International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Dynamic Trust Management for Community Based Mobile Grid Application

Grantej Vinod Otari, Vijay Ram Ghorpade

Abstract*: Mobile Grid is the inter-networking of heterogeneous physical as well as virtualdevices. Each device transfer and share the information with each other. Trust management plays a significant role in network based applications for information collection, data mining, qualified services with context-awareness, upgraded client protection and data security. It assists individuals with beating impression of vulnerability, threat and participates in client acknowledgment to utilization on grid services and applications. In this paper a unique trust management protocol is proposed for network based mobile grid application to manage misbehaving nodes whose status or performance may change dynamically. Trust plays an important role for handling the security in the community based system. Trust management provides facilitate to identify malfunctions and also make legitimate collaboration and enhance the user privacy and information security.

Keywords: Trust Management, Dynamic trust management. Grid network.

I. INTRODUCTION

Mobile Grid network uses the internet facility to communicate with different devices in community. This correspondence system help devices to physically associate with each other. Various applications and services which are meant for mobile grid like e-healthcare, food sanctuary, traffic control and remote home automation are increasing in the market. Such services and applications are useful to people in a community. These all applications and systems are worthless without proper measures of security and privacy. So security plays a very important role in such kind of applications [1]. It is very essential for people to overcome perceptions of uncertainty and risk and engage in user acceptance and consumption of community based services and applications. The concept of trust not only contains the security but also reliability, goodness, strength and different other properties of an entity [8]. Community based network contains different heterogeneous components like smart phones, laptops, PDAs, Sensors, digital equipment's and so on. These heterogeneous devices collaborate together in the form of mobile grid network and are responsible for providing the services to each other. This also establishes a social relationship between the owners of the devices and devices themselves. The owners and their devices communicate with each other and also provide different services to each other. In such type of social environment, it is very important to identify the trustworthiness of every device as well as their services[5]. Malicious or misbehaving owners as well as misbehaving devices may perform biased attacks on their social connections at the cost of devices providing similar services. Further, malicious nodes with close social ties may connive and dominate a class of services. Since trust provisioning in this scenario inalienably is completely incorporated with service provisioning the idea of trust-based service management is of principal significance [11]. The contributions of this paper are as follows:

1) Build a dynamic trust management protocol to identify and detect misbehaving nodes in community based system.
2) Provide a conventional strategy of the combination, exactness, and strength properties of dynamic trust management protocol.
3) Validate the ability of the dynamic trust management protocol that enhances the performance of the application by selecting the best trust parameters as per the dynamic changes in the community based mobile grid network [5].

The rest of this paper is organized as follows. Section 2 discusses related work in trust management for community based systems. Section 3 describes the system model. Section 4 details our Dynamic trust management. Finally, Section 5 concludes the paper.

II. RELATED WORK

The methodology proposed by R. Roman, P. Najera and J. Lopez describes the issues encountered while applying the conventional methods of security, privacy and trust in the IoT frameworks due to the highly scalable and heterogeneous resources and the relationship between the resources [2].

Atzori et al. [3] recommended the idea of social IoT and identifies different types of social relationships among things. The author classified these relations as parental object relation, social contact object relation, collaborate object relation, and owner relation. The proposed methodology focuses more on the relationship among things than the clients. Bao and Chen [4], [5] proposed a trust management protocol in which both social and QoS trust parameters are considered. The proposed model update the trust using both direct observations and indirect recommendations. Here a dynamically changing social IoT environment is considered such that the number and activities of the misbehaving node increases, the behaviour of the nodes changes, nodes participate and release in the network rapidly and pattern of interaction is dynamic [12]. Using a scalable storage management strategy the authors proposed a scalable trust management protocol [5] to solve the scalability issue of social IoT.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
Grantej Vinod Otari, Department of Computer Science & Engg., Shivaji University Kolhapur, India. grantejv@gmail.com
Dr. Vijay Ram Ghorpade, Department of Computer Science & Engg., Bharati Vidyapeeth's College of Engineering, Kolhapur, India.

A key management scheme that contains the key agreement and forward and backward secure key evolution policy is proposed by W. Ren [6] for heterogeneous IoT frameworks. A Quality of Service (QoS) enhancement is designed by the authors.

A trust management protocol for SOA-based IoT frameworks is proposed by F.Bao, I.R. Chen and J. Guo [6]. To select the trust feedback from nodes sharing common interests a distributed collaborative filtering method is used. The effectiveness of the proposed trust management system is validated by applying it to the SOA-based IoT application.

III. SYSTEM MODEL

A. Network Model

The proposed model assumes a social network environment which is user centric. In this user-centric environment nodes use communication network for physical connection and users' social network for social connection as shown in Figure 1. Each node is uniquely identified by an address known as URI. There is no trusted authority which works centrally [11]. The nodes are of : device and clients (or proprietors). The connection among client and device is one-to-numerous. In our trust the board, the trustor is a client and the trustee is a device (possessed by another client). Client claims an assigned very good quality device which is utilized to store the processed trust assessment data for every client. Trust is assessed dependent on both direct client fulfillment encounters of past connection encounters and proposals from others. Specifically, for suggestions from others, the idea of disseminated working together separating [9], [10] is utilized to choose trust criticism from hubs having comparative social interests.0

The proposed model considers following three social relationships: friendship, social contact, and community of interest (CoI).

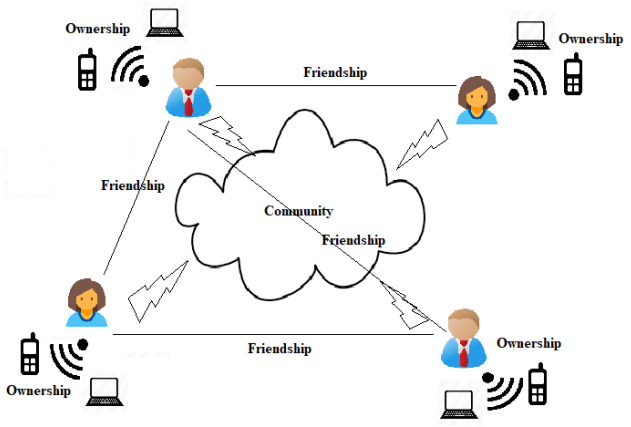

Figure 1: System Model for a community based System

These parameters represent a similar subjective trust view between the trustor and the trustee. The social relationship between the trustor and the trustee is then used as a weighing factor to weigh the recommendation about the trustee given by the recommender to the trustor [12].

Each user owns one or more high end device such as laptop or smartphone. One of these devices store the profile created for its owner containing the list of friends, list of frequently visited locations and list of devices and their owner belonging to the Community of Interest (CoI) as shown in Figure 2.The device storing the user profile may also share it with the other low end devices belonging to the same user such as sensors with limited capacity.

B. Attack Model

Malicious and selfish nodes also cause serious threats in a social networking environment. They may impose communication protocol attacks interfering the operations in the network causing irreversible damages to the environment [5]. In the proposed model only trust related attacks are focused which disrupt the trust management system.

The attacks imposed by such malicious or selfish nodes in mobile grid social network are as follows:

1) Self-Promoting attacks:

In this type of attack the malicious or selfish node pretends to be trustworthy by providing positive feedback or recommendation about itself in order to participate in the service provisioning process and then provide malicious services causing harmful damage to the environment.

2) Bad-mouthing attacks:

In this type of attack a malicious or selfish node provides negative feedback or recommendation about a trustworthy node to prevent it from participating in the service provisioning process.

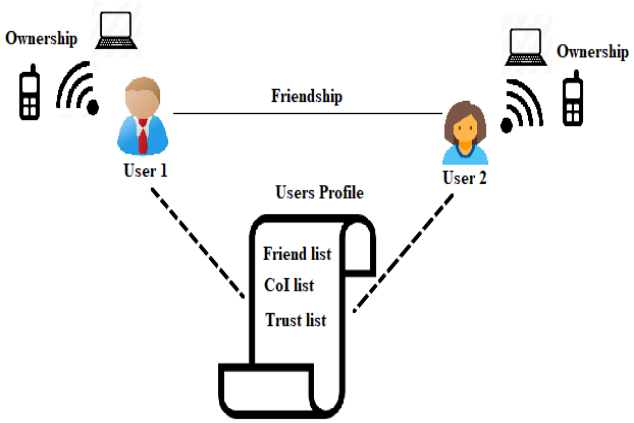

Figure 2: Users Profile

IV. DYNAMIC TRUST MANAGEMENT

A distributed approach is used in the proposed trust management system, where each user or device evaluates the trustworthiness of all other users or devices and exchange the trust information with each other. The architecture of the proposed dynamic trust management system is shown in Figure 3. It contains four main components: Trust composition, Trust propagation, Trust aggregation and Trust formation. Trust composition is the process of selecting the best parameter for the trust evaluation based on the requirements of the application in social community based network. Trust propagation is dissemination of trust information [11].

Trust aggregation is the accumulation of the trust information to obtain the accurate trust value all the devices. Trust formation is the evaluation of global trust value by considering the local trust value from individual devices and using the globally trusted node to improve the system performance.

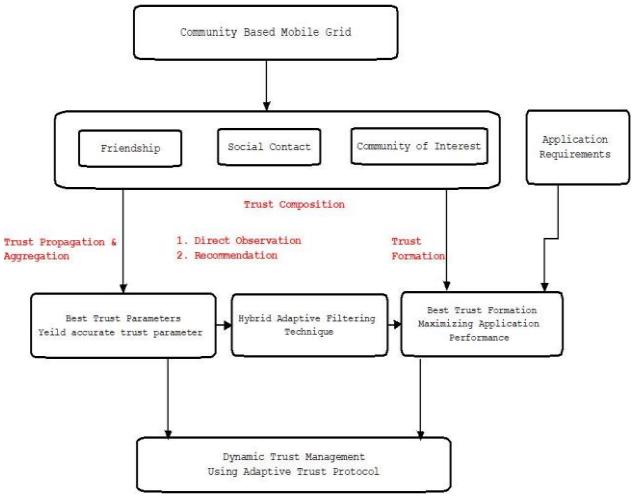

Figure 3: System Architecture

In most of the community based social networks there is no central point of control, hence a distributed trust management approach is required. In this approach each node evaluates and stores the trust value and the recommendation information of only those nodes who share common interest. The trustor trusts the recommendations from only those nodes that are part of the CoI and are involved in frequent interactions with it. This reduces the storage requirement for the mobile node with limited storage capacity to store the trust information of only limited devices with which it shares common interest and has frequently interacted. Whenever a new interaction of action takes place in the environment, the trust value of the node is updated by the trustor. The updated trust information is then exchanged by each node with all other nodes in the community [12].

1) Trust Composition: In this phase three parameters are considered to compose the social trust relationship. These parameters are friendship, social contact and Community of Interest (CoI). These parameters are represented by three lists as shown in Figure 3. Since users belonging to the CoI are most likely to have similar social interest and share common knowledge or opinion about the particular service, there is more possibility of establishing a social trust relationship between them. Hence these three parameters are considered prominently to compose a social trust value for the trustee.

2) Trust Propagation and Aggregation: Trust management is an iterative process in which pat information and current information is aggregated continuously. The current information is obtained through direct interactions (first hand information) and recommendations (second hand information). A distributed approach is used by the system to propagate and exchange the information for trust estimation.

The trust assessment of node a towards node b at time t is denoted by $T_{ab}^{P}(t)$ where user profile P = friendship, Social Contact, or community interest. The trust value $T_{ab}^{P}(t)$ is a real number in the range of [0, 1] where 1 indicates complete trust, 0.5 ignorance and 0 distrust.When node a encounters or directly interacts with another node c at time t, node a will update its trust assessment T_{ab}^{P} as follows:

$$T_{ab}^{p}(t) = \begin{cases} (1-\alpha)T_{ab}^{p}(t-\Delta t) + \alpha T_{ab}^{p,direct}(t), if\ b == c; \\ (1-\gamma)T_{ab}^{p}(t-\Delta t) + \gamma T_{cb}^{p,recom}(t)\ if\ b! = c; \end{cases} \quad (1)$$

Here, Δt is the elapsed time since the last trust update. If the trustee node b is node c itself, node a will use its new trust assessment toward node b based on direct observations. Parameters α and γ are the parameters to control trust propagation for direct and indirect sources of information.

3) Recommendation: In this phase a distributed collaborative filtering [9][10] mechanism is used . Whenever a trustor needs recommendations about the trustee from the recommender in the friend list, the trustor initially checks if the recommender shares similar “Social interest” and belongs to the CoI. Recommendations received from frequently interacted nodes and belonging to same CoI are considered to be more trustworthy and are of more importance for trust composition. Privacy of the recommender can be preserved by applying hash function along with the session key.

4) Trust Formation: In this phase the overall trust of a node is estimated by considering multiple trust parameters depending on the requirement of the applications in the dynamic social trust environment. The problem of computing the overall trust from the three Tij(t)’s where P=friendship, social contact and CoI , is the trust formation issue. Each of these three parameters belonging to P can be assessed separately by node i to measure the overall trust of node j.

V. RESULT AND ANALYSIS

In this section, the graphical representation of Trust value of user, execution time of algorithm and analysis of attack model is done.

Trust value is calculate by random algorithm. In random algorithm, the rank is assigned to the user based on the analysis of the recommendations or reviews about a product. Trust Value is in Between 0 to 1. If trust value is greater than threshold value then the user is trusted user otherwise the user is untrusted user. Threshold value is set to 0.5. Table 1 and 2 shows the list of trusted and untrusted users.

Table 1: Top 5 trusted users

User Id	Trust Value
4	1
19	0.9
10	0.8
17	0.7
7	0.6

Table 2: Top 5 untrusted users

User Id	Trust Value
11	0.4
9	0
12	0
16	0
14	0

Table 4: Number of Attacks

Attack Detection Graph			
Comment Id	**Self-promoting Attack (SPA)**	**Ballot Attack(BA)**	**Bad mounting attack(BMA)**
1	40	100	25
2	25	75	50
3	100	0	50
4	6.67	80	0
5	57.14	42.86	71.43
6	50	60	50
7	33.33	33	100

Figure 4. shows the graph of the trust values of the user based on the analysis of the recommendations.

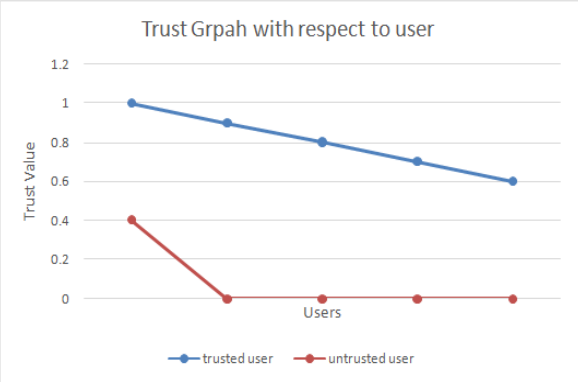

Figure 4: Trust Graph with respect to user

The graph shown in Figure 5 displays the actual execution time of self-promoting attack, Bad mounting attack, ballot attack as shown in Table 3.

Table 3: Execution time

Algorithm	Time
Self-promoting attack	8.98
Ballot Attack	36.72
Bad mounting Attack	22.02

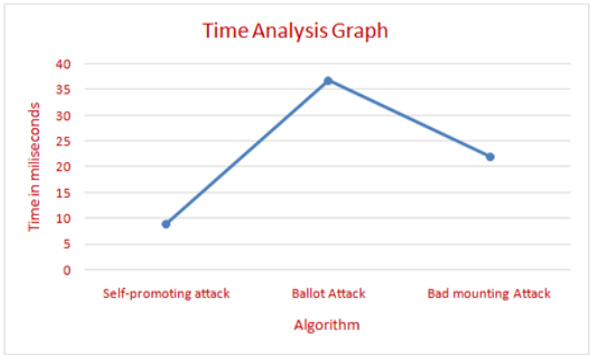

Figure 5: Execution time graph

The graph in Figure 6 considered the review messages and the number of attacks detected as shown in Table 4

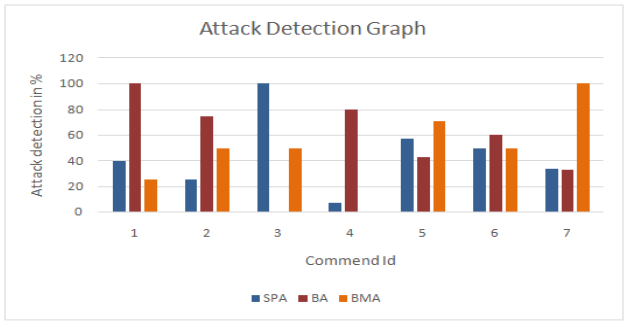

Figure 6: Attack detection graph

Attack module includes self-promoting attack, Ballot Attack, Bad mounting Attack.

Accuracy analysis is done by using precision-recall method on given dataset of reviews about products given by user. In this system gives different types reviews i.e. it may be True Positive (TP), True Negative (TN), False Positive (FP) or False Negative (FN).

Table 5: Accuracy and Precision

Total No. Of Cases	TP	TN	FP	FN	Precision	Recall (sensitivity
100	88	3	5	4	95	96
	92	3	3	2	97	98
	90	2	5	3	95	97
	85	4	9	2	90	98
	85	5	5	5	94	94

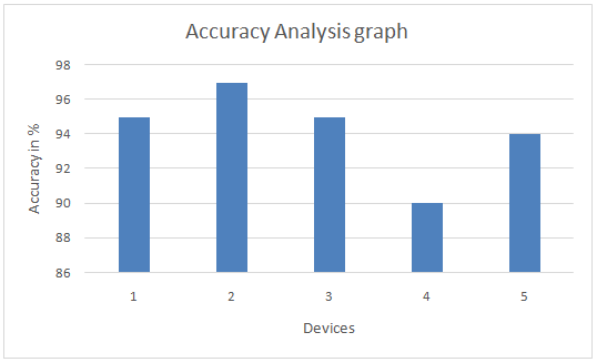

Figure 7: Accuracy Analysis graph

VI. CONCLUSIONS

In this paper, we proposed a dynamic trust management protocol for community based application in community based network in mobile grid. Here three social relationships, i.e., friendship, social contact, and community of interest are considered for measuring social similarity and filtering trust feedback based on social similarity. The protocol is distributed. Each node only updates trust towards others of its interest upon encounter or interaction events. The trust assessment is updated by both direct observations and indirect recommendations, with parameters and being the design parameters to control trust propagation for these two sources of information.

REFERENCES

1. Ing-Ray Chen, JiaGuo, and FenyeBao , "Trust Management for SOA-Based IoT and ItsApplication to Service Composition," IEEE Transactions On Services Computing, Vol. 9,No. 3, May/June 2016.J.
2. R. Roman, P. Najera, and J. Lopez, "Securing the internet of
3. things," Computer, vol. 44, no.9, pp. 5158, Sep. 2011.
4. L. Atzori, A. Iera, and G.Morabito "SIoT: Giving a social structure to the internet of things,"IEEECommun. Lett., vol. 15, no. 11, pp. 11931195, Nov. 2011.
5. A B Kathole , "Optimization of Vehicular Adhoc Network Using Cloud Computing", 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing,IEEE.
6. J. W. Ren,"QoS-aware and compromise-resilient key management scheme for heterogeneouswireless Internet of Things," Int. J. Netw. Manage.,,vol. 21, no. 4, pp. 284299, Jul.2011.
7. F. Bao and I. R. Chen, "Dynamic trust management for internet of things applications," inProc. Int. Workshop Self-Aware Int. Things, San Jose,CA, USA, 2012.
8. F. Bao and I. R. Chen, "Scalable, adaptive and survivable trust management for communityof interest based internet of things systems" in Proc 11th Int. Symp,Mexico,2013.
9. I. R. Chen, J. Guo and F. Bao, "Trust management for service composition in SOA-basedinternet of things systems," in Proc. IEEE WCNC, Istanbul, Turkey.Apr. 2014
10. ZhengYan,PengZhang,Athanasios V. Vasilakos "A survey on trust management for Internetof Things," Journal of Network and Computer Applications, March. 2014.
11. Atul B Kathole, Dr.Dinesh N.Chaudhari, " Fuel Analysis and Distance Predication using Machine learning", 2019 ,International Journal on Future Revolution in Computer Science & Communication Engineering, Volume: 5 Issue: 6.
12. Atul B Kathole, Dr.Dinesh N.Chaudhari, "Pros & Cons of Machine learning and Security Methods ", 2019, http://gujaratresearchsociety.in/index.php/JGRS, ISSN: 0374-8588 ,Volume 21 Issue 4.
13. Z. Huang, D. Zeng, and H. Chen, "A comparison of collaborativefilteringrecommendation algorithms for E-commerce," IEEEIntell. Syst., vol. 22, no. 5, pp. 68–78, Sep./Oct. 2007.
14. X. Yang, Y. Guo, Y. Liu, and H. Steck, "A survey of collaborativefiltering based social recommender systems," Comput. Commun.,vol. 41, pp. 1–10, 2014.

AUTHORS PROFILE

Grantej Vinod Otari completed his Master's degree in CSE from Shivaji University, Kolhapur. Currently, he is a PhD candidate in CSE at Shivaji University. His area of interest includes distributed systems, Grid Technology and mobile computing.

Prof. Dr. Vijay Ram Ghorpade completed ME and PhD in Computer Engineering. He is a Professor in Computer Engineering department and Principal at BVCOE, Kolhapur. He is an eminent academician and researcher with papers published in various reputed journals. His area of research includes information security, mobile computing, ad-hoc networks, etc.