



www.uom.gr

ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΟΙΚΟΝΟΜΙΚΩΝ ΚΑΙ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ



**ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ
ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΑ
ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ (M.I.S.)**

Καθηγητής/ Professor:

Αναστάσιος Α. Οικονομίδης/
Anastasios A. Economides

Μάθημα/ Course:

Δίκτυα Υπολογιστών/ Computer Networks

Τίτλος εργασίας/ Subject of the essay:

Δίκτυα για Ομότιμες Εφαρμογές/
Networks for P2P Applications

Συγγραφέας/ Author:

Άγγελος Γεωργούλας/
Angelos Georgoulas

**Θεσσαλονίκη
Δεκέμβριος, 2010**

Περιεχόμενα

<u>ΠΕΡΙΛΗΨΗ</u>	<u>3</u>
<u>ABSTRACT</u>	<u>3</u>
<u>ΠΑΡΟΥΣΙΑΣΗ ΘΕΜΑΤΟΣ</u>	<u>4</u>
ΤΑΞΙΝΟΜΗΣΗ	4
ΑΠΟΔΟΣΗ	5
ΑΞΙΟΠΙΣΤΙΑ	5
ΑΣΦΑΛΕΙΑ	6
ΑΝΑΒΑΘΜΙΣΙΜΟΤΗΤΑ	6
ΚΟΣΤΟΣ	7
<u>ΕΦΑΡΜΟΓΕΣ P2P</u>	<u>7</u>
NAPSTER	7
GNUTELLA	8
FASTTRACK	9
FREENET	10
KAZAA	11
BITTORRENT	12
SKYPE	12
JOOST	13
SOPCAST	14
<u>ΣΥΜΠΕΡΑΣΜΑΤΑ</u>	<u>16</u>
<u>ΒΙΒΛΙΟΓΡΑΦΙΑ</u>	<u>19</u>

Περίληψη

Σκοπός της εργασίας αυτής είναι η μελέτη των δικτύων ομότιμων εφαρμογών (P2P). Αυτό γίνεται εφικτό μέσα από την διάκριση της ταξινόμησης τους δηλαδή σε δομημένα, χαλαρά δομημένα και αδόμητα, κεντροποιημένα, υβριδικά ή διανεμημένα αλλά και σε ιεραρχημένα ή όχι. Επίσης, για την ορθή μελέτη των ομότιμων δικτύων, πλεονεκτημάτων και μειονεκτημάτων τους, απαιτείται η μελέτη των κριτηρίων αξιολόγησης δικτύων, δηλαδή απόδοση, αξιοπιστία, ασφάλεια, αναβαθμισιμότητα και κόστος. Στο δεύτερο τμήμα της εργασίας μελετάται η αρχιτεκτονική κάποιων συγκεκριμένων ομότιμων δικτύων και ειδικότερα των Napster, Gnutella, FastTrack, Freenet, KaZaA, BitTorrent, Skype, Joost και SopCast. Τέλος, αναλύονται τα συμπεράσματα της μελέτης αυτής και γίνονται προτάσεις για μελλοντική έρευνα.

Abstract

The objective of this essay is the study of the networks for Peer-to-Peer applications. This is made possible through the distinction of their classification, in other words those which are structural, loosely structured and non structural, centralized, hybrid or decentralized and those which are classified or not. Furthermore, for the correct study of peer networks, of their advantages and disadvantages, it is required the study of the criteria of evaluation of networks, that is to say the efficiency, the reliability, the security, the upgrade and the cost. In the second part of the essay it is studied the architecture of some particular peer networks and specially the Napster, the Gnutella, the FastTrack, the Freenet, the KaZaA the KaZaA, the BitTorrent, the Skype, the Joost and the SopCast. Finally, the conclusions of this study are analyzed and proposals are made for future research.

Παρουσίαση Θέματος

Περίπου 10 χρόνια αφού το World Wide Web έγινε απαραίτητο για την χρήση του διαδικτύου εμφανίστηκαν τα ομότιμα δίκτυα. Τα Ομότιμα Δίκτυα (P2P networks) είναι ευρέως γνωστά διανεμημένα συστήματα όπου κάθε σύνδεσμος μπορεί να αντιπροσωπεύει τόσο τον πελάτη όσο και τον διακομιστή. Αυτά τα δίκτυα χρησιμοποιούνται για να διαμοιράζονται μεγάλες ποσότητες δεδομένων (<http://manuals.kerio.com/kwfag/en/glossary.html>). Τα ομότιμα δίκτυα χωρίζονται σε Voice over P2P (VoP2P), P2P εφαρμογές file sharing και P2PTV, που είναι ένας συνδυασμός των 2 προηγούμενων με την προσθήκη χρήσης βίντεο. Το μεγαλύτερο θετικό τους είναι ότι τα περισσότερα τους είναι δωρεάν για τον χρήστη και έτσι μπορεί να κάνει την εργασία που θέλει χωρίς χρηματικό κόστος.

Από την άλλη όμως αυτό κρύβει τον κίνδυνο της καταπάτησης των πνευματικών δικαιωμάτων, πράγμα που έχει οικονομικές επεκτάσεις. Παρότι αρχικά, σύμφωνα με την νομοθεσία, τα πνευματικά δικαιώματα προστατεύονταν από την αντιγραφή, τώρα προστατεύονται ακόμα και από τις παράγωγες εργασίες. Δεν υπάρχει αμφιβολία ότι η ψηφιακή τεχνολογία απειλεί τη παραδοσιακή θεωρία της θεμιτής χρήσης ή τους περιορισμούς και τις εξαιρέσεις του δικαιώματος πνευματικής ιδιοκτησίας. Χωρίς την τεχνολογία, εάν κάποιος θελήσει να πάρει ένα προστατευόμενο έργο για μελέτη και έρευνα, μπορεί δίκαια να το χρησιμοποιήσει χωρίς άδεια και δεν χρειάζεται να καταβάλει κάποια αμοιβή στον ιδιοκτήτη του πνευματικού δικαιώματος, αλλά με τη τεχνολογία, πρέπει νομίμως να πάρει τα πνευματικά δικαιώματα του έργου πριν από τη χρήση του.

Αυτό σημαίνει ότι ο χρήστης πρέπει να φέρει μεγαλύτερη νομική ευθύνη για να επιδιώξει τον ίδιο σκοπό, και το δικαίωμα της δίκαιης χρήσης που ανήκει στο χρήστη έχει μερικώς καταπατηθεί. Αυτό είναι χειρότερο για κάποια έργα του δημόσιου τομέα, τα οποία εξαιτίας κάποιων τεχνολογικών μέτρων δεν μπορούν να χρησιμοποιηθούν από απλούς πολίτες. Έτσι μαζί με την ταχεία ανάπτυξη της ψηφιακής τεχνολογίας θα υπάρξουν περισσότερες προκλήσεις σε ολόκληρο το νομικό σύστημα. Είναι αναγκαίο να συνεργαστούν τα κατάλληλα τεχνολογικά μέτρα προστασίας με τα νέα μοντέλα παραχώρησης αδειών και άλλων ορθολογικών κανονισμών για να πιέσουν τη νομική εξέλιξη της τεχνολογίας P2P διαμοιρασμού αρχείων.

Ο χρήστης κατεβάζει το P2P σύστημα από το διαδίκτυο και το εγκαθιστά στον υπολογιστή του. Όταν εκτελείται η εφαρμογή, προσπαθεί να συνδεθεί μέσω του διαδικτύου με συγκεκριμένους hosts που είναι συνδεδεμένοι με το software για να μπορέσει να γίνει μετάδοση. Από αυτό το σημείο και μετά αρχίζει η χρήση των δικτύων των συστημάτων P2P (Chuanfu Chen, Congjing Ran(2007)).

Ταξινόμηση

Τα P2P δίκτυα ταξινομούνται ανάλογα με την προέλευση των δεδομένων και του δικτύου σε αδόμητα (unstructured), χαλαρά δομημένα (loosely structured) και αρκετά δομημένα (highly structured) (Li & Wu, 2004):

- Τα αδόμητα δεν ακολουθούν κανέναν κανόνα σχετικά με τον τόπο που τα δεδομένα αποθηκεύονται, ενώ η τοπολογία του δικτύου είναι αυθαίρετη. Τέτοιου είδους δίκτυο χρησιμοποιείται από το Gnutella.
- Τα χαλαρά δομημένα δίκτυα έχουν μη καθορισμένη περιοχή δεδομένων και αρχιτεκτονική δικτύου. Παράδειγμα χαλαρά δομημένου δικτύου είναι το Freenet.
- Τέλος, στα αρκετά δομημένα δίκτυα τόσο η αποθήκευση των δεδομένων όσο και η τοπολογία του δικτύου είναι καλώς ορισμένα. Όπως το Chord.

Ακόμα, τα δίκτυα P2P μπορούν να ταξινομηθούν με βάση τον αριθμό των κεντρικών διευθύνσεων στις τοποθεσίες εγγράφων σε:

- Κεντροποιημένα (centralized), διατηρούν ένα κεντρικό ευρετήριο δεδομένων σε μία συγκεκριμένη τοποθεσία, π.χ. Napster
- Υβριδικά (hybrid), διατηρούν παραπάνω από ένα μεγάλο ομότιμο ευρετήριο δεδομένων, π.χ. Kazaa
- Διανεμημένα (decentralized), δεν διατηρούν τα δεδομένα σε κεντρικό ευρετήριο, π.χ. Chord.

Τέλος, τα P2P δίκτυα μπορούν να ταξινομηθούν σε ιεραρχημένα και μη (hierarchical and nonhierarchical) ανάλογα με το αν η συνολική τους δομή είναι ιεραρχημένη ή όχι. Είναι σύνηθες τα διανεμημένα συστήματα να είναι μη ιεραρχημένα, ενώ τα υβριδικά και τα περισσότερα κεντροποιημένα συστήματα έχουν συνήθως κάποιο βαθμό ιεράρχησης. Τα ιεραρχημένα συστήματα παρέχουν αυξημένη αποτελεσματικότητα, είναι εύκολα στη διερεύνηση και υψηλής αποτελεσματικότητας δρομολόγηση. Από την άλλη μεριά, συστήματα χωρίς ιεράρχηση προσφέρουν φορτωτική ισοροπία (load-balance) και αυξημένη αντοχή (Jialie Shen, John Sheperd, Bin Cui & Ling Liu (2008), p.192).

Απόδοση

Απόδοση ενός δικτύου είναι η συνολική αποτελεσματικότητα λειτουργίας ενός δικτύου. Εξαρτάται κυρίως από:

- Αριθμό χρηστών. Αν και ο μεγάλος αριθμός χρηστών δημιουργεί πρόβλημα στην ταχύτητα του δικτύου, συγκριτικά με τα Client/Server δίκτυα ο αντίκτυπος των χρηστών στις ώρες αιχμής είναι πολύ μικρότερος. Τα P2P δίκτυα είναι τα κυρίαρχα όσον αφορά το εύρος ζώνης χρήσης.
- Δυνατότητα μέσου μεταφοράς
- Υλικό- Λογισμικό που χρησιμοποιείται

(Kolbe, H.J., Kettig, O., Golic, E (2009)).

Αξιοπιστία

Ο βαθμός της αξιοπιστίας ενός δικτύου P2P εξαρτάται από τη δυνατότητα του να ανιχνεύσει σύνδεση και να αφήσει γεγονότα από άλλους peers, καθώς και από την ιδιότητα του να επιλέξει νέες εισόδους για την κατάσταση δρομολόγησης του. Οι δύο μέθοδοι για την επικάλυψη της αξιοπιστίας είναι ο ενεργός (active) και ο ευκαιριακός (opportunistic):

- Στην ενεργή διατήρηση, ένα peer διαχειρίζεται την αποτυχία ή εγκατάλειψη ενός γείτονα του στέλνοντας αντίγραφο του νέου γείτονα σε όλους τους άλλους peers του δικτύου. Αυτό είναι χρήσιμο για τα μικρά δίκτυα, γιατί τα μεγάλα μπορούν να καταρρεύσουν εάν γίνουν αρκετά λάθη στην αναγνώριση των γειτονικών ως αποτυχημένων peers.
- Στην ευκαιριακή διατήρηση, ένας peer περιοδικά μοιράζεται τους γείτονες του με τα υπόλοιπα μέλη του δικτύου. Το αρνητικό αυτής της μεθόδου είναι ότι κάποιοι peers που έχουν φύγει από το δίκτυο συνεχίζουν να θεωρούνται κομμάτια του για κάποιο χρονικό διάστημα. Έτσι, η ευκαιριακή διατήρηση αντιμετωπίζεται καλύτερα για δίκτυα με πολλούς γειτονικούς peers και μεγάλο ρυθμό μεταφοράς δεδομένων.

(John F. Buford, Heather Yu, Eng Keong Lua (2009), p.109-110).

Ασφάλεια

Τα συστήματα στο διαδίκτυο εξελίχθηκαν από πελάτη/διακομιστή σε P2P και έτσι αυξάνεται και η επικινδυνότητα του διαδικτύου στο θέμα ασφάλειας εξαιτίας της άναρχης δομής των δικτύων P2P, όπως στην αποκέντρωση, στην αυτονομία και στη δυναμικότητα τους. Επομένως, υπάρχει η πιθανότητα ο χρήστης να βρει κάλπικα αρχεία, κακής ποιότητας, ή κάποιον ιό ή Trojan με το όνομα του αρχείου που αναζητά ο χρήστης (Xiaowen Chu, Xiaowei Chen, Kaiyong Zhao and Jiangechuan Liu (2010)).

Τρόποι προστασίας:

- Κρυπτογράφηση (cryptographic solutions)
- Αντίμετρα, όπως εφεδρεία αρχείων, φιλτράρισμα, αντιδραστικός εντοπισμός. (DoS countermeasures)
- Ασφαλείς δρομολογήσεις σε δομημένα P2P (secure routing in structured P2P)
- Ασφαλής εισαγωγή των κωδικών πρόσβασης (secure nodeId assignment)
- Ασφαλής δρομολόγηση ανανέωσης (secure routing table maintenance)
- Ασφαλής προώθηση μηνυμάτων (secure message forwarding)
- Εντιμότητα στο μοίρασμα πηγών (fairness in resource sharing)

(John F. Buford, Heather Yu, Eng Keong Lua (2009), p.328-334).

Έτσι, τα περισσότερα δίκτυα P2P έχουν πλέον τα δικά τους συστήματα για την προστασία τους, αλλά και οι χρήστες μπορούν να εγκαταστήσουν στον υπολογιστή τους προγράμματα που να τους προστατεύουν ακόμα περισσότερο.

Αναβαθμισιμότητα

Αναβαθμισιμότητα είναι η δυνατότητα του δικτύου να ανταπεξέλθει σε νέες επιχειρησιακές ανάγκες. Κάτι τέτοιο μπορεί να υπολογιστεί όπως φαίνεται στον παρακάτω πίνακα.

		<i>Ασφάλεια/Έλεγχος</i>	
		Χαμηλό	Υψηλό
<i>Κόστος Ιδιοκτησίας/ Αναβαθμισιμότητα</i>	Υψηλό	<i>Αγνό (Pure) P2P</i>	<i>Κεντροποιημένα (Centralized) P2P</i>
	Χαμηλό		<i>Client- Server</i>

(Jialie Shen, John Sheperd, Bin Cui & Ling Liu (2008), p.182).

Κόστος

Το κόστος χρησιμοποίησης της P2P εφαρμογής για τον χρήστη είναι η ανταλλαγή του υπερβάλλοντα υπολογιστικού χώρου και των πηγών δικτύου για κάτι διαφορετικό με αξία για τον χρήστη, όπως πρόσβαση σε άλλες πηγές, υπηρεσίες ή συμμετοχή σ' ένα κοινωνικό δίκτυο. Σε αυτό το κόστος πρέπει να προστεθεί και το αντίτιμο που πληρώνουν οι πελάτες για να έχουν πρόσβαση στο δίκτυο αλλά και στη συγκεκριμένη εφαρμογή, εάν είναι συνδρομητική.

Το κόστος για την κατασκευή της εφαρμογής P2P εξαρτάται από το πιθανό μέγεθος της βάσης των πελατών, τα όρια εισόδου και τα επίπεδα δυνατότητας εξέλιξης (John F. Buford, Heather Yu, Eng Keong Lua (2009), p.14-15).

Εφαρμογές P2P

Παρακάτω μελετώνται κάποιες περιπτώσεις P2P συστημάτων. Πρώτα αναφέρονται τα file-sharing δηλαδή το Napster, το Gnutella, το FastTrack, το FreeNet, το KaZaA και το BitTorrent, μετά το Skype που είναι VoP2P, και τέλος, το Joost και το SopCast που είναι P2PTV.

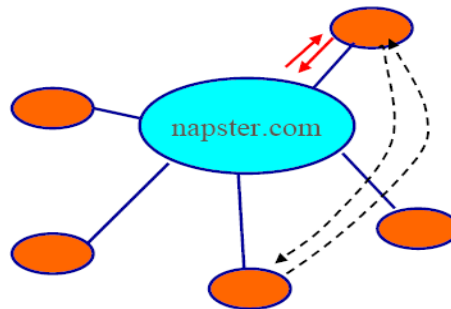
Napster

Το Napster ήταν η πρώτη εφαρμογή δικτύου P2P. Πρωτοεφαρμόστηκε το 1999 από τον Shawn Fanning και ήταν δυνατό να διαμοιράζονται μόνο αρχεία μορφής MP3. Είναι κεντροποιημένο δίκτυο, όπου η αναζήτηση γίνεται με λέξεις κλειδιά, χρησιμοποιώντας ένα αδόμητο μηχανισμό. Έτσι, έχει το πλεονέκτημα της πολύ εύκολης και αποτελεσματικής αναζήτησης.

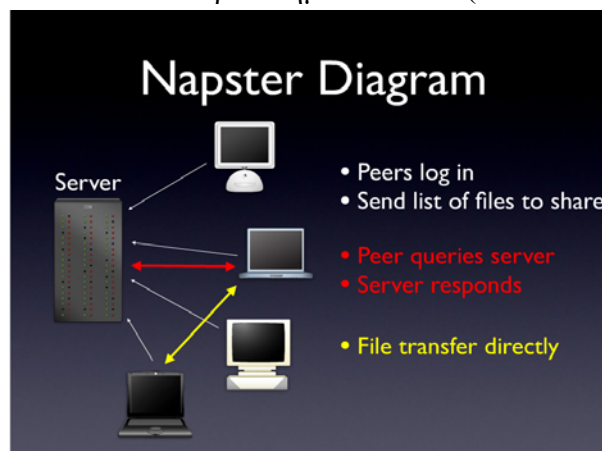
Ο server συλλέγει και διανέμει αρχεία, παρέχει δωμάτια επικοινωνίας και ανεξάρτητη προοπτική μοιράσματος αρχείων. Οι χρήστες δεν μπορούν να δώσουν ψεύτικο IP. Επειδή είναι κεντροποιημένο δίκτυο, το κεντρικό δίκτυο γνωρίζει σχεδόν τα πάντα, που σημαίνει πως μπορεί να ανιχνεύσει σχεδόν όλα τα ελαττωματικά αρχεία που μοιράζονται, και έτσι είναι θεωρητικά και πιο ασφαλές.

Τα δυνατά του σημεία είναι ότι είναι αρκετά εύκολο στην χρήση, υπάρχει μεγάλη διαθεσιμότητα και είναι αρκετά αξιόπιστο.

Napster Topology



Η παραπάνω εικόνα δείχνει την τοπολογία του Napster και έτσι γίνεται αντιληπτό οπτικά ότι είναι ένα κεντροποιημένο δίκτυο (Steven M. Bellovin (2001)).



(Uwe Schmidt (2007))

Το μειονέκτημα του Napster είναι το κόστος του, το οποίο είναι 50\$ τον χρόνο ή 96\$ αν το θέλει ο χρήστης και για το κινητό του. Σε μηνιαία συνδρομή είναι 5\$ για υπολογιστή και άλλα 5\$ αν το θέλει και σε κινητό. (www.napster.com)

Gnutella

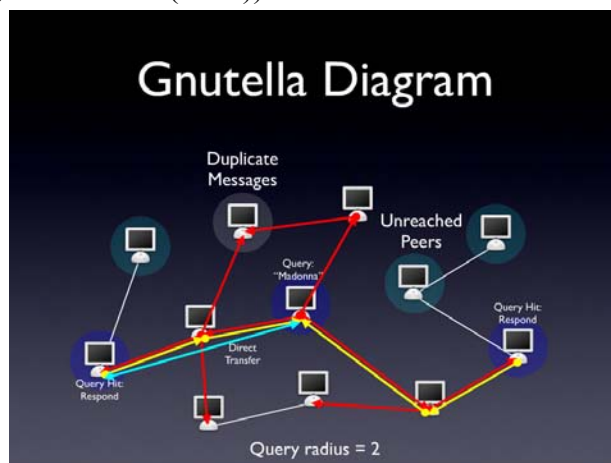
Το Gnutella ήταν το πρώτο ολοκληρωτικά δωρεάν P2P σύστημα διακίνησης αρχείων και η εξέλιξη του Napster. Είναι ένα αδόμητο, δυναμικό δίκτυο, του οποίου η τοπολογία αλλάζει όταν ο χρήστης συνδέεται στο δίκτυο και χρησιμοποιεί αποκεντρωτικούς αλγόριθμους αναζήτησης. Στο Gnutella η αναζήτηση γίνεται μέσω πλημμύρας (flooding). Πλέον το Gnutella έχει υιοθετήσει μία αρχιτεκτονική superpeer σύμφωνα με τη οποία οι peers μεγάλης χωρητικότητας είναι superpeers και όλες οι ενέργειες δρομολογούνται, δια της χρησιμοποίησης ενός μηχανισμού πλημμύρας μεταξύ των superpeers. Το Gnutella χρησιμοποιεί είτε πρωτόκολλο TCP είτε UDP (Yatin Chawathe, Sylvia Ratnasamy, Lee Breslau, Lee Breslau, Nick Lanham, Scott Shenker(2001)).

Για την ασφάλεια των χρηστών του Gnutella οι διακομιστές κρατάνε πληροφορίες για τους χρήστες με κακή φήμη, δηλαδή αυτούς που διαδίδουν Trojans και ιούς.

Επιμερισμός της φήμης βασίζεται σε ένα διανεμημένο αλγόριθμο δημοσκοπήσεων με τον οποίο οι αιτούντες των πόρων μπορούν να εκτιμήσουν την αξιοπιστία των πάροχων με προοπτική πριν ξεκινήσει «το κατέβασμα».

Αυτή η προσέγγιση συμπληρώνει τα υπάρχοντα P2P πρωτόκολλα και έχει μια μικρή επίπτωση στις τρέχουσες υλοποιήσεις. Ακόμα περισσότερο κρατάει το τρέχων επίπεδο ανωνυμίας των αιτούντων και πάροχων καθώς και αυτό των ομάδων που μοιράζονται τη φήμη για την άποψη για τους άλλους (Ernesto Damiani, Sabrina De Capitani di Vimercati, Stefano Paraboschi, Pierangela Samarati (2003)).

Παρόλα αυτά δεν υπάρχει αρκετά καλή ασφάλεια καθώς υπάρχουν συχνά φαινόμενα πλημμύρας, μη έγκυρου περιεχομένου, διάδοσης ιών και λανθασμένη απάντηση στις ερωτήσεις/ μη εξυπηρέτηση (Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005)).



Η παραπάνω εικόνα δείχνει πως κάθε κόμβος επικοινωνεί και μοιράζεται αρχεία με τους γειτονικούς του κόμβους, δηλαδή δείχνει πως είναι αδόμητο και διανεμημένο δίκτυο (Uwe Schmidt(2007)).

FastTrack

Το FastTrack είναι άλλο ένα αδόμητο P2P που εμφανίστηκε σχεδόν μαζί με το Gnutella και χρησιμοποιούνταν από clients που μοιράζονταν αρχεία όπως Grokster και Imesh. Είναι ένα ιδιωτικό σύστημα που χρησιμοποιεί κωδικοποιημένο πρωτόκολλο. Μπορεί να χρησιμοποιηθεί δωρεάν από τους χρήστες. Το FastTrack που είναι υβριδικό δίκτυο, χρησιμοποιεί αρχιτεκτονική με superpeers στην οποία οι peers με μεγάλη χωρητικότητα είναι μεγάλοι κόμβοι και αυτά με μικρή χωρητικότητα είναι κανονικοί κόμβοι. Σε ένα σύνολο 3.000.000, οι μεγάλοι κόμβοι κυμαίνονται από 25.000 έως 40.000. Κάθε απλός κόμβος συνδέεται με έναν μεγάλο. Ο μεγάλος κόμβος παρέχει στους απλούς μία λίστα με τους υπόλοιπους μεγάλους που ο απλός μπορεί να συνδεθεί. Όταν ο απλός κόμβος κάνει μια ερώτηση στον μεγάλο και λαμβάνει τις απαντήσεις, αποσυνδέεται από τον εκάστοτε μεγάλο κόμβο και συνδέεται με κάποιον άλλον της λίστας. Με την επανασύνδεση λαμβάνει νέα λίστα με τους μεγάλους κόμβους που μπορεί να συνδεθεί.

Ένας απλός κόμβος διατηρεί περίπου 40 με 50 συνδέσεις με άλλους μεγάλους κόμβους. Ενώ, ένας μεγάλος κόμβος με σύνδεση μεγάλου εύρος ζώνης διατηρεί σύνδεση με περίπου 50-80 απλούς κόμβους.

Οι συνδέσεις μεγάλου με απλό κόμβο και μεγάλο με μεγάλο φαίνεται να έχουν πολλαπλούς σκοπούς, συμπεριλαμβάνοντας τη διανομή φορτίων μεταξύ των μεγάλων κόμβων, βελτιώνοντας την τοπικότητα των συνδέσεων και ανακατευόντας τις συνδέσεις από τους απλούς κόμβους για να αυξηθεί η κάλυψη στις μεγάλες αναζητήσεις πάνω στην επικάλυψη. Μεγάλη εντροπία σύνδεσης κάνει τον εντοπισμό των μεταφορών μέσω peers πιο δύσκολο, μία πιθανή παρακίνηση λαμβάνοντας υπ' όψιν τις δικαστικές διαμάχες με άλλα συστήματα διαμοιρασμού αρχείων (John F. Buford, Heather Yu, Eng Keong Lua (2009), p55).

Αν και υβριδικό δίκτυο όπου μπορεί να υπάρχει έλεγχος μέσω των μεγάλων κόμβων, η ασφάλεια του FastTrack είναι αρκετά ανεπαρκής καθώς απειλείται εύκολα από πλημμύρες, κακό ή ψεύτικο περιεχόμενο και ιούς. Το Spyware παρακολουθεί τις δραστηριότητες των Peers στο παρασκήνιο (Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005)).

Freenet

Το Freenet δημιουργήθηκε το 1999 από τον Ian Clarke και εκδόθηκε στο κοινό το 2000 ως ένας διανεμημένος και χαλαρά δομημένος P2P μηχανισμός διαμοιρασμού αρχείων με ασφάλεια και ανωνυμία. Παρέχει ραδιοφωνικές υπηρεσίες, υπηρεσίες φωνητικών συνομιλιών και διάφορα άρθρα όλο το εικοσιτετράωρο. Η χρήση του είναι δωρεάν και αν κάποιος χρήστης επιθυμεί μπορεί να κάνει δωρεά (www.freenet.com).

Τόσο τα αντικείμενα όσο και οι peers έχουν αναγνωριστικά ταυτότητας. Ταυτοποιητές δημιουργούνται με τη χρήση SHA-1 μονόδρομης συνάρτησης κατακερματισμού. Οι peer ταυτοποιητές αποκαλούνται κλειδιά δρομολόγησης. Κάθε peer έχει ορισμένο μέγεθος πίνακα δρομολόγησης που αποθηκεύει τους συνδέσμους προς άλλους peers. Κάθε είσοδος περιέχει το κλειδί δρομολόγησης των peers. Το ελεύθερο δίκτυο χρησιμοποιεί διαδρομές που βασίζονται σε κλειδιά για την εισαγωγή και ανάκτηση των αντικειμένων στο πλέγμα. Οι αιτήσεις διαβιβάζονται στα peers με το πλησιέστερο κλειδί χάραξης. Αν ένα αίτημα κατά μήκος του άλματος αποτύχει, ο peer θα δοκιμάσει το επόμενο κοντινότερο κλειδί στον πίνακα δρομολόγησης. Ο αλγόριθμος δρομολόγησης είναι σαν απότομη άνοδος λόφου με διάυλο οπισθοδρόμησης έως ότου το αίτημα TTL υπερβεί. Συνεπώς, εξαρτώμενο από την οργάνωση των συνδέσμων και τη διαθεσιμότητα των peers, είναι πιθανό ότι οι αιτήσεις μπορεί να αποτύχουν. Το ελεύθερο διαδίκτυο αντιδρά σ' αυτό με απόκρυψη αντικειμένων κατά μήκος του δρόμου επιστροφής της αναζήτησης και εισαγωγής αιτήσεων. Ένα αντικείμενο αποθηκεύεται σε έναν peer μέχρις ότου δεν υπάρχει πια διαθέσιμος χώρος και είναι το πιο πρόσφατο χρησιμοποιημένο αντικείμενο σε αυτόν τον peer (John F. Buford, Heather Yu, Eng Keong Lua (2009), p56-60).

Όσον αφορά την ασφάλεια είναι αρκετά χαμηλή γιατί υποφέρει από επιθέσεις ιών (Trojans και man-in-middle) (Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005)).

Σε αντίθεση με τα υπόλοιπα P2P, το Freenet δεν μεταδίδει απλά δεδομένα, αλλά και τα αποθηκεύει. Έτσι κάθε κόμβος ξοδεύει αρκετά μεγάλη ποσότητα μνήμης. Τα αρχεία χωρίζονται σε μικρά κομμάτια και μπορεί ένα αρχείο να έχει κομμάτια

στοιβαγμένα σε διαφορετικούς κόμβους. Αυτά κάνουν το Freenet να κρατά περιττά αρχεία και να είναι δύσκολο στην χρήση/ αναζήτηση.

Τέλος, το Freenet χρησιμοποιεί ανοικτού τύπου κώδικα (<http://en.wikipedia.org/wiki/Freenet>).

KaZaA

Το KaZaA είναι το πρώτο σύστημα P2P που μοιράζει τραγούδια με νόμιμη έγκριση, δημιουργήθηκε το 2001 από τον Niklas Zennstrom. Συνδυάζει το Napster και το Gnutella. Η χρήση του είναι δωρεάν και αν κάποιος χρήστης επιθυμεί μπορεί να κάνει δωρεά. Το KaZaA χρησιμοποιεί το πρωτόκολλο TCP επειδή χρειάζεται μία απ' άκρο εις άκρο αξιόπιστη ροή byte. Μοιάζει με το Gnutella στην δομή όσον αφορά ότι δεν χρησιμοποιεί έναν συγκεκριμένο server για τον εντοπισμό των αρχείων (αδόμητο), έχει όμως δύο ειδών κόμβους, τους κανονικούς και τους μεγάλους, σε αντίθεση με το Gnutella. Είναι υβριδικό δίκτυο, όπως δηλαδή και το FastTrack, που μοιάζουν πάρα πολύ. Σε αντίθεση με το Napster, το KaZaA δεν τερματίζεται απλά κλείνοντας τον κεντρικό server του συστήματος.

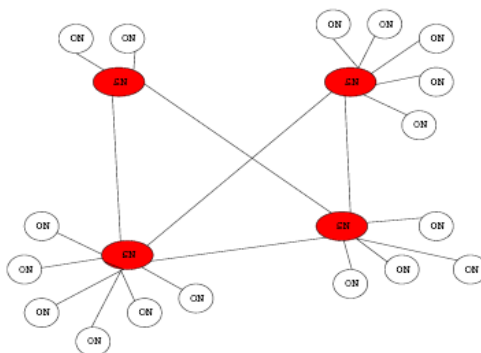


Fig. 1. Supermode and Ordinary nodes in KaZaA network

Έχει ιεραρχική οργάνωση των peers. Χρησιμοποιεί καταναμημένο σχέδιο, προσπαθεί να έχει ισορροπία στην κίνηση των κόμβων και χρησιμοποιεί τοπικότητα σε γειτονικές επιλογές, έτσι ώστε να μειώνεται η καθυστέρηση αντίδρασης. Η τοπολογία του KaZaA είναι ισχυρά δυναμική -ανακατεύει τις συνδέσεις-, δηλαδή αν και οι ταυτόχρονες συνδέσεις ταλαντεύονται σ' ένα κατώτατο όριο, οι ανεξάρτητες αλλάζουν συχνά (Jian Liang, Rakesh Kuma, Keith W. Ross (2005)).

Για να μπορούν τα αρχεία να μοιράζονται πρέπει να μπορούν να παρακάμπτουν τα τείχη προστασίας και το NAT, τα οποία και είναι κυρίαρχα στο διαδίκτυο. Έτσι το KaZaA χρησιμοποιεί δυναμικές εισόδους σε συνδυασμό με την ιεραρχημένη της δομή για να αποφεύγει τα τείχη προστασίας και χρησιμοποιεί αντιστροφή σύνδεσης για να επιτρέπει τους peer με NAT να μοιράζονται αρχεία (Jian Liang, Rakesh Kuma, Keith W. Ross (2004), The KaZaA overlay: a measurement Study). Η ασφάλεια του KaZaA, παρόλα αυτά, είναι αρκετά ανεπαρκής καθώς απειλείται εύκολα από πλημμύρες, κακό ή ψεύτικο περιεχόμενο και ιούς. Το Spyware παρακολουθεί τις δραστηριότητες των Peers στο παρασκήνιο (Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005)).

BitTorrent

Το BitTorrent είναι ένα πρωτόκολλο σχεδιασμένο για μοίρασμα μεγάλων αρχείων σε κομμάτια χρησιμοποιώντας ένα αμοιβαίο μοίρασμα των κομματιών μεταξύ των peers (swarm). Η χρήση του είναι δωρεάν και είναι δομημένο δίκτυο. Δεν χρησιμοποιεί μηχανή αναζήτησης, την δουλειά αυτή την κάνουν κάποιες ιστοσελίδες όπως supernova.org ή btjunkie.org. Στην μεταφορά των δεδομένων χρησιμοποιεί την τεχνική pipeline προκειμένου να έχει καλύτερα αποτελέσματα (J.A.Pouwelse, P.Garbacki, D.H.J. Epema, H.J. Sips (2007)).

Το BitTorrent χρησιμοποιεί το πρωτόκολλο TCP επειδή είναι απαραίτητη η αξιοπιστία του και η αρχιτεκτονική του μπορεί να αναλυθεί σε πέντε βασικά συστατικά:

- ένα αρχείο που περιέχει όλες τις απαραίτητες πληροφορίες για την λειτουργικότητα του (metainfo file),
- έναν server που βοηθάει την διαχείριση του (tracker),
- χρήστες που ανταλλάζουν δεδομένα μέσω του BitTorrent (peers),
- τα δεδομένα που μοιράζονται (data) και
- το πρόγραμμα που χρησιμοποιεί ο χρήστης προκειμένου να χρησιμοποιήσει το BitTorrent(client).

Όσον αφορά την ασφάλεια, κινείται σε μέτρια επίπεδα

- κάποιος δεν θέλει να υπάρχει διαθέσιμο κάποιο αρχείο και έτσι δέχεται αυτός όλα τα συγκεκριμένα αρχεία τερματίζοντας έτσι το εύρος ζώνης ανεβάσματος του (Pollution),
- άρνησης διανομής της υπηρεσίας (DDOS) και βλάβες στην μεταφορά δεδομένων (bandwidth shaping) (Abhishek Sharma(2007)).
- Όμως, είναι κεντροποιημένο δίκτυο άρα υπάρχει περισσότερος έλεγχος και έτσι γίνεται δυσκολότερο να υπάρξουν ψεύτικες IP διευθύνσεις ή αριθμοί διόδου (Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005)).

Skype

Το Skype είναι μια εφαρμογή P2P που δημιουργήθηκε το 2003 στο Λουξεμβούργο, όπου άτομα μπορούν να συνομιλούν μεταξύ τους γραπτά, με ήχο ή με βίντεο αλλά και να ανταλλάζουν αρχεία. Δημιουργήθηκε από την ίδια ομάδα που δημιούργησε και το KaZaA, με το οποίο έχει και παρόμοια αρχιτεκτονική.

Στο Skype ελέγχονται από έναν κεντρικό server οι συνδέσεις και οι λογαριασμοί και χρησιμοποιεί κόμβους και μεγάλους κόμβους, έχει δηλαδή ιεραρχημένη αρχιτεκτονική ως υβριδικό δίκτυο. Ο πηγαίος του κώδικας είναι κρυφός για τους χρήστες (David Tacconi (2008)).

Μετά την σύνδεση όλες οι επικοινωνίες γίνονται χωρίς να επικοινωνούν με τον κεντρικό server. Αυτό που γίνεται είναι κάποιοι κόμβοι αρκετά δυνατοί να προωθούνται σε μεγάλους κόμβους που δρουν σαν δρομολογητές μεταξύ των απλών χρηστών. Για να είναι λειτουργικό αυτό το σύστημα πρέπει οι μεγάλοι κόμβοι να γνωρίζουν την πλειοψηφία των υπόλοιπων. Οι μεγάλοι κόμβοι παρέχουν λίστα με

τους συνδεδεμένους χρήστες στους υπόλοιπους χρήστες, αλλά παίζουν και σπουδαίο ρόλο στις μεθόδους διαπέρασης του τείχους προστασίας του Skype (Pascal Wibmann (2008)).

Η χρήση του είναι δωρεάν για την απλή χρήση του σε επικοινωνία υπολογιστή με υπολογιστή, όμως εάν ο χρήστης θέλει να μπορεί να καλεί σε κινητά νούμερα πρέπει να πληρώνει 6,89€ τον μήνα για κλήσεις στην Ευρώπη ή 11,49€ ανά μήνα εάν θέλει να επικοινωνεί με ολόκληρο τον κόσμο. Για λόγους ασφαλείας οι εργασίες στο Skype -όπως επικοινωνία μεταξύ χρηστών- γίνονται με κρυπτογράφηση χρησιμοποιώντας ισχυρούς κρυπτογραφημένους αλγόριθμους. Σε μερικές περιπτώσεις, η επικοινωνία μπορεί να δρομολογείται μέσω άλλων χρηστών στο P2P δίκτυο (<https://support.skype.com/en/faq/FA143/Is-Skype-secure>).

Η αναζήτηση στο Skype είναι αρκετά εύκολη και χρησιμοποιεί την παγκόσμια τεχνολογία καταλόγου (Global Index Technology). Τα αποτελέσματα της αναζήτησης αποθηκεύονται σε κόμβους.

Για τις κλήσεις χρησιμοποιείται το πρωτόκολλο TCP, ενώ για την συνομιλία χρησιμοποιείται το πρωτόκολλο UDP επειδή δεν πειράζει ιδιαίτερα το αποτέλεσμα μία μικρή απώλεια δεδομένων, σε αντίθεση με το πρωτόκολλο TCP όπου και μία πιθανή καθυστέρηση θα ήταν καταστροφική.

Για την παράκαμψη του NAT χρησιμοποιεί STUN και TURN πρωτόκολλα (Luca De Cicco, Saverio Mascolo, Vittorio Palmisano (2008)).

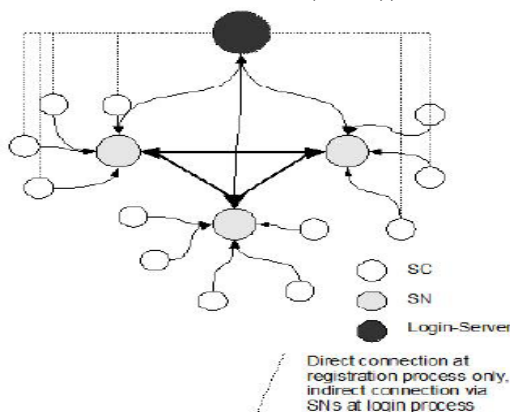


Figure 1: Scheme of the Skype network of 15 SCs, three of them promoted to supernodes

(Pascal Wibmann (2008), Security review of the Skype Network)

Joost

Οι δημιουργοί του KaZaA και του Skype δημιούργησαν και το Joost. Χρησιμοποιεί τεχνολογίες προβολής video και προσπαθεί να ενώσει την τηλεόραση με το διαδίκτυο με νόμιμα μέσα. Είναι μία υπηρεσία Internet protocol-based television (IPTV).

Τα προτερήματα του Joost:

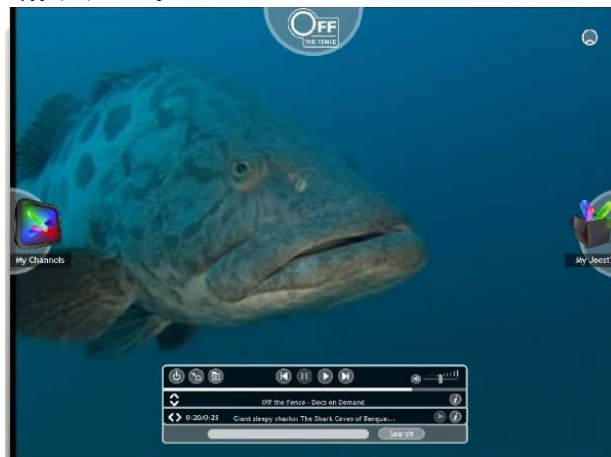
- Αποτρέπει την εικόνα να παγώνει
- Κατηγοριοποιεί τα περιεχόμενα
- Ελεύθερα προσβάσιμο
- Επαγγελματική εμφάνιση

- Μηχανή αναζήτησης
- Συμβατό με iPod και iPhone
- Έχει υπογράψει συμβάσεις με αρκετές εταιρίες προκειμένου να διανέμονται τα media νόμιμα.
- Χρησιμοποιείται για να είναι ορατό το περιεχόμενο και να αλληλεπιδρά με άλλους χρήστες ταυτόχρονα
- Βλέπεις τι βλέπουν οι φίλοι σου
- Μπορούν να δημιουργηθούν ομάδες βάση των ενδιαφερόντων.

Χρησιμοποιεί κρυπτογράφηση σε επίπεδο byte. Δεν εγγυάται ασφάλεια για τα προσωπικά δεδομένα του χρήστη, αφενός γιατί μοιράζεται τα δεδομένα του για στατιστικούς λόγους ή διαφήμιση και αφετέρου γιατί υπάρχει φόβος πως θα μπορούσε κάποιος κακόβουλος να υποκλέψει τα δεδομένα του χρήστη, αλλά και τις επιθέσεις ιών και trojans. Όμως η επικοινωνία μεταξύ Joost servers και peers γίνεται μέσω κρυπτογραφημένων μηνυμάτων, οπότε και τα δεδομένα αυτά είναι δύσκολο να προσβληθούν από κάποιον τρίτο (<http://www.joost.com/about/joost/>).

Εκτός από το θέμα της ασφάλειας, το joost έχει το μειονέκτημα ότι αν και φορτώνει πολύ αποδοτικά ισορροπημένες υπολογιστικές πηγές, το πετυχαίνει έχοντας μεγάλες επιπτώσεις στην αποδοτικότητα του δικτύου. Ακόμα έχει μικρή προσαρμογή στο ρυθμό πρόσβασης (Udo R. Krieger, Ronny Schwebinger (2008)).

Το Joost, αρχικά, ήταν ένα κεντροποιημένο δίκτυο. Όμως όσο αυξάνονταν οι χρήστες του γινόταν περισσότερο αποκεντρωμένο, με πιο διανεμημένη αρχιτεκτονική. Χρησιμοποιεί τόσο απλούς κόμβους όσο και μεγάλους κόμβους. Τώρα είναι σε ένα υβριδικό στάδιο. Όσον αφορά το τι πρωτόκολλο χρησιμοποιεί, η απάντηση είναι πως χρησιμοποιεί UDP ή TCP ανάλογα με την περίπτωση (UDP για βίντεο, TCP για έλεγχο) (Yensy James Hall, Patrick Piemonte, Matt Weyant (2007)).



SopCast

Το SopCast είναι μία ελεύθερη P2PTV εφαρμογή και έχει πάρα πολλές ομοιότητες όσον αφορά την δομή του με το Joost. Τρέχει προγράμματα που προβάλλονται στην τηλεόραση με ταχύτητα αναμετάδοσης συνήθως από 250 έως 400 Kbps που όμως κάποιες φορές φτάνει και στα 800Kbps. Ακόμα μέσω του SopCast κάποιος μπορεί να δημιουργήσει το δικό του κανάλι.

Χρησιμοποιεί κατά συντριπτική πλειοψηφία το πρωτόκολλο UDP, καθώς χρειάζεται ταχύτητα στις προβολές, και ελάχιστα το TCP. Από τις ζωντανές μεταδόσεις είναι κατά μισό λεπτό με σαράντα πέντε δευτερόλεπτα περίπου πιο αργό. Είναι υβριδικό δίκτυο, δηλαδή χρησιμοποιεί τόσο μεγάλους όσο και κανονικούς κόμβους, και δεν λαμβάνει υπ' όψιν του τη γεωγραφική τοποθεσία των peers κατά την διάρκεια της αναμετάδοσης.

Ο μέσος ρυθμός λήψης βίντεο είναι σχεδόν ίδιος σε κάθε peer. Η ταχύτητα ανεβάσματος είναι συνήθως σταθερή για έναν peer, όμως ποικίλει μεταξύ διαφορετικών peers.

Τα μειονεκτήματά του είναι ότι υποφέρει συχνά από καθυστερήσεις των peers γιατί κάποιοι peers που παρακολουθούν το ίδιο κανάλι μπορεί να μην είναι συγχρονισμένοι και το βίντεο και ο ήχος ίσως να μην είναι συγχρονισμένα. Επίσης, στα μειονεκτήματα μπορεί να προστεθεί η καθυστέρηση της εναλλαγής των καναλιών που είναι συνήθως γύρω στα πενήντα δευτερόλεπτα. Τέλος, το συνολικό ποσοστό χασίματος πακέτων είναι υψηλό (Benny Fallica, Yue Lu, Fernando Kuipers, Rob Kooij, and Piet Van Mieghem (2008)).

Όσον αφορά την ασφάλεια στο SopCast, για τον χρήστη που θέλει να δει κάτι δεν τίθεται θέμα ασφάλειας αφού δεν δίνει κάποιο στοιχείο του. Τα δεδομένα όμως αν και προστατεύονται από τους ελέγχους των μεγάλων κόμβων, κρυπτογραφώντας τα μηνύματα, είναι ορισμένες φορές τρωτά στους κακόβουλους χρήστες, όπως φυσικά και όλα τα άλλα P2P συστήματα. Ακόμα το SopCast χρησιμοποιεί ασφάλεια End-to-End, δηλαδή η σύνδεση τερματίζεται αν κριθεί ότι κάτι δεν είναι ασφαλές (www.sopcast.com).

Συμπεράσματα

Διάσταση	Μοντέλο P2P
Κόστος Ιδιοκτησίας	<p>ΧΑΜΗΛΟ: Περισσότερο Οικονομικό</p> <ul style="list-style-type: none"> • Δεν έχει γενικά έξοδα επειδή οι peers αποτελούν το δίκτυο. (O'Reilly,2001) • Τα κεντροποιημένα P2P, έχουν πολύ χαμηλό κόστος υποδομής και διατήρησης. (Rosenblatt, Trippe, & mooney, 2002)
Εξελιξιμότητα	<p>ΥΨΗΛΟ: Έμφατα οργανικά, κλίμακες των χρηστών</p> <ul style="list-style-type: none"> • Κλίμακες που αποφεύγουν την εξάρτηση από το κεντροποιημένο σημείο. (Milojicic et al., 2002) • Τα Π2Π είναι περισσότερο κατάλληλα για μεγάλο αριθμό υπολογιστών στο διαδίκτυο ή κινητών συσκευών. (Minar & Hedlung, 2001)
Επίδοση	<p>ΜΕΤΡΙΑ: Εξαρτάται από το εύρος ζώνης των Peers και τον αριθμό τους.</p> <ul style="list-style-type: none"> • Υψηλή: μείωση των περιττών δια μέσου της αντιγραφής των πληροφοριών σε πολλαπλούς κόμβους. (Kini & Shetty,2001) • Υψηλή: Τα P2P μπορούν να βοηθήσουν στην ελάττωση της συμφόρησης. Περισσότερο αποτελεσματική χρήση των διαδικτυακών πηγών με οριακή εξυπηρέτηση. • Στο επίπεδο ομότιμων δικτύων, τα απλά P2P, όταν εκτελούν λειτουργίες όπως αποστολή, το να λαμβάνουν και να διατηρούν τις επικοινωνίες απαιτούν πολύ κίνηση. • Προσφέροντας κάποιος μοίρασμα αρχείων σε άλλους χρήστες σημαίνει και μοίρασμα εύρους ζώνης και ίσως ελάττωση της δικιάς του ταχύτητας στο διαδίκτυο. (Kwok, Lang & Kar, 2002).
Ασφάλεια των Peer	<p>ΜΕΤΡΙΑ: Τρωτό αναγκάζοντας τους Peers να λειτουργούν ως servers.</p> <ul style="list-style-type: none"> • Τα Peer πρέπει να ανοίξουν αρκετά κομμάτια ή διόδους, που τα κάνει τρωτά σε hackers και επιθέσεις ιών. (Kwok, Lang & Kar, 2002).
Ασφάλεια για τον προμηθευτή του περιεχομένου	<p>ΧΑΜΗΛΗ: Διανεμημένα και Τρωτά</p> <ul style="list-style-type: none"> • Στα απλά P2P ο έλεγχος του που και πως το περιεχόμενο μοιράζεται χάνεται, αλλά όχι στα κεντροποιημένα δίκτυα P2P. (Lesavich, 2002) • Στα απλά P2P οι μηχανισμοί peer ανήκουν σε ιδιώτες αντί για ISP's, έτσι δεν είναι εύκολο να εντοπίσεις ή να ξεκινήσεις δικαστικό αγώνα εναντίον τους. (Lesavich, 2002) • Μικρές πιθανότητες ελέγχου επειδή στα δίκτυα P2P, ο έλεγχος ξεκινάει όταν ο χρήστης συνδέεται στο δίκτυο.
Ποιότητα Εξυπηρέτησης/ Ελέγχου	<p>ΥΨΗΛΗ: Οργανική Εξυπηρέτηση</p> <ul style="list-style-type: none"> • Δυναμική διαθεσιμότητα του περιεχομένου και πληροφόρηση για την ποσότητα των δεδομένων εξαρτάται από τον αριθμό των peers. • Ελεύθερη πλοήγηση, αλλά πιθανές απρόβλεπτες εξελίξεις. • Στα απλά P2P, χαμηλή ποιότητα εξυπηρέτησης.

(Jialie Shen, John Sheperd, Bin Cui & Ling Liu (2008), p.181)

Ακόμα, παρατίθεται ένας πίνακας με τα συμπεράσματα που βγαίνουν για τα συστήματα P2P που αναλύθηκαν παραπάνω.

	<i>Τύπος Δικτύου</i>	<i>Αποτελεσματική Αναζήτηση</i>	<i>Ασφάλεια</i>	<i>Αξιοπιστία</i>	<i>Κόστος</i>
<i>Napster</i>	Κεντροποιημένο (Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005))	Αρκετά εύκολη (Steven M. Bellovin (2001))	Μέτρια (Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005))	Εγγυάται να βρει τα δεδομένα χρησιμοποιώντας λέξεις κλειδιά(Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005)).	50\$/χρόνο ή 5\$/μήνα (www.napster.com).
<i>Gnutella</i>	Διανεμημένο (Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005))	Αρκετά Δύσκολη (Yatin Chawathe, Sylvia Ratnasamy, Lee Breslau, Lee Breslau, Nick Lanham, Scott Shenker(2001))	Χαμηλή (Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005))	Δεν είναι βέβαιο πως θα βρει το ζητούμενο, μεγαλύτερη πιθανότητα για διάσπαση περιεχόμενα(Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005)).	Καθόλου (www.gnutella.com)
<i>FastTrack</i>	Υβριδικό (Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005))	Μέτρια (John F. Buford, Heather Yu, Eng Keong Lua (2009))	Μέτρια (Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005))	Κάποια πιθανότητα να βρει τα ζητούμενα δεδομένα, ακόμα μεγαλύτερη πιθανότητα για διαδεδομένα περιεχόμενα(Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005)).	Καθόλου (www.fastrack.com)
<i>Freenet</i>	Διανεμημένο (John F. Buford, Heather Yu, Eng Keong Lua (2009))	Δύσκολη (John F. Buford, Heather Yu, Eng Keong Lua (2009))	Χαμηλή (Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005)).	Εγγυάται αξιόπιστη επικοινωνία όλο το 24ωρο, και να βρει τα δεδομένα χρησιμοποιώντας λέξεις κλειδιά, μέχρι να φτάσει στο επιτρεπτό όριο (John F. Buford, Heather Yu, Eng Keong Lua (2009)).	Καθόλου (www.freenet.com)
<i>KaZaA</i>	Υβριδικό (Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005))	Εύκολη (Jian Liang, Rakesh Kuma, Keith W. Ross (2005))	Μέτρια (Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005))	Κάποια πιθανότητα να βρει τα ζητούμενα δεδομένα, ακόμα μεγαλύτερη πιθανότητα για διαδεδομένα περιεχόμενα(Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005)).	Καθόλου (www.kazaa.com)
<i>BitTorrent</i>	Διανεμημένο (J.A.Pouwelse, P.Garbacki, D.H.J. Epema, H.J. Sips (2007))	Χρησιμοποιεί άλλες σελίδες (J.A.Pouwelse, P.Garbacki, D.H.J. Epema, H.J. Sips (2007))	Μέτρια (Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005))	Εγγυάται να βρει τα δεδομένα και εγγυάται καλή απόδοση για τα διαδεδομένα περιεχόμενα(Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005)).	Καθόλου (www.bittorrent.com)
<i>Skype</i>	Υβριδικό	Αρκετά εύκολη (Luca)	Καλή (Pascal Wibmann (2008),	Εγγυάται άριστη ποιότητα	Καθόλου/ Για

	(David Tacconi (2008))	De Cicco, Saverio Mascolo, Vittorio Palmisano (2008).	https://support.skype.com/en/faq/FA143/Is-Skype-secure	επικοινωνίας και απόλυτη επιτυχία στην αναζήτηση (Luca De Cicco, Saverio Mascolo, Vittorio Palmisano (2008)).	κλήσεις 6,89€ /μήνα για την Ευρώπη ή 11,49€/μήνα για ολόκληρο τον κόσμο (www.skype.com).
Joost	Υβριδικό (Yensy James Hall, Patrick Piemonte, Matt Weyant (2007))	Αρκετά Εύκολη (http://www.joost.com/about/joost/)	Χαμηλή (http://www.joost.com/about/joost/)	Εγγυάται καλή ποιότητα εικόνας και είναι νόμιμο (http://www.joost.com/about/joost/).	Καθόλου (www.joost.com)
SopCast	Υβριδικό (Benny Fallica, Yue Lu, Fernando Kuipers, Rob Kooij, and Piet Van Mieghem (2008))	Αρκετά Εύκολη (Benny Fallica, Yue Lu, Fernando Kuipers, Rob Kooij, and Piet Van Mieghem (2008))	Καλή (www.sopcast.com)	Εγγυάται καλή ποιότητα εικόνας (Benny Fallica, Yue Lu, Fernando Kuipers, Rob Kooij, and Piet Van Mieghem (2008)).	Καθόλου (www.sopcast.com)

Κατά την διάρκεια της μελέτης για την εργασία αυτή, διαπίστωσα πως θα πρέπει να εισαχθούν περισσότερα μοντέλα παροχής άδειας στην εξουσιοδότηση ενός P2P συστήματος, έτσι ώστε να έχει το σύστημα P2P περισσότερα νομικά εγκεκριμένα αντικείμενα προς μοίρασμα.

Επίσης, διαπίστωσα πως για να προστατευθούν τα πνευματικά δικαιώματα από την πειρατεία στο Διαδίκτυο, θεσπίστηκαν διάφοροι νόμοι που βοηθούν τους δημιουργούς να διατηρούν την διαχείριση τους και οι καταναλωτές να πρέπει να πληρώσουν κάποιο αντίτιμο για να τα χρησιμοποιήσουν. Ακόμα, οι εταιρίες χρησιμοποιούν για την προστασία των πνευματικών δικαιωμάτων τους διάφορες τεχνολογίες.

Τέλος, αν κάποιος που ήθελε να κατασκευάσει το δικό του P2P ρωτούσε την γνώμη μου θα του πρότεινα να το κάνει αρκετά δομημένο ώστε η αποθήκευση των δεδομένων και η τοπολογία του δικτύου να είναι καλώς ορισμένα. Θα του πρότεινα να το κάνει διανεμημένο ώστε να μην εξαρτώνται όλα από ένα κεντρικό Peer, αλλά να υπάρχει έτσι μεγαλύτερη ευελιξία. Όμως, θα του τόνιζα να προσέξει την ασφάλεια και να προσπαθήσει και να σιγουρευτεί πως το σύστημα θα είναι ασφαλές από τους διάφορους κινδύνους όπως hackers, υπερχείλιση, κατεστραμμένα αρχεία κλπ.

Βιβλιογραφία

1. Jialie Shen, John Sheperd, Bin Cui & Ling Liu (2008), Intelligent Music Information Systems(1st ed.), New York: Information Science Reference.
2. John F. Buford, Heather Yu, Eng Keong Lua (2009), P2P Networking and Applications(1st ed.), United States: Morgan Kaufmann
3. Udo R. Krieger, Ronny Schweßinger (2008) , Analysis and Quality Assessment of Peer-To-Peer IPTV Systems, IEEE xplore, Retrieved from <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4559462>
4. Kolbe, H.J., Kettig, O., Golic, E(2009), Monitoring the impact of P2P users on a broadband operator's network, IEEE xplore, Retrieved from http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5188835
5. Chuanfu Chen, Congjing Ran(2007), P2P Copyright Protection: Current States and Future Prospective with Particular on China, IEEE Computer Society, Retrieved from <http://www.computer.org/portal/web/csdl/doi/10.1109/UBICOMM.2007.26>
6. Ernesto Damiani, Sabrina De Capitani di Vimercati , Stefano Paraboschi , Pierangela Samarati (2003), Managing and Sharing Servents' Reputations in P2P Systems, IEEE Computer Society, Retrieved from <http://www.computer.org/portal/web/csdl/doi/10.1109/TKDE.2003.1209003>
7. Mihajlo Jovanovic (2001), Modeling peer-to-peer network topologies through “small-world” models and power laws, CiteSeerX, Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.110...%20-%201k>
8. Yatin Chawathe, Sylvia Ratnasamy, Lee Breslau, Lee Breslau, Nick Lanham, Scott Shenker(2001), Making gnutella-like P2P systems scalable, CiteSeerX, Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.10.... - -1k>
9. Jian Liang, Rakesh Kuma,Keith W. Ross(2005), Understanding KaZaA, CiteSeerX, Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.9.6...%20-%201k>
10. Jian Liang, Rakesh Kuma,Keith W. Ross (2004),The KaZaA overlay: a measurement Study, CiteSeerX, Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.81.... - -1k>
11. J.A.Pouwelse, P.Garbacki, D.H.J. Epema, H.J. Sips(2007), A Measurement Study of the BitTorrent Peer-To-Peer File-Sharing System, CiteSeerX, Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.3.6... - 3k>
12. Xiaowen Chu, Xiaowei Chen, Kaiyong Zhao and Jiangchuan Liu(2010), Reputation and trust management in heterogeneous peer-to-peer networks , SpringerLink, Retrieved from <http://www.springerlink.com/content/htut5t25713014r4/>
13. Luca De Cicco, Saverio Mascolo, Vittorio Palmisano(2008), Skype video responsiveness to bandwidth variations, ACM Digital Library, Retrieved from <http://portal.acm.org/citation.cfm?id=1496065>

14. Uwe Schmidt(2007), Peer- To- Peer Systems, viewed 28 October 2010, viewed 28 October 2010, Retrieved from <http://www.slideshare.net/uschmidt/peertopeer-systems>
15. David Tacconi(2008), Peer to Peer NetWorking, viewed 28 October 2010, Retrieved from http://www.slideshare.net/david.tacconi/p2p-seminar?src=related_normal&rel=112477
16. Abhishek Sharma(2007), Bit Torrent, viewed 28 October 2010, Retrieved from <http://www.slideshare.net/abhipesit/bit-torrenttechnology>
17. Li X.& Wu J. (2004), Searching techniques in peer-to peer networks, Viewed 28 October 2010, Retrieved from http://www.cis.temple.edu/~wu/research/publications/Publication_files/p2psearching.pdf
18. Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, Steven Lim (2005), A survey and comparison of Peer-to-Peer overlay network schemes, 28 October 2010, Retrieved from <http://app2.mans.edu.eg/eulc/Libraries/itemsAttach/IssueArticle/1026565/survey.pdf>
19. Steven M.Bellovin(2001), Security Aspects Of Napster and Gnutella, viewed 28 October 2010, Retrieved from <http://www.usenix.org/event/usenix01/invitedtalks/bellovin.pdf>
20. Yensy James Hall, Patrick Piemonte, Matt Weyant(2007), Joost: A Measurement Study , viewed 28 October 2010, Retrieved from <http://www.patrickpiemonte.com/15744-Joost.pdf>
21. Pascal Wibmann(2008), Security review of the Skype Network, viewed 28 October 2010, Retrieved from http://nds.hgi.rub.de/lehre/seminar/WS07/papers/Wi08fin_skype.pdf
22. Benny Fallica, Yue Lu, Fernando Kuipers, Rob Kooij, Piet Van Mieghem (2008), Assessing The Quality of Experience of Sopcast , viewed 28 October 2010, Retrieved from <http://www.nas.its.tudelft.nl/people/Fernando/papers/SopCastIJIPT.pdf>
23. <http://manuals.kerio.com/kwfag/en/glossary.html>
24. <https://support.skype.com/en/faq/FA143/Is-Skype-secure>
25. <http://www.joost.com/about/joost/>
26. www.napster.com
27. <http://en.wikipedia.org/wiki/Freenet>
28. www.freenet.com
29. www.sopcast.com