Security Based Trustworthy Service Evaluation In Service Oriented Mobile Social Networks

Deepa.v
Faculty of Department of CSE
Velammal Engineering College
Anna University Chennai,India
Email:deeptrinu@gmail.com

Mariyaselvi.J
Student of Department of CSE
Velammal Engineering college
Anna University Chennai,India
Email:jmariyaselvi@gmail.com

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 with out logical central authority. SybilGuard identifies sybils that which every person exchanges keys with a limited numberof 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.
INDEXTERMS:Mobilesocialnetworks,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 amoung several sites.If the local entity has no knowledge about 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 betweenservice composition approaches.

I.1 LITERATURE SURVEY

One promising way to defend against sybil attacks in social networks is to leverage the social network topologies. SybilGurad 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.For example, suppose service A invokes service B, which may invoke E and F with probabilities denote PE and PF

II.PROPOSED SYSTEM

II. 1 TRUST AUTHORITY

Review submission may need cooperations 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 amoung 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.

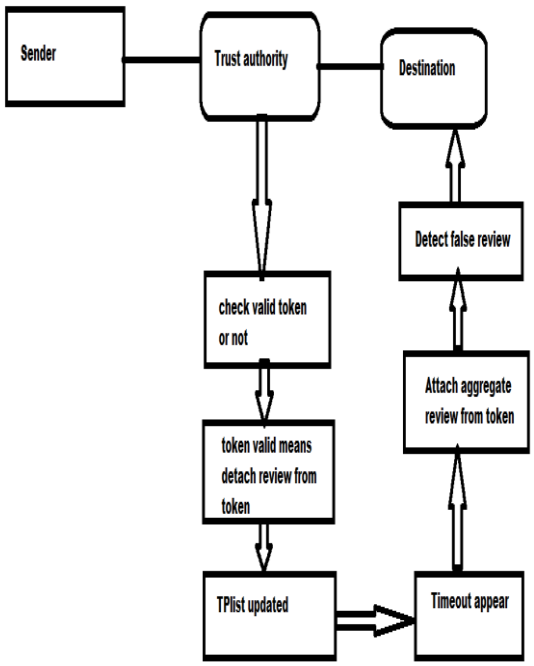

Fig: II. 1 overview of trust authority

III. IMPLEMENTATION MODELS AND ALGORITHMS

III.1ADVANCEDENCRYPTION STANDARD(AES)

It is a symmetric key algorithm .Sender can send the message to the destination that key can be encrypting with 64 bits in my paper.each and every message is very secure in due to the AES algorithm because us government also top secret information are using 192 and 256 key length used.In my project intermediate node will set that is called trust authority.Trust authority can send the request will pass amoung the nodes.AES is more secure than DES because that AES send maximum amount of data transfer with single encryption key with 32 GB.The DES is feistel structure that smaller key size and block size.In the DES block size use 64 bits but in my project use AES concept.In this way maximum amount of transfer 256 exa bytes.In the AES is unbreakable and also using substitution and permutation method..

III.2 THE DESIGN OF TA

In my project TA means trust authority that is intermediate node concept between sender and destination.the review consisits 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 linkability reviews can be linked to real identities.

III.3 DESIGNING PROTOCOL

In my exixting system using DSDV that means distance sequence destination vectorIn this protocol using table driven scheme in mobile adhoc network.Each and every source and destination using routing table that contains routing table information and sequence number.In this protocol that have loss of information is more.

In my proposed system using AASR that means anonymous authenticated security routing.In this protocol is onion routing that means appear in onion layers.In this technique use anonymous communication.originator select set of nodes that chosen make a path which is contain chain or circuit.originator can send the message from first node to second node.second node only decrypt not use the first node.same message can send second node to third node.third node only decrypt it.

III.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 kmeans 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.

III.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.

III.4.1GENERATION OF KEYS

A user ui 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 SYBILATTACK

There are two sybil attacks appear in our project.

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[19] 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[19] 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.

.

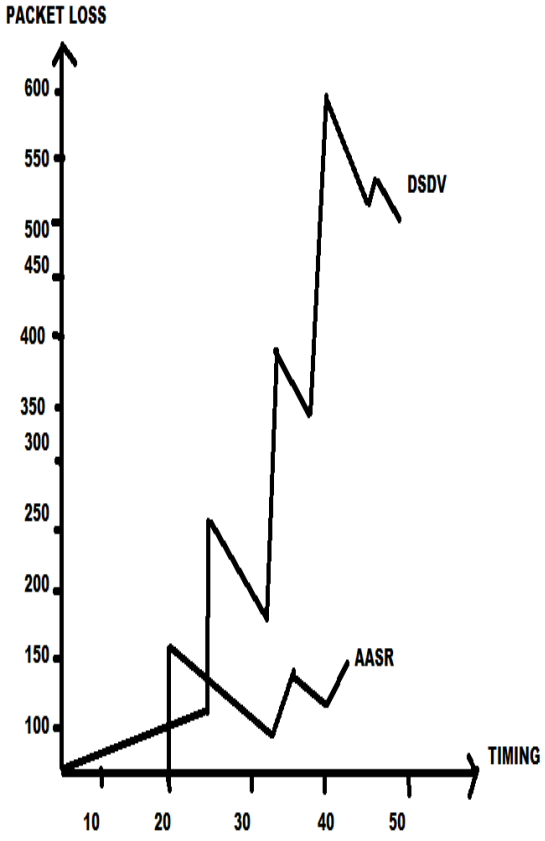

Fig: V. .DELAY RATIO IN TA

.

Delay ratio in TA ,Fig V a) total loss in exist(DSDV), fig V b) Total loss in proposed(AASR)

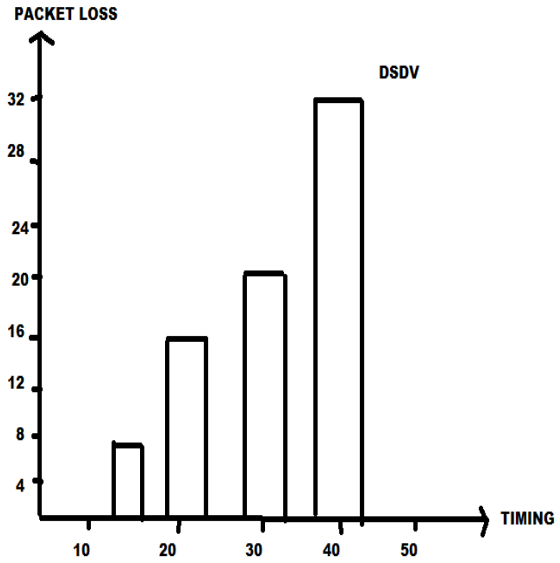

Fig: V a) TOTAL LOSS IN EXISTING PROTOCOL

.

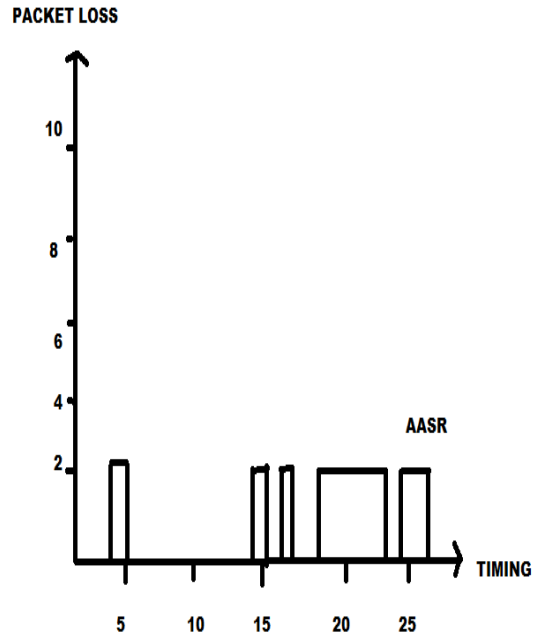

Fig: V b) TOTALLOSSIN PROPOSED(AASR)

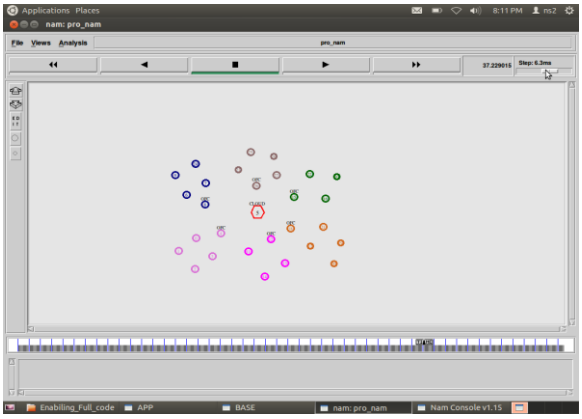

Fig: V C) USING CLOUD SERVICE PROVIDER

VI. CONCLUSION

In this project we explored Trust Authority of intermediate node between source and destination in a 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 serviceoriented web. In Proceedings of the 3rd IEEE International Conference on Industrial Infor-matics (INDIN). IEEE Computer Society, Los Alamitos, CA, USA, 104–109.

[2]F.Dabek,M.F.Kaashoek,D.karger,R.Morris,I.Stoica"widearea 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(1), pp. 86-96, Jan. 2012.