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 bTSE 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 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.

**PROBLEM DEFINITION:**

- 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.

**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. 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.
ADVANTAGES OF PROPOSED SYSTEM:

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

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System: Pentium IV 2.4 GHz.
- Hard Disk: 40 GB.
- Floppy Drive: 44 Mb.
- Monitor: 15 VGA Colour.
- Ram: 512 Mb.

SOFTWARE REQUIREMENTS:

- Operating system: Windows XP/7.
- Coding Language: JAVA/J2EE
- IDE: Netbeans 7.4
- Database: MYSQL

REFERENCE:

Xiaohui Liang, Student Member, IEEE, Xiaodong Lin, Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE “Enabling Trustworthy Service Evaluation in Service-Oriented Mobile Social Networks” IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014.