IPHV8I1019X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

EFFICIENT SECURITY PROOFS FOR TRUST WORTHY SERVICES IN MOBILE SOCIAL NETWORKS

[#1]K.CHANDRASENA CHARY, Associate Professor,
[#2]GANTA SOWMYA, M.Tech Student,
Dept of CSE,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, T.S., INDIA.

Abstract: Mobile Social Network is network which allows mobile users to discover and interact with existing and potential friends. A Trustworthy Service Evaluation (TSE) system is a system that enables users to share service reviews in Service oriented mobile social networks (S-MSNs). Each service provider should independently maintain a TSE for itself that collects and stores users' reviews about its services without requiring any third trusted authority. These service reviews can be made available to interested users to make service selection decisions. In this three unique service review attacks are identified, i.e., link ability, rejection, and modification attacks, and then develop security mechanisms for the TSE to deal with these attacks. In this we extend the bTSE(basic TSE) to a Sybil-resisted TSE (SrTSE) which enable the detection of two typical sybil attacks. In SrTSE if a user generates multiple reviews toward a vendor in a predefined time slot with different pseudonyms, the real identity of that user will be revealed. Hence a Trustworthy Service in Mobile Social Network is introduces so that users can access services securely. After identifications with various grammars they are categorized in order and trustworthy service evaluation system is enabled for the users to share their reviews of a particular music sheet they are buying through their smart phones or tabs in service oriented mobile social networks(S-MSN)without any third trusted party. Since there are no third trusted parties there are many chances for Sybil attacks and other modification review attacks which are to be avoided.

Keywords: Mobile social networks trust evaluation, Sybil attack, and distributed system..

I.INTRODUCITON

Trustworthy service evaluation (TSE) systems [7] enable the service providers or any third authority to receive user feedback, such as service reviews or simply reviews, as compliments and complaints about their services. By using the TSE, the service providers come to know the service experiences of the users and are able to improve the service strategy in time. The collected reviews can then be made available to the public, which enhances service advertising and assists the users in making wise service selections. The TSE is maintained by a third trusted authority that is trusted to host authentic reviews. Popular TSE can found in web based social networks such as Facebook and 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.

In the S-MSNs, service providers offer location based services to local users and attract the users by various advertising approaches, for example, sending e-flyers to the nearby passengers via wireless connections. With a higher reputation, a service provider is likely to be chosen by the users. However, the S-MSNs are autonomous and distributed networks where no third trusted authority needed for bootstrapping the trust relations. Therefore, for the users in the S-MSNs, enable the trust evaluation of the service providers that is a challenging problem. Location-based services now 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.

In the design of the TSE for the S-MSN, security mechanisms must be included for these attacks. Notorious Sybil attacks [5], [6], [7], [8] cause damage to the effectiveness of the TSE. The multiple pseudonym techniques [9] are adopted in many distributed networking systems for privacy preservation and locations of users. On the one hand, users are able to frequently change their pseudonyms to prevent the linkage of their behaviors at different time/location. Their behavior cannot be tracked as well as their personal information cannot be disclosed. As a result, they are more willing to use mobile applications. We consider S-MSN composed of static vendors and mobile users that. Each vendor should equip with a wireless communication

device that is having a large storage space [4]. In the TSE, vendor stores and disseminates service information to the users. Without in-network third authorities in the SMSN, vendor is required to manage reviews for themselves. These requirements bring unique security problems to the review submission process. For example, vendors can reject or delete negative reviews and insert forged positive ones, and the malicious users may leave false negative reviews or drop reviews from others to decrease reputation of some particular vendors. In design of the TSE for S-MSN, security mechanisms are included to resist these attacks. In the design of TSE for the S-MSN, security is present to deal with these attacks. Under Sybil attacks, the bTSE cannot work as expected because single user can abuse pseudonyms to generate multiple unlikable false reviews in a short time.

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. 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.

II.RELATED WORK

Mobile social networks extend social networks in the by allowing mobile users to discover and interact with existing and potential friends. Despite their promise to enable exciting applications, serious security and privacy concerns have hindered wide adoption of these networks [1].

A. Secure Friend Discovery

An important capability offered by mobile social networks is that to allow mobile users to discover and interact with friends. Suppose you are waiting for your flight in an airport and your mobile phone discovers your friend's friend is in the next aisle and you can talk with face-to-face. Or you visit a new place and your mobile phone finds someone in your vicinity shares similar attributes as you so that you can interact with. Suppose you are waiting for your flight in an airport and your mobile phone discovers your friend's friend is in the next aisle and you can talk with face-to-face. Or you visit a new place and your mobile phone finds someone in your vicinity shares similar attributes as you so that you can interact with.

One way to address the privacy and security issues is to take advantage of a trusted central server, which collects information from individual users, computes and disseminates the proximity results on demand. Server-based solution is not suitable for mobile social networks for the following reasons. First, users in a mobile social network may not have direct access to a computer or the Internet.

B. Dynamic Privacy-Preserving Key Management

For vehicle user's privacy preservation to improve key update efficiency of location based services (LBSs) in vehicular ad -hoc networks (VANETs), we propose a dynamic privacy-preserving key management scheme, called DIKE. We divide session into several time slots so t each time slot holds a different key, when no vehicle user departs from the service session. In this also integrate a novel dynamic threshold technique in traditional V-2-V and V-2-I communications to achieve session key's backward-secrecy. Performance evaluations for extensive simulations demonstrate the efficiency and effectiveness of the proposed DIKE scheme for low key update delay and fast key update ratio.

In this paper, we achieve vehicle user's privacy Preservation and to improve the key update efficiency. In this a Dynamic privacy-preserving Key management scheme, called DIKE, for the LBSs in VANETs. With this scheme, each user can use a pseudo-id to conceal its real identity during a service session. First, introduce a privacy-preserving authentication (PPA) mechanism, which can derive from an efficient group Signature. However, each vehicle user can hold multiple pseudonyms; so cannot prevent a compromised but unrevoked vehicle user to do double registration in the same session. That's why we divide a session into several time slots, and each time slot can hold a different session key. When no vehicle departs from the service session, each joined user use forward-secrecy technique to autonomously update new session key to reduce key update delay. To achieve backward-secrecy, we integrate a novel dynamic threshold technique in traditional V-2-V and V-2-I communications.

C. The Sybil Attack

The Sybil attack was first introduced by Douceur in the context of peer-to-peer networks. In this, we investigate the Sybil attack, which is a harmful attack in sensor networks. In Sybil attack, a malicious node behaves like it was a larger number of nodes, like by impersonating other nodes or simply by claiming false identities. We propose novel techniques to defend against Sybil attack, and analyze their effectiveness

properly. In this paper, we examine how the Sybil attack can used to attack several protocols in wireless sensor network. So first consider attacks on distributed storage an algorithm, similar to the Douceur describes in the peer-to-peer environment.

To defend the Sybil attack, we can value that each node identity is an identity presented by the corresponding physical node. There are two types to validate an identity we define the Sybil attack and establish taxonomy of that attack by distinguishing different attack types. The definition and taxonomy are important in understanding and analyzing the threat that defenses of Sybil attack. We present several novel methods by which a node can be verified whether other identities are Sybil identities.

A Sybil attack is like computer hacker attack on a peer-to-peer (P2P) network. It is named by the novel Sybil, which recounts medical treatment of a woman with extreme dissociative identity disorder. The attack target only reputation system of the P2P program and also allows the hacker to have an unfair advantage in influencing the reputation and the score of files stored on the P2P network. Several factors determine that how a Sybil attack can be equally affects the reputation system and how easy it is to make an entity; finally whether the program accepts non-trusted entities and their input. Validating accounts can be the best way for administrators to prevent these kinds of attacks, but this sacrifices the anonymity of users.

III. EXISTING SYSTEM

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.

IV. 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 [4] 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 [10] 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.

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.

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 [13], service discovery [14], security, and privacy problems [15]. 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. Rajan and Hosamani used an extra monitor deployed at the untrusted vendor's site to guarantee the integrity of the evaluation results. Wang and Li [10] 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. Dasand 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.

V. PROPOSED SYSTEM

In the proposed system, we are requiring service providers that will maintain the TSE by themselves. In this, we consider the users that participate in the TSE in a cooperative manner. So we are going to study possible malicious behaviors that are conducted by the service providers and users. Due to the proposed system, there are advantages that offer the user of the services, it identifies three unique review attacks, i.e., review link ability attack, review rejection attack, and review modification attack in the bTSE each user should firstly register in the social network and then they can use the services provided by the service provider. Similarly each service provider should also provide their credentials to register in a social network. After using the services the user should also provide reviews for every service. So that the users who wanted to use that services should get the idea about that service.

As the system is trustworthy so each service provider and user should provide valid credentials. The system uses the Ranking technique for making the ranking easy. Using the TSE, service providers learn that the service experiences of the users and that are able to improve their service strategy in time. The collected reviews can then make available to the public, which are enhances service advertising and helpful the users in making wise service selections. They are important tools for service providers who target the global market. In this, we move the TSE into the S-MSN settings. Each user should firstly register in the social network and then they can use the services provided by the service provider. Similarly each service provider should also provide their credentials to register in a social network. We develop security mechanisms for the TSE to deal with the attacks that are arise during mobile social network. The basic TSE (bTSE) is enables users to distribute and cooperatively should submit their reviews in an integrated chain form by using hierarchical and aggregate signature techniques. It restricts the service providers to reject, modify, or delete the reviews. Thus, the integrity and authenticity of reviews are improved. Further, we extend the bTSE to a Sybil-resisted TSE (SrTSE) to enable the detection of two types of Sybil attacks. In the SrTSE, if a user generates multiple reviews toward a vendor in a time slot with different pseudonyms, the real identity of the user will be revealed. Through security analysis and numerical results, we show that the bTSE and the SrTSE effectively resist the service review attacks and the SrTSE additionally detects the Sybil attacks in an efficient manner. Through performance evaluation, we show that the bTSE achieves better performance in terms of submission rate and delay than a service review system that does not adopt user cooperation. First, users in a mobile social network cannot have direct Access to service providers or any third trusted authority to receive user feedback that is service reviews or simply reviews, such as compliments and complaints about their services or products.

VI.CONCLUSIONS

In this paper, we proposed a TSE system for S-MSNs. The system uses hierarchical signature and aggregate signature techniques to transform independent reviews into structured review chains. This transformation includes distributed user cooperation, which improves review integrity and significantly reduces vendors' modification capability. We have presented three review attacks which shows that the bTSE can effectively resist review attacks without relying on a third trusted authority. Construction of pseudonyms and the secret keys in the bTSE, and obtained a SrTSE system.

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] 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] 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.