SECURE TRUSTWORTHY SERVICE EVALUATION IN SOCIAL NETWORKS

T.Chindrella Priyadharshini[1], M.Swarnalatha[2], P.Mugilan[3]

[1,2,3]*Assistant Prof, IT Dept, RMKCET, Puduvoyal, Tamil Nadu, (India)*

ABSTRACT

Large scale systems face security threads from faulty or hostile remote computing elements. Portable devices and call it MobID. The extent to which MobID reduces the number of interactions with sybil attackers. One approach preventing Sybil attacks without logical central authority. Sybil Guard identifies sybils that which every person exchanges keys with a limited number of well-known trusted friends. To develop trustworthy mechanism to detect Sybil nodes. Proposed trust authority that means discover intermediate nodes between sender and receiver that detects sybils using mobile -social networks.

Keywords: Mobile social networks, Trust authority, Sybil attack, Distributed system.

I INTRODUCTION

In service-oriented computing (SOC) [Singh and Huhns 2005] [1]environments, computing resources are modeled as services, which can be used directly or composed into other services We argue that it is practically impossible in a distributed computing environment, with no logical central authority to vouch for one–to-one correspondence between entity and identity. Many systems [2] replicate computational or storage task among several sites.

1.1 Literature Survey

One promising way to defend against sybil attacks in social networks is to leverage the social network topologies. Sybil Gurad suffers from high false negatives, as each attack edge may introduce O(√n log n) sybil nodes without being detected. SybilInfer [9], a centralized sybil defense algorithm, leverages a Bayesian inference approach that assigns a Sybil probability, indicating the degree of certainty, to each node in the network. sybil community detection algorithm can effectively detect the sybil community around a sybil node with short running time. Milanovic and Malek [2004] [10]compare various modern web service composition approaches. For example, suppose service A invokes service B, which may invoke E and F with probabilities denote PE and PFabout remote entities .it call identities. Local entity select subset of identities to perform remote operation. We term the forging of multiple identities a Sybil attack on system. Researchers have recently proposed general infrastructures with which portable devices in proximity of each other opportunistically trade various services within a scalable and decentralized way [3], [4], [5].The problem is that collaborative applications are easily disrupted by uncooperative and malicious individuals. creating very large number of bogus identities. In literature, those individuals are called sybil attackers or simply sybils [6].

This problem by making three main contributions:

- The key idea is that each device manages two small nodes in which it enlists the devices it meets: honest nodes and Sybil nodes
- MobID guarantees the honest nodes that reject bogus identities and accept honest identities. It provides

trust aware service selection approach. Trust is a key basis interaction between services.

II PROPOSED SYSTEM

2.1 Trust Authority

Review submission may need co operations from other users when the vendor is not in the transmission range of the user, or when direct submission fails due to communication failure. The location client message passing among nodes that identify where is source and destination. The vendor spontaneously initializes a number of tokens and issues them to one per user. . A user cannot submit a review unless it currently holds one of the tokens. A token may be lost due to malicious users. each token is linked to a pseudonym[20] that belongs to a user who most recently submitted a review using the token. Trust authority node between sender and receiver. That prevent the packet loss. Sender send the all the information to trust authority node then trust authority node passing the information to destination.

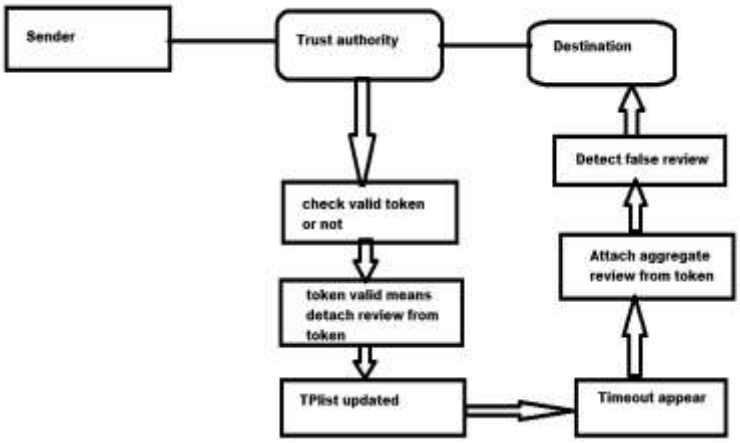

Fig.1 Overview of trust authority

III. IMPLEMENTATION MODELS AND ALGORITHMS

3.1 Bayesian Approach

A Bayesian network [16] denote atomic and composite services with lowercase and uppercase, respectively. An edge from service a to B means B is composed of a. we use the Bayesian network terminology in this paper. A conditional probability associated with each node represents trust (a probability) of the node variable given an estimate of its parent's trustworthiness. use trust aware service selection model represent trust based on the beta probability distribution [Evans et al. 2000][17],which can be integrated with Wang and Singh's model. we can estimate the trustworthiness of service xi by applying maximum likelihood estimation (MLE) to maximize the likelihood of the observations [Buntine 1994][18].In this Bayesian network terminology a is B's parent then A's, B's child. This terminology opposite composite hierarchy. In this case we can use expectation maximization(EM) Algorithm.The maximizing likelihood function using the distribution parameters π and θ. Estimation using EM Algorithm.

$$P(D)=\sum \pi jpj(D|\theta j)$$

Where D={j1,j2,……jN} are the observations. Pj is the jth component distribution with parameter πj and pj.

3.2 The Design of Ta

In my project TA means trust authority that is intermediate node concept between sender and destination. The review consists of two parts. One is content of review and another one is proving signature authenticity. There are two Sybil attacks can appear that produce inaccurate information. Propose intermediate node of trust authority to generate one review in predefined timeslot. In the review submission process that link ability reviews can be linked to real identities.

3.3 Finite Mixture Model

Finite mixture model can be formulated as. where D = {x1, . . . , xN} are the observations, pk is the kth component distribution. MobID ensures that sybil attackers are detected with high probability.

3.4 System Model

We use graph G that means consider edges and vertices. There are two sets "sybil set" and "honest set". The simplest way is using the k means clustering algorithm[19]. This algorithm generates k clusters and determines which circles belong to which cluster circles belong to which cluster depending on the structure of the data. The circles are denoted by centroid. Top of the centroid is consider as honest set. Bottom of the centroid is denoted as Sybil set.

3.5 Security Model

The S-MSN is vulnerable to various security threats due to lack of centralized control. That is central trusted authorities in the network. The user can manipulate the malicious nodes. The aggregation technique [20] is used to reduce the signature size of different user from different social groups. By this technique token size can be reduced. In this method communication cost can be reduced.

3.6 Generation of Keys

A user u_i if the registering to a group Authority chi. Each and every time bunch of pseudonym secret keys[21] can be received to the corresponding ids. It produce the secret keys which that token is valid or not.TP list can accept valid tokens. Each review is a value ranged in [0, 1]. A review is negative if its value is lower than 0.5. To produce the trust authority mechanism prevent packet or information loss.

IV. DETECTION OF SYBIL ATTACK

There are two sybil attacks appear in our project, Sybil attack1 and Sybil attack2. This aggregate signature technique is in srTSE. Using intermediate node concept that preventing sybil attack. A user having a review to submit transmits a token request message that particular time then receiving request. Tokens can be exchanged between sender and destination. The requesting user accepts the first arrived valid token and replies with an ACK message. The vendor maintains a token-pseudonym list. In this list, each token is linked to a pseudonym that belongs to a user who most recently submitted a review using the token.

V. RESULTS AND DISCUSSION

In the social network graph consists of vertices V and Edges E. There are two region one is Sybil region and another one is honest region. Sybil region consists of Sybil nodes, honest region consists of honest nodes. The user can generate false reviews. The aggregate signature technique that reduce the token size and cost. It will receive a bunch of pseudonym secret keys that produce corresponding ids. The token pseudonym list that check corresponding id that produce secret keys that produce corresponding ids. The token pseudonym list that check

corresponding id that produce secret keys. The token recording the history and the vendor will detect review missing. The trusted node declares the Sybil node and non Sybil nodes in the network. Pseudonyms that produce corresponding ids. The token pseudonym list that check corresponding id that produce secret keys. The token recording the history and the vendor will detect review missing. The trusted node declares the Sybil node and non Sybil nodes in the network.

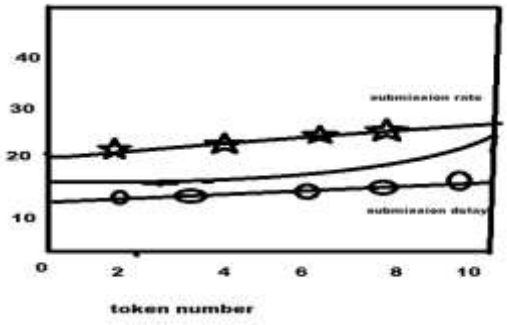

Fig.2 performance evaluation of TA

Rate of relationship named to the face book application. In my project using activity network. Activity network this network contains nodes and edges but it have limit no of attack edges. In the ER model build topologies that interaction between the nodes and edges. The Sybil region connect to the real world of social network. Fig.2 each and every token have the token Number that display that submission rate and Submission delay. Fig.3 display the Sybil node and honest node Fig.4 display the attacks

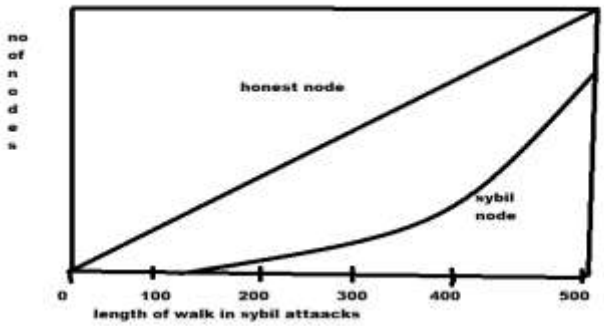

Fig.3 Performance of attacks

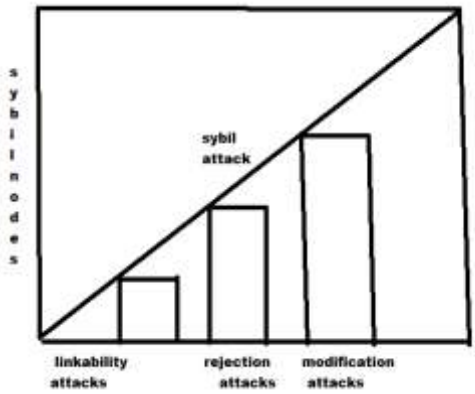

Fig.4 Evaluation of attacks

VI. CONCLUSION

In this project we explored Trust Authority of intermediate node between source and destination in mobile social networks. Main focus of this project is implementing intermediate node concept. For this we use trust authority and evaluated using in different scenarios. This project also explains how to achieve the trustworthiness of service .To prevent the loss of information

REFERENCES

[1] Liu, W. 2005. Trustworthy service selection and composition—reducing the entropy of service oriented web. In Proceedings of the 3rd IEEE International Conference on Industrial Informatics (INDIN). IEEE Computer Society, Los Alamitos, CA, USA, 104–109.

[2] F.Dabek, M.F.Kaashoek, D.karger, R.Morris, I.Stoica ”wide area cooperative storage with CFS”, 18TH sosp,2001,pp 202-215

[3] R. Chakravorty, S. Agarwal, S. Banerjee, and I. Pratt. MoB: A mobilebazaar for wide-area wireless services. In Proc. of ACM MobiCom.

[4] L. McNamara, C. Mascolo, and L. Capra. Media Sharing based on Colocation Prediction in Urban Transport. In Proc. of the ACM MobiCom, 2008.

[5] D. Zhu and M. W. Mutka. Promoting Cooperation Among Strangers to Access Internet Services from an Ad Hoc Network. In Proc. Of PERCOM, 2004.

[6] J. R. Douceur. The Sybil Attack. In Proc. of IPTPS, 2002.

[7] A. Nicholson, I. Smith, J. Hughes, and B. Noble. Lokey: Leveraging the sms network in decentralized, end-to-end trust establishment. In Proc.of Pervasive, 2006

[8] M.E. J. Newman. A measure of betweenness centrality based on random walks. Social Networks, 2005.

[9] R. Chakravorty, S. Agarwal, S. Banerjee, and I. Pratt. MoB: A mobile bazaar for wide-area wireless services. In Proc. of ACM MobiCom

[10] Milanovic, N. and Malek, M. 2004. Current solutions for web service composition. IEEE Internet Computing 8, 6, 51–59.

[11] Liu, W. 2005. Trustworthy service selection and composition—reducing the entropy of serviceoriented web. In Proceedings of the 3rd IEEE International Conference on Industrial Infor-matics (INDIN). IEEE Computer Society, Los Alamitos, CA, USA, 104–109.

[12] X. Pan, J. Xu, and X. Meng, “Protecting location privacy against location-dependent attacks in mobile services,” IEEETransactions on Knowledge and Data Engineering, 2011.

[13] Z. Zhu and G. Cao, “Towards privacy-preserving andcolluding-resistance in location proof updating system,” IEEETransactions on Mobile Computing, 2011.

[14] C. Gentry and Z. Ramzan, “Identity-based aggregate signatures,”in PKC, 2006, pp. 257–273.

[15] R. Lu, X. Lin, T. Luan, X. Liang, and X. Shen, “Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs,” IEEE Trans. Vehicular Technology, vol. 61, no. 1, pp. 86-96, Jan. 2012

[16] “Trustworthy Service Selection and Composition “CHUNG-WEI HANG and MUNINDAR P. SINGH North Carolina State University

[17] Evans, M., Hastings, N., and Peacock, B. 2000. Statistical Distributions, 3rd ed. Wiley-Interscience, New

York, NY, USA.

[18] Buntine, W. L. 1994. Operations for learning with graphical models. Journal of Artificial Intelligence Research 2, 159–225

[19] "Sybil Attacks Against Mobile Users: Friends and Foes to the Rescue" Daniele Quercia, Stephen Hailes

[20] C. Gentry and Z. Ramzan, "Identity-based aggregate signatures," in PKC, 2006, pp. 257–273.

[21] R. Lu, X. Lin, T. Luan, X. Liang, and X. Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs," IEEE Trans. Vehicular Technology, vol. 61, no. 1, pp. 86-96, Jan. 2012

[22] D. Boneh and X. Boyen, "Short Signatures without Random Oracles," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), pp. 56-73, 2004

[23] R.Lu,X.Lin and X.Shen,"ECPP:Efficient conditional privacy preservation protocol for secure vehicular communications",in proc 27th ,phoenix,apr2008