International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

A Novel Approach to Provide Trustworthy Service Evaluation in Mobile Social Networks

Macharla Lokesh[1]; B.Maria Joseph[2]& M. Narendhar[3]

[1]PG Scholar, Dept of CSE, Dept of CSE, SCIENT Institute of Technology & Sciences, Ibrahimpatnam,R.R.Dist, Telangana.

[2]Assistant professor, Dept of CSE, SCIENT Institute of Technology & Sciences, IbrahimpatnamR.R.Dist, Telangana.

[3]Associate Professor, Dept of CSE, SCIENT Institute of Technology & Sciences, IbrahimpatnamR.R.Dist, Telangana.

Abstract:

In this paper, a new approach proposed Trustworthy Service Evaluation (TSE) aims to enable users to share opinions in service oriented mobile social networking (S-MSN). Each service provider retains independently a TSE itself, which collects and stores user reviews about their services without any third party trusted authority. The reviews on services can be made available to interested users in making wise decisions for selecting services. Review identified three unique service, that is, link ability, rejection or modification attacks, and develop sophisticated security mechanisms for the TSE to deal with these attacks. Specifically, the basic TSE (bTSE) allows users to submit a distributed and cooperative their views in 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 TSE, Sybil-resisted (SrTSE) to allow detection of two typical Sybil attacks. In the SrTSE, if a user generates multiple criticisms of a vendor in a predefined time slot with different pseudonyms, it will be given to know the real identity of the user. Through security analysis and numerical results it shows that the bTSE and SrTSE effectively resist review attacks & SrTSE service and also detect Sybil attacks in an efficient manner.

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

I. INTRODUCTION

SERVICE-ORIENTED mobile social networks (S-MSNs) are emerging social networking platforms over which one or more individuals are able to communicate with local service providers using handheld wireless communication devices such as smartphones. In the S-MSNs, service providers (restaurants and grocery stores) offer location based services to local users and aim to attract the users by employing various advertising approaches, for example, sending e-flyers to the nearby passengers via wireless connections.

Unlike the global counterparts, the interests of the local service providers are in serving the users in close geographic vicinity because most users choose services based on the comparison of the service quality and the distance advantage. In the S-MSNs, to establish the trust relations between the service providers and the users is particularly important. With a higher reputation, a service provider is more likely to be chosen by the users. However, the S-MSNs are autonomous and distributed networks where no third trusted authority exists for bootstrapping the trust relations. Therefore, for the users in the S-MSNs, how to enable the trust evaluation of the service providers is a challenging problem.

Trustworthy service evaluation (TSE) systems enable service providers or any third trusted authority to receive user feedback, known as

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

service reviews or simply reviews, such as compliments and complaints about their services or products. By using the TSE, the service providers learn the service experiences of the users and are able to improve their service strategy in time. In addition, the collected reviews can be made available to the public, which enhances service advertising and assists the users in making wise service selections. The TSE is often maintained by a third trusted authority who is trusted to host authentic reviews. Popular TSE can be found in web based social networks such as Facebook and online stores like eBay.

They are important marketing tools for service providers who target the global market. In this paper, we move the TSE into the S-MSN settings. We require service providers to maintain the TSE by themselves. In the meantime, we consider the users participate in the TSE in a cooperative manner. We will study possible malicious behaviors conducted by the service providers and the users. For ease of presentation, we refer to service providers as vendors in the sequel.

We consider an S-MSN composed of static vendors and mobile users that interconnect opportunistically. Each vendor is equipped with a wireless communication device that has a large storage space. 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.

Without in-network third trusted authorities in the SMSN, vendors are required to manage reviews for themselves. This requirement brings unique security problems to the review submission process. For example, vendors may reject or delete negative reviews and insert orged positive ones, and the malicious users can leave false negative reviews or drop the reviews from others to decrease the reputation of some particular vendors. In the design of the TSE for the S-MSN, security mechanisms must be included to resist these attacks. Notorious sybil attacks also cause huge damage to the effectiveness of the TSE

II. 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.

- In this project proposed trace based simulation to enable user to share service review in service oriented mobile social network.
- Trace based simulation refers to system simulation performed by looking at trace of program execution or system component access with purposed of performance prediction.
- 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.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

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

- SR. It is defined as the ratio of the number of successfully submitted reviews to the total number of generated reviews in the network.
- 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

III. 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 behaviour cannot be tracked and their personal information cannot be disclosed. A user generates and submits a non-forgeable review to the vendor.

- 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 non-forgeable review to the vendor.
- In existing system used TSE system that system have time taken more for message sending and receiving by user and vendor.

IV. 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.

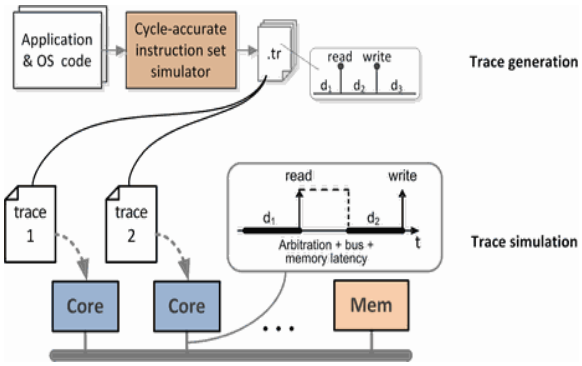

Figure 1: System Architecture

Once a token's information is published, the vendor cannot simply remove the token from the TP list because any modification to the list will cause inconsistency with previously published information and be noticed by the public.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

V. Justifications of Results

In this paper we consider attacks where legitimate users generate false reviews. As reviews are subjective in nature, it is difficult to determine whether the content of an authentic review is false or not. However, the TSE must prevent the sybil attacks, which subvert the system by creating a large number of pseudonymous entities, using them to gain a disproportionately large influence. Since the TSE assigns multiple pseudonyms to a registered user, the sybil attacks can easily happen in the TSE as follows

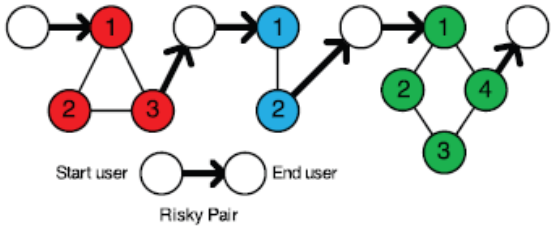

Figure 2: Chain and Ring Structure

Therefore, in the bTSE, we adopt a hybrid structure (chain and ring), as shown in Fig. 3, to limit the modification capability of the vendor below Oð1Þ. Because this structure has a chain as its skeleton, in the sequel we refer to it as "chain" for ease of our presentation.

VI. Related Works

Popular social networks including Facebook, Myspace andFlickr, and validated thesmall-worldand power-law characteristics (i.e., in a social network, the probability that a nodehas degree *k* is proportional to k¡r, r >1) of online social networks using data mining techniques. Also using data miningtechniques, McCollum et al. discovered the social roles(e.g., *a* chief financial officer or in-house lawyer) and socialrelationships (e.g., partnership in a fundingapplication) in anemail based online social network of further analyzed the influence of social interactionsbetween buyers on the purchase decisions made by a buyer in buying products in online shopping websites. Trust is a critical factor in the decision-making of participants in online social networks. In this field, several trust management methods have been proposed. A Mobile Social Network (MSN) is a type of Delay Tolerant Networks (DTNs) but considers an environment where users contact each other in their daily activity. Prior works on MSNs or DTNs can be classified into three categories: unicast, multicast, and content dissemination.

VII. CONCLUSION

In this paper, we proposed a TSE system for S-MSN. The system involves the hierarchical aggregates signature and signature techniques to transform independent reviews on the revision structured chains. This transformation involves distributing user cooperation, enhancing the integrity of opinion and significantly reduces the ability to change vendors. We have presented three attacks revision shows that the bTSE can effectively resist the attacks of review without relying on a third trusted authority. We have also considered the notorious Sybil attacks and proved that such attacks cause enormous damage to the bTSE. We then modified the construction of pseudonyms and secret keys corresponding to the bTSE and obtained SrTSE system. The SrTSE allows users to leave only a criticism of a supplier in a preset time. If multiple views with different aliases of a user are generated, the true identity will be revealed to the public. Safety analysis and numerical results show the effectiveness of SrTSE to resist Sybil attacks. Further study of simulation based on the footprint shows that thebBTSE can achieve high SRs and low standard deviations.

VIII.REFERENCES

[1] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure Friend Discovery in Mobile Social Networks," Proc. IEEE INFOCOM, pp. 1647-1655, 2011.

[2] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, "Seer: A Secure and Efficient Service Review System for Service-Oriented Mobile Social Networks," Proc. IEEE 32nd Int'l Conf. Distributed Computing Systems (ICDCS), pp. 647-656, 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 Trans. Vehicular Technology, vol. 61, no. 7, pp. 3209-3222, Sept. 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," Proc. IEEE CS Eighth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. Networks (SECON), pp. 359-367, 2011.

[5] J.R. Douceur, "The Sybil Attack," Proc. Revised Papers First Int'l Workshop Peer-to-Peer Systems (IPTPS), pp. 251-260, 2002.

[6] J. Newsome, E. Shi, D.X. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," Proc. Third Int'l Symp. Information Processing in Sensor Networks (IPSN), pp. 259-268, 2004.

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

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

[9] 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.

[10] 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.

[11] 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.

[12] C. Gentry and Z. Ramzan, "Identity-Based Aggregate Signatures," Proc. Int'l Conf. Public Key Cryptography, pp. 257-273, 2006.

[13] Y. Zhang, Z. Wu, and W. Trappe, "Adaptive Location-Oriented Content Delivery in Delay-Sensitive Pervasive Applications," IEEE Trans. Mobile Computing, vol. 10, no. 3, pp. 362-376, Mar. 2011.

[14] H. Tsai, T. Chen, and C. Chu, "Service Discovery in Mobile Ad Hoc Networks Based on Grid," IEEE Trans. Vehicular Technology, vol. 58, no. 3, pp. 1528-1545, Mar. 2009.