Enabling Trustworthy Service Evaluation in Service-Oriented Mobile Social Networks

Abstract—In this paper, we propose 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 basic TSE (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 basic TSE to a Sybil-resistant 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 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.

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 smart phones. 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 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.
Proposed System

Our contributions can be summarized as follows: We propose a basic trustworthy service evaluation (bTSE) system and an extended Sybil-resistant TSE (SrTSE) system for the S-MSNs. In both systems, no third trusted authorities are involved, and the vendor locally maintains reviews left by the users. The vendor initializes a number of tokens, which are then circulated among the users to synchronize their review submission processes. After being serviced by a vendor, a user generates and submits a non forgeable review to the vendor. The user cannot proceed with the review submission until it receives a token from the vendor.

If the review submission succeeds, the user will forward the token to a nearby user who is wishing to submit a review to the same vendor; otherwise, the user will forward both the token and its own review to the receiver, expecting that receiver user will cooperate and submit their reviews together. During token circulation, a hierarchical signature technique is adopted to specify and record each forwarding step in the token, and a modified aggregate signature technique is employed to reduce token size. Both signature techniques are also used during cooperative review submission for reducing communication overhead and improving review integrity. Specifically, we identify three unique review attacks, i.e., review link ability attack, review rejection attack, and review modification attack in the bTSE. We also introduce two typical sybil attacks, which cause huge damage to the bTSE. Under the sybil attacks, the bTSE system cannot work as expected because a single user can abuse the pseudonyms to generate multiple unlinked false reviews in a short time. To resist such attacks, in the SrTSE, the pseudonyms are embedded with a trapdoor; if any user leaves multiple false reviews toward a vendor in a predefined time slot, its real identity will be revealed to the public. Through the security analysis and numerical results, we show that both the bTSE and the extended SrTSE are secure against the possible attacks. We further evaluate the performance of the proposed bTSE in comparison with a noncooperative (NCP) system that does not engage cooperative review submission. Simulation results indicate that the bTSE achieves significantly (up to 100 percent) higher submission rates (SRs) in the presence of the review rejection attacks, and (up to 75 percent) lower submission delays (SDs) in general than the NCP system, at the cost of reasonable cooperation overhead.

Advantages of Proposed System

In this paper, we have proposed a TSE system for S-MSNs. The system engages hierarchical signature and aggregate signature techniques to transform independent reviews into structured review chains.

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System: Pentium IV 2.4 GHz.
- Hard Disk: 40 GB.
- Floppy Drive: 1.44 Mb.
- Monitor: 15 VGA Colour.
- Mouse: Logitech.
- Ram: 512 Mb.
SOFTWARE REQUIREMENTS:

• Operating system : - Windows XP.
• Coding Language : Java.
• Data Base : MY SQL