Enhancement of High SRs and Low SDs of bTSE using Trace Based Simulation in Mobile Social Network

Rajesh Kumar[1], R. Hariharan[2]

[1]MCA Final year , Veltech Technical University, Avadi Chennai, India

[2]Asst Prof.of IT Department, Veltech Technical University, Avadi Chennai, India

Abstract: ***In this paper we are going to 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 performance prediction.Trace based simulation works on two component one that executes action and stores the result and another which reads the log files. The simulator reads log file and simulation performance of very large application based on the execution trace on much smaller number of nodes.Trace based mechanism will enhanced the submission rate because files are submitted in the log file and this mechanism also reduce the (SDs) submission delay increase the (SRs) submission relay in (TSE) trustworthy service evolution. This paper describes a new trace-based simulation technology that captures dependencies between social network messages observed in full-system simulation of multithreaded applications.Validation of protocols for these network relies almost exclusively on simulation. Using trace – based simulation to study different network topologies and properties which can be done much faster unfortunately unless the traces that are used include information about dependencies between messages (packets), full system simulation is very slow the execution time can grow quadratic ally with increased node counts.These traces only include information about the order of and time between packet transmissions. Trace based simulation we have developed a technique that allows us to add dependency information to traces.***

Keywords: Trace – based simulation, Log file, Mobile social network, bTSE.

1. Introduction

Trustworthy service evaluation[3] (TSE) system used for service provider or any third trusted authority to receive of user feedback is called review.Mobile Social networks have provided the infrastructure for a number of emerging applications in recent years, e.g., for the recommendation of service providers or the recommendation of files as services. In these applications, trust is one of the most important factors in decision making by a serviceconsumer, requiring the evaluation of the trustworthiness of a service provider along the social trust paths from a service consumer to the service provider. However, there are usually many social trust paths between two participants who are unknown to one another. In addition, some social information, such as social relationships between participants and the recommendation roles of participants, has significant influence on trust evaluation but has been neglected in existing studies of online social networks. 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. 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 path.

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), [6] the source participant can evaluate the trustworthiness of the target one based on the trust information of the target on of the trust based information.This process is called [5] trust propagation and the path with trust information linking

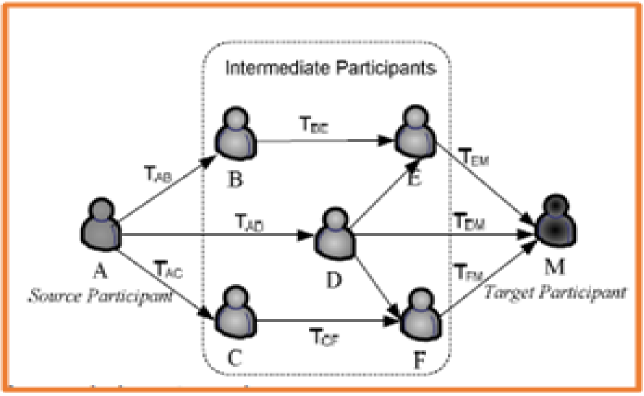

Fig.ure 1: A social network

The source participant and the target one is called a social trust path For example, in Fig. 1, if A is a buyer and M is a seller, A can evaluate the trustworthiness of M using the social trust paths from A to M. We refer to A as the source participant and M as the target participant. This paper describes a new trace-based simulation technology that captures dependencies between social network messages observed in full-system simulation of multithreaded applications.

2. 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.

3. 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 behaviour 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.

4. 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 [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. 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.

5. 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.

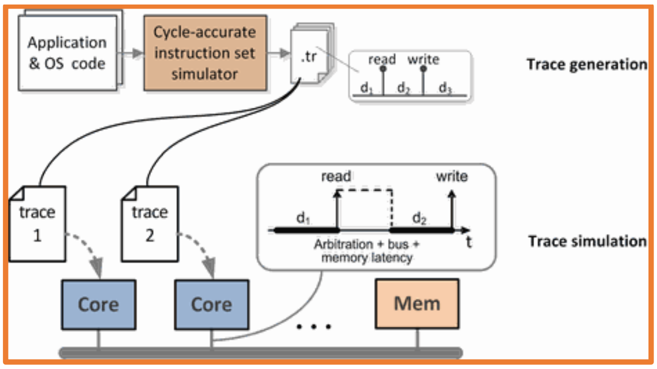

Figure 2: System Architecture

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.

6. 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

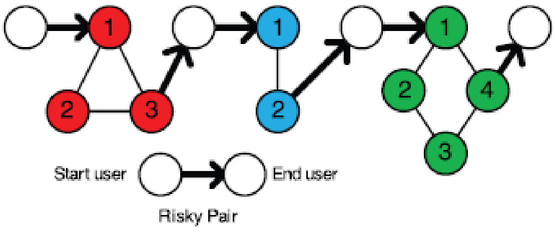

Figure 3: Chain and Ring Structure

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.

7. Related Works

Popular social networks including Facebook, Myspace andFlickr, and validated the small-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.

Conclusion

In this paper, we have proposed a trace 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.

Reference

[1] S. Fiske. *Social Beings: Core Motives in Social Psychology*. John Wiley and Sons, 2009.
[2] Q. Gao, Q. Qu, and X. Zhang. Mining social relationships in microblogging systems In *HCII*, pages 110–119, 2011.

[3] S. Guo, M. Wang, and J. Leskovec. The role of social networks in online shopping information passing, price of trust, and consumer choice. In *EC'11*, pages 130–137, 2011.

[4] H. Liu, E.-P. Lim, H. W. Lauw, M.-T. Le, A. Sun, J. Srivastava, and Y. A. Kim. Predicting trusts among users of online communities: an epinions case study. In *EC*, pages 310–319, 2008.

[5] H. Ma, T. Zhou, M. Lyu, and I. King. Improving recommender systems by incorporating social contextual information. *ACM Transactionson Information Systems*, 29(2), 2011.

[6] A. McCollum, X. Wang, and A. Corrode-Emmanuel. Topic and role discovery in social networks with experiments on Enron and academic email. *Journal of Artificial Intelligence Research*, 30(1):249–272, 2007.

[7] W. Wei, F. Xu, C.C. Tan, and Q. Li, "Sybil defender: Defend against Sybil Attacks in Large Social Networks," Proc. IEEE INFOCOM, pp. 1951-1959, 2012.

[8] "Social Group, "Wikipedia, http://en.wikipedia.org/wiki/Social_group, 2013.

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

[10] 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.

[11] G. Hendry et al., "Analysis of photonic networks for a chip multiprocessor using scientific applications, "Networks-on-Chip, International Symposium on, vol. 0, pp. 104–113, 2009.

[12] Y. Pan et al., "Firefly: illuminating future network-on-chip with Nano photonics," SIGARCH Compute. Archit. News, vol. 37, no. 3, pp. 429–440, 2009.

[13] X. Li, N. Mitton, and D. Simplot-Ryl, "Mobility Prediction Based Neighborhood Discovery for Mobile Ad Hoc Networks," Proc. IFIP Int'l Conf. Networking (NETWORKING), pp. 138151, 2011.

[14] B. Viswanath, A. Post, P.K. Gummadi, and A. Mislove, "An Analysis of Social Network-Based Sybil Defenses," Proc. ACM SIGCOMM, pp. 363-374, 2010.

[15] A. Mohaisen, N. Hopper, and Y. Kim, "Keep Your Friends Close: Incorporating Trust into Social Network-Based Sybil Defenses," Proc. IEEE INFOCOM, pp. 1943-1951, 2011.