ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
An ISO 3297: 2007 Certified Organization Vol.3, Special Issue 4, April 2015
National Conference On Emerging Trends in Information, Digital & Embedded Systems (NC'e-TIDES -15)
Organized by
Dept. of ECE, Annamacharya Institute Of Technology & Sciences, Rajampet, Andhra Pradesh-516126, India held on 28th February 2015

Entitle Credible Service Outline in Mobile Social Networks

G Yamini

Dept. of C.S.E., AITS, Rajampet, Andhra Pradesh, India

ABSTRACT: To setup users to share service reviews in service-oriented mobile social networks (S-MSNs). Each service provider independently maintains a TSO for itself, which collects and then 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 informed service selection decisions. We identify three unique service review intrusions, i.e., linkability, rejection, and modification intrusions, and develop sophisticated security mechanisms for the TSO to deal with these intrusions. basic Trusty Service Outline (bTSO) enables users to It restricts the service jobholders to reject, modify, or delete the reviews. extend the bTSO to a Sybil-resisted Trusty Service Outline (SrTSO) to empower the detection of two typical sybil attacks. In the SrTSO, 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.

KEYWORDS: Mobile social networks, trust evaluation, Sybil attack, distributed system, Performance Evaluation.

I. INTRODUCTION

SERVICE-ORIENTED mobile social networks (S-MSNs) [1], [2], [3] 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 offer location based services to local users and aim to attract the users by employing various advertising approaches 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.

This requirement brings unique security problems to the review submission process. Propose a basic trusty service outline (bTSO) system and an extended Sybil-resisted TSO (SrTSO) 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. To resist such attacks, in the SrTSO, 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.

II. RELATED WORK

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 [4], service discovery [5], security, and privacy problems [6]. 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
An ISO 3297: 2007 Certified Organization Vol.3, Special Issue 4, April 2015
National Conference On Emerging Trends in Information, Digital & Embedded Systems (NC'e-TIDES -15)
Organized by
Dept. of ECE, Annamacharya Institute Of Technology & Sciences, Rajampet, Andhra Pradesh-516126, India held on 28th February 2015

that the service providers can obtain profits used an extra monitor deployed at the untrusted vendor's site to guarantee the integrity of the evaluation results.

III. PROPOSED ALGORITHM

a. Design Considerations:

- Reviews should be collected from the user independently.
- Avoid the linkability, rejection and modification attacks.
- Avoid Sybil attacks.
- Using distributed network for reviews.
- Maintain hybrid review Structure.
- Synchronization of tokens is necessary.

B.Description of the Proposed Algorithm:

SECURITY MODEL:

Due to the lack of centralized control, the S-MSN is vulnerable to various security threats. The group authorities are trusted but not a part of the network. In the following, we describe several malicious attacks that aim particularly at the TSO. Review attack 1. Review linkability attack is executed by malicious users, who claim to be members of a specific group, but disable the group authority to trace the review back to its unique identity, thus breaking review linkability. Review attack 2. Review rejection attack is launched by the vendor when a user submits a negative review to it. In the attack, the vendor drops the review silently without responding to the submission request from the user, and hides public opinions and mislead users. Review attack 3. Review modification attack is performed by the vendor toward locally stored review collections. The vendor inserts forged complimentary reviews, or modifies/deletes negative reviews in a review collection. Sybil attack 1. Such an attack is launched by malicious users: One registered user leaves multiple reviews toward a vendor in a time slot, where the reviews are false and negative to the service.

Sybil attack 2. Such an attack is launched by malicious vendors with colluded users: A malicious vendor asks one registered user to leave multiple reviews toward itself in a time slot, where the reviews are positive to the service. The above two sybil attacks produce inaccurate information, which is unfair to either vendors or users, and disrupt the effectiveness of the TSO. To this end, we propose another security mechanism to effectively resist the sybil attacks by restricting each user to generate only one review toward a vendor in a predefined time slot. If any user generates two or more than two reviews with different pseudonyms toward a vendor in a time slot, its real identity will be exposed to the public.

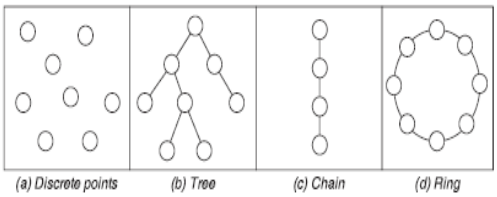


Fig. 1. Basic Review Structures

STRUCTURED REVIEWS:

In the bTSO, reviews are structured to reflect their adjacency (i.e., submission order) through user cooperation. As such, vendors simply rejecting or modifying reviews will break the integrity of the review structure, thus being detected by the public. Consider a collection of n reviews received by a vendor v. We define four basic review structures (as illustrated in Fig. 1) and indicate vendors' review modification capabilities corresponding to them. In Fig. 1, reviews appear as discrete points, meaning that they are submitted separately and independent of each other. This independence gives the vendor maximum capability of manipulating the n reviews, and its modification capability is therefore O(log n).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
An ISO 3297: 2007 Certified Organization Vol.3, Special Issue 4, April 2015
National Conference On Emerging Trends in Information, Digital & Embedded Systems (NC'e-TIDES -15)
Organized by
Dept. of ECE, Annamacharya Institute Of Technology & Sciences, Rajampet, Andhra Pradesh-516126, India held on 28th February 2015

SYNCHRONIZATION TOKENS

The chain structure requires reviews to be submitted sequentially. The bTSO uses a token technique to synchronize review submission. The vendor spontaneously initializes a number of tokens and issues them to distinct users, one per user. The tokens will then be circulated among users according to their local decision on token forwarding. A user cannot submit a review unless it currently holds one of the tokens. A token may be lost due to user mobility or malicious dropping. The vendor considers a token lost if it has not received any review submission associated to the token for a predefined maximum time duration-exp. It replaces lost tokens with new ones so as to maintain a constant number of active tokens and stable system performance. Each token leads to an independent review chain. The vendor's review modification capability is proportional to the number of review chains. The more review chains, the less trustworthy the reviews from users' viewpoint. Thus, the vendor has the motivation to keep the token number as small as possible. On the other hand, there should be sufficient tokens to avoid token starvation problem, where some user never obtains a token to leave its review. A user, when having a review to submit, transmits a token request message. After receiving the request, a nearby user currently holding a token or the vendor (if having a spare token) may send the token to the requesting user. The requesting user accepts the first arrived valid token and
replies with an ACK message. For other received tokens, it replies with a RETURN message, indicating that it no longer needs a token. The token request, ACK and RETURN messages are signed by senders using (pseudonym) secret keys, which are non forgeable.

IV. PSEUDO CODE

Step 1: Generate all possible Reviews and generate token by the vendor for submitting particular review to service provider.
Step 2: Reducing token size by signature aggregation
Step 3: Let G and GT be two cyclic additive groups with the
same order q, and e : G* G→ GT be a bilinear pairing
P is a generator of G. Key generation. A user uj if registering to a group authority chj will receive a bunch of pseudonym secret keys corresponding to randomly generated pseudonyms
Pidj,hj Within a social group, the pseudonyms are never repeatedly assigned to users. The pseudonym secret keys
$psk_{j,h_j,*} = (k_{j,0}, k_{j,1})$, where $k_{j,0} = s_{h_j} P_{j,0} = s_{h_j} H_1(pid_{j,h_j,*} \| 0)$
and $k_{j,1} = s_{h_i} P_{j,1} = s_{h_i} H_1(pid_{j,h_i,*} \| 1)$.
Signing. uj generates a string as str == "v'', where v
represents the identity of the vendor. Note that, all tokens are toward a specific vendor at a time period t. Therefore, the string can be obtained by other similar users.
Step 4: The signature on m will be
$\sigma_j = Sign_{psk_{j,h_j,*}}(m_j) = (str, S_j, R_j)$
where Ps=H1(str), Bj=H2(mj, Pidi,hj,*,str) and randomly chosen from Z/qZ Aggregation. Multiple signatures with the common str can be aggregated.
Step 5: User generates and submits non forgeable review to the service provider.
Step 6: End

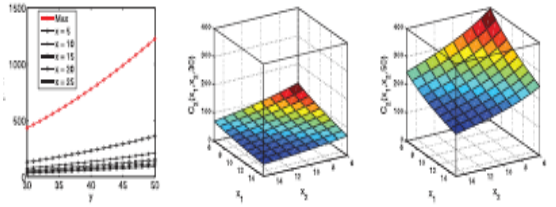
V. SIMULATION RESULTS

If a user leaves two or more false reviews with different pseudonyms toward a vendor in a time slot, its real identity can be derived by the vendor and other users. P2. If a user leaves only one review toward a vendor in a time slot, its real identity can be protected.
We first consider the property P1 of the SrTSO. We consider a malicious user uj generates two false reviews that include two signatures on mj. The two pseudonyms are different.
From the signature, j,1 can be obtained. If both signatures are valid, the relations of j,1,j,2,j,3 can be verified. Since j,2 and j,3 are included in the message of j,4 their authenticity can also be verified. From the two reviews, anyone can obtain j,1H1(m,j) and j,2H1(m,j) and derive

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
An ISO 3297: 2007 Certified Organization Vol.3, Special Issue 4, April 2015
National Conference On Emerging Trends in Information, Digital & Embedded Systems (NC'e-TIDES -15)
Organized by
Dept. of ECE, Annamacharya Institute Of Technology & Sciences, Rajampet, Andhra Pradesh-516126, India held on 28th February 2015

$$id_j H_1(m_j) = \frac{H_2(pid_{j,h_j,2})a_{j,1} - H_2(pid_{j,h_j,1})a_{j,2}}{H_2(pid_{j,h_j,2}) - H_2(pid_{j,h_j,1})} \cdot H_1(m_j). \quad (6)$$



(a) 1 attacker (b) 2 attackers (y = 30) (c) 2 attackers (y = 50)

Fig. 4. Efforts on detecting the Sybil Attack.

choose to compare the bTSO 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 three 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. population density dm of the spots and highlights the selected hotspots, which are the candidate places to host the vendor.

VI. CONCLUSION AND FUTURE WORK

Proposed a TSO system for S-MSNs. 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 bTSO 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 bTSO. We have subsequently modified the construction of pseudonyms and the corresponding secret keys in the bTSO, and obtained a SrTSO system. The SrTSO allows users to leave only one review toward a vendor in a predefined time slot. If multiple reviews with different pseudonyms from one user are generated, the real identity will be disclosed to the public. Security analysis and numerical results show the effectiveness of the SrTSO to resist the sybil attacks. Further trace-based simulation study demonstrates that the bTSO can achieve high SRs and low SDs.

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] Y. Zhang, Z. Wu, and W. Trappe, "Adaptive Location-Oriented Content Delivery in Delay-Sensitive Pervasive Applications," IEEE Trans. Mobile Computing, vol. 10, no. 3, pp. 362-376, Mar. 2011.
[5] H. Tsai, T. Chen, and C. Chu, "Service Discovery in Mobile Ad Hoc Networks Based on Grid," IEEE Trans. Vehicular Technology, vol. 58, no. 3, pp. 1528-1545, Mar. 2009.
[6] Z. Zhu and G. Cao, "Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System," IEEE Trans. Mobile Computing, vol. 12, no. 1, pp. 51-64, Jan. 2013.

BIOGRAPHY

G Yamini persuing M.Tech in Computer Science & Engineering in the college of AITS,Rajampet. And have presented the papers in national conference.