Trust based Leader Selection Methodology for P-LeaSel: a Multicast Group Communication Model

Mary Vennila S
Associate Professor
Department of Computer Science
Presidency College, Chennai, India

ABSTRACT
Multicast is an internetwork group communication service which reduces the transmission overheads. The data can be secured by encrypting it with a group key, shared among all group members [6]. Whenever members join/leave in a group communication, it is essential to preserve the forward and backward confidentiality by sending new keys for transmission. When members join/leave frequently, it gives rise to transmission overhead. Leasel is a multicast group communication model which addresses the problem of scalability due to the multicast transmission overheads. Being a de-centralized group model, a top ranking member of the sub-group is designated as a Leader and authorized to perform key generation and distribution. The identity as "Leader" is hidden to the sub group members. The P-Leasel model, instead of a single leader, identifies 'p' leaders and is alternated for every transaction. Any one leader from the 'p' leaders is authorized to perform key management. This study proposes a trust based leader selection methodology by analyzing trust in selecting Leaders for key generation and distribution. In addition to selecting Leaders based on the static trust computation, allowing the controllers to judge the trustworthiness of leaders dynamically, making better use of the received recommendations directly and indirectly. The simulation experiments show improvements in the security aspects which makes P-Leasel more secured multicast group communication model.

General Terms
Security, Multicast

Keywords
LeaSel, P-LeaSel, Trust, Group Communication, Multicast Security.

1. INTRODUCTION

The inherent advantage of multicast communications over unicast communications has attracted the Internet community to adopt the multicast technique for group communications [10]. With the widespread use of the Internet, securing multicast communications is very essential. A multicast security infrastructure preserves authentication and confidentiality for all group communication so that only registered senders can send packets and only registered receivers can receive packets in the group[14]. Data encryption ensures message confidentiality since there is no network level access control in the Internet. This requires a group key management protocols to distribute and manage encryption keys with the registered members of the group or service [8]. Similarly, authentication schemes verify the authenticity of the received packets.

Most researchers on secured group communication have focused on the architecture of secured groups and in the problems of group key management [13]. The great challenge to them had been the development of multicast models which preserve forward and backward confidentiality, computationally efficient, to remove crucial point of failure, to solve '1 affects N' scalability problem, and exhibit self-stabilization property [12]. In the literature, different approaches were proposed which solves one problem or the other.

Secure multicast communication involves issues like forward and backward confidentiality, as dealt in [7]. In a multicast group, whenever members join and leave during the course of a session, then the encryption key should be updated for every join and leave operation to prevent the former group member accessing the future communications (forward confidentiality) and a new member accessing the past communications (backward confidentiality)[15]. Moreover, when a member joins or leaves the group, it affects all other members of the group. This is referred as "1 affects n" scalability problem [10].Thus the essential components for secure multicast are group membership control, secure key distribution and secure data transfer [6].

P-LeaSel multicast model is a distributed subgroup model in which a leader selected from the set of 'p' leaders, performs the key generation and distribution. This is an extension of LeaSel, a secured scalable distributed sub-group model [1]. In these models, the leader selection methodology plays an important role. This paper proposes a trust based leader selection methodology which makes P-LeaSel more secured multicast group communication model.

Selecting Leaders based on trust in an important step in achieving security to P-LeaSel model. In this context, without human judgment, the challenge for controllers is to distinguish other peers' identities and behaviors autonomously. In our earlier research [4], it is proposed a deterministic trust management scheme for leader selection; in which the deputy controller/ group controller can independently handle the trust issues under the absence of a central management. Due to the dynamism of the environment a direct and indirect way of computing the trust is investigated in P-LeaSel model. To this effect, a trust management scheme is proposed which co-operating with all the nodes and collect the trust values. This trust management scheme provides a mechanism of allowing neighbor nodes to judge the trustworthiness of the node in which you are interested to calculate the trustworthiness.

2. P-LEASEL OVERVIEW

The architecture 'P-LEASEL' is an adopted version of LeaSel architecture, already proposed for both wired and wireless environment [1].

LeaSel model is mathematically proven model and has been verified through implementation [2]. In LeaSel, though the identity of the leader is kept secret and is known only to the deputy controller, a proper traffic analysis can reveal the identity of the leader. A Leader is changed either at the end of the session or when hacked. If it is hacked, then the Leader Selection Algorithm is executed to find the next Leader. This introduces a small delay in the session. LeaSel did not follow any special authentication mechanism for initial member join event. This makes LeaSel vulnerable to external hackers. To overcome these pitfalls, an extension of LeaSel model called P-LeaSel[1] has been introduced by the author, incorporating the concept of 'p' leaders. This model, instead of selecting a single leader, selects 'p' leaders of top remarks. This ensures a greater security and increased availability.

The Leader selection algorithm in P-LeaSel differs from LeaSel. Instead of a single leader, the Deputy Controller selects a set of 'p' leaders. At a given time, only one of them acts as a leader and the leader is alternated for every transaction. Thus, the 'p'-Leaders share the key management work load among them. Moreover, attacking this sub group becomes 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 [1]. Thus the model achieves high scalability with secure key generation and distribution. Authentication by the controller makes the system to be secured from external hackers. Hence this model is not easy to attack. Thus the model achieves high scalability with secure key generation and distribution without compromising the design requirements, making it an efficient model.

The key management and distribution process is distributed among a set of 'p' leaders who are faithful members selected from the sub-group and this process is hidden from all other members of the sub-group. Based on the capability credentials, the Deputy Controller decides the rank of the members in the sub-group and identifies a set of 'p' leaders. The Deputy Controller selects one from the set of 'p' leaders as a leader and authorizes it to perform key generation and distribution. The Leader is alternated for every membership transaction. Moreover, only the Deputy Controller knows the active leader and it is hidden from all the members of the sub-group.

Now the 'Leader' becomes more critical by means of security and availability. The capacity credentials based selection of leaders often reduces the trust of the group communication. Hence the trust of the leaders becomes an important parameter to be considered in the leader selection. This paper proposes a leader selection methodology for P-LeaSel, taking trust of the Leaders worthiness into consideration.

3. TRUST BASED LEADER SELECTION IN P-LEASEL

The P-LeaSel multicast model in conjunction with the trust computation for leader selection is given in figure 1. The Central controller and the deputy controllers jointly perform the multicast group communication. The authentication mechanism in this model besides authenticating the users also maintains a black-list of malevolent nodes [9]. The Black listing helps to prevent malicious nodes from re-entering into the system exploit any vulnerability. The trust computation system proposed for the selection of leaders in P-LeaSel improves the security further which makes it more secured multicast group communication.

3.1 Trust Calculation

The data communication between different entities in the internet has grown increasingly complex to analyse. Trust assessment in the recent internet era has become difficult even for personal human interactions though these interactions can have context and many other related cues. But still many forms of trust exist and evaluating them has been a challenge. Hence, assessing trust and its manifestation in computer communication has become a challenge. Trust assessment is accurate when enough evidence is collected for evaluation of trust. But collection of evidence without burdening the network is difficult [11,16].

Trust can be evaluated based on measures collected, based on the referrals or ratings from members in a community. Individual's subjective trust evaluation consists of the combination of received referrals and personal experience. Considering referrals can cause loops in the trust computation and hence in order to remove dependence and cycles only referrals based on first-hand experience along be considered [9]. As a consequence, an individual should only give subjective trust referral when it is based on first hand evidence or when second hand input has been removed from its derivation base.

Trust can relate to a group or to an individual. A group's trust can for example be modelled as the average of all its members' individual trust, or as the average of how the group is perceived as a whole by external parties.

Some fundamental objectives that were considered in designing the trustworthiness calculation of an entity, which is to be entrusted with the task of performing the function of a Leader, are:

- Identify information elements that are most suitable for deriving measures of trust in a given sub-group.
- Collection and capturing of the identified information elements.
- Resistant to attacks of manipulation by strategic agents.
- Inclusion of the information provided by such systems in the decision process.

These are important objectives required to determine the potential for trust in open groups.

3.2 P-LeaSel Trustworthiness Calculation

A centralized trust system is used. The information about the performance of a given participant is collected as ratings from other members in the sub-group who have had direct experience with that member. The central authority (trust centre/Deputy Controller) that collects all the ratings typically derives a trust score for every member.

Figure 2 below shows a typical centralized trust framework, where A and B denote members belonging to same sub-group with a history of transactions in the past, and who consider transacting with each other in the present in a group communication environment.

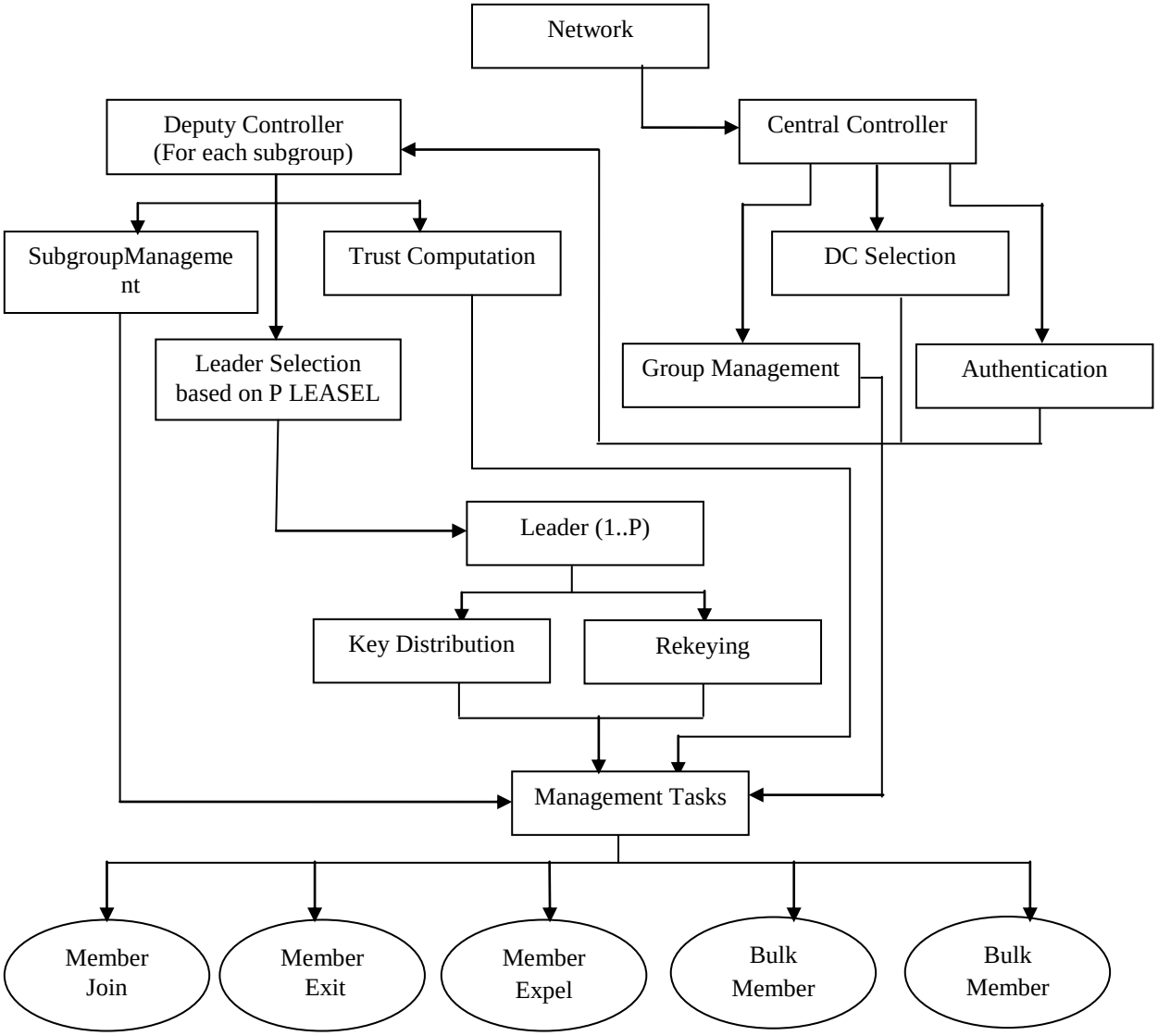

Figure 1: Trust based P-LeaSel Multicast Model

The two fundamental aspects of this centralized trust system are [9]:

(i) Centralized communication protocols which allow members to provide ratings about members to which it has transacted previously to the central authority.

(ii) A trust computation engine used by the central authority to derive trust scores for each member, based on received ratings, and possibly also on other information.

3.3 Trust Computation Engine

The procedure for computing trust scores is to compute a weighted average of all the ratings.

The rating weight can be determined by factors such as

- Rate trustworthiness.(w_1)
- Age of the rating.(w_2)
- Distance between ratings.(w_3)
- Current score.(w_4)

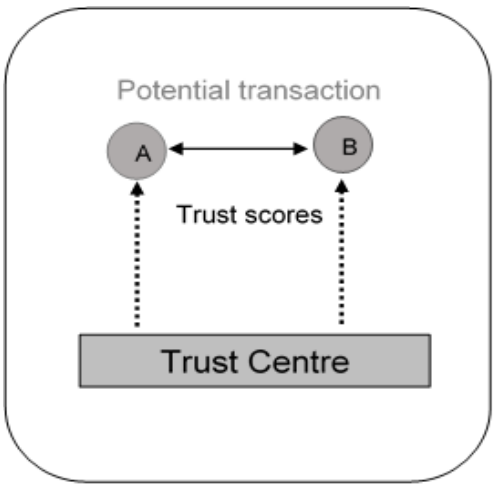

Figure 2: Centralised Trust Framework

The parameters for trust scores that are considered and reported to the central authority by the members are:

- Number of previous compromises.(s_1)
- Power capability.(s_2)
- Link stability.(s_3)
- Computational capability.(s_4)

The score of an member A given by i^{th} member is given by,

$$Score^{A_i} = \frac{s_2 + s_3 + s_4}{s_1}$$

By the formula, it can be inferred that a node with frequent history of compromises will have the lowest score. Depending on the situation, s_1 can also take absolute values like, 1 if it has no history of compromises and 0 otherwise. This will eliminate that particular member or node from being considered (since, its score will be 0, if s1 equals 0).The rating of a member A given by the i^{th} member is then calculated by the sum as given below:

$$Rating^{A_i} = (w_1 + w_2 + w_3 + w_4)$$

x Score A_i

The rating of the member A is then sum of all the ratings calculated.

$$Rating^{A} = \sum Rating^{A_i}$$

3.4 Leader Selection Algorithm

The algorithm for selecting a set of 'p' leaders is as given below:

Step 1: Periodically, the central authority (deputy controller) collects the scores from the members.

Step 2: Calculates the Ratings for every member belonging to its sub-group as described in the previous section.

Step 3: Sorts the Ratings by ranking the highest rated member as first rank and others subsequently (sorting in descending order with respect to Ratings).

Step 4: Chooses first 'p' members from the sorted list based on a heuristic threshold value. The first 'p' members in the sorted list falling above the threshold value form the set of 'p' leaders.

Step 5: The first member is chosen as the leader for the current session.

Whenever deputy controller initiates membership transaction, it performs the leader selection algorithm and updates the set of 'p' leaders as required. By monitoring the credentials of the members continuously, the DC updates the set of 'p' leaders as required. The threshold value for the leader selection algorithm is decided based on the application and the level of security requirement.

Leader Selection

During leader selection, a simple randomized leader selection algorithm is used [3]. It selects one leader among the 'p' leaders. The current leader is asked to stop and the new leader is activated.

$$DSP \rightarrow Old\ Leader: [STOP]_{KUoldleader}$$

$$DSP \rightarrow NL: [LEADERCHANGE||SA]_{KUnewleader}$$

where,NL is New Leader and SA is subgroup address.

4. PERFORMANCE OF TRUST BASED LEADER SELECTION

The Trust based leader selection methodology was incorporated into P-LeaSel with the above mentioned modifications and was implemented using ns2. The proposed trust based leader selection methodology on P-LEASEL model, was investigated in terms of security.

Keeping in mind the adverse influence of hackers on Internet, the security level of the P-LeaSel multicast model with the proposed trust based leader selection methodology is analysed. The security level of a model is determined based on the level of difficulty to hack the model. On an average, if the hacker takes more number of attempts to successfully hack the model then the security level is regarded as high. i.e., the more difficult to hack, the better is the security of the model.

An ratio of successful Hack attempt is a metric for testing the security of P-LeaSel model. It is defined as the number of successful Hacks by total Number of Hack attempts. Lower the value is, more secure the system is.

$$Ratio\ of\ Sucessful\ Hack\ attempts = No.of\ Successful\ Hacks\ /\ Total\ Hack\ Attempts$$

The implementation was carried out for all the essential three threat categories on the P-LEASEL model and the security improvements are plotted. Simulation results were traced for up to 2000 nodes for all the threats with and without the proposed trust methodology and the sample graphs are given in Figures 3, 4 and 5.

4.1 Simulation Results

A hacker is being simulated to test the resilience of the system against possible attacks. Three types of methods have been employed for this purpose – Snooping, Denial of Service and Information Disclosure [5]. The input of the system is to select the nodes as hackers within the sub group and the final result is aBoolean value representing whether the key has been compromised for that transaction.

4.1.1 Experiment: Snooping Attack

Snooping Attack is defined as the attack on the identity of the leader. If the information about the identity of the leader is disclosed then an armed hacker can launch attacks to compromise the leader. The identity can be found by snooping the traffic flowing out of member nodes as the leader will be transmitting many packets relatively (due to rekeying). Leader spoofing is an important threat in P-LeaSel, because a leader is one who is involved in the key generation and distribution process.

The simulation is carried out for a sub-group with different percentages of malicious nodes and then generalized for the whole system. The partially and fully armed hackers are made to launch attacks in such a way that the identity of the leader is disclosed. A snoop attempt is said to be successful if the random number generated and the sequence number of the packet are same. Observations are made for number of successful attempts for given different percentages of malicious nodes among the member nodes. The average result is plotted in figure 3.

If a leader is spoofed, the key generation and distribution process gets some malicious treatment. Figure 3 shows the

number of successful spoof attempts with the effect of number of nodes, with and without the trust based leader selection. The effect is around 2%.

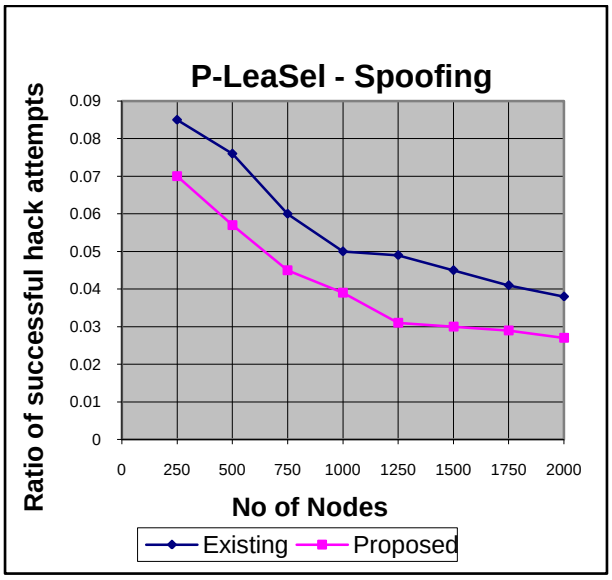

Figure 3: Spoofing Threat

4.1.2 Experiment: Information Disclosure Attack

Information Disclosure attack is defined as an attack on confidentiality of the packet carrying the session key during a re-keying operation. When the confidentiality is compromised then the information contained in the re-key packet is revealed enabling an external member to decrypt multicast messages sent only to the subscribers.

The simulation is carried out for a sub-group with different percentages of malicious nodes and then generalized for the whole system. The partially and fully armed hackers are made to launch attacks in such a way that the identity of the leader is disclosed. A hack attempt is said to be successful if the random number generated and the sequence number of the packet are same

This reasoning is justifiable as a partially or fully armed hacker can compromise and also there are no white or black boxes for security testing. Any vulnerability in a system is disclosed only after a successful hack attempt. Observations are made for number of successful attempts for given different percentages of malicious nodes among the member nodes. The average result is plotted in figure 4.

Information Disclosure, in our context is the exposure of the identity of the leader of a group. Regarding Information Disclosure, it is evident from the graph that nearly 5% of the leaders' identities are exposed when the number of nodes is 250. When the number of nodes scales to 2000 nodes, this reduces to about less than 1%, with and without the trust based leader selection.

4.1.3 Experiment: Denial of Service Attack

Denial of service is attack on the availability of the multicast service. The simulation is carried out for a sub-group with different percentages of malicious nodes and then generalized for the whole system. The partially and fully armed hackers are made to launch attacks in such a way that the service becomes unavailable to the subscribers or members of the sub-group.

The malicious node is made to flood the DC with join and leave requests. The DC gets engaged in servicing the counterfeit requests rather providing the multicast service to the members so that the service becomes unavailable.

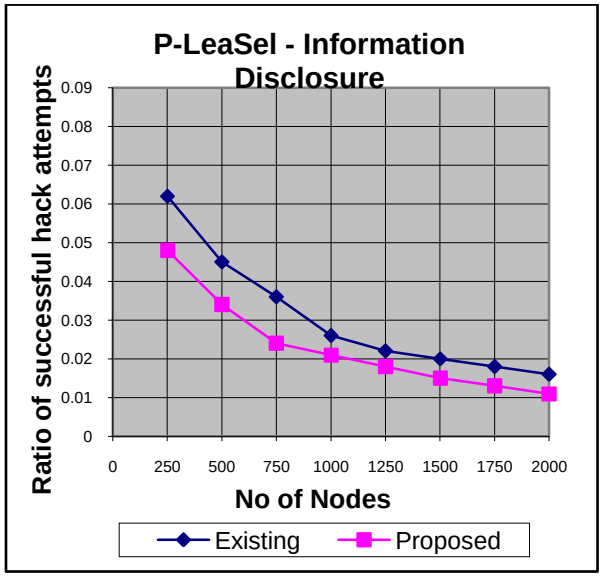

Figure 4: Information Disclosure Threat

Observations are made for number of successful DoS attempts for given different percentages of malicious nodes among the member nodes. The average result is plotted in figure 5.

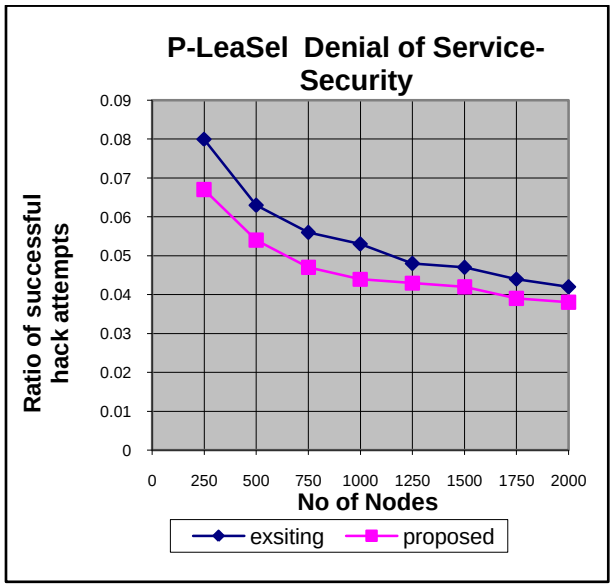

Figure 5: Denial of Service – Threat

Regarding the Denial of Service, P-LeaSel with trust based leader selection stands above. The ratio of successful hack attempts, which is around 0.08 for 250 nodes declines to nearly 0.04 as number of nodes reaches 2000.

5. CONCLUSION

The P-LeaSel model, with the proposed trust based leader selection methodology enhances the security of the model. The direct and indirect methods of trust calculation for the QoS parameters helps to selects the 'P' leaders effectively which in-turn improves the P-LeaSel model more secured for

multicast group communications. Assigning a security level to each node and performing a trust computation to decide on the most trusted node as the leader do election of a leader. The P-LeaSel model is used to perform the task of leader selection. If more than one leader is computed to be having a trust value fit for assigning it the leader status, one of the leaders are selected by using a random function and is giving the role of the leader. This brings about a great deal of security in it because the leader changes for each transaction and hence it is difficult to predict and hack the leader. Re-election of a P-leader is done on a periodic basis and hence the same leader is not valid for more than one transaction. The Trust based leader selection was implemented in the P-LeaSel multicast model and has shown significant improvement in resistance offered to attacks like snooping, information disclosure and denial of services. From the simulation results it is shown that the trust based leader selection methodology in P-LeaSel, reduces the internal threats like Leader Spoofing, Information Disclosure and Denial of service. It can be very well seen that the effectiveness of P-LeaSel is sustained even in the presence of security threats

6. REFERENCES

[1] Mary Vennila S, Sankaranarayanan V,(2006) , " PLEASE, 'p' Leaser Selection for Multicast Group Communication", IJCSNS : International Journal of Computer Science and Network Security, Vol. 6, No. 11, pp. 277-285.

[2] Elijah Blessing R, Rhymend Uthariaraj V,(2002), " LEASEL : An efficient key management model for scalable secure multicast system", in Procedings of ICORD, India

[3] Mary Vennila S, Sankararanarayanan V, (2007), " G-Leasel : A secure Multicast Model for Grid", IEEE Xplore, Communication Systems Software and Middleware (COMSWARE)

[4] Mary Vennila S, Sankaranarayanan.V,(2007), " Kerberized Leasel Model for Grid", IJCSNS International Journal of Computer Science and network security, Vol.6, No.9A,206 pp.154-160.

[5] Mary Vennila S, Sankaranarayanan V,(2008), " Threat Analysis for P-LeaSel, a multicast group communication model", Asian Journal of Information Technology, Vol.7, pp. 64-68.

[6] Mittra S,(1997), " IOLUS : A frame work for scalable secure multicasting", Procedings of ACM SIGCOMM, pp. 277-288.

[7] Sugnaya Devi D, Padmavathi G,(2010), " Secure Multicast key distribution for Mobile adhoc networks", International Journal of Computer Science and information Security, Vol. 7, No. 2, pp. 218-222.

[8] Ballardie T, Crowcroft J,(1995) "Multicast specific Secutity Threats and counter measures", Proc. Symposium on Networks and Distributed System Security, San Diego, California, pp. 216.

[9] Butler D, Engert D, Foster I, KesselmanC, Tuecke S, Volmer J, Welch V,(2000), " A national Scale authentication infrastructure" , IEEE Computer, Vol.33, No.12, pp.60-66.

[10] Liu Jing, Zhou Mingtian,(2003), " Secure group communication for large dynamic multicast group", Journal of Electronics, Vol. 20, No.4, pp. 418-422

[11] SivakamiPriya S, Sumathi G,(2013), " In improved Security and Trusting Model for Computational Grid", International Journal of Grid and Distributed Computing, Vol. 4, No.1, pp, 57-63.

[12] Bibo Jiang,(2008), " A survey of Group Key Management", International Conference on Computer Science and Software Engineering", pp. 994-1002.

[13] Hong X, Gerla M, Pei G, Chiang C,(1999), "A Group Mobility Model for Ad Hoc Wireless Networks". Proceedings of the 2nd ACM International Workshop on Modeling, Analysis, and Simulation of Wireless and Mobile Systems., pp. 53-60.

[14] D.Huang, D.Medhi, (2008), "A Secure Group Key Management Scheme for Hierarchical Mobile Adhoc Networks", Adhoc Networks, pp 560-577.

[15] Renuka, K.C.Shet, (2009), "Hierarchical Approach for Key Management in Mobile Ad hoc Networks," IJCSIS , Vol. 5 No. 1,pp 47-53.

[16] Jøsang, Audun, Roslan Ismail, and Colin Boyd, (2007), "A Survey of Trust and Reputation Systems for Online Service Provision," Decision Support Systems,Vol.43, No.2, pp 618-644.