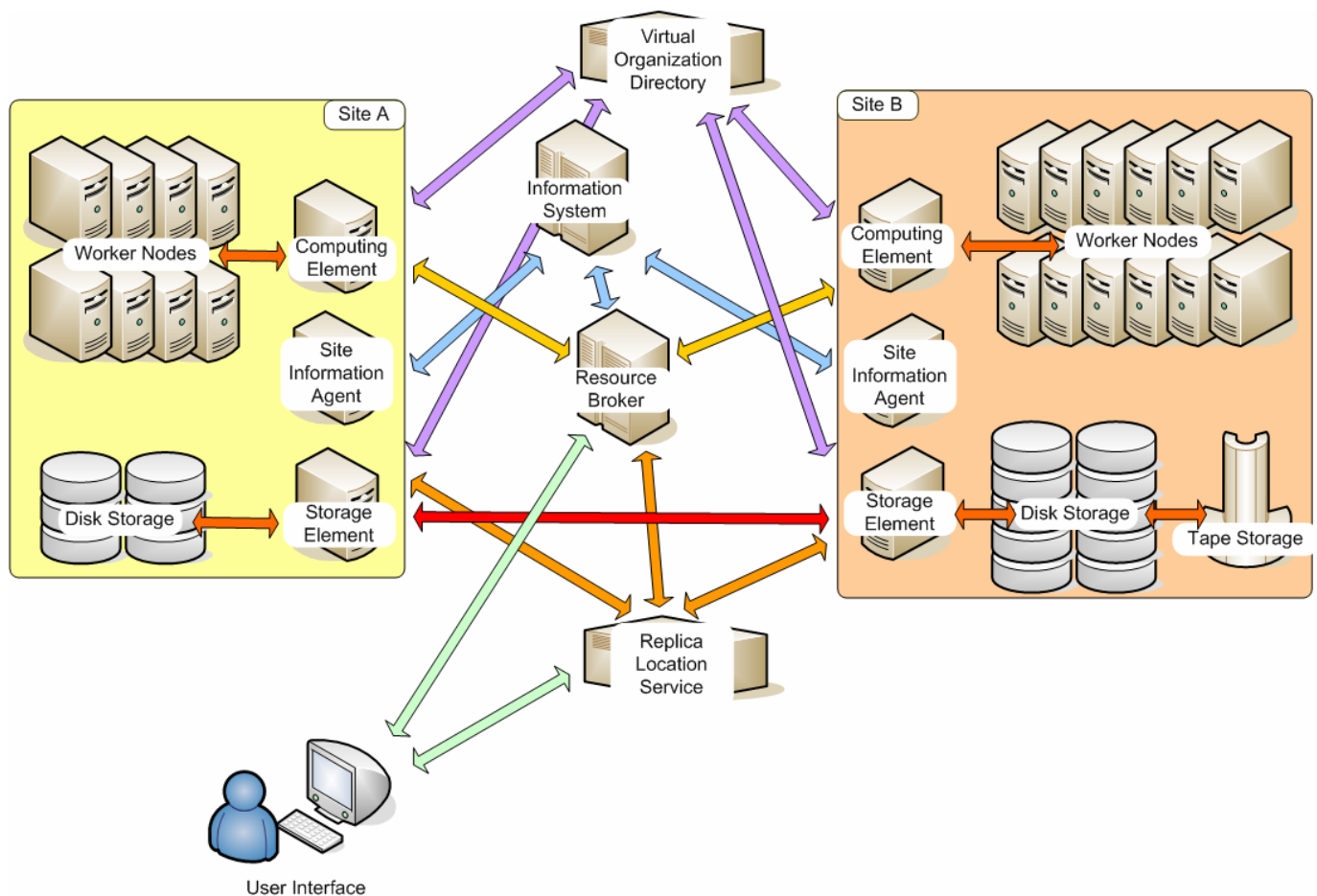




Θέματα Διπλωματικών Εργασιών

Ενημερωτικό Σημείωμα για Υπολογιστικά Πλέγματα (GRIDS)

Τα υπολογιστικά πλέγματα (Grid)[1][2][3][4] έχουν θεωρηθεί από πολλούς μια ανακάλυψη συγκρίσιμη με την τεχνολογία του ιστοχώρου. Η φιλοσοφία που κρύβεται πίσω από αυτή την δυναμική είναι η διαχείριση των υπολογιστικών και αποθηκευτικών πόρων σαν ένα αγαθό, το οποίο μπορεί να μοιράζεται στον καθένα με τρόπο απλό, σε αναλογία με τα ηλεκτρικά δίκτυα ή τα δίκτυα ύδρευσης. Εικονικοί οργανισμοί σχηματίζονται στα πλαίσια της τεχνολογίας αυτής, και δίνουν την δυνατότητα σε άτομα με κοινό στόχο να συνεργάζονται και να εκμεταλλεύονται την κοινή τους υπολογιστική υποδομή για το κοινό όφελος. Στην πρώτη τους μορφή δίνουν πρόσβαση με ασφαλή τρόπο σε διαμοιρασμένη υπολογιστική ισχύ και χώρο αποθήκευσης.



Εικόνα 1 Μια απλουστευμένη αποτύπωση αρχιτεκτονικής Grid

Μια απλουστευμένη αρχιτεκτονική ενός συστήματος Grid αποτυπώνεται στο παραπάνω σχήμα. Η αρχιτεκτονική αυτή υλοποιείται με το ενδιάμεσο λογισμικό gLite [5]. Ο χρήστης έχει ένα User Interface από το οποίο υποβάλλει τις εργασίες του στο Grid. Η εργασία αυτή περιγράφεται σε ένα αρχείο, στο οποίο υπάρχουν όλα τα κατάλληλα στοιχεία για να εκτελεστεί (όπως όνομα εκτελέσιμου αρχείου, ονόματα αρχείου εισόδου / εξόδου, εξαρτήσεις σε βιβλιοθήκες λογισμικού, επιθυμητή υπολογιστική δύναμη κλπ.). Κατά την υποβολή της εργασίας, τα παραπάνω δεδομένα φτάνουν στον Resource Broker, ο οποίος τα επεξεργάζεται ώστε να βρει το καλύτερο από τους διαθέσιμους υπολογιστικούς πόρους, ώστε να εκτελεστεί η εργασία. Για να μπορεί να πάρει αυτή την απόφαση συμβουλευείται μια υπηρεσία παρακολούθησης, που είναι συνδεδεμένη με όλους τους πόρους του Grid, και από εκεί αντλεί διάφορες πληροφορίες, όπως η διαθέσιμη υπολογιστική δύναμη, η ποσότητα του ελεύθερου αποθηκευτικού χώρου, το εγκατεστημένο λογισμικό κλπ. Αφού ο Resource Broker αποφασίσει ποιος υπολογιστικός πόρος πληρεί τις προϋποθέσεις που έχει θέσει ο χρήστης, επικοινωνεί με το αντίστοιχο Computing Element και στέλνει όλα τα απαραίτητα δεδομένα. Το Computing Element είναι ένας ενδιάμεσος δρομολογητής, που ελέγχει ένα σύνολο από όμοιους κόμβους (Worker Nodes), στους οποίους γίνεται και η εκτέλεση των εργασιών. Το Computing Element ξεκινάει την εργασία σε κάποιον κόμβο και μόλις αυτή εκτελεστεί τότε τα αποτελέσματα μέσω του Resource Broker στέλνονται πίσω στον χρήστη. Εκτός από το Computing Element, σε κάθε εγκατάσταση υπάρχει και ένα Storage Element, το οποίο είναι επιφορτισμένο με την διάθεση αποθηκευτικού χώρου. Έτσι, από το User Interface μπορεί κάποιος χρήστης, με τις κατάλληλες εντολές, να αποθηκεύει τα δεδομένα του στο Grid και στην συνέχεια να τα χρησιμοποιήσει κατά την διάρκεια κάποιας εργασίας που έστειλε για εκτέλεση. Επίσης, υπάρχουν και υπηρεσίες που παράγουν αντίγραφα δεδομένων μεταξύ των Storage Element, ώστε τα δεδομένα διασκορπίζονται στο Grid, να υπάρχουν αντίγραφα για λόγους ασφάλειας αλλά και για να είναι εφικτή ένας βέλτιστος χρονοπρογραμματισμός δεδομένων και εργασιών. Τέλος, ένα σημαντικό στοιχείο που υπάρχει σε κάθε βήμα αυτής της διαδικασίας, είναι η ασφάλεια που επιτυγχάνεται μέσω μιας υποδομής Public Key Infrastructure (PKI). Κάθε χρήστης και υπηρεσία πρέπει να έχει ένα πιστοποιητικό υπογεγραμμένο από μια ή περισσότερες Αρχές Πιστοποίησης για να μπορέσει να συνδεθεί στην υποδομή Grid. Οι Αρχές Πιστοποίησης είναι προκαθορισμένες από τους συμβαλλόμενους σε κάθε Grid και δεν υπάρχει μια κεντρική. Σαν ένα δεύτερο βήμα ασφάλειας για να μπορέσει να χρησιμοποιήσει κάποια υπηρεσία, θα πρέπει ο χρήστης να είναι μέλος κάποιου εικονικού οργανισμού, ο οποίος να έχει πρόσβαση στην υπηρεσία αυτή.

Η έρευνα του εργαστηρίου εστιάζεται κυρίως στην σύγκλιση των τεχνολογιών grid και peer-to-peer. Οι ιδιότητες των αλγορίθμων που χρησιμοποιούνται στα σημερινά peer-to-peer δίκτυα μπορούν να προσφέρουν μεγαλύτερη αξιοπιστία και απόδοση σε συστήματα μεγάλης κλίμακας όπως είναι το GRID, εξαλείφοντας single-point-of-failures που παρουσιάζονται σε υπηρεσίες που έχουν αναπτυχθεί με το μοντέλο client-server.

Υλοποίηση peer-to-peer δικτύου με υποδομή ασφάλειας GRID

Μια σημαντική διαφορά μεταξύ των peer-to-peer δικτύων και των συστημάτων GRID, είναι το επίπεδο της ασφάλειας. Στο GRID πρέπει να γίνεται ταυτοποίηση του χρήστη (authentication) από κάθε υπηρεσία και σε δεύτερο βαθμό έλεγχος για τα δικαιώματα που έχει στην υπηρεσία (authorization).

Το authentication γίνεται βάση με την βοήθεια της κρυπτογραφίας δημοσίου κλειδιού (Public Key Cryptography). Στη κρυπτογραφία δημοσίου κλειδιού, υπάρχουν δύο κλειδιά το ιδιωτικό και το δημόσιο κλειδί. Τα δύο κλειδιά συνδέονται με ένα μαθηματικό τύπο και από το ιδιωτικό κλειδί μπορεί να προκύψει το δημόσιο, αλλά δεν συμβαίνει το αντίστροφο. Το ιδιωτικό κλειδί κρατείται κρυφό, ενώ το δημόσιο κλειδί διαδίδεται σε κάθε ενδιαφερόμενο. Κάθε τι που έχει κρυπτογραφηθεί από το ένα κλειδί μπορεί να αποκρυπτογραφηθεί από το άλλο.. Με τον τρόπο αυτό μπορεί ο χρήστης A να αποστείλει ένα κείμενο ή ένα πιστοποιητικό με τα στοιχεία του, παραθέτοντας στο τέλος την κρυπτογραφημένη εκδοχή του κειμένου/πιστοποιητικού. Ο παραλήπτης αποκρυπτογραφεί την παράθεση χρησιμοποιώντας το δημόσιο κλειδί του χρήστη A και τη συγκρίνει με το πραγματικό κείμενο, οπότε και βεβαιώνεται για την ταυτότητα του αποστολέα. Για την παραπάνω διαδικασία της ψηφιακής υπογραφής, έχει δημιουργηθεί ένα πρότυπο ψηφιακού πιστοποιητικού (X509 [15]), το οποίο περιλαμβάνει σε μια σαφώς ορισμένη δομή τα στοιχεία του χρήστη και το δημόσιο κλειδί του και τη ψηφιακή υπογραφή μιας τρίτης έμπιστης οντότητας. Αυτή η οντότητα κοινής εμπιστοσύνης, σε μια υποδομή δημοσίου κλειδιού (Public Key Infrastructure), ονομάζεται Αρχή Πιστοποίησης (Certification Authority [16]). Η Αρχή Πιστοποίησης ταυτοποιεί με κάποιο φυσικό τρόπο τον χρήστη και υπογράφει το δημόσιο κλειδί του. Με τον τρόπο αυτό όποιος εμπιστεύεται την Αρχή Πιστοποίησης - έχει το δημόσιο κλειδί της - εμπιστεύεται και τα πιστοποιητικά των χρηστών που υπογράφει η Αρχή.

Το authorization γίνεται βάση ενός κεντρικού καταλόγου (VOMS: Virtual Organization Membership Service [17]). Στο κεντρικό κατάλογο εγγράφονται όλοι οι χρήστες και το είδος των δικαιωμάτων που έχουν μέσα στον εικονικό οργανισμό που ανήκει (Virtual Organization). Έτσι, όταν ένας χρήστης προσπαθεί να αποθηκεύσει ένα αρχείο στο GRID, πρώτα θα του ζητηθεί το ψηφιακό πιστοποιητικό για να γίνει η ταυτοποίησή του και μετά θα ερωτηθεί ο κεντρικός κατάλογος για να ερευνηθούν τα δικαιώματα του στο GRID. Πχ εάν έχει δικαίωμα να χρησιμοποιήσει τον συγκεκριμένο αποθηκευτικό χώρο, πόσος χώρος μπορεί να χρησιμοποιηθεί κλπ.

Αυτή τη στιγμή στα peer-to-peer δίκτυα όλοι οι χρήστες είναι ομότιμοι και δεν υπάρχουν μηχανισμοί ταυτοποίησης. Αντικείμενο της διπλωματικής είναι η ενσωμάτωση υποδομής δημοσίου κλειδιού [6] σε ένα peer-to-peer του δίκτυο. Για την υλοποίηση θα χρησιμοποιηθούν έτοιμες βιβλιοθήκες PKI και του peer-to-peer δικτύου kademia [7] που έχει αναπτυχθεί ή άλλα που υπάρχουν ελεύθερα διαθέσιμα στο δίκτυο [8][9].

Βασικά προαπαιτούμενα για την πραγμάτωση της διπλωματικής εργασίας είναι:

- Γνώση και εμπειρία στο προγραμματιστικό περιβάλλον του Linux. (μαθήματα: Λειτουργικά Συστήματα και Εργαστήριο Λειτουργικών Συστημάτων).
- Γνώση και εμπειρία στο προγραμματισμό σε C/JAVA

Στάδια Εργασίας

- Βιβλιογραφική Μελέτη σχετικά με Public Key Infrastructure (PKI)
- Βιβλιογραφική Μελέτη σχετικά με peer-to-peer δίκτυα
- Εγκατάσταση και εξοικείωση με το προγραμματιστικό περιβάλλον
- Μελέτη των βιβλιοθηκών και της υπάρχουσας υλοποίησης
- Ενσωμάτωση της υποδομής PKI στην peer-to-peer υλοποίηση
- Ενσωμάτωση της υπηρεσίας VOMS στην peer-to-peer υλοποίηση
- Πειραματικά αποτελέσματα / DEMO

Κατανεμημένη υπηρεσία αναζήτησης στο GRID

Μια βασική υπηρεσία στο GRID αποτελεί το Information System. Το σύστημα αυτό αποτελεί ουσιαστικά ένα ευρετήριο για όλους τους διαθέσιμους πόρους του GRID [10][11]. Η σημερινή δομή του συστήματος είναι ιεραρχική. Αποτελείται από τοπικά ευρετήρια (local index) και κεντρικά ευρετήρια (central index). Κάθε site έχει τουλάχιστον ένα τοπικό ευρετήριο. Το τοπικό ευρετήριο περιέχει πληροφορίες για το συγκεκριμένο site. Οι πληροφορίες είναι δύο ειδών:

- Στατικές, πχ
 - ο τι τύπου/πόσοι επεξεργαστές υπάρχουν σε κάθε κόμβο
 - ο πόση μνήμη έχει κάθε κόμβος
 - ο τι τύπου λειτουργικό σύστημα υπάρχει στους κόμβους
 - ο τι είδους αποθηκευτικός χώρος υπάρχει (δίσκοι/βιβλιοθήκη ταινιών - tape library)
- Δυναμικές
 - ο Πόσοι επεξεργαστές είναι διαθέσιμοι;
 - ο Πόσο μέγεθος του αποθηκευτικού χώρου είναι διαθέσιμο;
 - ο Πόσες εργασίες εκτελούνται αυτή τη στιγμή στους κόμβους του site;

Όλη αυτή η πληροφορία είναι δομημένη. Δηλαδή, χρησιμοποιείται ένα σχήμα, ώστε να γίνεται εύκολη η αποθήκευση/παρουσίαση/αναζήτηση σε αυτή. Το σχήμα που χρησιμοποιείται ευρέως είναι το GLUE Schema. Υπάρχουν δύο υλοποιήσεις του σχήματος που μπορούν να χρησιμοποιηθούν. Μια σε XML[18] και μια σε LDAP[19].

Το αντικείμενο της διπλωματικής είναι η δημιουργία ενός κατανεμημένου ευρετηρίου με την βοήθεια ενός peer-to-peer δικτύου. Ένα ιδιαίτερο πρόβλημα στα peer-to-peer δίκτυα είναι η αναζήτηση ενός συνόλου κλειδιών (range queries) σε αντίθεση με την αναζήτηση ενός συγκεκριμένου κλειδιού (exact match). Για το πρόβλημα αυτός υπάρχουν αρκετές λύσεις στη βιβλιογραφία. Μια λύση είναι η χρησιμοποίηση ενός Content Addressable Network (CAN) [12]. Το Content Addressable Network έχει δύο σημαντικές ιδιότητες:

- είναι δομημένο [13],
- μπορεί εκ-φύσεως να απαντήσει σε ερωτήματα συνόλου τιμών (range-queries) όπως πχ. «Ποιοι είναι οι διαθέσιμοι πόροι με μνήμη μεγαλύτερη από 1GB» [14]

Χρησιμοποιώντας τις παραπάνω ιδιότητες, το CAN θα αντικαταστήσει την υπηρεσία ευρετηρίου, δημιουργώντας ένα κατανεμημένο ευρετήριο. Μέσα στους στόχους της διπλωματικής είναι η υλοποίηση του Content Addressable Network και η δημιουργία ενός Web Service interface για την πρόσβαση σε αυτό. Το Web Service interface θα χρησιμοποιείται από άλλους χρήστες ή υπηρεσίες στο GRID για την αναζήτηση στοιχείων, οπότε θα πρέπει να είναι συμβατό με τα υπάρχοντα πρότυπα (πχ Globus WS-MDS [15]).

Βασικά προαπαιτούμενα για την πραγμάτωση της διπλωματικής εργασίας είναι:

- Γνώση και εμπειρία στο προγραμματιστικό περιβάλλον του Linux. (μαθήματα: Λειτουργικά Συστήματα και Εργαστήριο Λειτουργικών Συστημάτων).
- Γνώση και εμπειρία στο προγραμματισμό σε C/JAVA

Στάδια Εργασίας

- Βιβλιογραφική Μελέτη σχετικά με τα peer-to-peer δίκτυα Content Addressable Network
- Βιβλιογραφική Μελέτη σχετικά με Web Services
- Εγκατάσταση και εξοικείωση με το προγραμματιστικό περιβάλλον
- Μελέτη των βιβλιοθηκών
- Ανάπτυξη εφαρμογής
- Πειραματικά αποτελέσματα / DEMO

[Αναφορές]

- [1] What is Grid, Presentation, Dr. Rüdiger Berlich Forschungszentrum Karlsruhe
<http://www.egee.nesc.ac.uk/trgmat/events/040920GridKa/talks/slides/whatIsGrid.pdf>
- [2] The Anatomy of the Grid: Enabling Scalable Virtual Organizations. I. Foster, C. Kesselman, S. Tuecke. International J. Supercomputer Applications, 15(3), 2001.
<http://www.globus.org/research/papers/anatomy.pdf>
- [3] The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration. I. Foster, C. Kesselman, J. Nick, S. Tuecke, Open Grid Service Infrastructure WG, Global Grid Forum, June 22, 2002
<http://www.globus.org/research/papers/ogsa.pdf>
- [4] GridCafe, the place for everybody to learn about the Grid
<http://gridcafe.web.cern.ch/gridcafe/>
- [5] gLite - Lightweight Middleware for Grid Computing - <http://www.glite.org/>
- [6] Overview of the Grid Security Infrastructure - <http://www.globus.org/security/overview.html>
- [7] The Kademia peer-to-peer network - <http://en.wikipedia.org/wiki/Kademia>
- [8] Khashmir: Python implementation of Kademia - <http://khashmir.sourceforge.net/>
- [9] KadC: C implementation of Kademia - <http://kadc.sourceforge.net/>
- [10] GT 4.0: Information Services - <http://www.globus.org/toolkit/docs/4.0/info/>
- [11] GT4 Monitoring and Discovery
http://www.globus.org/toolkit/presentations/GlobusWorld_2005_Session_9c.pdf
- [12] A Scalable Content-Addressable Network
<http://www.acm.org/sigs/sigcomm/sigcomm2001/p13-ratnasamy.pdf>
- [13] Unstructured and structured P2P networks
http://en.wikipedia.org/wiki/Peer_to_peer#Unstructured_and_structured_P2P_networks
- [14] Scalable, Efficient Range Queries for Grid Information Services
<http://doi.ieeeecomputersociety.org/10.1109/PTP.2002.1046310>
- [15] X.509, ITU-T standard for public key infrastructure (PKI)
<http://en.wikipedia.org/wiki/X.509>
- [16] Certification Authority (CA) - http://en.wikipedia.org/wiki/Certification_authority
- [17] VOMS: Virtual Organization Membership Service
http://www.globus.org/grid_software/security/voms.php
- [18] GLUE Schema in XML - <http://glueschema.forge.cnaf.infn.it/Mapping/XMLSchema>
- [19] GLUE Schema in LDAP - <http://glueschema.forge.cnaf.infn.it/Mapping/LDAP>
- [20] Globus Toolkit 4.0: Information Services - <http://www.globus.org/toolkit/docs/4.0/info/>

Για περισσότερες πληροφορίες, Αντώνης Ζήσιμος, 21.34Α, κτ. Ηλεκτρολόγων, +30 (10) 772-2402

<http://www.cslab.ece.ntua.gr/~nkoziris>
<http://www.cslab.ece.ntua.gr/~azisi>

Νεκτάριος Κοζύρης, Επίκουρος καθηγητής
Αντώνης Ζήσιμος, υποψήφιος διδάκτωρ