An Improved Security and Trusting Model for Computational Grid

P.Sivakami Priya, Dr.G.Sumathi
Department of Computer Science, Department of Information Technology
Sri Venkateswara College of Engineering, Sriperambudur
Tamil Nadu,India
sivakamipriya@gmail.com , gsumathi@svce.in

Abstract

Grid Computing in today's world is a boon for high speed computing. Grids are composed from intersection of clusters, which provide huge volume of computing power. An environment with broadly distributed resources is liable to various types of security attacks. To solve this problem, we use P-LEASEL algorithm, which provides secure multicast communications in grid environment. Kerberos is used for authentication. Trust computing is incorporated to perform trust evaluation for the nodes to prevent the entry of malicious nodes in a group.

Keywords: *Grid computing, Kerberos, P-leasel, Qgrid, and Resource management*

1. Introduction

Grid computing is a term referring to the combination of computer resources from multiple administrative domains to reach a common goal. The goal is to allow the sharing of computing and data resources for a number of workloads and to enable collaboration both within and across organizations. In multicasting data can be secured by encrypting it with a group key, which is shared among all the members of the group. But whenever the group member joins or leaves, the group key has to be changed to preserve forward and backward confidentiality. It gives rise to scalability problem when there is a frequent member change [3]. Hence there is a need to design an efficient model for secure multicast communication. P-leasel model has been used to provide secure multicast communications in grid environment. P-leasel model 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 is used as the authentication protocol into the grid P-leasel model.

The main objective of grid computing is to promote resource sharing and cooperation among different parties. However, there remains a challenging problem faced by grid environments. Malicious or selfish nodes consume resource without making any contribution or even try to destroy the system deliberately [6]. This can severely reduce the performance of the system. To encourage resource sharing and fight against malicious behaviors, we use an adaptive resource management framework Qgrid, which concatenates trust factor into resource allocation mechanism. Each provider allocates resource according to the bidding price and trust value of a requester by controlling the corresponding threshold of price and trust value. The incomplete information is a key for provider in determining the two thresholds [1].We use a Q-learning technique to resolve the issue, which can adapt to the

dynamics of grid environments. We use an isolation scheme to secure the grid system by frustrating malicious participants from joining the system.

The rest of the paper is organized as follows. Section II presents related work. Section III describes the P-leasel model. Section III explains Qgrid in detail, which includes price determination of consumers, allocating mechanism of providers. Section IV presents the performance evaluation and section V concludes this paper.

2. Related work

Security in grid is provided by two mechanisms namely grid security infrastructure (GSI) and kerberos. GSI is based on public key infrastructure (PKI). It requires the two entities in communication to mutually authenticate those using digital certificate, before communication can commence.

Mary Vennila presented leasel model, which is a scalable, secure and distributed security model for group communication [2]. Leasel model has two trusted entities called deputy controller (DC), one per subgroup and the controller (CR) to manage and control groups and subgroups. The deputy controller manages each subgroup, and the controller manages all deputy controllers. The controller participates in the creation of a multicast group session, but does not take part during the key management of the session. When a member joins the group, the controller performs authentication and after approval the deputy controller prepares a rank list for all the members of the group [2].

The deputy controller alone knows the identity of the leader and it is hidden from all the members in the group. The deputy controller can change the leader dynamically to make the model more secure.

In leasel, the components of secure multicast are performed by deputy controllers and leaders. The identification of leader is a critic issue in leasel. Though the identity of the leader is hidden from group members, through proper traffic analysis the identity of the leader can be disclosed. Also the leader single-handedly manages the key distribution process, thus over loading it.

The primary advantage of distributed shared clusters like the grid and planet lab is their ability to pool together shared computational resources. This increases the throughput because of statistical multiplexing and the bursty utilization pattern of typical users [12].

However resource allocation in these systems remains as a major challenge. The problem is how to allocate a shared resource both efficiently and fairly. In price-anticipated scheme in which a user bids for a resource and receives the ratio of his bid to the sum of bids for that resource. This proportional scheme is simpler, more scalable, and more responsive than auction-based schemes. Suppose that there are m users and n machines. Each user can be continuously divided for allocation to multiple users. An allocation scheme $w=(r_1,.....,r_m)$,where $r_i=(r_{i1},...,r_{in})$ with r_{ij} representing the share of machine j allocated to user i, satisfies that for any $1<=j<=m$ and $1<=j<=n, r_{ij}>=0$.

In price anticipated mechanism each user places a bid to each machine, and the price of the machine is determined by the total bids placed. Formally, suppose that user i submit a non-negative bid x_{ij} to machine j. The price of machine j is set to the total bids placed on the machine j. When $Y_j = 0$, i.e. When there is no bid on a machine, the machine is not allocated to anyone .The additional consideration is that each user i has a budget constraint x_i. Therefore, user i's total bids have to sum up to his budget. The budget constraints come from the fact that users do not have infinite budget. Pricing schemes approach fall in the hard incentive category in which resource allocation is solely based on bidding price of

consumers with the higher price a node is able to get more resources. However only considering the bidding price cannot fight against malicious behaviors.

3. Security in grid computing

3.1. P-leasel model

P-leasel model is an adopted version of leasel model. As shown in figure.1, instead of a single leader, the deputy controller selects a set of P-Leaders [3]. At a given time, only one of them acts as a leader and the leader is alternated for each and every transaction. Thus the P-leader shares the key management workload 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 performed by the 'p' leaders of the group and it is completely hidden from the group members. Thus the model has high scalability with secure key generation and distribution.

The controller distributes the individual member key k to all the members of the group in advance. Then the controller prepares the group access control list (GACL) and the subgroup access control list (SACL). The SACL is distributed to the deputy controllers. The access control list contains the time duration and session for which the group member is authorized to receive the multicast data. The controller generates group key (GK) and shares it with deputy controller. [3]

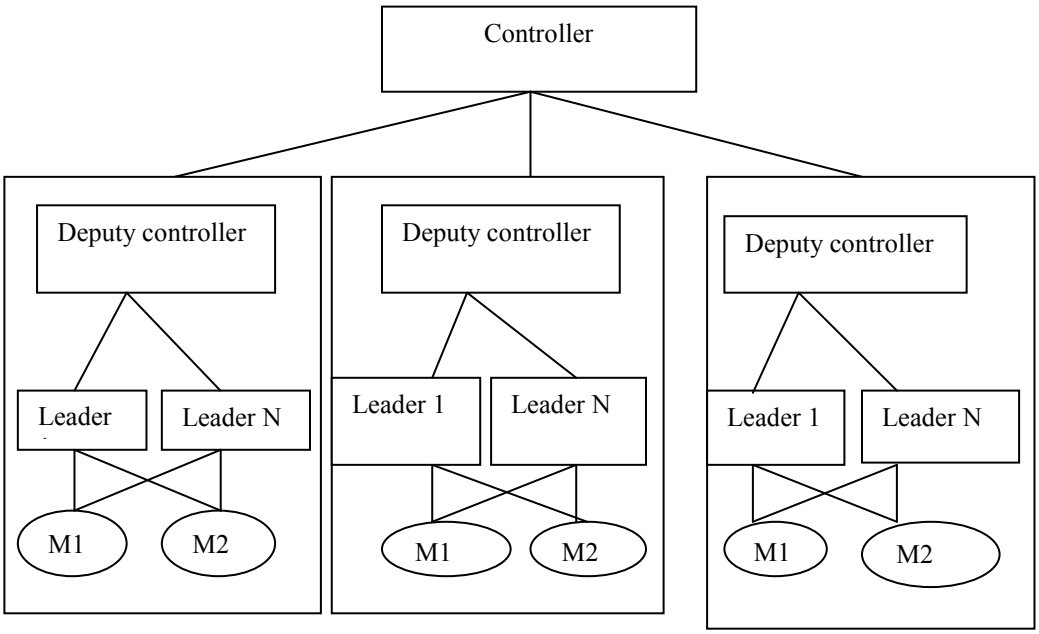

Figure 1. P-leasel model

Grid-P-leasel, is an adopted version of the P-leasel model for the grid, is used to provide secure multi cast 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. This model addresses 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. The group formation is dynamic. New users can join the group to get the services and users may also leave the group.

One node is designated as the controller and it provides the overall multicast security service. Service providers, one from each sub group, are designated as deputy service providers(DSP). DSPs provide access to all other service under them. They rank the other members of the sub-group and select pi numbers of thrust worthy members as leaders and assign one among them as Li, the current leader of the sub-group and alternated them for every transaction. The Controller and the DSPS share a common group key GK. Each subgroup has a common subgroup key Ski. Each node has its own private key, PK. There is a GACL at the controller, which stores the details for authenticating users, user private keys and other pertinent details. The controller distributes part of GACL as SACL to the DSPs, which use it also for determining if a user is authorized 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. [2]

3.2. Kerberos

P-leasel model does not have any special authentication protocol. But adaptation of the model for an environment such as the grid entails a secure authentication protocol. Kerberos can be plugged in as the authentication protocol into the grid-P-leasel model. [4].This would strengthen the security of the grid-P–leasel model, providing robust authentication and also provide single sign-on feature there by reducing the workload of the Controller. What make kerberos the automatic choice is that the entities used in kerberos can be mapped entities in grid-P-leasel. Here, the functions of authentication server (AS) and ticket granting server (TGS) are fixed with the Controller and the deputy service providers respectively as illustrated in figure.2. Thus, plugging in kerberos to grid-P-leasel improves the security of the model vastly with minimal additional complexity.

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 allows 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 multi cast services in grid-P-leasel involves joining the subgroup and holding the sub group key. DSP performs the verification with the SACL and sends an Approval Ticket (AT) [4]. 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.

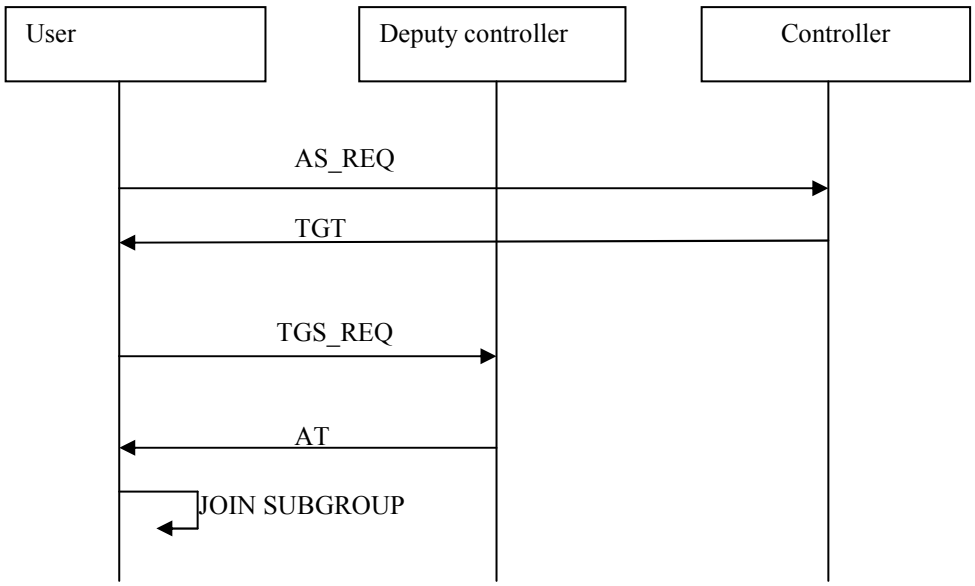

Figure 2. Authentication using kerberos

4. Trust in grid computing

4.1. Qgrid

Nodes in grid domain need to transact with each other strange nodes to acquire the service provided by other nodes. Recently trust has been recognized as an important factor for grid security. It is important to make trust evaluation for those strange nodes before transaction because some nodes may be dishonest. Some malicious nodes contribute high trust value through numerous good interaction behaviors at first and then change to attack. To address the issues an adaptive resource management framework based on Q-learning technique, named Qgrid, which encourage resource sharing and fights against malicious behavior. Integrating trust into resource allocation process, Qgrid deploys different roles of consumers and provider. Consumers try to maximize their own benefits under constraint of budget and deadline. Providers allocate resources according to bidding price and the trust value of a requester by controlling the corresponding threshold of price and trust value. Qgrid formulates the decision problem for resource consumers and providers respectively and then gives an appropriate solution for the corresponding optimal decision policy, which makes nodes have enough incentive to stay and play in the grid [1].

The incomplete information is a key issue for a provider in determining the threshold of price and trust value. Exploiting Q-learning technique, we introduce learning capability to providers, by which they are able to infer the dynamics of the grid environment, and to adjust their threshold efficiently.

4.2. Qlearning algorithm

Q-learning is a recent form of reinforcement learning algorithm. Reinforcement learning is a process in which a node senses a world, takes actions in it and rewards and punishments from reward function based on the consequences of the action it takes. By trial

and error, the node learns to a decision policy. Q-Learning works by learning Q-value function and Q- value as associated with state action pair. Q-Learning is a training to learn about unknown environment. Exploiting this Q-Learning technique in grid, Sink nodes will have the good learning capability, by which they are able to infer the dynamics of the grid environment then adjust threshold setting policies efficiently. The distinctive feature of Q-learning is its capability to choose between immediate reward and delayed reward [1].

STEP 1: Set the gamma parameter, and environment rewards in matrix R.
STEP 2: Initialize matrix Q to zero.
STEP 3: Select a random initial state.
STEP 4: Select one among all possible actions for the current state.
STEP 5: Using this possible action, consider going to the next state.
STEP 6: Get maximum Q value for this next state based on all possible actions.
STEP 7: Compute: Q(state, action) = R(state, action) + Gamma * Max[Q(next state, all actions)]
STEP 8: Set the next state as the current state.

5. Integration of security and trusting in grid computing

Plugging in security and trusting in grid Computing improve the performance of grid System and encourage resource sharing and cooperation among different nodes. The average time to attack a system with kerberos will be higher when compared to attacking a system without kerberos because the single sign on mechanism of kerberos requires the use of a host's private key only once. Hence the same ticket granting ticket can be reused for different services and possibility of spoofing by capturing the authentication data is reduced greatly. Moreover in P-leasel model, the attacker has to attack the set of 'p' leaders to break the rigid. Introducing learning capability into providers will deal with system dynamism and adjust their behavior efficiently and increases the resource utilization as well as fight against malicious behaviors.

The experimental setup consists of a node moving in a discrete state space represented by a grid where each state is represented by a cell in the grid as shown in figure.3. The grid contains terminal states represented by goal states and obstacles represented by walls. If the node tries to transit from one state to another and hits a wall instead then the node is penalized and stays in the same state. There is a path cost associated with every transition that the node makes from one state to another. The aim of the node is to find that path to the goal state which has least cost associated with it.

Q Learning is a model free algorithm that maintains the values for the state action pairs, called Q values, it experiences. The action in each state is chosen according to the €-greedy policy. It uses a parameter called as learning rate, α is used to update the Q values for each state it experiences.

In a noisy environment the node executes an action but does not reach the desired next state. Instead, the node is pushed against its will to any of its neighboring states with certain probability as shown in figure.4. Under such a noisy environment the node might execute the optimal action yet end up in a bad state or receive a penalty.

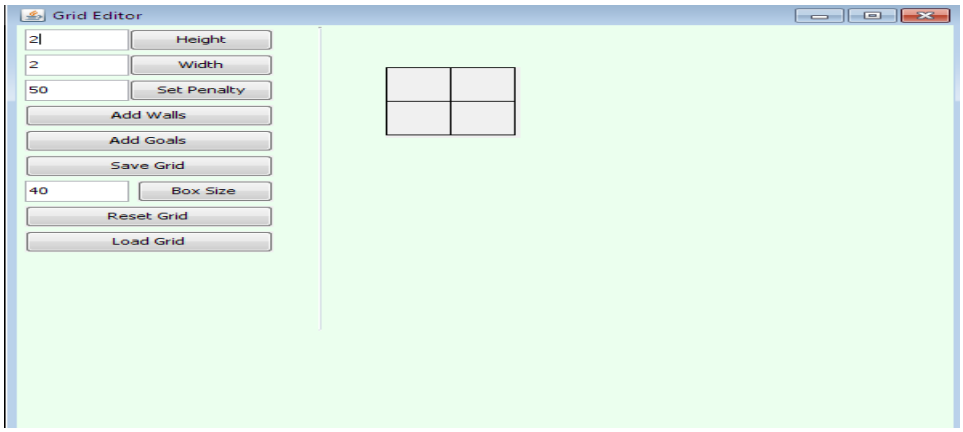

Figure 3. Creation of grid

To model the noise in the environment a parameter named 'pjog' is used. Each state has a finite number of successors, N. If in a particular state s the agent decides to perform action a then the agent will end up in the valid successor of s with a probability equal to (1-pjog) and end up in any one of the N-1 successors.

Learning rate determines how much current Q-value is changed on the basis of new observation. Learning rate can take value between 0 and 1. In noisy environment, high learning rate would not allow the system to stabilize and low learning rate makes learning very slow. Thus decaying learning rate is used in such case. According to this scheme the agent interacts with the environment with a very high learning rate initially so that it can quickly settle down to a near optimal policy. As the agents interactions with the environment increase the learning rate decays and the agent now makes only minor modifications to its near optimal policy to obtain the optimal policy.

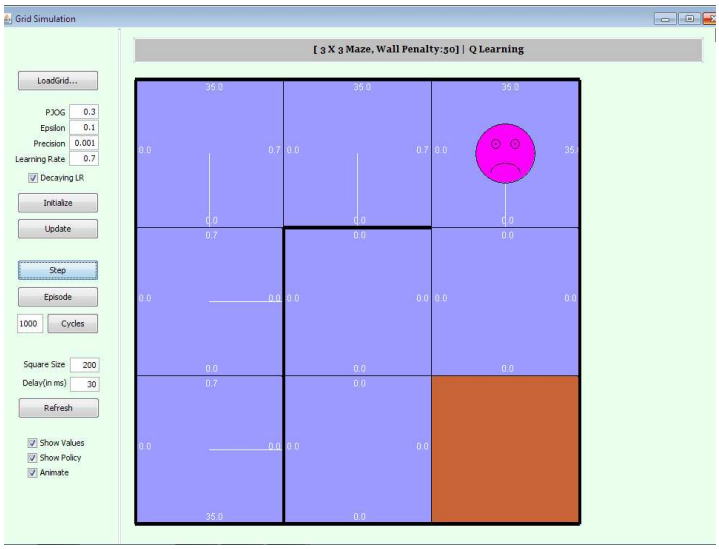

Figure 4. Qlearning

6. Conclusion

The main objective of grid computing is to encourage resource sharing and cooperation among different nodes. It is very difficult, however, in view of several challenges that arise in real grid environments. An environment with widely distributed resource such as grid is in need of security and trusting as it is prone to various security attack and malicious activities which degrades the performance of the system. Hence the security is provided using P-leaSel model with kerberos plugged into it and trusting is done by adapting Qgrid Framework

References

[1] Jinpeng Huai and Li Lin (2009), 'Qgrid: An adaptive Trust Aware Resource Management Frameword', IEEE SYSTEMS JOURNAL, Vol. 3, No.1.

[2] Mary Vennila and Sankaranarayanan V. (2008), 'P-LeaSel for Grid Environment', IJCSNS International Journal of Computer Science and Network Security, vol. 8, No. 4.

[3] Mary Vennila,Srinivasan S,Rangarajan T.C,Rhymend Uthariaraj and Sankaranarayanan V. (2006), 'PLEASE, 'P'-LEAder Selection for Multicast Group Communication ', IJCSNS International Journal of Computer Science and Network Security, vol. 6,No. 11.

[4] Mary Vennila, Rhymend Uthariaraj and Sankaranarayanan V. (2006), 'Kerberized LeaSel model for grid', IJCSNS International Journal of Computer Science and Network Security, vol. 6, No. 9A.

[5] Kevin Lai, Li Zhang, and Michal Feldman (2005),'A price anticipated Resource Management Framework,ACM.

[6] Jinpeng Huai,Li Lin,Yu Zhang(2007), 'Sustaining Incentive in Grid Resource Allocation:A Reinforcement Learning Approach',IEEE International Symposium on Cluster Computing and the Grid'.

[7] Doug Olson,Robert Cowles(2002), 'CA-based Trust Model for Grid Authentication and Identity Delegation' , GWD-C.

[8] DaSilva, Luiz A, Mohamed Tamer(2010), ' Adaptation of Reputation Management Systems to Dynamic Network Conditions in Adhoc Networks' IEEE Transactions of Computers, Vol.59, No.5.

[9] Y.Zhang, L.Lin, and J.Huai, "Balancing trust and incentive in peer-to-peer collaborative system," Int. J.Netw.Security, vol. 5, no.1, pp.73-81, jul.2007.

[10] R.Buyya and S. Vazhkudai, "Compute power market:Towards a market-oriented grid," in proc. 1st Int. Symp. Cluster Comput. Grid, 2001, pp. 574-581.

[11] L. P. Kaelbling, M. Littman, and A. Moore, Reinforcement learning: A survey, Journal of Articial Intelligence Research, vol. 4, pp. 237–285, 1996.

[12] M. Feldman, K.Lai, and L.Zhang, "A price- anticipating resource allocation mechanism for distributed shared clusters," presented at the ACM E-Commerce Conf., Vancouver, BC, Canada, 2005.

Authors

P.Sivakami Priya obtained her B.Tech degree in Information Technology from National Engineering College, Kovilpatti, and currently pursuing M.E in computer science in Sri Venkateswara College of Engineering. Her research interest is grid computing.

Dr.G.Sumathi obtained her B.E. degree in Electronics and Communication from Bharathidasan University, M.E. degree in Computer Science and Engineering from Regional Engineering College, Tiruchirappalli and Ph.D in Computer Science and Engineering from National Institute of Technology, Tiruchirappalli. She had been trained at Carnegie Mellon University, Pittsburgh, U.S.A. Presently, she is working as a Professor in the Department of Information Technology, Sri Venkateswara College of Engineering, Sriperumbudur, Tamil Nadu, India. She is the life member of ISTE. Her research interest includes grid & cloud computing and clusters.