Volume 2, Issue 12, December-2015, pp. 1192-1197 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

In Service-Oriented MSN Providing Trustworthy Service Evaluation

[1]D.RAMANJANEYULU , [2]U.USHA RANI

[1]M.Tech (CSE), Priyadarshini Institute of Technology & Science

[2] Associate Professor (Dept.of CSE), Priyadarshini Institute of Technology & Science

Abstract: In this paper, we are going to propose survey based administration assessment to empower clients to share administration audit in administration situated versatile interpersonal organization. Every administration supplier freely keeps up a TSE for itself, which gathers and stores clients' surveys about its administrations without requiring any third trusted power. The administration surveys can then be made accessible to intrigued clients in settling on savvy administration choice choices. This paper portrays how the audit related normal dangers are destroyed and makes these surveys more fitting and valid. It portrays two frameworks bTSE and SrTSE, these frameworks are depicted to survey related issues and their suitable arrangements. The regular dangers of audits are Linkability, survey dismissal and change which are evacuated by utilizing bTSE; which makes utilization of tokens give incorporated surveys and the framework is progressed and the most vital risk called as Sybil assault is uprooted by utilizing SrTSE; which makes utilization of pseudonyms. Through execution assessment, we demonstrate that the bTSE accomplishes better execution as far as accommodation rate and defer than an administration audit framework that does not receive client collaboration.

Keywords: Mobile Social Networks, Trust Evaluation, Sybil Attack, Distributed System

I. INTRODUCTION

Trustworthy service evaluation (TSE) framework utilized for administration supplier or any third trusted power to get of client input is called audit. Portable Social systems have given the framework to various developing applications as of late, e.g., for the suggestion of administration suppliers or the proposal of documents as services. In these applications, trust is a standout amongst the most essential components in choice making by an administration buyer, requiring the assessment of the reliability of an administration supplier along the social trust ways from an administration shopper to the administration supplier. Be that as it may, there are generally numerous social trust ways between two members who are obscure to each other. Likewise, some social data, for example, social connections in the middle of members and the suggestion parts of members, has critical impact on trust assessment yet has been dismissed in existing investigations of online social systems. Furthermore, it is a challenging problem to search the optimal social trust path that can yield the most trustworthy evaluation result and satisfy a service consumer's trust evaluation criteria based on social information. Privacy is the last aspect of safety in MSNs that has recently gained unprecedented attention. This is particularly because of the social aspect of MSNs in which information relevance like users' location and identity is considered critical issues for both the attackers and system administrators. Many researchers have suggested ways to reveal users' information selectively and for them to remain unnoticed or unidentified over the network. To do this, privacy preferences are generally specified to obfuscate users' private information and present it in a coarser and falsified manner. Moreover, fairness encouragement strategies have been included to prevent heavy congestion in a

particular collaborative node. The goal is to encourage nodes to forward messages and distribute their private information equally. This prevents malicious nodes from intruding into the network and gaining an unauthorized access to valuable resources. Furthermore, as attackers are in direct correlation with the personal profiles in MSNs, methods for private matching have been designed to let two users conceal their personal profiles while in connection. To deliver location based services in MSNs, privacy should be maintained. It can be achieved through different techniques such as obfuscation based schemes, social-based schemes, dynamic pseudonymity, and key anonymity. Meanwhile, the information of each individual should be protected while communicating with the other, so communication privacy should be considered vital for every network. Which allows Business professionals to analyze customers' conversations on social networking sites, and as a consequence, provides real-time status updates about their products and services accordingly in the above situations, trust is one of the most important factors for participants' decision making, requiring approaches and mechanisms for evaluating the trustworthiness between participants who ;are unknown to each other. As an example, if a social network consists of lots of buyers and sellers, it can be used by a buyer to find the most trustworthy/reputable seller who sells the product preferred by the buyer. In social networks, each node represents a participant and each link between participants corresponds to the real-world interactions or online interactions between them (e.g., A→B and A →C in Fig. 1). One participant can give a trust value to another based on the direct interactions between them. For example, a trust rating can be given by a participant to another based on the quality of the movies recommended by the latter at FilmTrust3. As each participant usually interacts with many other participants multiple trust paths. For example, in Fig. 1, A&M are indirectly linked by two paths, A →B →E →M and A →D →M. If a trust path links two nonadjacent participants (i.e., there is no direct link between them), the source participant can evaluate the trustworthiness of the target one based on the trust information of the target one of the trust based information. This process is called trust propagation and the path with trust information linking.

II. SAFETY CHALLENGES IN MSNS

Are considered as a particular type of OppNets, and they share a lot of common characteristics with OppNets and DTNs. As a result, MSNs cover some of the safety concerns related to OppNets as their challenges are partially the same. The first set of works to distinguish safety challenges in an OppNet goes back to the introduction of OppNets were the first to propose OppNets along with a classification of safety challenges, containing privacy and security, in six different steps. They proposed a general safety scheme for OppNets in five mandatory functions in the absence of initial authentication mechanism. Another categorization was deployed where safety challenges in opportunistic people centric sensing were studied and general suggestions to make solutions were discussed. Further attempts to classify safety issues in opportunistic communication were made. This work itemizes basic challenges in OppNets into authenticity, confidentiality, cooperation enforcement, trust establishment, and integrity privacy according to the concerns provided. MSNs include more vital and complex safety concerns in comparison to other resembling networks and contain tons of safety challenging problems, specifically in trust, security, and privacy. There have been few attempts proposing a clear categorization of safety in MSNs. To take an example of these efforts, presented issues around privacy and security for MSNs, along with some methods and implementation for their solutions. They classified problematic issues in three groups, namely: direct anonymity issues, indirect or kanonymity issues, and attacks (eavesdropping, spoofing, replay, and wormhole). Furthermore, they expanded their proposition by designing an identity server (IS) which adopts established privacy and security technologies to provide solutions for these problems. Although some efforts have been made to take safety issues into consideration and make a classifiable observation to enumerate safety challenges and solutions in MSNs, they have been neither comprehensive nor detailed. As far as we know, there has never been an obvious categorization followed by a comprehensive clarification on MSN safety issues. To do this, we classify these issues in three main groups, trust, security, and privacy, and explain noble and novel approaches for possible solutions

III. MOTIVATION

In this paper, we proposed trace – based simulation technique for TSE. TSE system is taken more time for message sending and receiving by user and vendor. That system provide secret key for verification both time ask verification no then process start in proposed system used trace based simulation technique. Time taken is less than according to the existing system. A number of messages can be passing frequently. The dependency information is stored along with packet data in the network trace. By enforcing the ordering constraints in a network simulator, the proposed technique can greatly increase the fidelity of trace driven evaluation with little impact on simulation speed. . Trace based simulation works on two component one that executes action and stores the result and another which reads the log files to trace and interpolates then to new scenario. In the case of large computer design the execution takes place on a small number of nodes and trace are left in log file .In propose system used trace- based simulation technique for increase the work fast. Some important point related to motivation.

1.In this project proposed trace based simulation to enable user to share service review in service oriented mobile social network.

2.Trace based simulation refers to system simulation performed by looking at trace of program execution or system component access with purposed of performance prediction.

3.Trace based simulation works on two component one that executes action and stores the result and another which reads the log files to trace and interpolates then to new scenario.

4.In the case of large computer design the execution takes place on a small number of nodes and trace are left in log file. In this section, we evaluate the performance of the bTSE through trace-based custom simulations. We choose to compare the bTSE with a NCP system, where each user directly submits its review to the vendor without any synchronization constraint (use of tokens).

We use the following performance metrics A. Problem Definition There may be elects of attacks problem review

1. Link ability attack review

2. Rejection attacks

3. Modification and Sybille attack:

Under Sybille attack the bTSE system cannot work as expected. Because single user can also use the pseudonyms to generate multiple unlike fuse review in short time. Time taken is more this mechanism is not portable user. Trustworthy service evaluation (TSE) systems enable service providers or any third trusted authority to receive user feedback, known as service reviews or simply reviews In existing system engages hierarchical signature and aggregate signature techniques to transform independent reviews into structured review chains. Vendors may reject or delete negative reviews and insert forged positive ones the malicious users can leave false negative reviews or drop the reviews from others to decrease the reputation of some particular vendors. In the TSE, the vendor stores and disseminates service information to the users. Note that the adoption of the TSE is subject to vendors' own decisions. However, the users expect to read comprehensive and authentic reviews of services, and this expectation makes vendors who support the TSE appear more attractive than the others. Attacks problem 1review link ability attack 2review rejection attacks modification. Sybille attack: under Sybille attack the BTSE system cannot work as expected. Their behavior cannot be tracked and their personal information cannot be disclosed.

A user generates and submits a no forgeable review to the vendor.

1. Attacks problem 1review link ability attack
2. Review rejection attacks modification. Sybille attack: under Sybille attack the BTSE system cannot work as expected to their behavior cannot be tracked and their personal information cannot be disclosed.
3. A user generates and submits a non-forgeable review to the vendor.
4. In existing system used TSE system that systems have time taken more for message sending and receiving by user and vendor.

B. Innovative Content Location-based services recently emerge as an imperative need of mobile users. It can be integrated into various types of networks to

obtain promising applications while their implementation has many outstanding and independent research issues, such as content delivery, service discovery, security, and privacy problems. Trust evaluation of service providers is a key component to the success of location-based services in a distributed and autonomous network. Location based services require a unique and efficient way to impress the local users and earn their trust so that the service providers can obtain profits used an extra monitor deployed at the untrusted vendor's site to guarantee the integrity of the evaluation results proposed a two-dimensional trust rating aggregation approach to enable a small set of trust vectors to represent a large set of trust ratings. Ayden and Fekri approached the trust management as an inference problem and proposed a belief propagation algorithm to efficiently compute the marginal probability distribution functions representing reputation values. Das and Islam introduced a dynamic trust computation model to cope with the strategically altering behavior of malicious agents. In this paper, we enable mobile users to submit their reviews to a system maintained by the local vendor, where the reviews represent the evaluation results toward the services of the vendor. We consider the malicious behaviors by the vendor and the users including the review attacks and the Sybil attacks. Instead of using an extra monitor device on the vendor's site, we explore user cooperation efforts and make use of efficient cryptography-based techniques to increase SR, reduce SD, and mitigate the effect of the malicious behaviors.

C. Architecture Diagram The vendor maintains a token-pseudonym (tp) 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. The list is updated whenever the vendor receives a new review, and is periodically broadcasted to all users in the vendor's transmission range. Once a token's information is published, the vendor cannot simply remove the token from the TP list because any modification to the list

IV. PROPOSED APPROACH

In the proposed system, we are requiring service providers that maintain the TSE for them. In this regard, we believe that users participating in the TSE cooperatively. So we will study possible malicious behaviors that are performed by service providers and users. The proposed system is fewer to user, it gives more advantages to user based on the different services. Here we identified three different unique review attacks, those are review link ability, review rejection attack and review modification attack. To utilize this services user should register with service provider, here the bTSE is providing the trustworthy between user and service provider. After successful registration user can access the service provider services and user can share his or her reviews. Similarly all service providers should need to maintain the services in this format to provide the user review comments. The system is so reliable that every service provider to user must provide valid credentials. The system uses the technique of classification for easy ranking. Using the TSE, service providers learn that the experiences of service users and are able to improve their service strategy over time. The views expressed can then make available to the public, which are enhanced service announcements and useful to users in making wise selections services. They are important for service providers that target the global market tools. In this, the S-TSE we move in the configuration MSN. Each user must first register on the network and then you can use the services provided by the service provider. Similarly each service provider must also provide their credentials to register on a social network. We develop security mechanisms for the TSE to deal with the attacks that occur during the mobile network. The basic TSE (bTSE) is allows users to distribute and cooperatively should submit their views in the form of integrated chain using techniques hierarchical and aggregates signature. Restricts service providers to reject, modify or delete comments. Thus, integrity and authenticity of comments are improved. We extend the bTSE to a Sybil TSE (SrTSE) resisted to allow detection of two types of Sybil attacks. In the SrTSE, if a user generates multiple criticisms of a seller at a time interval with different pseudonyms, he will release the actual identity of the user. Through security analysis and numerical results it shows that the BTSE and effectively resist attacks SrTSE review SrTSE service and also detect Sybil attacks in an efficient manner. Through performance evaluation, we show that the bTSE achieves better performance in terms of rate and delay submission of a review system service that does not take the user cooperation. First, users of mobile social network cannot directly access service providers or trusted third authority to receive comments from users that is a review of service or

simply revised, as compliments and complaints about their services or products. IV. RESULTS To demonstrate the proposed approach, we implemented a prototype application using java technology and its related API with support of MySQL database provider. Here we used the hardware configuration as Intel core processor, 1GB RAM and 100 GB HDD. The following screen1 shows the vendor login page.

IV. PERFORMANCE EVALUATION

In this section, we evaluate the performance of the bTSE through trace-based custom simulations. We choose to compare the bTSE with a NCP system, where each user directly submits its review to the vendor without any synchronization constraint (use of tokens). We use the following three performance metrics: 1. SR. It is defined as the ratio of the number of successfully submitted reviews to the total number of generated reviews in the network. 2. SD. It is defined as the average duration between the time when a review is generated and the time when it is successfully received by the vendor.

We conduct two sets of simulations under the situations with/without the review rejection attacks (R). We vary SR between 150 and 300 m, and token number TN between 1 and 10. As analyzed in, the bTSE resists the review link ability and modification attacks through cryptography techniques and specially designed review structure, and mitigates review rejection attack through cooperative review submission. The first two attacks have no influence on review submission. In our simulation study, we are, therefore, interested only in the impact of review rejection attack on the system performance. Each review is a value ranged in [0, 1].

A review is negative if its value is lower than 0.5. The vendor performs review rejection action by rejecting all negative reviews. When multiple reviews are aggregated and submitted together, the vendor accepts them all if their average value is no less than 0.5, or rejects them all otherwise. We place the vendor at the centers of the 10 hotspots in turn and conduct 50 simulation runs for each placement. Using the total 500 simulation runs, we obtain the average results to be analyzed in the next section.

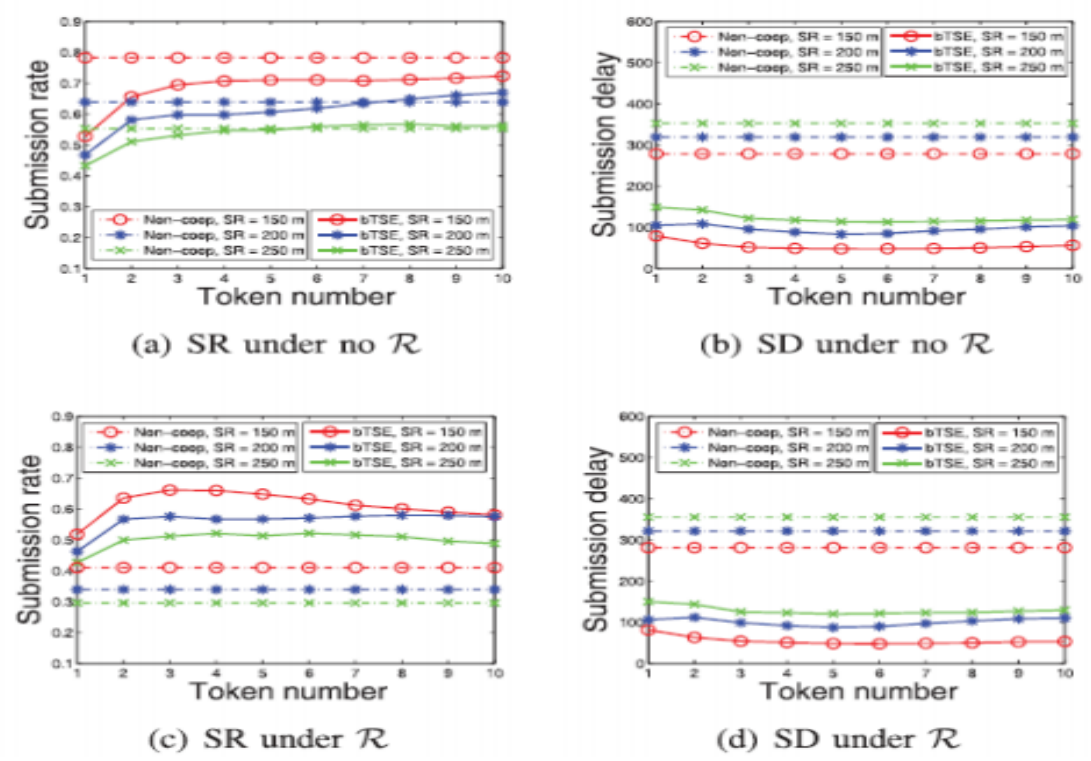

Fig.1. Performance evaluation of TSE.

V. CONCLUSION

In this paper, we have proposed review based simulation for TSEs. The system engages hierarchical signature and aggregate signature techniques to transform independent reviews into structured review chains. This transformation involves distributed user cooperation, which improves review integrity and significantly reduces vendors' modification capability. We have presented three review attacks and shown that the bTSE can effectively resist the review attacks without relying on a third trusted authority. We have also considered the notorious Sybil attacks and demonstrated that such attacks cause huge damage to the bTSE. We have subsequently modified the construction of pseudonyms and the corresponding secret keys in the bTSE, and obtained a Security analysis and numerical results show the effectiveness of the SrTSE to resist the Sybil attacks. Further trace-based simulation study demonstrates that the bTSE can achieve high SRs and low SDs. we plan to develop a social network based trust-oriented social service and service provider search engine, which maintains a database of participants and the complex social network among them. In this system, our proposed method will be applied, for instance, to help a buyer identify the most trustworthy.

REFERENCES

[1] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure Friend Discovery in Mobile Social Networks," IEEE, 2011.

[2] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, "Seer: A Secure and Efficient Service Review System for ServiceOriented Mobile Social Networks," IEEE, 2012.

[3] X. Liang, X. Li, T. Luan, R. Lu, X. Lin, and X. Shen, "Morality- Driven Data Forwarding with Privacy Preservation in Mobile Social Networks," IEEE, 2012.

[4] T.H. Luan, L.X. Cai, J. Chen, X. Shen, and F. Bai, "VTube: Towards the Media Rich City Life with Autonomous Vehicular Content Distribution," IEEE, 2011.

[5] J.R. Douceur, "The Sybil Attack," Proc. Revised Papers First Int'l Workshop IPTPS, 2002.

[6] J. Newsome, E. Shi, D.X. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," IPSN, 2004.

[7] D. Quercia and S. Hailes, "Sybil Attacks Against Mobile Users: Friends and Foes to the Rescue," IEEE, 2010.

[8] D. Quercia and S. Hailes, "Sybil Attacks Against Mobile Users: Friends and Foes to the Rescue," Proc. IEEE INFOCOM, pp. 336- 340, 2010.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, "A Dynamic Privacy-Preserving Key Management Scheme for LocationBased Services in VANETs," IEEE Trans. Intelligent Transportation Systems, vol. 13, no. 1, pp. 127-139, Mar. 2012.

[10] 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.

[11] X. Boyen and B. Waters, "Full-Domain Subgroup Hiding and Constant-Size Group Signatures," Proc. 10th Int'l Conf. Practice and Theory Public Key Cryptography, pp. 1- 15, 2007.

[12] X. Liang, Z. Cao, J. Shao, and H. Lin, "Short Group Signature without Random Oracles," Proc. Ninth Int'l Conf. Information and Comm. Security (ICICS), pp. 69-82, 2007.

