P-LeaSel for GRID Environment

Mary Vennila S[1] and Sankaranarayanan V[2]
[1]Senior Lecturer, Department of Computer Science, Presidency College, Chennai, India.

[2]Director, Crescent Engineering College,India.

Summary

Multicast services, grid computing and wireless interconnection networks are among the emerging technologies of the last decade. Incorporating security features in multicast communications gives rise to overheads and computational complexities at the server. Designing an efficient model for secure multicast is a challenging area for the researchers. Grid environment in today's world is a boon for high speed computing, but at the same time, security and anonymity are important features in grid. In this paper, P-LeaSel algorithm has been modified to provide secure multicast communications in Grid environment. The experimental results prove that this approach is really effective and has increased throughput with minimum additional complexity and minimum overheads. Kerberos is used for authentication.

Key words: Grid Computing, P-LeaSel, Kerberos and Multicast Network Security.

1. Introduction

The Grid is a collection of resources (processors, storage devices, peripherals etc) which may be used, shared by several applications to compute faster and more efficiently. The goal here is to create a simple, large, powerful and self managing virtual computer out of a large collection of connected heterogeneous systems sharing various combinations of resources, as put across in [3]. [8] Provides a three point checklist to determine the class of systems that can be grouped under the term 'grid'. An environment with widely distributed resources such as the grid is prone to various types of security attacks, since applications may involve migration of code between the various sites. Thus, security assumes a role of vital importance in grid [12]. Collaborative grid applications involve multiple users who co-operate together on a single shared task. Such applications can use multicasting to transmit the same data to a group of users. By using efficient multicast routing protocols, the network load can be minimized in such a scenario of one to many transmissions. Category of grid applications that may be referred to as "wide-area distributed computing" need Multicast as well as very high computational power. Grid is the best source for relatively cheap and enormous computational power. For example, [7] quotes several applications like Computational Steering [13], Video Conferencing and Online Network Gaming. The stringent security needs of collaborative grid applications necessitate the development of a secure multicast security model exclusively for grid.

2. Existing Security Features of Grid

Security in grid, is now provided by two mechanisms, namely GSI (Grid Security Infrastructure) and Kerberos. GSI, which is explained in detail in [9], [14], [15], is based on PKI (Public Key Infrastructure). It requires the two entities in communication to mutually authenticate those using Digital Certificates, before communication can commence. After the mutual authentication is over, GSI moves aside and the communication can then be secured using a shared secret key. On the other hand, Kerberos [11] is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. It enforces a stringent authentication mechanism by providing users with authenticator, after initial authentication process. Once the client is authenticated, the TGS (Ticket Granting Server) provides access to the service using a ticket. Interoperability can also be provided between GSI and Kerberos [10]. Both GSI and Kerberos emphasize on the Single sign-on feature.

3. LeaSel

The LeaSel model [1] [3] is a scalable, secure and distributed security model for group communication. The model reduces the amount of multicast services affected by entity failure, due to its distributed nature [6].After initial authentication by the Controller; the member is allocated to a subgroup under a Deputy Controller. The deputy controller decides the rank of all the members in the subgroup. The first ranked member is designated as the Leader and is entrusted with the responsibility of key generation and distribution. The deputy controller alone knows the identity of the leader and sender anonymity is achieved by hiding the identity of the leader from the other members of the sub group. The deputy controller is also empowered to change the leader dynamically, to make the model more secure.

Manuscript received April 5, 2008
Manuscript revised April 20, 2008

4. P-LeaSel

P-LeaSel [17] is an adopted version of LeaSel architecture. The Leader selection is where P-LeaSel differs from LeaSel. Instead of single leader, the DC selects a set of ‘p’ leaders. At a given time, only one of them acts as a leader and leader is alternated for every transaction. Thus the ‘p’ leader shares the key management work load among them. More over, attacking the subgroup is more difficult, as it involves attacking all the ‘p’ leaders, instead of one. Thus the group key generation and distribution is not performed by any dedicated controller, but instead by the ‘p’ leaders of the group and it is completely hidden from the group members. Thus the model achieves high scalability with secured key generation and distribution.

5. Grid-P-LeaSel

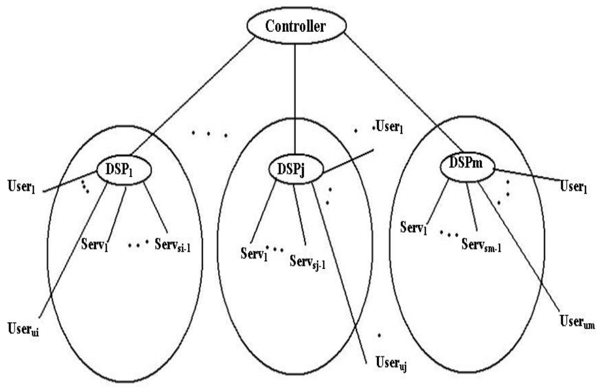


Fig. 1. Grid-P-LeaSel Multicast Security Model for Grid.

Grid-P-LeaSel [16], an adaptation of the P-LeaSel model for the grid, is proposed to provide secure multicast communication services. The gestation of Grid-P-LeaSel from P-LeaSel involves taking a service-oriented approach to the problem. Grid-P-LeaSel is a highly secure, dynamic, distributed sub group model, which caters to the needs of the group communication in grid. The model aims to address issues like forward confidentiality, backward confidentiality, scalability, fault tolerance and computational efficiency. The group of ‘n’ nodes is split into ‘m’ subgroups, based on the service-classes, as shown in Fig. 1, such that

$$\Sigma\, si = n$$

where i=1 to m and si = no of service-offering nodes or service nodes in the ith subgroup.

The group formation is dynamic. New users can join the group to get the services and users may also leave the group. So the actual number of nodes in the ith sub-group can be expressed as

$$si + ui$$

where i= 1 to m and ui is the number of service-requesting nodes or user-nodes in the ith sub group.

One node is designated as the Controller (C) and it provides the overall multicast security service. ‘m’ Service providers, one from each sub group, are designated as Deputy Service Providers (DSP). DSPs provide access to all other services under them. They rank the other $s_i + u_i - 1$ members of the sub-group$_i$ and select pi numbers of thrust worthy members as leaders and assign one among them as L_i, the current leader of the sub-group$_i$ and alternated them for every transaction. The Controller and the DSPs share a common group key GK. Each subgroup has a common subgroup key SK_i. Each node has its own private key; PK. There is a GACL (Group access control list) at the controller, which is used for storing details for authenticating users, user private keys and other pertinent details. The controller distributes parts of GACL as SACL (Sub group Access Control List) to the DSPs, which use it also for determining if a user is eligible for a service. Each node is also provided with a key generation module (KGM) and the leader’s KGM would be used to generate the sub-group key. The leader is responsible for encrypting and decrypting all data within the subgroup. The identity of the leader is kept secret, known only to the DSP which selects it. The leader is dynamically selected. Hence, Grid-P-LeaSel nullifies the chance of the hacker easily attacking the key generating node, since the identity of the Leader is not revealed.

6. Plugging Kerberos and P-LeaSel to Grid

P-LeaSel model [1] does not have any special mechanism for authentication. But adaptation of the model for an environment such as the grid entails a secure authentication protocol. Kerberos [11] can be plugged in as the authentication protocol into the Grid-P-LeaSel model. This would strengthen the security of the Grid-P–LeaSel model, providing robust authentication and also provide Single Sign-on feature reducing the workload of the Controller. What makes Kerberos the automatic choice is that the entities used in Kerberos can be mapped exactly to respective entities in Grid-P-LeaSel. Here, the functions of Authentication Server (AS) and Ticket Granting Server (TGS) are vested with the Controller and the Deputy Service Providers respectively. The sturdiness and the level of security of Kerberos are already proven. Thus, plugging in Kerberos to Grid-P-LeaSel improves the security of the model vastly with minimal additional complexity.

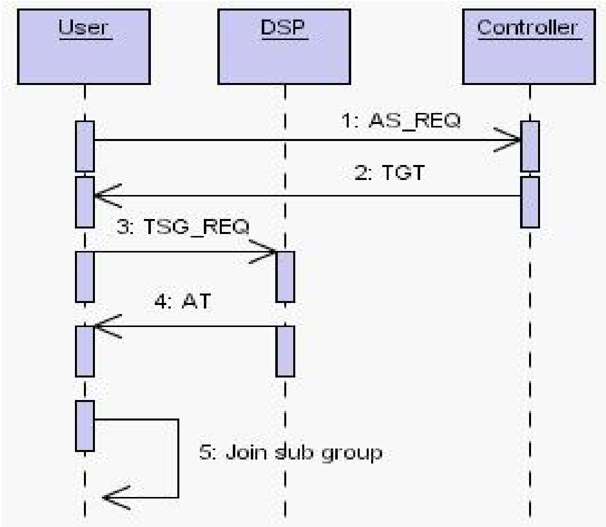


Fig. 2. Authentication using Kerberos

The authentication procedure for Grid-P--LeaSel model using Kerberos is presented in Fig. 2. The user requests the Controller for a Ticket to a Deputy Service Provider that hosts the required service (AS_REQ). The controller authenticates the user and returns the Ticket Granting Ticket (TGT) that permits the user to communicate with the DSP. The user requests the DSP for the appropriate service using the TGT (TGS_REQ). The standard Kerberos mechanism is slightly modified here to suit the needs of Grid-P-LeaSel. In case of standard Kerberos, obtaining a service involves getting a TICKET to the host providing the security. Obtaining multicast services in Grid-P-LeaSel involves joining the subgroup and holding the sub group key. DSP verifies with the SACL and sends an Approval Ticket (AT). The DSP initiates the KGM of the current Leader of the subgroup and the leader distributes the new sub group key. The leader is alternated for every transaction by the DSP.

7. Group Formation Scenarios

Grid-P-LeaSel embarks on a different approach to group formation. The group scenarios are chosen such that they reflect the varied needs of the multicast applications over the grid. Each scenario depicts a group of users requesting a set of services from a DSP. The scenarios for group formation are identified as follows.

Scenario 1: u_i user-nodes in the sub-group, request for services to the DSP. Here, the services are available with the DSP and the message transfers are confined to the sub-group

Scenario 2: u_i user-nodes request for services that are not available under the DSP. DSP, in turn, acts as a moderator between user and another DSP that actually hosts the requested services. This scenario is typical of the grid environment, where the service is available elsewhere and an intermediate node acts as a broker to get the service. Grid-P-LeaSel handles the second scenario, splitting it into two sub-scenarios (2a, 2b).

A. Services under Single DSP (Scenario 1)

Here, u_i users request services from the DSP_i and the services are available within the sub group. A multicast group is formed, which includes the DSP, the user-nodes and the service-nodes under the DSP as shown in Fig. 2. This scenario satisfies service needs of only those users, who were allotted initially to that sub group. The number of user-nodes obtaining the services is a fraction of the total number of user-nodes. The Leader selection process ensures that sender anonymity is preserved during communication.

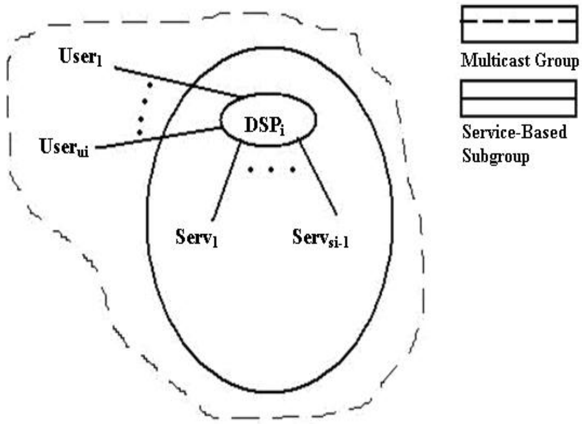


Fig. 3. Service Requested to a Single DSP.

B. Non-Overlapping User, Multiple DSP (Scenario 2a)

Here, users request services from the DSP and the services are not available with the DSP. The DSP, in turn, acts as a broker and gets the required service from some other DSP, which offers the requested services. In the process, DSP becomes a member in the sub-group offering the services and also remains as a part of the original sub-group containing the user-nodes as shown in Fig. 4. This scenario provides services belonging to a different service class than the service class of the sub group, which the requesting users were allotted to, on the first place. In a special case, all the user-nodes in the entire group may request for a single set of services belonging to a specific service class. In such a case, all the DSPs join the sub group, which actually provides the requested set of services. They get the services from the sub group and pass them on to their respective user-nodes through the Leader.

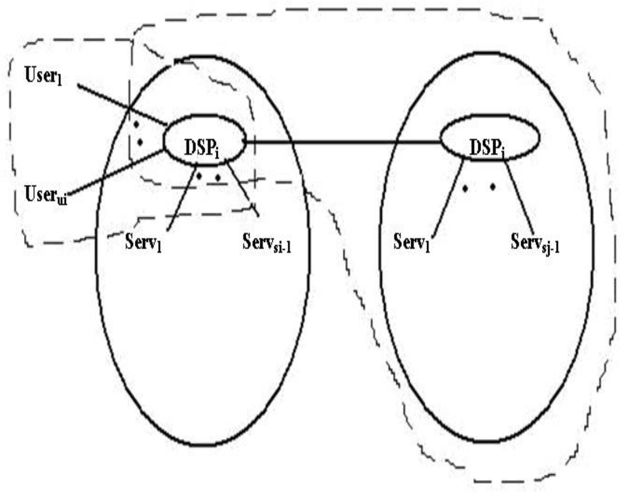


Fig. 4. Non-Overlapping user, Multiple DSP.

C. Overlapping Users, Multiple DSP (Scenario 2b)

Here also, the services requested are not available with the DSP. In cases, where the DSP is busy doing other job and cannot moderate with another DSP to get the service, it can allocate the users directly to the sub-group which offers the requested services. The user-nodes join the multicast group of new DSP, and avail services as in (1), as shown in Fig 5. But, the transferred users remain as part of the original sub-group too. Here also, the serviced users may be requesters of services that were not available in their initial sub group. Sender anonymity is again assured. This scenario services more users than (1), due to the additional members from the other sub groups.

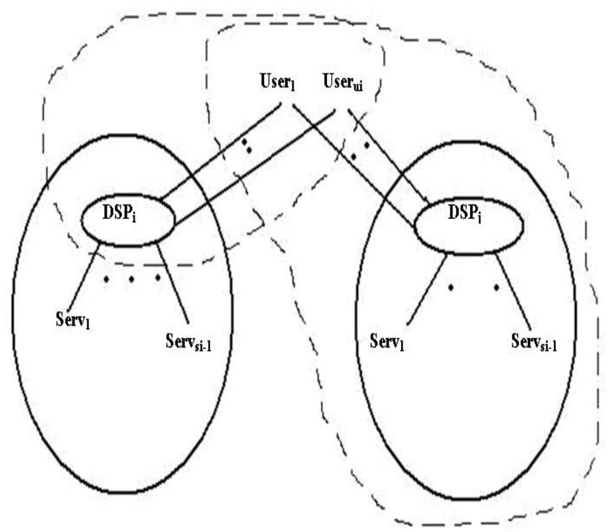


Fig. 5. Overlapping users, Multiple DSP.

8. Membership Events

Having identified the group formation scenarios, it is now necessary to elucidate the Membership events, Join, Leave and Transfer. The stepwise algorithms for these events are presented below. Let DSP denote the set of all Deputy Service providers and

A->B: K [D]

denotes 'A' sending a message 'D' to 'B', using a symmetric encryption algorithm with key 'K', known to both A and B. Let SK_i denote the subgroup key of the i^{th} subgroup and PK_A denote the private key of 'A'.

D. ***Join***

Step 1: Initial Kerberos authentication using the procedure described in section IV, upto sending of message 3 by the User.
Step 2: DSP_i verifies with $SACL_i$ and if the user is entitled for the services requested, goes to step 7 or else does not authenticate the user and the data transmission is uninterrupted.
Step 3: DSP_i sends an Approval Ticket (AT) to user and triggers KGM of the subgroup leader L_i. u_i becomes $u_i + 1$.
Step 4: L_i updates its subgroup membership database, and generates new subgroup public key SK_i'
Step 5: L_i stops data transmission
Step 6: L_i performs encryption and distributes new subgroup public key as follows. This achieves backward confidentiality. Let $user_k$ denote the k^{th} user-node in the subgroup.

$L_i \rightarrow user_j$: $SK_i\ [SK_i']$ *(Multicast);* $1 \le j \le u_i - 1$
$L_i \rightarrow user\ u_i$: $PKuser_{ui}\ [SK_i']$ *(unicast)*

Step 7: Data transmission resumes and stops only when the session ends or when L_i stops data transmission.

E. ***Leave***

There can be two types of leave events – Voluntary leave and Compelled Leave. The DSP may ask the leader to expel a member from the group if it finds the member unworthy of continuing in the group.

1) ***Voluntary Leave***

Let a user leave the subgroup i.

Step 1: User sends LEAVE message to DSP_i
Step 2: DSP_i approves and sends an approval message to user and triggers KGM of the subgroup leader L_i.

***Step 3**:* L_i updates its subgroup membership database, and generates new subgroup public key SK_i'. u_i becomes $u_i - 1$, with the user being excluded.
Step 4: L_i stops data transmission
Step 5: L_i performs encryption and distributes new subgroup public key SK_i' as follows. This achieves forward confidentiality. Let $user_k$ denote the k^{th} user-node in the subgroup

$$L_i \rightarrow user_k: PKuser_k\,[SK_i'] \text{ (unicast)}; 1 \le k \le u_i$$

Step 6: Data transmission resumes and stops only when the session ends or when L_i stops data transmission.

2) ***Compelled Leave***

Let a user be expelled from the subgroup i.

***Step 1**:* DSP_i sends EXPEL message to L_i.
***Step 2**:* DSP_i triggers KGM of the subgroup leader L_i.
***Step 3**:* L_i updates its subgroup membership database, and generates new subgroup public key SK_i'. u_i becomes $u_i - 1$.
Step 4: L_i stops data transmission
***Step 5**:* L_i performs encryption and distributes new subgroup public key SK_i' as follows. This achieves forward confidentiality. Let $user_k$ denote the k^{th} user-node in the subgroup.

$$L_i \rightarrow user_k: Pkuser_k\,[SK_i'] \text{ (unicast) } 1 \le k \le u_i$$

Step 6: Data transmission resumes and stops only when the session ends or when L_i stops data transmission

F. ***Transfer***

Transfer can be achieved through Join and Leave. Let an user be transferred from $subgroup_i$ to $subgroup_j$

***Step 1**:* User is expelled from $subgroup_{i\ using}$ compelled leave algorithm
Step 2: User is redirected to $DSPj$.
Step 3: User joins $subgroup_j$ using the join algorithm.

9. Threat Model

Threat model is a formal specification of various attacks that are inherent to the deployment environment and their counter measures. To validate a model against a threat model, various attacks are simulated and the response of the model to them is studied. Threat model usually contains a number of security parameters that are of vital importance to ensure the security of the model

Authentication

Authentication is a security mechanism through which only the legitimate user in allowed to get access to the system. Authentication in the model is handled by Kerberos.

Threat:
A possible threat would be to crack Kerberos using a cracking tool like Kerbcrack or crack the user's password and spoof a session. This attack is targeted mainly against Windows hosts.

Thwart:
Most firewalls and anti-virus software today detect password cracks and other malware. Blocking RPC-DCOM attacks through port 139, so that intruder cannot gain access to the host.

Authorization

In a Grid context, the potentially large numbers of users and resources with differing management and policies does not permit the use of *general access rights.* Authorization means to enable an user with the proper access rights to a apposite service and preventing users with insufficient access rights from gaining access to other services. Authorization in the model is handled by DSP.

Threat:
Hacker can get a ticket to a service that he is not entitled to access. This may result in financial or some other form of loss to the service provider.

Thwart:
Rigorous checking is done at the DSP to check if the ticket bearer is authorized to access the service.

Revocation

Revocation is the mechanism of issuing security credentials to a user for a limited session time and repealing the same after the expiration of the session. Revocation is vital for both authentication and authorization. For a Grid to be trustworthy it must support an instant withdrawal of access rights. Such dynamic mechanism of revocation is an important part of manageability.

Threat:
A user may continue to stay even after the session has expired. Thus, he may enjoy more services than what he paid for.

Thwart:

DSP has a revocation list and records when the session expires for everyone. The member is expelled when time is up.

Secrecy

Secrecy is also known as Confidentiality. This ensures that the message sent over the line is not visible to hackers who may sniff the messages off the wire. Confidentiality within a Grid is not just concerned with data that is stored upon a resource; it also extends to the privacy requirements of the actual users and resources, to protect the deducibility of data, and to ensure consistence of confidentiality in data replication process within the Grid.

Threat:
Hacker is able to see the messages sent over the system using keys known to him. There are two types of secrecy to preserve in group communication – forward secrecy and backward secrecy.

Thwart:
Kerberos authentication eliminates external hackers from the system. Only internal hackers are able to gain access to the system. Key management is done effectively to preserve both types of secrecies. Rekeying after JOIN and LEAVE ensure this. Group key is also changed periodically to thwart brute-force attacks.

Distributed Trust

Distributed trust is also closely bound up with but broader than authorization. Since the driving application of many grids requires users to be able to compile and run arbitrary code, this ability is built into that trust model. This requires the trust components of the model to be robust and the trust be split across more than one component so that the failure of a single component does not affect the system totally and also the system is self repairing.

Threat:
Hacker destroys the trusted entities in the system- DSP and Controller.

Thwart:
DSP and Controller are run as high users. Leader is built as Daemon. Hence, the critical trust entities are secure from DOS attacks. This problem however falls under system security rather than network security.

Integrity

This becomes a grid problem when copies or subsections of those data are managed automatically and stored at dispersed, separately managed locations. Integrity requirements also extend to the mechanisms by which users' rights are delegated. The malicious hacker should not be able to modify the messages in transit so that either they are meaningless (active attack) or they convey a different meaning (passive attack).

Threat:
Hacker modifies the message sent over the system and causes havoc. He can carry out an active attack since he does not require any knowledge about the message content to modify the message. This, in turn, causes decryption to fail at the receiver.

Thwart:
All messages are encrypted. Thus, carrying out a passive attack is ruled out. When decryption fails, retransmission is done and the lost session is played back. DSP identifies the hacker and expels him.

Non-Repudiation

Non-repudiation, in the view of service provider, means a user should not be able to prove that he did not access a service when he actually did access it. Non-repudiation, in the view of the user, is when he is not charged unduly for a service by the service provider. Non-repudiation is not a security aspect that has been considered in any detail within the grid, but it will become important as the grid technology matures and is used by applications involving financial exchanges. If accessing resources starts costing money, then both parties must be assured that the other fulfils their duty; in the cases where one party fails, proof of commitment is necessary to formally resolve the dispute.

Threat:
An attack of this kind, involving spoofing of the leader, may be carried out. Hacker may send messages to the group as if he is the leader.

Thwart:
DSP listens to the group's messages and expels the hacker when it detects that message is originating from a non-leader. DSP only knows the identity of the leader and he is apt entity to do the thwarting of the attack.

10. Experimental results

The Grid-P-LeaSel model, proposed in the preceding sections was analyzed on a test bed built from Open Mosix enabled systems for the following parameters – System throughput, Scalability and Average time taken for Hacking. The results obtained were interpreted and are presented below. Throughput of the model refers to the total amount of data transferred in a given unit of time. It is affected by communication overheads within the system. Scalability is the ability of the model to adjust its performance suitably at different concentrations of users. Scalability of Grid-P-LeaSel is analyzed based on the group formation scenarios. Average time taken for Hacking is the average time needed by the hacker to disrupt multicast services, by carrying out various kinds of attacks.

Application Throughput

The system throughput (figure 6) was found to match closely with the performance of the P-LeaSel model, proposed. This goes to prove the adaptability of the P-LeaSel model to grid environment, without any degradation of performance.

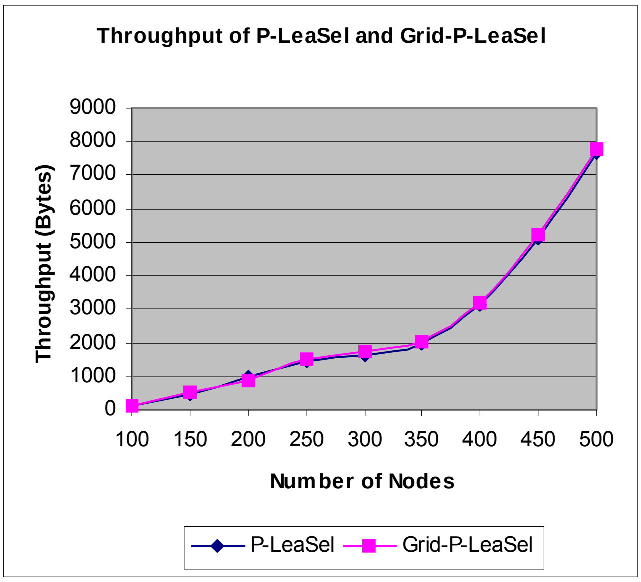


Fig. 6. Throughput of P-LeaSel vs. Grid-P-LeaSel Model.

Scalability

The three group formation scenarios, put forth already, were analyzed based on the number of users (figure 7); the sub-group provides service to, when the sub-group is formed by each of the scenarios. The results indicate that scenario (1) serves only the users that are initially allotted to it by the controller. On the other hand, scenario (2A) is liable to serve more users than scenario (1) because in addition to the users originally allotted by the controller, the sub-group may include some DSP s also. But, Scenario (2B) supers (2A) because the sub-group can include users from other subgroups in addition to the users allocated originally. Since the number of DSP s are quite small compared to the number of users in a sub-group, there is a drastic increase in the number of users serviced in case of (2B). The results are derived out of mathematical inference.

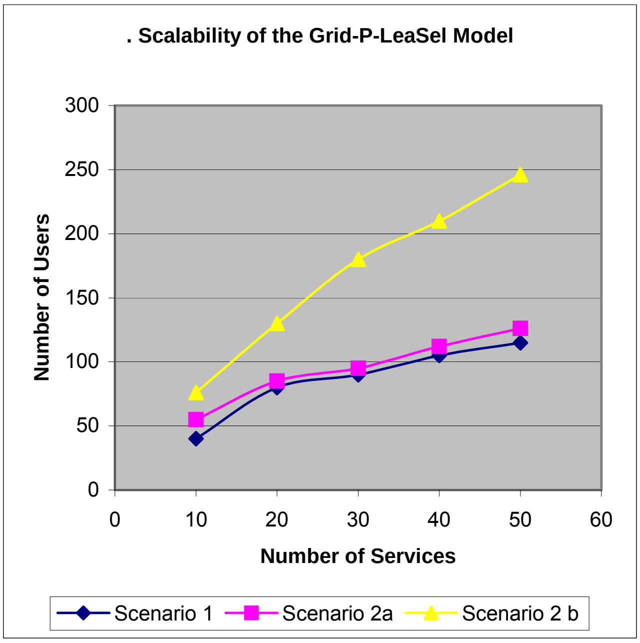


Fig. 7. Scalability of the G-LeaSel Model.

Mathematical Inference

Let the 'n' users be split across 'm' subgroups. Let u [1: m] denote an array which denotes the number of users in each sub group. Let xi denote the no of services offered in the i th Subgroup. Let yi denote the number users obtaining services in i the subgroup. The number of users in a subgroup depends on the number of services offered and the converse is also true.

No of services in subgroup i,

$Si = k\ (u[i] + kj);\ j=1,2,\ 0 \le kj \le n$

Scenario 1: $yi= u[i]$

Scenario 2a: $yi=u[i]+k1$ *where* $0 \le k1 \le m-1$

Scenario 2b: $yi=u[i] +k2$ *where* $0 \le k2 \le n-u[i]$

As can be inferred, the scenario 2b scales better i.e. supports large number of users since n is much greater than m.

Self-Stabilization

. For a group of 30 members, the members are equally divided into three subgroups and are placed under three different Deputy Service Providers. The packet delivery rate is set to 50 packets/sec. The time taken to distribute 450 packets to the members when there is a fault at the entity and when there is no fault are experimentally determined (figure 8). Without any fault, the number of packets per second is constant and this depicts the ideal situation. In the Centralized approach, key generation and distribution due to fault at the central KDC node is to be done over a large number of nodes and this overhead increases the number of packets sent per second. In Grid-P-LeaSel, the key generation and redistribution have to be done only to the nodes under the faulty subgroup. This reduces the overhead present in the centralized approach to an appreciable level. The results are shown in Figure 8, for single and three faults for Grid-P-LeaSel.

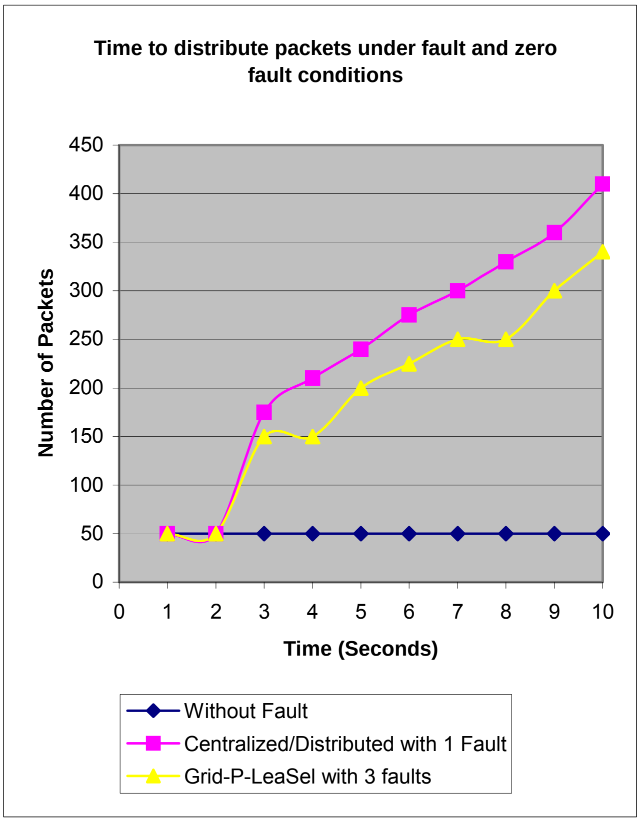


Fig. 8. Time to distribute packets under fault and zero fault conditions.

Mathematical Inference of Self Stabilization Property

In the Grid-P-LeaSel multicast model, there is a decrease in the percentage of the multicast service affected, when the number of Deputy Service Providers is increased and the percentage of the multicast service affected follows the equation

$$y = 100x^{-1.0001}$$

It is obvious that, in the Centralized approach, 100% of the multicast service is affected when there is a fault. Figure 8 shows that the Grid-P-LeaSel model is less affected due to fault and the model stabilizes within a few seconds. On the other hand, the results also show that the Centralized approach does not possess the self-stabilizing property and is not tolerant to faults.

Throughput Based on Group Formation Scenarios

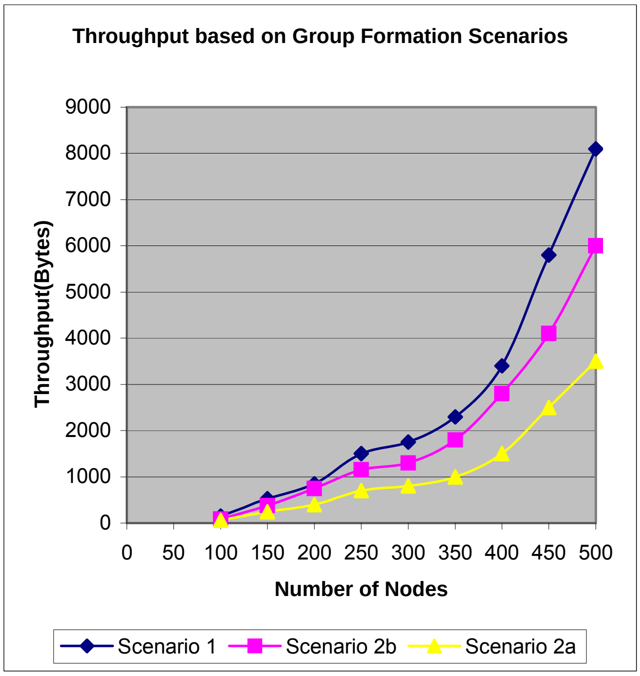


Fig 9. Throughput based on Group Formation Scenarios.

The throughput was also analyzed separately for subgroups formed based on the different group formation scenarios. The results indicate that (2A) provides the lowest throughput since it involves considerable overhead at the DSP, in getting the service from another subgroup and then multicasting it to its users. (1) Offers the best throughput since it involves no additional overhead. (2B) offers an intermediate level of throughput since it involves some overhead in transferring the users to the subgroup, where the requested service is available. The results are derived out of mathematical inference.

Mathematical Inference

Scenario 1: is comparable with the centralized approach. Let the throughput of such a subgroup be 'C'.

Scenario 2a: is comparable with the P-LeaSel model. Let the throughput of such a subgroup be 'L'

Scenario 2b: is an intermediate between the two and so its throughput 'I' is

$$L < I < C$$

Hence $I = L + s1$ and $I = C – s2$

s1, s2 are variances in throughput for the Scenario 2b. Taking Tc as the minimum time taken for data to reach all nodes, $TI=T_C+ 4V$, where V is the total no of subgroups from which nodes are in 2B.

$$TL=2T_C$$

Fixing T_C from Centralized approach results, the other two can be fitted.

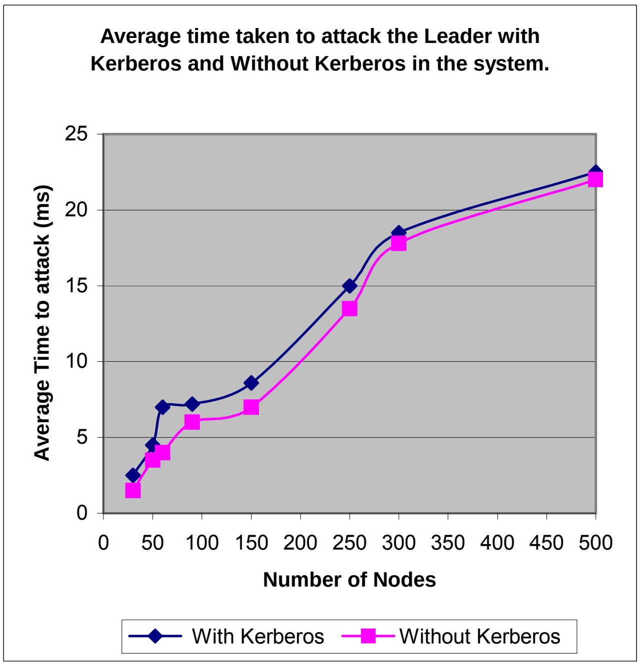


Fig. 10. Average time taken to attack the Leader with Kerberos and Without Kerberos in the system.

The model was also tested by introducing Hackers into the system. The Hackers carry out various security attacks. The average time for attack was measured under two conditions, namely with and without Kerberos. It was found that the average time to attack was higher when Kerberos was incorporated, as shown in Fig. 10. The single sign-on mechanism of Kerberos requires the use of a host's private key only once. Hence, same TGT can be reused for different services and possibility of spoofing by capturing authentication data is reduced greatly Moreover, the model hides dynamically changing services behind the Controller (acting as AS) and any external hacker can get into the system only after a breaking a rigid authentication protocol. This indicates that the model benefits from the use of a proven authentication protocol and offers stable performance under different circumstances.

10. Conclusion and Future Work

The P-LeaSel model was modified to suit to securely multicast messages in the Grid environment. The model was designed, simulated, tested and analyzed in terms of complexity, overheads and throughput, for all the multicast events in the Grid environment. The model also provides the crucial Sender anonymity, which is becoming increasingly important in secure application throughout the world. The architecture is also comprehensive in its coverage of all scenarios that may arise in group communications over the grid. It also goes to prove the adaptability of the P-LeaSel model for different environments.

The Grid-P-LeaSel proves to be potential choice for a secure multicast security model for grid. This is a hortatory stride forward towards solving the security problem for a wide class of applications.

Thus, Grid-P-LeaSel with Kerberos as authentication protocol strengthens up the security level of the system and proves to be a potential choice for a secure multicast security model for grid. This is an encouraging step forward towards solving the security problem for a wide class of applications.

This is an encouraging stride forward and future work will be aimed at optimizing the performance of the model in terms of computational complexity and load balancing, which is indispensable in the grid environment.. Future research will also be targeted at solving resource allocation problems within this model using operation research techniques.

References

[1] Elijah Blessing. R, Rhymend Uthariaraj V., "Leasel: A Highly Secure Scalable Multicast Model", WSEAS Transactions on Computers, Issue 2, Vol.2 April 2003, (pp 349-354).

[2] Elijah Blessing. R, Rhymend Uthariaraj V., "Evaluation and Analysis of Computation Complexity for Secure Multicast Models", Lecture Notes in Computer Science, Vol.2668, (pp 684-694), Springer Verlag Publication, 2003.

[3] Elijah Blessing's, "Design and Analysis of Secure Multicast Models for Wired and Mobile Networks", Ph.D thesis submitted at Anna University, 2004.

[4] Elijah Blessing. R, Rhymend Uthariaraj V., "Leasel: An efficient Key Management Model for Scalable Multicast System", in Proceedings ICORD 2002, December 2002.

[5] Elijah Blessing. R, Rhymend Uthariaraj V., "Secure and Efficient Scalable Multicast Model for Online Network Games", in Proceedings of 2nd International Conference on Applications and Development of Computer Games, ADCOG 2003, (pp 8-15)

[6] Elijah Blessing, Rhymend Uthariaraj V., "Fault Tolerant Analysis of Secure Multicast Models", in Proceedings of IEEE International Conference ICICS-PCM 2003, Dec. 2003, Singapore.

[7] Maziar Nekovee, Marinho P. Barcellos, Michael Daw, "Reliable multicast for the Grid: a case study in experimental computer science", Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, Volume 363, Number 1833, Pages 1775 - 1791, August, 2005.

[8] I. Foster, "What is the Grid? A Three Point Checklist", GRID Today, July 20, 2002.

[9] "Introduction to grid computing with globus", ISBN 0738427969, IBM Corporation, 2003.

[10] Von Welch, Frank Siebenlist, Ian Foster1, John Bresnahan, Karl Czajkowski, Jarek Gawor, Carl Kesselman, Sam Meder, Laura Pearlman, Steven Tuecke, "Security for Grid Services ", Proceedings of the 12th IEEE International Symposium on High Performance Distributed Computing (HPDC'03)

[11] Neuman, B. C. and Ts'o, T., "Kerberos: An Authentication Service for Computer Networks", IEEE Communications Magazine, 32 (9). 33-88. 1994.

[12] Broadfoot P. and Martin A., A,"Critical Survey of Grid Security Requirements and Technologies", Technical Report PRG-RR-03-15, Oxford University Computing Laboratory, August 2003.

[13] Anjan Pakhira, "Computational Steering on the Grid using DIVE", thesis submitted for MSc in High Performance Computing, The University of Edinburgh, September 2003.

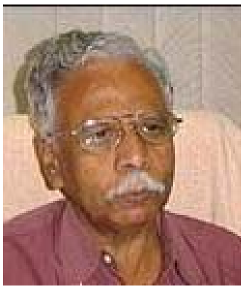
[14] I. Foster, C. Kesselman, G. Tsudik, and S. Tuecke, "A security architecture for computational grids," in Proc. 5th ACM Conf. Computer and Communications Security, 1998, pp. 83–92.

[15] R. Butler, D. Engert, I. Foster, C. Kesselman, S. Tuecke, J. Volmer, and V.Welch, "A national-scale authentication infrastructure," IEEE Computer, vol. 33, no. 12, pp. 60–66, Dec. 2000.

[16] Mary Vennila S, Vinoth Chandar, Vinoth Govindarajan, Sankaranarayanan V and Rhymend Uthariaraj V, "Kerberized LeaSel Model for Grid**",** IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.9A, pp. 154-160, September 2006.

[17] Mary Vennila S, Vinoth Chandar, Vinoth Govindarajan, Sankaranarayanan V and Rhymend Uthariaraj V," PLEASE, 'P'-LEAder SElection for Multicast Group Communication**,** IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.11, pp . 277-282, November 2006.

Mary Vennila .S received the M.Sc (Computer Science) from Bharathidasan University and M.Phil (Computer Science) from Mother Therasa University. She is now working as a Senior Lecturer in the Department of Computer Science in Presidency College, India. Her research area includes Network Security, Adhoc Networks, and Grid Technology.



Dr. V Sankaranarayanan received the PhD from Indian Institute of Technology, Chennai, India. He had worked as a Professor & Director at Anna University, Chennai, India and the last position he hold was Director, Tamil Virtual University, Chennai, India. At present he is working as a Director, Crescent Engineering College. He has completed many commendable projects. His research area includes Computer Networks, OOP and Optimization.