SYBILDEFENDER: DEFEND AGAINST SYBIL ATTACKS IN LARGE SOCIAL NETWORKS

Sumalatha[1],S.RaijaSulthana[2]
[1]Mtech,cse,bcetw,A,p,India
[2]Mtech,cse,bcetw,A,p,India

ABSTRACT

A Trustworthy Service Evaluation (TSE) system to enable users to share service reviews in service-oriented mobile social networks (S-MSNs). Each service provider independently maintains a TSE for itself, which collects and stores users' reviews about its services without requiring any third trusted authority. The service reviews can then be made available to

interested users in making wise service selection decisions. We identify three unique service review attacks, i.e., linkability, rejection,and modification attacks, and develop sophisticated security mechanisms for the TSE to deal with these attacks. Specifically, the basicTSE (bTSE) enables users to distributedly and cooperatively 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 typical sybil attacks. In the 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.

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.

INTRODUCTION

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.

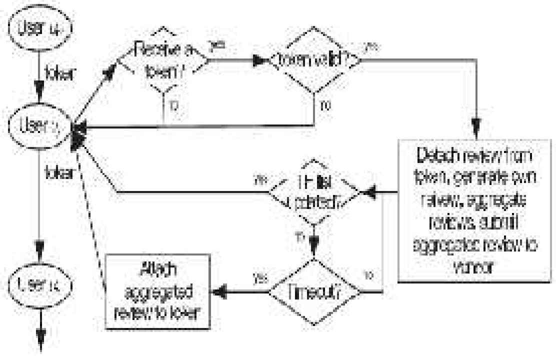
User u
token
Receive a token?
yes
no
Token valid?
yes
no
User u
token
Detach review from token, generate own review, aggregate reviews, submit aggregated review to vendor
yes
The last contacted?
no
User u
Attach aggregated review to token
yes
Timeout?
no

Fig:Review generation and submission.

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.

PROPOSED SYSTEM

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.

CONCLUSION

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.

Further trace-based simulation study demonstrates that the bTSE can achieve high SRs and low SDs.

REFERENCE

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