Ant based Resource Discovery and Mobility Aware Trust Management for Mobile Grid Systems

Arjun Singh
Computer Science & Engineering Department
SGVU Jaipur
vitarjun@gmail.com

Prasun Chakrabarti
Computer Science & Engineering Department
Sir Padampat Singhania University,Udaipur
prasun.chakrabarti@spsu.ac.in

***Abstract*— In Mobile Grid systems, the automatic service deployment initially requires the node discovery. Most of the existing security mechanisms on Grid systems rarely consider the mobility of the nodes which may affect the applied security mechanisms leading to insufficient and inaccurate security. In order to overcome these issues, in this paper, we propose an ant based resource discovery and mobility aware trust management for mobile grid systems. Initially the super-grid nodes are selected in the network using ant colony optimization based on the parameters such as distance, CPU speed, available bandwidth and residual battery power. These selected nodes are utilized in the resource discovery mechanism. In order to maintain strong security with mobility management system, a proficient trust reputation collection method has been adopted. By simulation results, we show that the proposed approach is efficient and offers more security.**

Keywords— reception power ; transmission power; wavelength; transmitter gain; i receiver gain ; super node; mobile grid

I. INTRODUCTION

A. Mobile Grid

GRID technology is a new paradigm which has the potential to completely change the way of computing and data access. Generally speaking, we could consider the Grid as the new enabling technology to transparently access computing and storage resources anywhere, anytime and with guaranteed Quality of Service (QoS) [1]. Grid computing has emerged to cater the need of computing-on-demand due to the advent of distributed computing with sophisticated load balancing, distributed data and concurrent computing power using clustered servers. The Grid enables resource sharing and dynamic allocation of computational resources, thus increasing access to distributed data, promoting operational flexibility and collaboration, and allowing service providers to scale efficiently to meet variable demands [2]. Grid computing is a paradigm shift in computing built on Internet protocols and services. It supports the creation and use of computation and data-enriched environments. A mobile grid constitutes static and mobile nodes (MN) participating in computation. [3].

B. Attacks in Mobile Grid

In mobile grid some of the following attacks are available.

Access control attacks: It defines risks with unauthorized entities, as well as authorized entities, bypassing or defeating access control policy.

Defeating Grid auditing and accounting systems: It includes threats to the integrity of auditing and accounting systems unique to an enterprise Grid environment. This may include false event injection, overflow, event modification, and a variety of other common attacks against auditing systems.

Denial of Service (DoS): This describes an attack on service or resource availability. As an enterprise Grid is often expected to provide a better availability compared to a non-Grid environment.

Malicious code/"malware": This describes any code that attempts to gain unauthorized access to the Grid environment, to subsequently elevate its privileges, hide its existence, disguise itself as a valid component, or propagate itself in clear violation of the security policy of the enterprise Grid.

Object reuse: This describes how sensitive data may become available to an unauthorized user, and used in a context other than the one for which it was generated. In the enterprise grid context, this is a risk if a Grid component is not properly decommissioned.

Masquerading attacks: It describes a class of attacks where a valid Grid component may be fooled into communicating or working with another entity masquerading as valid Grid component. Such an attack could permit the disclosure or modification of information, the execution of unauthorized transactions, etc.

Sniffing/snooping: It involves watching packets as they travel through the network. An enterprise Grid potentially introduces additional network traffic between applications/services, the system and grid components that should be protected. Failure to address this threat may result in other types of attacks including data manipulation and replay attacks. [4]

978-1-4673-4529-3/12/$31.00 ©2012 IEEE

C. Issues in Mobile Grid

In mobile grid we have to consider the following issues.

- The lack of adequate development methods for this kind of systems since the majority of existing Grid applications have been built without a systematic development process and are based on ad-hoc developments suggests the need for adapted development methodologies
- Due to the fact that the resources in a Grid are expensive, dynamic, heterogeneous, geographically located and under the control of multiple administrative domains and the tasks accomplished and the information exchanged are confidential and sensitive, the security of these systems is hard to achieve.
- Because of the appearance of a new technology where security is fundamental together with the advances that mobile computation has experienced in recent years that have increased the difficulty of incorporating mobile devices into a Grid environment [2].
- Poor local resources (in terms of computation speed, memory), battery constraints, unreliable connectivity status, weak security [3].

D. Problem Identification

To enable automatic service deployment in an ad hoc grid environment, the participating nodes must be discovered first. Due to the potentially large size of future grids, manual discovery as practiced in existing grid environments is not an option. An automatic discovery mechanism is needed to find nodes willing to participate in the grid. For mobile grids, a decentralized discovery mechanism is vital to cope with the fluctuating topology and large number of participants.

Existing security mechanisms on Grid systems rarely considers the mobility of the nodes which may affect the applied security mechanisms leading to insufficient and inaccurate security.

II. RELATED WORK

Dario Bruneo et al [1] have proposed using the mobile agent paradigm in order to develop a middleware layer that takes care of all the details to allow mobile users to access distributed resources in a transparent, secure and effective way.

Sang-Min Park et al [3] have developed a new job scheduling algorithm for mobile grid system and evaluate it by various methods. They particularly focus on a disconnected operation problem in that paper since mobile resources are prone to frequent disconnections due to their confined communication range and device mobility.

David G. Rosado et al [5] have presented the service-oriented security architecture for Mobile Grid Systems which considers all possible security services that may be required for any mobile Grid application. That paper showed part of a development process that they are elaborating for the construction of information systems based on Grid Computing, which are highly dependent on mobile devices in which security plays a highly important role.

Congfeng Jiang et al [6] have proposed a security-aware parallel and independent job scheduling algorithm based on adaptive job replications to make sure the job scheduling decision secure, reliable and fault tolerant. In risky and failure-prone grids, the replication number is changed according to the current security conditions and the end-user settings.

Sze-Wing Wong [7] has proposed a middleware framework that supports mobile grid services in a secure manner. Mobile grid services, the extension of the original static grid services, are characterized by the ability of moving from nodes to nodes during execution. The framework is constructed by combining an existing mobile agent system (JADE) and a generic grid system toolkit (Globus). The Mobile Grid Services are realized as Globus grid services with JADE mobile agent support.

III. PROPOSED SOLUTION

A. overview

In this paper, we propose an ant based resource discovery and mobility aware trust management for mobile grid systems. Initially the super-grid nodes are selected in the network using ant colony optimization based on the parameters such as distance, CPU speed, available bandwidth and residual battery power. These selected nodes are utilized in the resource discovery mechanism. In order to maintain strong security with mobility management system, a proficient trust reputation collection method has been adopted.

B. Estimation of Metrics

1) Estimation of Distance

The distance (d_{ij}) among the sender node (N_i) and receiver node (N_j) can be estimated based on free space propagation model. It considers the wavelength utilized for transmission and reception. [8]

The Free-space propagation model is defined using the following equation

$$P_{rx} = P_{tx} * \left(\frac{\eta}{4\pi d_{ij}} \right)^2 * \alpha * \beta \qquad (1)$$

Where P_{rx} = reception power
P_{tx} = transmission power
η = wavelength
α = transmitter gain
β = receiver gain

2) Estimation of Residual Battery power

After time t, the power consumed by the node (P_c (t)) is computed as follows.

$$P_c(t) = DP_{tx} * a_1 + DP_{rx} * a_2 \quad (2)$$

Where,
DP_{tx} = Number of data packets transmitted by the node after time t.
DP_{rx} = Number of data packets received by the node after time t.
a_1 and a_2 are constants in the range of (0, 1).

If P_i is the initial battery power of a node, the residual battery power P_{res} [9] of a node at time t, can be calculated as:

$$P_{res} = P_i - P_c(t) \quad (3)$$

3) Estimation of Available Bandwidth

Each node that wants to transmit the data has to be aware of its local bandwidth and its neighboring nodes information within the interference range. As bandwidth is shared among neighboring nodes, the node pays attention to the channel and estimates local bandwidth (BW_L). It depends on the ratio of idle and busy time period for a predefined interval. [10]

$$BW_L = C_{CH} * (T_i / T_{in}) \quad (4)$$

Where C_{CH} = channel capacity

T_i = Idle time period in the predefined time period T_{in}.

The minimum bandwidth (BW_{min}) of all the nodes with the interference range is identified as the result of prior collection of neighboring node information. Hence the difference among BW_{min} and BW_L gives the residual bandwidth (RBW) of the node.

$$RBW = BW_L - BW_{min} \quad (5)$$

4) Estimation of Local Trust and Global Trust (T_G)

Let n denote the total number nodes in the network

The local trust value (T_{Li}) represents the trust value of the node N_i. Its value ranges from (0, 1), i.e., the value 0 corresponds to the hazardous site and value 1 corresponds to fully trusted scenario. It is defined as the sum of the historical security performance data of the grid sites that includes the rate of successfully executed task, cumulative utilization rate of the site and security measures. The global trust value is estimated from the local trust values of all the nodes in the network.

$$T_{Li} = w_1 * e^{-T_{SET_i}} + w_2 * R_{SET} + w_3 * R_{Ui} \quad (6)$$

where T_{SETi} = time interval from the final successful execution of task on N_i, ($T_{SETi} > 0$)

R_{SETi} = cumulative rate of successfully executed task ($0 < R_{SETi} < 1$)

R_{Ui} = collective utilization rate of N_i, ($0 < R_{Ui} < 1$)

w_1, w_2, and w_3 = weighting factors in the range of (0, 1)

$$\text{Global Trust Value } T_G = \sum_{i=1}^{n} TL_i \quad (7)$$

5) Estimation of Mobility

The mobility of the node j with respect to node i (M^i_j)) is estimated based on the ratio of received signal strength (RSS) among the two consecutive packet transmissions from a neighbor node. [11]

$$M^i_j = 10 \log_{10} \frac{RSS^{new}_{i \to j}}{RSS^{old}_{i \to j}} \quad (8)$$

$$\text{Where RSS} = \lambda * \sigma * P_{tx} \quad (9)$$

λ = constant that depends on the wavelength and the antennas.
σ = channel gain.

C. Proposed technique

Our proposed mechanism mainly focuses on providing security along with mobility management system in mobile grid environment. It involves the following two phases.

i. Ant based resource discovery mechanism
ii. A mobility aware trust management system

1) Phase 1 - Ant based Resource Discovery Mechanism

In this phase, we consider a swarm intelligence technique based on ant colony optimization (ACO) in order to select the super grid nodes. The forward ant agent (FANT) establishes the pheromone track to the source node (S), while backward ant agent (BANT) establishes the pheromone track to the destination node (D).

The parameters contained in the header of the ant agents are shown in Table I.

TABLE I: Header of Ant Agent

Header of Ant Agent					
Node ID	Sequence Number	Residual Battery power (P_{res})	CPU Speed (Z)	Distance (d)	Residual bandwidth (RBW)

The algorithm involved in the selection of super-grid nodes is as follows:

I. Initially, FANT is launched in S and it traverses through all nodes along the path towards D.

II. When FANT reaches every node, it computes the parameters that includes residual battery power, residual bandwidth, CPU speed, and distance (Explained in section 3.2.1- 3.2.3), and updates its header with the node's information.

The mobility of FANT is based on the following probabilistic decision rule.

$$P_r(N_i, S) = \begin{cases} \dfrac{[a(N_i,S)]^{\rho}.[b(N_i,S)]^{\psi}}{\sum_{N_i \in N_{rx}}[a(N_i,S)]^{\rho}.[b(N_i,S)]^{\psi}} \\ 0, otherwise \end{cases}$$

, if $r \notin RT(N_i)$ (10)

Where $a(N_i, S)$ represent pheromone value

$b(N_i, S_o)$ represent the heuristic value related to bandwidth.

N_{rx} represents the receiver node.

$RT(N_i)$ represents the routing table for N_i.

ρ and ψ are the parameters that control the relative weight of the pheromone and heuristic value respectively.

III. After collecting the entire node's information along the path, FANT reaches D.

IV. D then generates BANT and transfers all the information of FANT into BANT. The BANT takes the same path as that of its corresponding FANT, however in the reverse direction.

V. The BANT updates the header field at the neighboring nodes for all the entries related to the FANTs destination node.

VI. The BANT upon reaching S delivers the status of all the nodes.

VII. S then selects the super-grid nodes based on the following condition.

If (Z > Th) & (P_{res} > Th) & (RBW > Th) & (d < Th)

Where: Th=threshold value
Then
The respective node is marked as super-grid nodes (SGN).

End if

VIII. Each SGN_i monitors the neighboring nodes within its transmission range and collects the nodes resource information in the resource table (Shown in Table -II).

The parameters that will be updated in the resource table include the grid node ID, resource availability list and distance.

TABLE II: Resource table

Resource Table			
Grid Node ID	Sequence Number	Resource availability list	Distance

IX. The SGN_i exchanges the collected information with its neighbour SGNs.

X. When any node wants a specific resource, it transmits the request message (REQ) to the nearest super-grid node.

$$N_i \xrightarrow{REQ} Nearest\ SGN_i$$

XI. SGN_i that receives the request analyses its resource table and sends a reply message (REP) that includes the node ID matching the resource request.

$$N_i \xleftarrow{REP} SGN_i$$

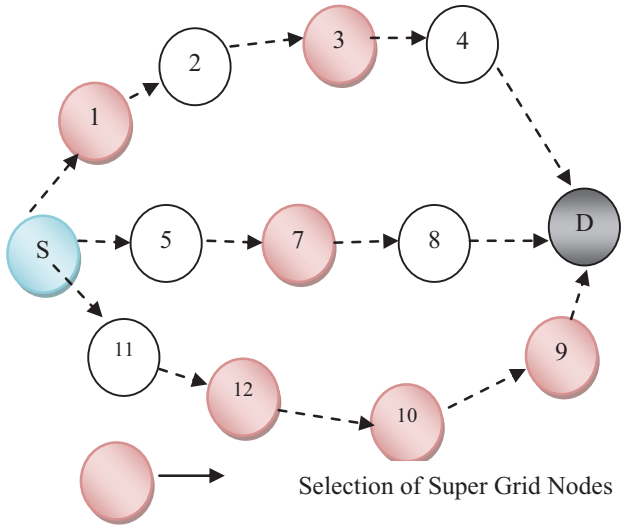

Fig 1: Selection of Super Grid Nodes

Fig. 1 illustrates the selection of super grid nodes. The nodes N_1, N_3, N_7, N_9, N_{10} and N_{12} that satisfy the condition in step 7 are chosen as super-grid nodes. In case N_5 necessitates a resource, it sends the request to its nearest SGN_7. SGN_7 replies N_5 with the node ID that contains the required resource.

2) Phase 2 - A mobility aware trust management technique

In order to maintain strong security with mobility management system, a proficient trust reputation collection method has been designed.

The steps involved the mobility aware trust management technique is as follows :

- Each node N_i estimates the local and global trust value (described in section 3.2.4) based on the parameters such as rate of successfully executed task, time of lastly executed task and cumulative utilization rate of the site. These parameters are collected based on the feedback from the user.
- N_i updates its trust value based on the mobility scenario following the completion of each task.

If M_j^i is high
Then
The node is penalized.
i.e. the trust value is reduced by a step value
Else
The node's trust value is incremented by a step value.
End if

The mobility is high reveals that residence time of the node in the network is very low. This may cause the node to leave the network. Hence its trust value is decremented. While the low mobility reveals that the residence time of the node is very high. This assures the nodes stay within the network and hence it is marked as trusted node with the incremented trust value.

I. Following is the updation of the trust value, N_i applies the following secured encryption mechanism to secure the trust values.

a) Trust value Encryption

Let p and q represent the large prime values such that q divides p-1
Let f and g be the two generated values of sub-group Gq of order $q \in Z_p^*$

N_i randomly chooses two values u_i and v_i from Z_p^*. It then computes the A_i, B_i, C_i using the following equation

$$Ai = u_i \bmod q \quad (11)$$

$$B_i = v_i \bmod p \quad (12)$$

$$C_i = f^{u_i} g^{v_i} \bmod p \quad (13)$$

N_i broadcasts the estimated values of A_i and B_i to its neighbors. When N_i receives A_j and B_j from each neighbor, it computes the following signature.

$$A_{ij} = u_i - u_j \bmod q$$

$$B_{ij} = v_i - v_j \bmod q$$

N_i stores the values (C_i, C_j, A_{ij}, B_{ij}) in its memory. The trust values are encrypted and signed using the generated signatures.

b) Advantages of this proposed approach

i. The proposed system is efficient since it is not distributed.

ii. The encryption and signing ensures confidentiality and authentication of the system.

iii. The mobility aware trust management provides connectivity apart from providing security.

D. Simulation Results

1) Simulation Settings

We use NS2 [12] to simulate our proposed protocol. Figure 2 gives the sample network topology used in our simulation. In our simulation, 30 grid nodes are deployed in a 1000 meter x 1000 meter region for 50 seconds simulation time. Among the total 30 grid nodes, 20 nodes act as mobile grid nodes (indicated as "G" and blue color in figure 2) and 10 nodes act as super grid nodes (indicated as "SG" and red color in figure 2). We assume each mobile grid node moves independently with the same average speed. The speed of the mobile grid node is varied from 2m/s to 10m/s. All nodes have the same transmission range of 250 meters.

We have taken the Service Location Protocol (SLP) for service discovery. A SLP service agent is attached to the nodes for providing the services and SLP user agent is attached to the clients for requesting the service. In our simulation, clients send service requests to the super grid nodes. The super grid nodes select the grid nodes matching the service request and assign the tasks as per our algorithm. The simulation settings and parameters are summarized in table III. Fig. 2 shows simulation toplogy.

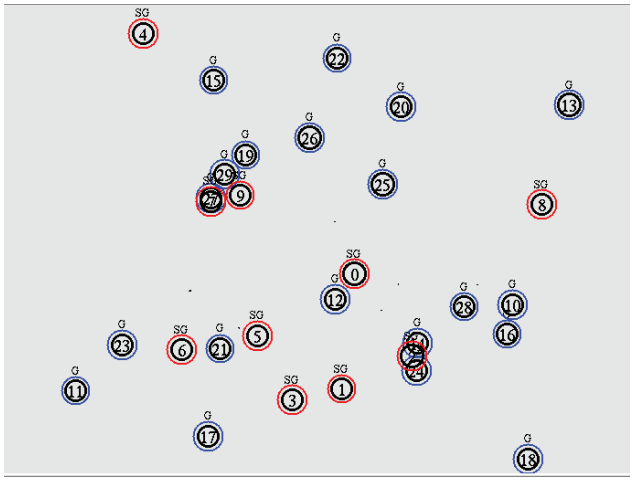

Fig. 2. Simulation Topology

TABLE III: SIMULATION PARAMETERS

No. of Grid Nodes	20
No. of Super Grid Nodes	10
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Service Discovery Protocol	SLP
Server Application	SLPsa
Client Application	SLPua
Speed	2m/s to 10m/s
clients	4
Requested Load	10kb to 50kb

We compare our **A**nt based **R**esource **D**iscovery and **M**obility-aware **T**rust **M**anagement (ARDMTM) technique with Replication Based Job Scheduling (RBJS) technique [6]. We evaluate mainly the performance according to the following metrics.

Average Delay: It is measured as the average delay occurred for each client while getting the requested service.

Average Throughput: It is measured as the received throughput for each client in terms of Mb/sec.

Packet Delivery Ratio: It is the ratio of number of packets received successfully to the number of packets sent.

Packet Drop: It is the average number of packets dropped at the clients.

a) Based On Load

In our first experiment we vary the load of the clients as 10 to 50 kb with speed as 2m/s.

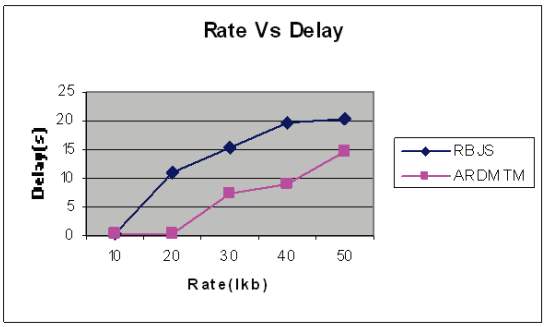

Fig 3: Rate Vs Delay

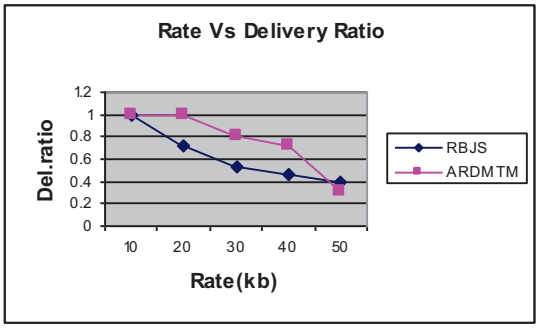

Fig. 4. Rate Vs Delivery Ratio

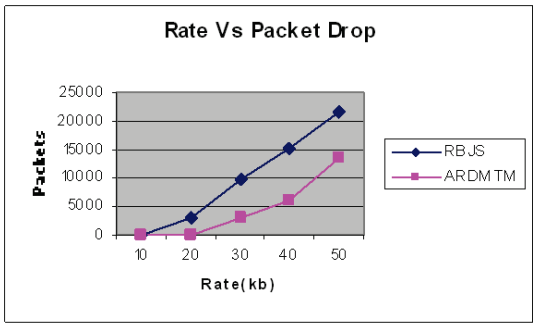

Fig. 5. Rate Vs Packet Drop

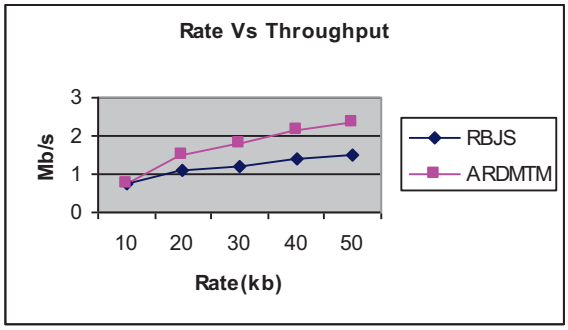

Fig. 6. Rate Vs Throughput

Fig. 3 shows the delay when the load is increased. When load is increased from 10 to 50kb, it results in more processing and hence increasing the delay. But we can see that ARDMTM has less delay than RBJS, when the rate is increased, because of the use of super-grid nodes.

From Fig 4, 5 and 6, we can see that ARDMTM has better performance than RBJS in terms of packet delivery ratio, drop and throughput, respectively. This is because of the fact that ARDMTM selects the grid nodes mobility and trust.

b) Based on Speed of Mobile Grid node

In the second experiment the speed of the mobile grid node is varied from 2m/s to 10m/s keeping the rate as 10kb.

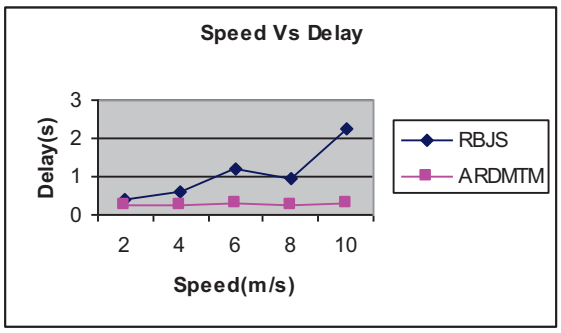

Fig. 7. Speed Vs Delay

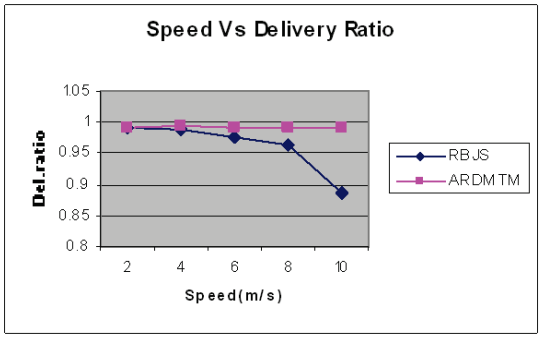

Fig. 8. Speed VS Delivery Ratio

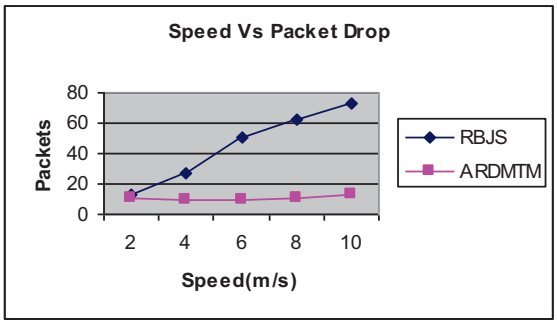

Fig. 9. Speed Vs Packet Drop

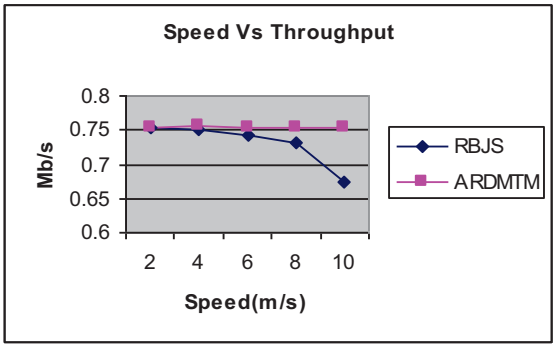

Fig. 10: Speed Vs Throughput

Fig. 7 shows the delay when the speed of the grid node is increased. When speed of the node is increased, it results in more query processing operations and hence increasing the delay. But we can see that ARDMTM has less delay than RBJS, when the rate is increased, since the nodes are selected based on the mobility.

From Fig. 8, 9 and 10, we can see that ARDMTM outperforms RBJS in terms of packet delivery ratio, drop and throughput, respectively. This is because of the fact that ARDMTM selects the grid nodes based on the connectivity and trust values.

CONCLUSION

In this paper, we have proposed an ant based resource discovery and mobility aware trust management for mobile grid systems. Initially the super-grid nodes are selected in the network using ant colony optimization based on the parameters such as distance, CPU speed, available bandwidth and residual battery power. These selected nodes are utilized in the resource discovery mechanism. In order to maintain strong security with mobility management system, a proficient trust reputation collection method has been adopted that includes the estimation of local and global trust values for the grid nodes, followed by mobility management system which can effectively predicts the residence time of each grid node. Finally encryption mechanism is utilized to encrypt the trust values such that the information is confidential and cannot be modified. By simulation results, we have shown that the proposed approach provides more throughputs while reducing the delay and drop.

REFERENCES

[1] Dario Bruneo, Antonio Puliafito, Angelo Zaia "An Agent-based Architecture for Mobile Grid Users", Published on 4th International Workshop MATA Barcelona, Spain, October 2002.

[2] David Rosado, Eduardo Fernandez-Medina and Javier Lopez "Security in the Development Process of Mobile Grid Systems", ICSOFT (1) 2010. 133-138

[3] Sang-Min Park, Young-Bae Ko, and Jai-Hoon Kim "Disconnected Operation Service in Mobile Grid Computing", First International Conference on Service Oriented Computing (ICSOC'2003) in Trento, Italy, Dec 2003.

[4] David G. Rosado, Eduardo Fernández-Medina, Javier Lopez and Mario Piattini "Obtaining Security Requirements for a Mobile Grid System", IJGHPC 1(3): 1-17 2009.

[5] David G. Rosado a, Eduardo Fernández-Medina a, Javier Lopez b "Security services architecture for Secure Mobile Grid Systems", Journal of Systems Architecture, 2010.

[6] Congfeng Jiang , Xianghua Xu, and Jian Wan " Replication Based Job Scheduling in Grids with Security Assurance", Proceedings of the Third International Symposium on Electronic Commerce and Security Workshops (ISECS '10) Guangzhou, P. R. China, 29-31, July 2010, pp. 156-159 , 2010.

[7] Sze-Wing Wong "A middleware framework for secure mobile grid services" Cluster Computing and the Grid, CCGRID-06. Sixth IEEE International Symposium, 2006.

[8] Mehajabeen Fatima, Roopam Gupta and T.K. Bandhopadhyay, "Route Discovery by Cross Layer Approach for MANET", International Journal of Computer Applications, Volume 37– No.7, January 2012.

[9] Vinay Rishiwal, S. Verma and S. K. Bajpai, " QoS Based Power Aware Routing in MANETs", International Journal of Computer Theory and Engineering, Vol. 1, No. 1, April 2009.

[10] Tung-Shih Su, Chih-Hung Hsieh Lin, Wen-Shyong, " A Novel QoS-Aware Routing for Ad Hoc Networks", Proceedings of the 9th Joint Conference on Information Sciences (JCIS), 2006.

[11] P. Basu, N. Khan, and T.D.C. Little, " A Mobility Based Metric for Clustering in Mobile Ad Hoc Networks", International Conference on Distributed Computing Systems Workshop, pp 413 – 418, 2001

[12] Network simulator, http://www.isi.edu/nsnam/ns