Quantum: Ένα δίκτυο ομότιμων κόμβων για κατανεμημένους υπολογισμούς με ενισχυμένη ιδιωτικότητα

Γεώργιος Σταματελάτος, Γεώργιος Δροσάτος, Παύλος Εφραιμίδης
Τμήμα Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών
Δημοκρίτειο Πανεπιστήμιο Θράκης
Πανεπιστημιούπολη, 67100 Ξάνθη
{gs6646, gdrosato, pefraimi}@ee.duth.gr

Περίληψη

Στην παρούσα εργασία παρουσιάζεται το Quantum, ένα δίκτυο ομότιμων κόμβων για την εκτέλεση κατανεμημένων υπολογισμών μεταξύ αυτόνομων agents (πρακτόρων). Βασικό χαρακτηριστικό του Quantum είναι η προστασία της ιδιωτικότητας των κόμβων που συμμετέχουν σε κάθε κατανεμημένο υπολογισμό. Επιπλέον το Quantum πρέπει να υποστηρίζει τοπολογίες που σχηματίζουν μεγάλο πλήθος agents που επικοινωνούν μέσω του διαδικτύου και να παρουσιάζει ανοχή σε προσθήκες/αφαιρέσεις κόμβων. Στη λύση που σχεδιάσαμε, επιλέξαμε μια αποκεντρωμένη αρχιτεκτονική για το δίκτυο και αξιοποιήσαμε τεχνολογίες ομότιμων (peer-to-peer) δικτύων.

1. Εισαγωγή

Θέλουμε να υποστηρίξουμε κατανεμημένες εφαρμογές όπου κάθε χρήστης θα αντιπροσωπεύεται από κάποιο προσωπικό agent. Χαρακτηριστικό του Quantum είναι ότι η λειτουργία του δε βασίζεται σε κεντρικό διακομιστή αλλά η επικοινωνία μεταξύ των χρηστών του είναι τελείως αποκεντροποιημένη, γεγονός που ενισχύει την ιδιωτικότητά του. Στο έργο Polis [2], αναπτύσσονται τεχνολογίες όπου κάθε χρήστης διαχειρίζεται ο ίδιος τα προσωπικά του δεδομένα και η πρόσβαση σε αυτά γίνεται αποκεντρωμένα με συμφωνίες μεταξύ agents. Η ανάγκη για την εκτέλεση σύνθετων υπολογισμών με τη συμμετοχή μεγάλου πλήθους κόμβων του Polis οδήγησε στην ανάπτυξη του Quantum.

Για την οργάνωση των κόμβων/agents σε τοπολογία επιλέγουμε την αποκεντρωμένη οργάνωση όπου όλοι οι κόμβοι συμμετέχουν ισότιμα. Ο λόγος είναι ότι έτσι εξασφαλίζουμε επεκτασιμότητα (scalability) του δικτύου ενώ μειώνουμε τους κινδύνους για την ιδιωτικότητα των κόμβων.

2. Σχετικές εργασίες

Αρκετές είναι οι υλοποιήσεις και τα πρωτόκολλα που έχουν προταθεί για δίκτυα ομότιμων κόμβων (peer-to-peer networks). Τα πρωτόκολλα Chord [4], Freenet [1] και Kademlia [3] που θα παρουσιαστούν παρακάτω αποτελούν κάποιες από τις υπάρχουσες ιδέες που εφαρμόζονται σήμερα.

Το *Chord* αποτελεί ένα πρωτόκολλο ομότιμου δικτύου που στοχεύει στην γρήγορη και αποτελεσματική αναζήτηση μεταξύ των κόμβων. Αυτό επιτυγχάνεται με τη χρήση αναφορών σε πολλαπλούς κόμβους σταθερής θέσης (Finger Tables), που αποτελούν σημεία με αποστάσεις τις δυνάμεις του δύο, έτσι ώστε να λογαριθμείται ο χρόνος που χρειάζεται να ταξιδέψει ένα αίτημα γύρω από τον κύκλο.

Το *Freenet* είναι ένα πρωτόκολλο αποκεντροποιημένης επικοινωνίας που επικεντρώνεται στην ιδιωτικότητα και την ανωνυμία των σταθμών του δικτύου. Κάθε κόμβος προστατεύει τα προσωπικά του στοιχεία με τη βοήθεια ενός ζεύγους δημοσίου-ιδιωτικού κλειδιού, διατηρώντας συνδέσεις ασφαλούς επικοινωνίας με τις αναφορές του.

Τα δίκτυα *Kademlia* διατηρούν την τυπική δομή δικτύων ομότιμων κόμβων που συναντάμε σε δίκτυα, όπως το Chord. Η κύρια διαφορά του Kademlia έγκειται στη χρήση δενδρικής δομής προκειμένου να οργανωθούν οι κόμβοι του.

3. Προσέγγιση - Περιγραφή

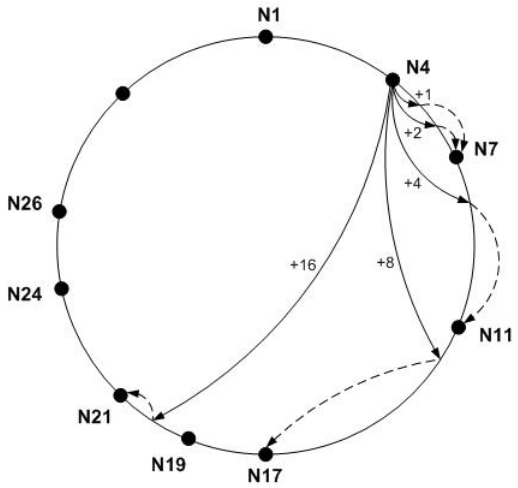
Το πρωτόκολλο Quantum που προτείνεται στην παρούσα εργασία βασίζεται σε ιδέες των προαναφερθέντων πρωτοκόλλων: Η βασική δομή του στηρίζεται στην αντίστοιχη του Chord, ενώ ταυτόχρονα θεωρείται απαραίτητη η έννοια της ιδιωτικότητας για τους κόμβους, όπως αυτή παρουσιάζεται στο Freenet. Αντίστοιχα, για τις ανάγκες των πειραμάτων πάνω σε δίκτυα Quantum θα χρησιμοποιηθεί η δομή δέντρου που συναντάει κανείς στα δίκτυα Kademlia. Τα κύρια χαρακτηριστικά του πρωτοκόλλου παρουσιάζονται στην επόμενη υποενότητα.

3.1. Χαρακτηριστικά δικτυακής οργάνωσης

Η δικτυακή αρχιτεκτονική του Quantum περιλαμβάνει βασικά χαρακτηριστικά του Chord, όπως η ένταξη

των κόμβων σε δακτύλιο, η διατήρηση αναφορών σταθερής θέσης (fingers), η σταθεροποίηση των αναφορών καθώς επίσης και είσοδος και έξοδος κόμβων από το δίκτυο. Ενδιαφέρον παρουσιάζει ο αλγόριθμος αναζήτησης ενός κλειδιού. Ένας κόμβος που θα λάβει/εκκινήσει ένα αίτημα αναζήτησης θα προωθήσει το αίτημα στην μεγαλύτερη αναφορά του που είναι μικρότερη από το ζητούμενο κλειδί. Σε αντίθεση με πρωτόκολλα peer-to-peer δικτύων, το Quantum δεν ασχολείται με αποθήκευση δεδομένων και τα κλειδιά χρησιμοποιούνται μόνο για τη δρομολόγηση των πακέτων.

Επίσης, εξετάζεται η δυνατότητα να υλοποιηθούν υπηρεσίες που θα βοηθούν έναν αυτόνομο agent να ενταχθεί στο δίκτυο, σε περίπτωση που αυτός δεν διαθέτει κάποιο τρόπο επικοινωνίας με τους άλλους κόμβους του ομότιμου δικτύου.



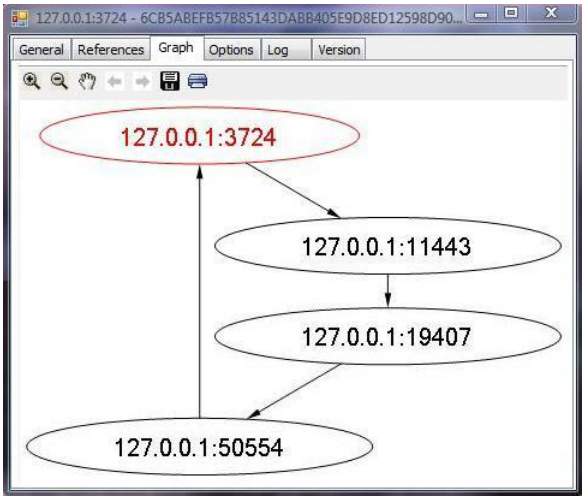
Σχήμα 1. Αναφορές του κόμβου N4 σε ένα δίκτυο Quantum.

3.2. Κατανεμημένοι υπολογισμοί

Η διαφοροποίηση του Quantum, από τις τεχνολογίες που αναφέρθηκαν, έγκειται στην δυνατότητα εκτέλεσης αποδοτικών κατανεμημένων υπολογισμών μεταξύ κόμβων-χρηστών μεγάλου πλήθους με ταυτόχρονη προστασία της ιδιωτικότητάς τους (χωρίς δηλαδή την αποκάλυψη των προσωπικών τους δεδομένων, παρά μόνο των ελάχιστων δυνατών) σε όλες τις φάσεις της διαδικασίας του υπολογισμού. Ένα τέτοιο παράδειγμα κατανεμημένου υπολογισμού είναι η εύρεση του εκατομμυριούχου (millionaire's problem), όχι μόνο ανάμεσα δύο κόμβων, αλλά του συνόλου που λαμβάνουν μέρος στο δίκτυο. Ο παραπάνω μηχανισμός μπορεί να επιτευχθεί λόγω της δενδρικής δομής των κόμβων που προκύπτει άμεσα από τη δυαδική αναπαράσταση των κλειδιών των agents.

4. Πλατφόρμα πειραμάτων - Συμπεράσματα

Για την παραπάνω δικτυακή αρχιτεκτονική, αναπτύχθηκε μια πιλοτική εφαρμογή σε προγραμματιστικό περιβάλλον .NET, η οποία αντιπροσωπεύει έναν agent-κόμβο. Δοκιμές πάνω στη λειτουργικότητα της εφαρμογής έχουν γίνει τοπικά, στο ίδιο μηχάνημα, με ταυτόχρονη λειτουργία αρκετών agents. Πρώιμα συμπεράσματα δείχνουν ότι ο μηχανισμός συγκρότησης του δακτυλίου επιτυγχάνεται, ενώ τα fingers είναι ακόμη σε δοκιμαστικό στάδιο μιας και υπάρχουν ορισμένα προβλήματα στο διαδικασία εκσφαλμάτωσης. Ο αλγόριθμος δρομολόγησης των αιτημάτων είναι υλοποιημένος και ακολουθεί τα πρότυπα που αναφέρθηκαν πιο πάνω.



Σχήμα 2. Γραφική απεικόνιση του δικτύου από έναν agent.

Αναφορές

[1] I. Clarke, O. Sandberg, B. Wiley, and T.W. Hong. Freenet: A distributed anonymous information storage and retrieval system. In *ICSI Workshop on Design Issues in Anonymity and Unobservability*, pages 46–66, 1999.

[2] P. S. Efraimidis, G. Drosatos, F. Nalbadis, and A. Tasidou. Towards privacy in personal data management. In *PCI 2008*, pages 3–7, Aug 2008.

[3] P. Maymounkov and D. Mazieres. Kademlia: A peer-to-peer information system based on the xor metric. In *IPTPS*, pages 53–65, Mar 2002.

[4] I. Stoica, R. Morris, D. Karger, M.F. Kaashoek, and H. Balakrishnan. Chord: A scalable peer-to-peer lookup service for internet applications. In *ACM SIGCOMM'01*, pages 149–160, Aug 2001.