήσει σε ένα κοινό πλαίσιο υπηρεσιών (services).

Η κάθε ομάδα χαρακτηρίζεται μοναδικά από ένα peer group ID και έχει τη δυνατότητα να εφαρμόσει τη δικιά της πολιτική ως προς την είσοδο (εγγραφή) νέων κόμβων σε αυτή. Για παράδειγμα σε μια ανοιχτή πολιτική ο κάθε κόμβος μπορεί να μπει στην ομάδα, αλλά το να κάνει το ίδιο σε μια κλειστή πολιτική απαιτεί πιθανώς διαπιστευτήρια (credentials). Τελειώνοντας, ένας κόμβος μπορεί να ανήκει ταυτόχρονα σε περισσότερες από μία ομάδες.

Οι κόμβοι χρησιμοποιούν «σωλήνες» (pipes) για να στέλνουν μηνύματα ο ένας στον άλλο. Το ίδιο κάνουν και οι υπηρεσίες που τρέχουν στους κόμβους. Οι σωλήνες, στη βασική τους μορφή, είναι μηχανισμοί ασύγχρονοι και προς μια κατεύθυνση.

Κάθε πόρος στο JXTA –κόμβος, ομάδα, σωλήμας, υπηρεσία- αναπαρίσταται με μια διαφήμιση. Πρόκειται για XML κείμενο που λέγεται advertisement. Οι διαφημίσεις αποθηκεύονται, ανταλλάσσονται, δημοσιοποιούνται και έχουν κάποιο χρόνο ζωής ο οποίος αντιστοιχεί στη διαθεσιμότητα του αντίστοιχου πόρου.

Βασικά σημεία του JXTA

Υπηρεσίες

Τα πρωτόκολλα του JXTA αναγνωρίζουν τις εξής δύο κατηγορίες υπηρεσιών.

Peer Services

Μπορεί κάποιος να έχει πρόσβαση σε μια τέτοια υπηρεσία μόνο στον κόμβο ο οποίος την διατηρεί. Αν αυτός ο κόμβος πέσει τότε παύει να είναι διαθέσιμη και η υπηρεσία. Γι' αυτόν τον λόγο διάφορες υποστάσεις της υπηρεσίας μπορούν να τρέχουν σε διαφορετικούς κόμβους. Όμως κάθε τέτοια υπόσταση οφείλει να διαφημίζεται μόνη της.

Peer Group Services

Μια Peer Group Service είναι ένα σύνολο από οντότητες μιας υπηρεσίας (που πιθανώς συνεργάζονται μεταξύ τους) και τρέχουν σε διάφορους κόμβους-μέλη ενός group. Αν ένας κόμβος πέσει τότε η διαθεσιμότητα της υπηρεσίας δεν επηρεάζεται, εφόσον παρέχεται από κάποιον άλλο κόμβο. Η διαφήμισή της γίνεται συνολικά για όλο το group. Ακολουθούν οι βασικές υπηρεσίες που αφορούν τα Peer Groups.

Discovery Service – χρησιμοποιείται από τα μέλη ενός group για να αναζητήσουν διαφημίσεις πχ άλλους κόμβους, υπηρεσίες και σωλήνες.

Membership Service – χρησιμοποιείται από τα μέλη ενός group για να απορρίψουν ή να δεχθούν την αίτηση ενός κόμβου που επιθυμεί να γίνει μέλος. Οι κόμβοι που θέλουν να μπουν σε μια ομάδα πρέπει πρώτα να εντοπίσουν ένα μέλος της και εκεί να κάνουν αίτηση.

Access Service – χρησιμοποιείται για να επικυρώσει αιτήσεις που γίνονται απ΄ τον έναν κόμβο στον άλλο. Ο κόμβος που λαμβάνει μια αίτηση προσδιορίζει τα απαιτούμενα διαπιστευτήρια για να αποφασίσει αν θα επιτρέψει την ζητούμενη ενέργεια ή όχι.

Pipe Service – χρησιμοποιείται για τη δημιουργία και τη διαχείριση σωλήνων μεταξύ των κόμβων που ανήκουν σε ένα group.

Resolver Service – επιτρέπει στους κόμβους να ορίζουν και να ανταλλάζουν queries για οποιαδήποτε πληροφορία που μπορεί να τους ενδιαφέρει (πχ την τρέχουσα κατάσταση μιας υπηρεσίας, να ανταλλάξουν έναν χαιρετισμό).

Monitoring Service – αυτή η υπηρεσία επιτρέπει σε έναν κόμβο να ελέγχει τα υπόλοιπα μέλη του group στον οποίο ανήκει.

Σωλήνες

Όπως έχουμε ήδη αναφέρει, οι κόμβοι στο JXTA χρησιμοποιούν τους σωλήνες για να στέλνουν μηνύματα ο ένας στον άλλο. Οι σωλήνες μπορούν να μεταφέρουν κυριολεκτικά τα πάντα˙ binary code, data strings και objects.

Ας φανταστούμε έναν σωλήνα που συνδέει δύο κόμβους Α και Β και ότι ο πρώτος στέλνει ένα μήνυμα στον δεύτερο. Τότε το άκρο του σωλήνα -στον Β- που δέχεται την πληροφορία ονομάζεται input pipe. Όμοια, το άκρο εκείνο απ' το οποίο στέλνεται το μήνυμα λέγεται output pipe.

Υπάρχουν δύο είδη σωλήνων:

- Point-to-point pipes – ένας σωλήνας σημείου προς σημείο συνδέει ακριβώς δύο άκρα: ένα input pipe σ' ένα κόμβο που δέχεται μηνύματα από το output pipe ενός άλλου κόμβου.

- Propagate pipes – ένας τέτοιος σωλήνας συνδέει ένα output pipe με πολλά input pipes. Αυτή η πολλαπλή διάδοση γίνεται πάντα στα πλαίσια ενός group

Μηνύματα

Το μήνυμα είναι η βασική μονάδα δεδομένων που ανταλλάσσεται μεταξύ κόμβων. Αποτελείται από μια σειρά ζευγαριών της μορφής όνομα/τιμή και αναπαρίσταται με δύο τρόπους: την XML και binary.
Αξίζει να σημειωθεί ότι τα μηνύματα στέλνονται και λαμβάνονται επιστρατεύοντας κυρίως την Pipe Service.

Διαφημίσεις

Όλοι οι πόροι ενός δικτύου –οι κόμβοι, οι ομάδες, οι σωλήνες και οι υπηρεσίες– αναπαρίστανται με διαφημίσεις δηλαδή με κείμενα XML. Οι κόμβοι αποθηκεύουν, δημοσιοποιούν και ανταλλάσσουν διαφημίσεις ώστε να ανακαλύπτουν τους διαθέσιμους πόρους. Έτσι ένας κόμβος που αναζητά μια υπηρεσία, ουσιαστικά αναζητά την διαφήμιση που αντιστοιχεί στη συγκεκριμένη υπηρεσία.

```
<?xml version="1.0"?>
<!DOCTYPE jxta:PGA>
<jxta:PGA xmlns:jxta="http://jxta.org">
    <GID> urn:jxta:jxta-NetGroup</GID>
    <MSID>urn:jxta:uuid-
NERDBEJFDEAFBADAFEEDBABE000000022348</MSI
D>
    <Name>NetPeerGroup</Name>
    <Desc>NetPeerGroup by default</Desc>
</jxta:PGA>
```

Πίνακας 5.2 :Διαφήμιση ομάδας στο JXTA

Στον πιο πάνω πίνακα φαίνεται η διαφήμιση ενός group. Στην αρχή έχουμε το μοναδικό peergroup ID. Ακολουθεί το module specification ID (το οποίο αναφέρεται σε μια άλλη διαφήμιση που περιγράφει τις διαθέσιμες στο group υπηρεσίες). Στη συνέχεια έχουμε το όνομα του group και μια περιγραφή.

Επιπλέον, σε κάθε διαφήμιση δίνεται ένας χρόνος ζωής. Αυτό σημαίνει ότι η διαφήμιση -και συνεπώς ο πόρος που περιγράφει- θα είναι διαθέσιμη στο δίκτυο για ένα καθορισμένο χρονικό διάστημα.

Υπάρχουν οι εξής τύποι διαφημίσεων.

- Peer Advertisement
- Peer Group Advertisement
- Pipe Advertisement
- Module Class Advertisement
- Module Spec Advertisement
- Module Impl Advertisement
- Content Advertisement
- Peer Info Advertisement
- Rendezvous Advertisement

Ταυτότητες (IDs)

Ένας κόμβος στο JXTA αναγνωρίζεται μοναδικά από την ταυτότητά του, η οποία του δίνει αναγνώριση ανεξάρτητα από την φυσική του διεύθυνση.
Με ταυτότητες προσδιορίζονται και άλλα στοιχεία του δικτύου όπως οι ομάδες και οι σωλήνες.

Οργάνωση δικτύου

Υπάρχουν 3 είδη κόμβων:

Simple peer

Ένας απλός peer μπορεί να στέλνει και να δέχεται μηνύματα, και συνήθως αποθηκεύει τοπικά διαφημίσεις. Χρησιμοποιεί μάλιστα την πληροφορία από τις αποθηκευμένες διαφημίσεις για να απαντάει σε queries. Όμως δεν προωθεί το query σε άλλον κόμβο, ακόμα και αν δεν έχει τη δυνατότητα να απαντήσει.

Rendezvous peer

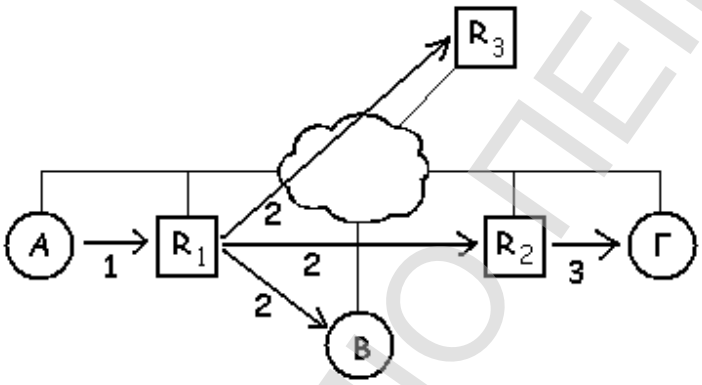
Το JXTA χρησιμοποιεί έναν μηχανισμό διασύνδεσης των πόρων που ονομάζεται Resolver. Η δουλειά του είναι να κάνει όλες εκείνες τις καίριες λειτουργίες που βρίσκονται στα παραδοσιακά κατανεμημένα συστήματα με αποκεντρωμένο τρόπο: πχ. η αντιστοιχία ονομάτων σε IP διευθύνσεις (όπως το DNS), η ένωση ενός socket σε ένα port, ο εντοπισμός μιας ζητούμενης υπηρεσίας μέσω ενός καταλόγου (όπως το LDAP). Όλα αυτά στηρίζονται σε κάτι απλό: τις διαφημίσεις. Αυτό που μας ενδιαφέρει είναι ότι η πολιτική του Resolver υλοποιείται μέσω των rendezvous peers.

Ένας rendezvous peer είναι λοιπόν ένα γνωστό σημείο όπου θα βρούμε χρήσιμους καταλόγους και διαφημίσεις. Επιπλέον διατηρεί μια λίστα με γνωστούς rendezvous peers, καθώς και με τους απλούς κόμβους που χρησιμοποιούν τον ίδιο ως σημείο συνάντησης.

Αξίζει να δούμε δύο παραδείγματα διάδοσης μηνυμάτων μέσω rendezvous peers.

Παράδειγμα:
Στο JXTA τα μηνύματα έχουν σαν default TTL=7. Οι κύκλοι αποφεύγονται διατηρώντας όλους τους ενδιάμεσους κόμβους κατά μήκος μιας διαδρομής.

Στο σχήμα που ακολουθεί Α, Β, Γ είναι απλοί κόμβοι ενώ R1, R2, R3 είναι κόμβοι συνάντησης. Μάλιστα οι Α και Β έχουν ρυθμιστεί να χρησιμοποιούν τον R1 ενώ ο Γ χρησιμοποιεί τον R2.



Εικόνα 5.3: RPs στο JXTA stable 1.0

Ο κόμβος Α θέλει να μάθει για κάποιο πόρο στο δίκτυο, γι' αυτό παράγει ένα query το οποίο αρχικά πηγαίνει στον R1. Επειδή ο R1 δεν διαθέτει την πληροφορία στις τοπικά αποθηκευμένες διαφημίσεις του (cache), προωθεί το query στους γνωστούς σε αυτόν rendezvous peers, δηλ. στους R2 και R3, καθώς επίσης και σε όποιον κόμβο γνωρίζει ότι χρησιμοποιεί τον ίδιο ως rendezvous peer, δηλ. στον Β μόνο (αφού ο Α έστειλε το query). Με τη σειρά του ο R2 προωθεί το query στον Γ. Φυσικά αν γνώριζε κι άλλους κόμβους ή αντίστοιχους κόμβους συνάντησης θα έκανε το ίδιο.

Παρατηρούμε ότι οι διαφημίσεις αποθηκεύονται τοπικά στους κόμβους συνάντησης κι αυτό είναι που τους δίνει τη γνώση τους. Επίσης, τα queries προωθούνται στους απλούς κόμβους. Αν σκεφτούμε ένα δίκτυο JXTA μεγάλης κλίμακας όπου ένας rendezvous peer αντιστοιχεί πχ σε 100 απλούς, τότε ίσως υπάρχει πρόβλημα συμφόρησης. Για τον λόγο αυτό στην επόμενη έκδοση JXTA 2.0 ένας rendezvous peer δεν αποθηκεύει τις ίδιες τις διαφημίσεις αλλά ένα ευρετήριο με τις διαφημίσεις των απλών κόμβων, δηλαδή δείκτες. Αυτό προσφέρει μεγάλη ευελιξία.

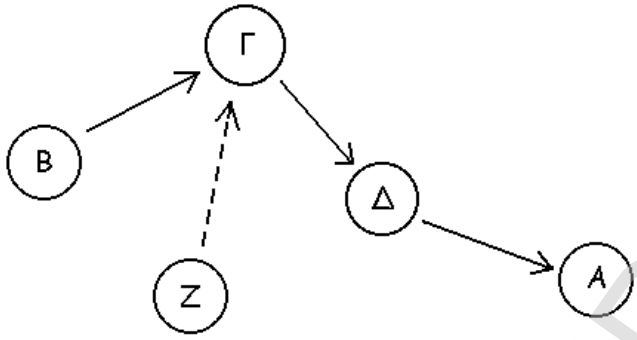
Με αυτόν τον τρόπο οδηγούμαστε στο λεγόμενο Shared Resource Distributed Index (SRDI). Είναι ο μηχανισμός μέσω του οποίου οι απλοί κόμβοι «αναρτούν» τις διαφημίσεις τους στους κόμβους συνάντησης. Ουσιαστικά οι κόμβοι όταν θέλουν να δημοσιοποιήσουν τις διαφημίσεις τους, σπρώχνουν τους δείκτες των διαφημίσεών τους. Αυτό μπορεί να γίνεται ασύγχρονα (μόλις δημιουργηθεί μια νέα διαφήμιση) ή και σύγχρονα (σε τακτά χρονικά διαστήματα).

Relay peer

Ένας relay peer διατηρεί πληροφορία για τις διαδρομές προς άλλους κόμβους και δρομολογεί μηνύματα. Κάθε κόμβος κοιτάει πρώτα στην τοπική cache για πληροφορία δρομολόγησης. Αν δεν βρει κάτι, στέλνει ένα query στους relay peers.

Οι διαδρομές στο JXTA κατασκευάζονται αρχικά στον αποστολέα, με βάση τις γνώσεις του και για λόγους αποκέντρωσης. Φυσικά αναπαρίστανται ως διαφημίσεις. Μια διαδρομή αποτελείται από τα διαδοχικά βήματα μέχρι τον κόμβο προορισμού. Κάθε βήμα προσδιορίζει το peer ID του επόμενου κόμβου, που είναι συνήθως relay peer.

Αξίζει να τονιστεί ότι η έννοια της διαδρομής είναι ανεξάρτητη από το αν και πού βρίσκεται στο μονοπάτι της ο αποστολέας. Με απλά λόγια, η διαφήμιση μιας διαδρομής μπορεί να χρησιμοποιηθεί από οποιονδήποτε κόμβο που θέλει να στείλει κάτι. Για παράδειγμα έστω η διαδρομή προς τον κόμβο Α, η οποία έχει τα βήματα <Β, Γ, Δ>. Ο Ζ θέλει να στείλει μήνυμα στον Α. Εξετάζει αυτή τη διαφήμιση και παρατηρεί τον Γ, με τον οποίο τυχαίνει να ξέρει πώς να μιλήσει. Κι αυτό ακριβώς κάνει. Χρησιμοποιεί δηλαδή μόνο τα βήματα <Γ,Δ> της διαδρομής.



Εικόνα 5.4: μια διαδρομή

Επιπλέον, οι relay peers χρησιμοποιούνται για να παρακάμπτονται με ευέλικτο τρόπο εμπόδια όπως τα firewalls και οι Network Address Translators (NATs).

Σημείωση: Η δρομολόγηση δεν στηρίζεται αποκλειστικά στους relay peers. Κάθε μήνυμα φέρει μια πλήρη ή μερική λίστα κόμβων μέσω των οποίων μπορεί να γίνει η παράδοση. Μάλιστα, κάθε κόμβος της λίστας μπορεί να βελτιώσει την διαδρομή με βάση τις γνώσεις του. Έτσι ένας κόμβος που δέχεται ένα μήνυμα μπορεί να χρησιμοποιήσει αυτήν την πληροφορία για να στείλει απάντηση στον αποστολέα.

Συνοψίζοντας, οι κόμβοι συνεργάζονται για την παράδοση των μηνυμάτων και η δρομολόγηση είναι δυναμική.

Τα πρωτόκολλα του JXTA

Το JXTA ορίζει μια σειρά από πρωτόκολλα βασισμένα στην XML για την επικοινωνία μεταξύ των κόμβων. Είναι ασύγχρονα και βασίζονται στο μοντέλο ερώτησης/ απάντησης.

Peer Discovery Protocol - PDP

Χρησιμοποιείται από τους κόμβους για να διαφημίζουν πόρους –πχ ομάδες, σωλήνες, υπηρεσίες– (δημοσιοποίηση) και για να ανακαλύπτουν πόρους από άλλους κόμβους (αναζήτηση). Αυτό λαμβάνει χώρα στα πλαίσια ενός group. Όπως έχει ήδη ειπωθεί, οι πόροι αναπαρίστανται από τις διαφημίσεις.

Peer Information Protocol - PIP

Χρησιμοποιείται από τους κόμβους για να λάβουν πληροφορίες κατάστασης από άλλους κόμβους (πχ uptime, λειτουργία, κίνηση). Στην περίπτωση που θέλουμε να μάθουμε τέτοιου είδους πληροφορίες, στέλνουμε στον κόμβο ένα **ping**. Αυτό μπορεί να ζητάει είτε ολόκληρη την peer advertisement του κόμβου είτε μια απλή απάντηση (alive & uptime). Ως απάντηση, ο κόμβος στέλνει ένα **peerinfo** μήνυμα. Αυτό περιέχει τα credentials του αποστολέα, την peerID του αποστολέα και του στόχου, το uptime και την peer advertisement.

Peer Resolver Protocol - PRP

Επιτρέπει στους κόμβους να ορίζουν και να ανταλλάζουν οποιαδήποτε πληροφορία χρειάζονται. Η διαφορά του από τα δύο προηγούμενα πρωτόκολλα έγκειται στο ότι εκείνα προσδιορίζουν ακριβώς τις ερωταποκρίσεις (πόροι στο PDP, πληροφορία κατάστασης στο PIP).

Το resolver query message περιέχει το credential του αποστολέα, ένα μοναδικό ID, ένα συγκεκριμένο service handler και το query.

Το resolver response message περιέχει το credential του αποστολέα, ένα μοναδικό ID, ένα συγκεκριμένο service handler και την απάντηση.

Pipe Binding Protocol - PBP

Χρησιμοποιείται απ' τους κόμβους για να εγκαθιστούν νοητά κανάλια επικοινωνίας, τους γνωστούς σωλήνες, μεταξύ τους.

Ένα query message του πρωτοκόλλου στέλνεται από ένα pipe endpoint για να βρει ένα άλλο pipe endpoint που αντιστοιχεί στην ίδια pipe advertisement.

Ένα answer message στέλνεται στον κόμβο που έστειλε το query από κάθε κόμβο που συνδέεται στον σωλήνα.

Endpoint Routing Protocol - ERP

Χρησιμοποιείται απ' τους κόμβους για να βρουν διαδρομές προς άλλους κόμβους. Η πληροφορία δρομολόγησης περιλαμβάνει τα peer IDs της πηγής και του προορισμού, ένα TTL και μια σειρά -όχι απαραίτητα πλήρη- από τα IDs των relay peers οι οποίοι μπορούν να οδηγήσουν το μήνυμα μέχρι τον προορισμό.

Rendezvous Protocol - RVP

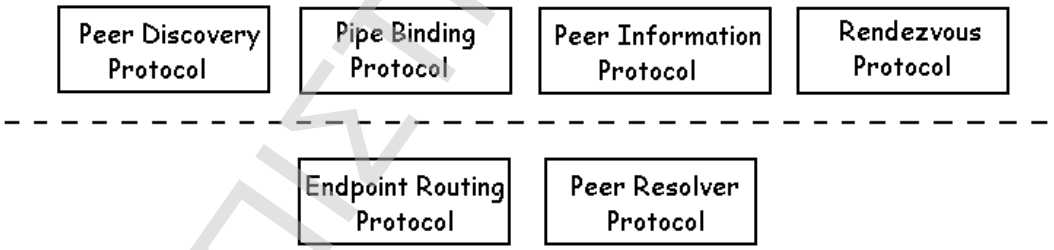
Χρησιμοποιείται απ' τους κόμβους για να διαδίδουν μηνύματα μέσα στα group τους.

Τα παραπάνω συνοψίζονται στον πίνακα που ακολουθεί. Τα πρωτόκολλα που έχουν υπογραμμισθεί είναι τα υποχρεωτικά και ονομάζονται πρωτόκολλα πυρήνα.

PRP	Queries
PDP	Advertisements
PIP	status information
PBP	Pipes
ERP	Routing
RVP	propagation of messages

Πίνακας 5.5: τα πρωτόκολλα του JXTA

Ακολούθως παρατίθεται η στοίβα των πρωτοκόλλων.



Εικόνα 5.6: Η στοίβα πρωτοκόλλων του JXTA

5.2 JXTA Ασφάλεια

Τα χαρακτηριστικά ασφάλειας που παρέχει η πλατφόρμα JXTA είναι :

• TLS ως ασφαλές στρώμα μεταφορών (TLS) — γνωστό επίσης ως Secure Sockets Layer (SSL) που είναι βασισμένο στην τεχνολογία δημόσιου κλειδιού. Η πλατφόρμα JXTA παρέχει το TLS ως μέσο ασφαλών επικοινωνιών. Οι εφαρμογές μπορούν να εκμεταλλευτούν τις ικανότητες TLS της πλατφόρμας με τη χρησιμοποίηση των ασφαλών σωλήνων, που χρησιμοποιούν εσωτερικά TLS, για να εξασφαλιστεί η ασφάλεια ενάντια στις παθητικές επιθέσεις.

• Peer certificates — το στρώμα TLS απαιτεί τη χρήση πιστοποιητικών για να λειτουργήσει σωστά. Συνεπώς, κάθε peer παράγει το πιστοποιητικό του και ενεργεί ως αρχή (CA) πιστοποίησης. Αυτό το πιστοποιητικό, αποκαλούμενο πιστοποιητικό ρίζας, χρησιμοποιείται για να υπογράψει τα πιστοποιητικά υπηρεσιών που οι peers εκδίδουν για κάθε υπηρεσία που αυτό υποστηρίζει.
Το πιστοποιητικό ρίζας διανέμεται μαζί με τη διαφήμιση του peer
Επομένως, κάθε άλλο peer μπορεί πάντα να ελέγξει ότι μια διαφήμιση είναι πράγματι από τον κόμβο που υποστηρίζει ότι την έχει εκδώσει.

•Το προσωπικό περιβάλλον ασφάλειας — κάθε κόμβος προστατεύεται από ένα peer ID και έναν κωδικό πρόσβασης. Αυτό χρησιμοποιείται για να αποκρυπτογραφήσει το ιδιωτικό κλειδί σε ένα προσωπικό περιβάλλον ασφάλειας ενός χρήστη.
Αυτό ενεργεί ως πρώτη γραμμή υπεράσπισης ενάντια σε έναν τοπικό επιτιθέμενο.

Απαιτήσεις ασφάλειας JXTA
Η πλατφόρμα JXTA εξαρτάται από τα ακόλουθα πακέτα και APIs για τις απαιτήσεις ασφάλειά της:
•*PureTLS* —καθαρό TLS είναι μια open-source Java εφαρμογή του πρωτοκόλλου TLS. Χρησιμοποιείται για να επιτύχει μυστικότητα μεταξύ των επικοινωνούντων κόμβων.
•*To Cryptix 3*—Cryptix παρέχει διεπαφές πρότυπα για τους κρυπτογραφικούς αλγορίθμους και υπηρεσίες.

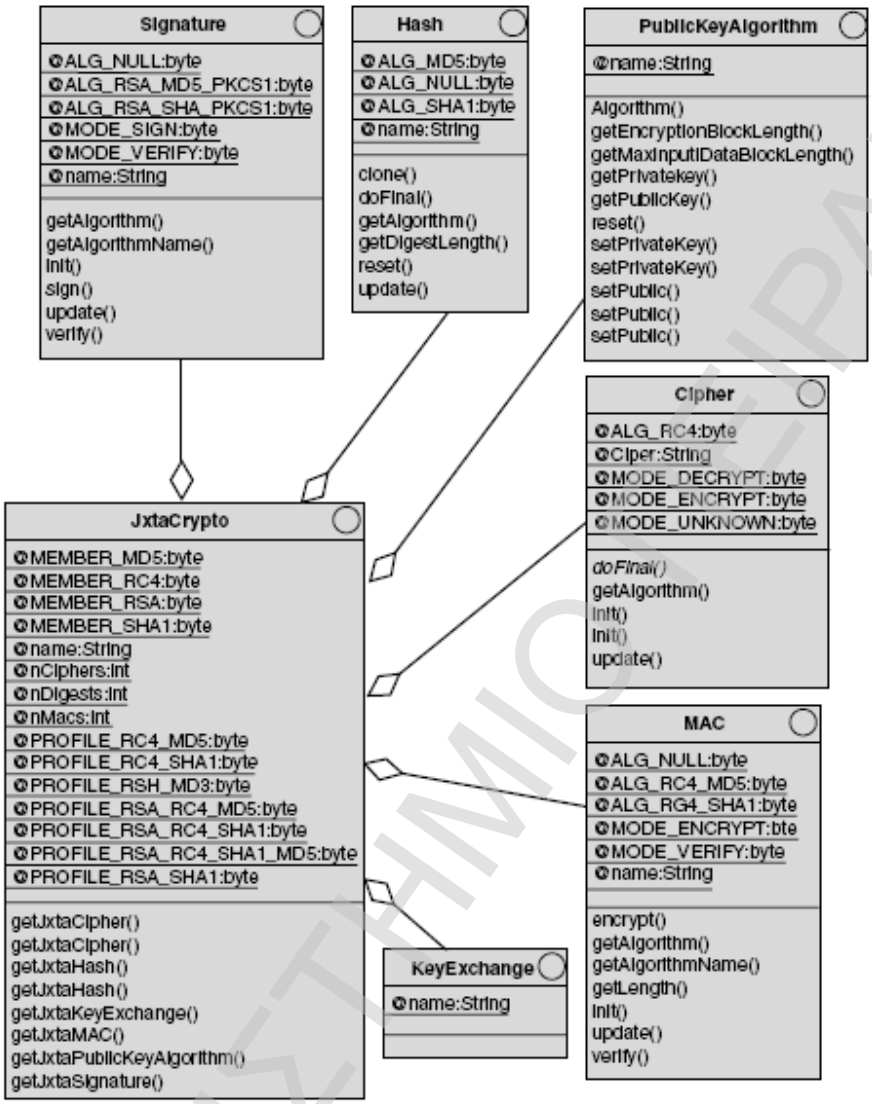
•*Cryptix ASN.1* είναι η γλώσσα που επιτρέπει τους ορισμούς των διάφορων τύπων στοιχείων, όπως οι ακέραιοι αριθμοί, σειρές, ακολουθίες, και τα λοιπά. Λόγω του απλοϊκού σχεδίου κωδικοποίησής της, μπορεί να χρησιμοποιηθεί για ανταλλαγή μηνυμάτων μεταξύ των διαφορετικών εφαρμογών δικτύων
•*Crypto APIs του Castle Bouncy* —μια άλλη ανοικτή εφαρμογή πηγής JCE που χρησιμοποιείται για να παράγει certificates.

The Cryptographic Toolkit

Εκτός από τα λίγα βασικά χαρακτηριστικά γνωρίσματα ασφάλειας που έρχονται με την πλατφόρμα JXTA,
Το πρόγραμμα ασφάλειας JXTA παρέχει ένα σύνολο εργαλείων ένα βασικό σύνολο αλγορίθμων ασφάλειας ου μπορούν να χρησιμοποιηθούν στις εφαρμογές JXTA.

JXTA Security Suites

Μια *ακολουθία ασφάλειας* αντιπροσωπεύει ένα ολοκληρωμένο σύστημα ασφάλειας. Αποτελείται από διάφορους αλγόριθμους ασφάλειας και υπηρεσίες που μπορούν να χρησιμοποιηθούν από τους πελάτες της ακολουθίας.



Σχήμα 5.7: UML σχέσεις στο JXTA Crypto package

Η ακολουθία JXTACrypto

Όντας η κατεξοχήν ακολουθία ασφάλειας της πλατφόρμας JXTA, JXTACrypto Υποστηρίζει διάφορους τύπους κρυπτογραφικών διαδικασιών, όπως η κρυπτογράφηση, hashing, κτλ Κάθε ένας από αυτούς τους τύπους διαδικασιών μπορεί να βελτιωθεί χρησιμοποιώντας διαφορετικούς αλγορίθμους.

Κεφάλαιο 6

Οι εξελίξεις στο τομέα του P2P και το μέλλον

Αν και δεν μπορούμε με απόλυτη σιγουριά να προβλέψουμε ποιο ακριβώς θα είναι, από πλευράς εφαρμογών και αρχιτεκτονικής, το μέλλον του Peer to Peer, μπορούμε με σιγουριά να πούμε ότι αυτό διαγράφεται αρκετά ελπιδοφόρο. Ήδη έχουν συγκροτηθεί αρκετά working groups και ομάδες έρευνας, οι οποίες προσπαθούν να δημιουργήσουν standards και frameworks τα οποία θα κάνουν την ανάπτυξη εφαρμογών πολύ πιο εύκολη. Το πιο ενθαρρυντικό απ' όλα είναι άλλωστε το γεγονός ότι οι περισσότερες από τις ομάδες αυτές δείχνουν διατεθειμένες να μην κρατήσουν την ανάπτυξη των τεχνολογιών υπό ιδιοκτησιακό καθεστώς, κάτι που -συν τοις άλλοις- θα συνεισφέρει στη γενικότερη εξάπλωση και ανάπτυξη του Peer to Peer.

Ερευνητές του Πανεπιστημίου του Wisconsin, που αναπτύσσουν μία τεχνολογία κατανεμημένης επεξεργασίας επονομαζόμενη Condor, εκτιμούν ότι οι περισσότερες επιχειρήσεις αξιοποιούν λιγότερο από το 25% της επεξεργαστικής ισχύος και του χώρου αποθήκευσης που διαθέτουν.

Κολοσσιαίες επιχειρήσεις όπως η Intel, η γιγάντια αεροδιαστημική βιομηχανία Boeing, αλλά και η εταιρεία πετρελαίων Amerada Hess, έχουν κάνει κάτι γι' αυτό, υιοθετώντας με επιτυχία συστήματα P2P. Η τελευταία, μέσω του Beowulf Project, έχει ενώσει 200 επιτραπέζιους υπολογιστές της Dell με Ethernet και Linux. Οι συγκεκριμένοι υπολογιστές απασχολούνται στην ερμηνεία πολύπλοκων σεισμικών δεδομένων και έχουν αντικαταστήσει στο έργο αυτό δύο υπερυπολογιστές IBM. Η ίδια εταιρεία έχει αναπτύξει ακόμη δύο σχετικά projects. Στο πρώτο από αυτά κάθε υπολογιστής στο δίκτυο "δανείζεται" κύκλους επεξεργασίας από διπλανά PCs, ενώ το δεύτερο λειτουργεί με τη φιλοσοφία του Napster και έχει ως στόχο την αξιοποίηση του συνολικού κατανεμημένου χώρου επεξεργασίας. Παράλληλα, εταιρείες όπως οι Applied MetaComputing και Groove Networks, αναπτύσσουν προϊόντα και υπηρεσίες αυτού του τύπου.

Στις Η.Π.Α. ο κρατικός τομέας κάνει τα πρώτα δειλά βήματα προς το P2P. Τα sites FedStats.gov και FedStats.net επιτρέπουν σε περισσότερους από 70 κρατικούς οργανισμούς, οι οποίοι χρησιμοποιούν 200 στατιστικά προγράμματα, να συνδέονται απευθείας και να ανταλλάσσουν στατιστικά δεδομένα "ταχύτερα, καλύτερα και φθηνότερα" όπως λένε οι υπεύθυνοί τους.

Ο οργανισμός DARPA (Defence Advanced Research Projects Agency) έχει ξεκινήσει ένα πειραματικό πρόγραμμα για τη δικτύωση P2P στρατιωτών στο πεδίο της μάχης. Οι πομποδέκτες των στρατιωτών αναπτύσσονται από την ITT, ενώ το δίκτυο θα βασίζεται στο Linux. Πλεονέκτημα του δικτύου αυτού είναι το γεγονός ότι οι πομποδέκτες θα χρειάζονται μικρότερη ισχύ, με αποτέλεσμα μεγαλύτερη διάρκεια της μπαταρίας και δυσκολότερο εντοπισμό ή παρεμβολές από τον εχθρό. Ανάλογο πρόγραμμα έχει και το αμερικανικό ναυτικό.

Παρ' ότι όλα τα ανωτέρω είναι ενθαρρυντικά, παραμένει το γεγονός ότι υπάρχουν αρκετά προβλήματα για τη σχεδίαση ενός απλού προγράμματος στην πλατφόρμα Peer To Peer .
Καταρχήν, θα πρέπει να προσδιοριστεί ο σκοπός του προγράμματος ώστε να μπορεί να συνεργαστεί με κατανεμημένο σύστημα. Όπως αναφέρουν οι ειδικοί, πρέπει το πρόγραμμα να είναι "αναίσθητο" στα υποκείμενα επίπεδα (layers). Επιπλέον, μία σοβαρή εφαρμογή θα πρέπει να χρησιμοποιεί κάποιου είδους πιστοποίηση για τους χρήστες που συνδέονται.

Γενικότερα, το θέμα της ασφάλειας είναι κάτι που σίγουρα επιδέχεται βελτίωσης στα Peer to Peer προγράμματα που έχουν δημιουργηθεί μέχρι σήμερα. Επίσης, όπως είναι της μόδας τελευταία, για να γίνει πιο προσιτή στο μέσο προγραμματιστή η δημιουργία μίας Peer to Peer εφαρμογής, πρέπει να παρουσιαστεί μια πλατφόρμα με τη μορφή βιβλιοθήκης (library). Με τον τρόπο αυτό η υλοποίηση μιας τέτοιας εφαρμογής θα γίνεται πιο γρήγορα και στην πράξη δεν θα χρειάζεται κάθε προγραμματιστής να "ξαναεφευρίσκει τον τροχό". Όλα αυτά είναι σαφή προβλήματα, τα οποία όμως οδεύουν προς τη λύση τους. Γι' αυτό και γίνονται ήδη προσπάθειες δημιουργίας κάποιων standards για το συγκεκριμένο είδος εφαρμογών. Τον πρώτο λόγο στις προσπάθειες αυτές έχει το "Peer To Peer Working Group" (http://www.peer-to-peerwg.org), μία ομάδα

από εταιρείες που προσπαθούν να ωθήσουν την αγορά προς το Peer to Peer computing. Εκτός από την Intel που το ξεκίνησε, σήμερα στο PTPWG έχουν προστεθεί πολλά ακόμα μεγαθήρια της πληροφορικής, όπως η Hewlett-Packard και η Fujitsu. Την υπόλοιπη ομάδα στελεχώνουν και εταιρείες που έχουν επενδύσει σε αυτή την τεχνολογία και δημιουργούν τέτοιου είδους εφαρμογές. Ήδη διατίθεται από το site του PTPWG μία βιβλιοθήκη για distributed πιστοποίηση χρηστών, με τη βοήθεια της βιβλιοθήκης OpenSSL (SSL=Secure Socket Layer). Η ομάδα έχει ικανοποιητική δραστηριότητα και προσπαθεί να μαζέψει τα απαραίτητα προγραμματιστικά εργαλεία ώστε να γίνεται ευκολότερα στο μέλλον η υλοποίηση μιας Peer to Peer εφαρμογής.

Από τη Sun MicroSystems το project JXTA, έχει σκοπό είναι να βοηθήσει την ανάπτυξη συστημάτων κι εφαρμογών με χαρακτηριστικό τη *διαλειτουργικότητα*, δηλ. εφαρμογές που θα μπορούν να συμπεριλάβουν σαν κόμβους υπολογιστές , PDAs , κινητά κλπ. Για παράδειγμα μία ασύρματη συσκευή που χρησιμοποιεί πρωτόκολλο επικοινωνίας το Bluetooth και ένα PC συνδεδεμένο μέσω TCP/IP θα είναι κόμβοι του ίδιου δικτύου μιας εφαρμογής βασισμένη στο JXTA.

Το peer to peer είναι μια σημαντική τεχνολογία που έχει ήδη βρει το δρόμο της με μια σειρά προϊόντων και ερευνητικών προγραμμάτων. Όσο ωριμάζει οι μελλοντικές του υλοποιήσεις θα βελτιώνονται. Θα υπάρχει αυξημένη διαλειτουργικότητα, περισσότερες συνδέσεις και καλύτερο software και hardware.
Καθώς ο κόσμος γίνεται ολοένα και περισσότερο αποκεντρωμένος και συνδεδεμένος θα υπάρξει μια αυξανόμενη ανάγκη peer to peer αλγορίθμων για την βελτίωση της επεκτασιμότητας, της ανωνυμίας και των προβλημάτων σύνδεσης. Οι εφαρμογές των peer to peer είναι πολύ πιθανόν να είναι εξίσου ή και περισσότερο επιτυχημένες στο μέλλον. Πλατφόρμες όπως το JXTA είναι αρκετά πιθανόν να υιοθετηθούν ευρέως.
Τα συστήματα peer to peer θα παραμείνουν μια σημαντική λύση σε συγκεκριμένα προβλήματα των αποκεντρωμένων συστημάτων. Ίσως δεν είναι η μόνη επιλογή και ίσως δεν είναι κατάλληλη για όλα τα προβλήματα αλλά θα συνεχίσει να είναι μια καλή εναλλακτική επιλογή σε περιπτώσεις που απαιτείται επεκτασιμότητα, ανωνυμία και ανέχεια σε σφάλματα. Οι αλγόριθμοι, οι εφαρμογές και οι πλατφόρμες των peer to peer έχουν την δυνατότητα να αναπτυχθούν περαιτέρω στο μέλλον.
Από την πλευρά της αγοράς το κόστος ιδιοκτησίας ίσως είναι ο κύριος παράγοντας ανάπτυξης των peer to peer συστημάτων. Η ισχυρή παρουσία peer to peer προϊόντων

δείχνει πως εκτός από μια ενδιαφέρουσα για έρευνα τεχνολογία το peer to peer είναι μια υποσχόμενη βάση προϊόντων.

Τέλος, δεδομένου ότι οι p2p τεχνολογίες εξελίσσονται ακόμα, υπάρχει ένα πλήθος ανοικτών ερευνητικών προβλήματων, κατευθύνσεων και ευκαιριών:

—Έρευνα για δρομολόγηση και για αλγορίθμους που θα συμβάλλουν στην απόδοση, την ασφάλεια και την εξελιξιμότητα τόσο στις δομημένες όσο και στις μη δομημένες δικτυακές αρχιτεκτονικές.

—Μελέτη αποδοτικότερων μέτρων ασφάλειας, της ανωνυμίας, και της αντίστασης σε σχέδια λογοκρισίας. Αυτά τα χαρακτηριστικά γνωρίσματα θα είναι κρίσιμα για το μέλλον των p2p συστημάτων και η υιοθέτησή τους αναγκαία για τις όλο και πιό ευαίσθητες εφαρμογές.

—Η σημασιολογική ομαδοποίηση των πληροφοριών στα p2p δίκτυα. Αυτή η κατεύθυνση έχει πολλά από κοινού με τις προσπάθειες στο Semantic Web Domain.

—Οι μηχανισμοί κινήτρων και τα συστημάτα φήμης που θα υποκινήσουν την συνεταιριστική συμπεριφορά μεταξύ των χρηστών, και θα κάνουν τη λειτουργία των p2p συστημάτων πιο δίκαιη.

—Η σύγκλιση του Grid και των p2p συστημάτων και ο συνδιασμός των οφελών του κατανεμημένου υπολογισμού.

Βιβλιογραφία

[1] Stephanos Andoutsellis-Theotokis and Diomidis Spinellis,*A Survey of Peer-to-Peer Content Distribution Technologies*

[2] Steve Bellovin. Security aspects of Napster and Gnutella. In *2001 Usenix Annual Technical Conference*, Boston, Massachusetts,June 2001. Invited talk.

[3] Miguel Castro, Peter Druschel, Y. Charlie Hu, and Antony Rowstron. *Exploiting network proximity in peer-to-peer overlay networks*. Technical Report MSR-TR-2002-82, Microsoft Research, May 2002.

[4] Roger Dingledine, Michael J. Freedman, and David Molnar. Accountability measures for peer-to-peer systems. In *Peer-to-Peer:Harnessing the Power of Disruptive Technologies*. O'Reilly and Associates, November 2000.

[5] John R. Douceur. The Sybil attack. In *Proceedings for the 1st International Workshop on Peer-to-Peer Systems (IPTPS '02)*, Cambridge, Massachusetts, March 2002.

[6] Stuart E. Schechter, Rachel A. Greenstadt, and Michael D. Smith Harvard University Trusted Computing, *Peer-To-Peer Distribution, and the Economics of Pirated Entertainment,*May 29, 2003

[7] Robert Nelson Gruia Pitigoi-Aron, *p2p Trust Infrastructure,*Computer Science Division,University of California, Los Angeles, CA 90024

[8] Sergio Marti, Hector Garcia-Molina, *Taxonomy of trust: Categorizing P2P reputation systems,Department of Computer Science*, Stanford University, Stanford, CA 94305, United States

[9] Michael J. Freedman, Robert Morris, *Tarzan: A Peer-to-Peer Anonymizing Network Layer*, NYU Dept of Computer Science 715 Broadway #715 New York, NY 10003 USA - MIT Lab for Computer Science 200 Technology Sq. #509 Cambridge, MA 02139 USA

[10] Dan S. Wallach, *A Survey of Peer-to-Peer Security Issues* Rice University, Houston, TX 77005, USA

[11] Miguel Castro, Peter Druschel, Ayalvadi Ganesh, Antony Rowstron1 and Dan S. Wallach, *Secure routing for structured peer-to-peer overlay networks*, Microsoft Research Ltd., 7 J J Thomson Avenue, Cambridge, CB3 0FB, UK,2Rice University, 6100 Main Street, MS 132, Houston, TX 77005-1892, USA

[12] Emil Sit and Robert Morris, *Security Considerations for Peer-to-Peer Distributed Hash Tabl*e, Laboratory for Computer Science, MIT

[13] Chris McKean, *Peer-to-Peer Security and Intel's Peer-to-Peer Trusted Library*, August 20, 2001

[14] The project JXTA web site. http://www.jxta.org

[15] Elias Athanasopoulos, Kostas G. Anagnostakis, and Evangelos P. Markatos, *Misusing nstructured P2P Systems to PerformDoS Attacks: The Network That Never* , Institute of Computer Science (ICS) Foundation for Research & Technology Hellas (FORTH)

[16] Allan Friedman, L Jean Camp, *Peer-to-Peer Security* , Harvard University

[17] Chris McKean *Peer-to-Peer Security and Intel's Peer-to-Peer Trusted Library*, August 20, 2001

[18]Simon Rieche, Klaus Wehrle, Olaf Landsiedel, Stefan G¨otz, Leo Petrak, *Reliability of Data in Structured Peer-to-Peer Systems*, Protocol Engineering and Distributed Systems Group University of T¨ubingen, Germany