

Spring 2015

Enabling Trustworthy Service Evaluation in Service-Oriented Mobile Social Network

Krishna Chaitanya Devabhakthini
Governors State University

Karthik Konda
Governors State University

Shravan Sydugari
Governors State University

Follow this and additional works at: <http://opus.govst.edu/capstones>

 Part of the [Systems Architecture Commons](#)

Recommended Citation

Devabhakthini, Krishna Chaitanya; Konda, Karthik; and Sydugari, Shravan, "Enabling Trustworthy Service Evaluation in Service-Oriented Mobile Social Network" (2015). *All Capstone Projects*. 132.
<http://opus.govst.edu/capstones/132>

For more information about the academic degree, extended learning, and certificate programs of Governors State University, go to http://www.govst.edu/Academics/Degree_Programs_and_Certifications/

Visit the [Governors State Computer Science Department](#)

This Project Summary is brought to you for free and open access by the Student Capstone Projects at OPUS Open Portal to University Scholarship. It has been accepted for inclusion in All Capstone Projects by an authorized administrator of OPUS Open Portal to University Scholarship. For more information, please contact opus@govst.edu.

Abstract

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. It identifies three unique service review attacks, i.e., linkability, rejection, and modification attacks, and develops 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, it extends 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 security analysis and numerical results, it shows 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, it shows that the bTSE achieves better performance in terms of submission rate and delay than a service review system that does not adopt user cooperation.

Table of Contents

Abstract.....	I
1. Introduction.....	1
2. Literature Review.....	4
3.1 Secure Friend Discovery in Mobile Social Networks.....	4
3. VTube: Towards the Media Rich City Life with Autonomous Vehicular Content Distribution.....	5
4. The Sybil Attack.....	7
5. The Sybil Attack in Sensor Networks: Analysis & Defences.....	8
6. Service Discovery in Mobile Ad Hoc Networks Based on Grid	9
7. Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System.....	11
8. Factors Affecting the Online Travel Buying Decision: A Review.....	15
9. Tisa: Toward Trustworthy Services in a Service-Oriented Architecture.....	16
10. Existing System.....	
10.1 Disadvantages.....	20
11. Proposed System.....	20
11.1 Advantages.....	21
12. Hardware Requirements.....	21
13. Software Requirements.....	21
14. Modules.....	22
15. S-MSN Formation.....	22
16. Providing Services.....	23
17. Review Generation and Submission.....	23
18. Sybil Attack Detection.....	24
19. Data Flow Diagram.....	25
20. UML Diagram	26
21. Screenshots of Execution.....	28
22. References.....	42

Introduction

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 Itb-based social networks such as Facebook and

online stores like eBay. They are important marketing tools for service providers who target the global market. In this paper, It move the TSE into the S-MSN settings. It require service providers to maintain the TSE by themselves. In the meantime, It consider the users participate in the TSE in a cooperative manner. It will study possible malicious behaviors conducted by the service providers and the users. For ease of presentation, It refer to service providers as vendors in the sequel. It 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. Without in-network third trusted authorities in the S-MSN, vendors are required to manage reviews for themselves. This requirement brings unique security problems to the review submission process. For example, vendors may reject or delete negative reviews and insert forged positive ones, and the malicious users can leave false negative reviews or drop the reviews from others to decrease the reputation of some particular vendors. In the design of the TSE for the S-MSN, security mechanisms must be included to resist these attacks. Notorious sybil attacks also cause huge damage to the effectiveness of the TSE. The multiple pseudonym techniques are generally adopted in many distributed networking systems for privacy preservation of the identities and locations of users. 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. As a result, they are more willing to use mobile applications. On the other hand, in trust systems like the TSE, if users abuse their

pseudonyms to leave reviews toward a vendor, the reputation of the vendor can be easily increased or decreased. Even if a trusted authority later identifies the malicious behavior, the detection delay cannot be tolerated in the TSE. It is necessary to tackle how to resist the Sybil attacks and guarantee both review integrity and review authenticity in the design of the TSE for the S-MSN. Our contributions can be summarized as follows: It propose a basic trustworthy service evaluation (bTSE) system and an extended Sybil-resisted 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-forgable 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, It identify three unique review attacks, i.e., review linkability attack, review rejection attack, and review modification attack in the bTSE. It also introduce two typical sybil attacks, which cause huge damage to the bTSE.

Literature Review

Secure Friend Discovery in Mobile Social Networks

With increasing popularity of mobile social networks, it is important to develop secure and practical protocols to enable users to effectively interact with each other. It develop a secure friend discovery protocol for mobile social networks, and use both analysis and real implementation to demonstrate its feasibility and effectiveness. It hope that it will inspire other researchers to explore protocol design for mobile social networks, which is a rapidly growing area. Mobile social networks extend social networks in the cyberspace in to the real world by allowing mobile users to discover and interact with existing and potential friends who happen to be in their physical vicinity. Despite their promise to enable many exciting applications, serious security and privacy concerns have hindered wide adoption of these networks. To address the seconcerns, It develop novel techniques and protocols to compute social proximity betlten two users to discover potential friends, which is an essential task for mobile social networks. It make three major contributions. First, It identify a range of potential attacks against friend discovery by analyzing real traces. Second, it develop a novel solution for secure proximity estimation , which allows users to identify potential friends by computing social proximity in a privacy - preserving manner. A distinctive feature of our solution is that it provides both privacy and verifiability, which are frequently at odds in secure multi-party computation. Third, It demonstrate the feasibility and effectiveness of our approaches using real implementation on smart phones and show it is efficient in terms of both computation time and poItr consumption.

VTube: Towards the Media Rich City Life with Autonomous Vehicular Content Distribution

Vehicular networks have attracted considerable attention from both academia and industry, the penetration of wireless communication in vehicles seems still to be a slow and gradual process. This raises the conflict between the every-increasing user demand on content sharing and limited communication device and capacity available. Therefore, deploying a large scale cost-effective infrastructure for content dissemination is necessary in an urban area. It has proposed VTube, an autonomous infrastructure for urban content distribution, to address the issue. VTube is built additively by stimulating distributed entities to deploy their own RSBs at very low cost and, more importantly, is self-organized to large scale with a fully distributed design. It has embodied the design of VTube with the system architecture, performance analysis of users and the formulation of optimal content replications. Based on the optimization formulation, It has developed a fully distributed random walk based algorithm. Using the trace-based simulations, It has demonstrated that the distributed content replication used in VTube can render users the near optimal download delay. In our future work, It intends to deploy VTube in practice and evaluate its performance in the real-world situations. Moreover, It will investigate VTube in a more heterogeneous environment over a wide area, where contents have diverse volumes and popularity in different regions of the area.

The copious social and user generated contents, like Facebook and Youtube, are reshaping the way people share, access, and digest information. Although flourishing in Internet, content sharing services are still considered expensive and not ready for mobile users of vehicular networks. In this paper, It proposes VTube, an autonomous and cost-effective infrastructure, to facilitate the localized content publish/subscribe in an urban area. VTube relies on the distributed low-cost light-tight storage buffers, namely roadside buffer, installed in the city facilities, such as stores, museums, cafeteria, etc., to cache and publish contents for mobile

users. The contents at different storage buffers are then transported to different locations by moving vehicles and cached collaboratively in both vehicles and storage buffers across the city. In this work, It unfold the design of VTube by first presenting the detailed design principles and practices of VTube. Given the content availability and capacity of the buffer storage, It then develop a mathematical model to evaluate the mean download delay of mobile users. Using the delay as an input, It formulate the content replication problem in roadside buffers as a stochastic programming problem to attain the mean system-wide minimum download delay. Finally, It propose a fully distributed random walk based algorithm to solve the optimization problem. Extensive simulations demonstrate that VTube can minimize the download delay of users because of the exploitation of vehicle mobility and distributed buffer storage at different locations.

The key of VTube is to replicate contents in RSBs placed in different locations towards the optimal user download experience. Notice that the considered network is not only large scale but also dynamic with hundreds of RSBs continuously publishing new contents. Therefore, the proposed content replication scheme of RSBs should be fully distributed and dynamically adapt to the changing network status. The global optimal replication should provide an optimal solution to OPT. However, as both A and D are global system parameters which may not be available to individual RSBs or vehicle nodes, the global optimal replication scheme is not practical for large scale real-world deployment; nevertheless, the global optimal replication provides a benchmark for performance comparison with other replication schemes. In what follows, It propose a decentralized algorithm to determine the content replication at RSBs.

The Sybil Attack

Peer-to-peer systems often rely on redundancy to diminish their dependence on

potentially hostile peers. If distinct identities for remote entities are not established either by an explicit certification authority (as in Farsite) or by an implicit one (as in CFS), these systems are susceptible to Sybil attacks, in which a small number of entities counterfeit multiple identities so as to compromise a disproportionate share of the system. Systems that rely upon implicit certification should be acutely mindful of this reliance, since apparently unrelated changes to the relied-upon mechanism can undermine the security of the system. For example, the proposed IPv6 privacy extensions obviate much of the central allocation of IP addresses assumed by CFS. In the absence of an identification authority, a local entity's ability to discriminate among distinct remote entities depends on the assumption that an attacker's resources are limited. Entities can thus issue resource-demanding challenges to validate identities, and entities can collectively pool the identities they have separately validated.

Large-scale peer-to-peer systems face security threats from faulty or hostile remote computing elements. To resist these threats, many such systems employ redundancy. However, if a single faulty entity can present multiple identities, it can control a substantial fraction of the system, thereby undermining this redundancy. One approach to preventing these "Sybil attacks" is to have a trusted agency certify identities. This paper shows that, without a logically centralized authority, Sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities.

An identity is an abstract representation that persists across multiple communication events. Each entity e attempts to present an identity i to other entities in the system. (Without loss of generality, we state our results with respect to a specific local entity l that is assumed to be correct.) If e successfully presents identity i to l , we say that l accepts identity i . A straightforward form for an identity is a secure hash of a public key. Under standard cryptographic assumptions,

such an identifier is unforgeable. Furthermore, since it can generate a symmetric key for a communication session, it is also persistent in a useful way. Each correct entity c will attempt to present one legitimate identity. Each faulty entity f may attempt to present a legitimate identity and one or more counterfeit identities. Ideally, the system should accept all legitimate identities but no counterfeit entities.

The reason for establishing the distinctness of identities is to allow the local entity to employ redundancy in operations it delegates to remote entities. One such operation it could conceivably delegate is the validation of other identities. Thus, in addition to accepting identities that it has directly validated using one of the challenge mechanisms described above, an entity might also accept identities that have been validated by a sufficient count of other identities that it has already accepted. If an entity that has presented identity i_1 claims to have accepted another entity's identity i_2 , it says that i_1 vouches for i_2 .

The Sybil Attack in Sensor Networks: Analysis & Defenses

It defines the Sybil attack and establishes a taxonomy of this attack by distinguishing different attack types. The definition and taxonomy are very important in understanding and analyzing the threat and defenses of a Sybil attack. It presents several novel methods by which a node can verify whether other identities are Sybil identities, including radio resource testing, key validation for random key pre-distribution, position verification and registration. The most promising method among these is the random key pre-distribution which associates a node's keys with its identity. Random key pre-distribution will be used in many scenarios for secure communication, and because it relies on well-understood cryptographic principles it is easier to analyze than other methods. These methods are robust to compromised nodes. In particular, it has been shown that in the multi-space pairwise scheme with each node storing 200 keys, the

attacker would need to compromise 400 nodes before having even a 5% chance of being able to fabricate new identities for the Sybil attack.

Security is important for many sensor network applications. A particularly harmful attack against sensor and ad hoc networks is known as the Sybil attack, where a node illegitimately claims multiple identities. This paper systematically analyzes the threat posed by the Sybil attack to wireless sensor networks. It demonstrate that the attack can be exceedingly detrimental to many important functions of the sensor network such as routing, resource allocation, misbehavior detection, etc. It establish a classification of different types of the Sybil attack, which enables us to better understand the threats posed by each type, and better design counter measures against each type. It then propose several novel techniques to defend against the Sybil attack, and analyze their effectiveness quantitatively.

Service Discovery in Mobile Ad Hoc Networks Based on Grid

we focus on hybrid service discovery protocol and improve its performance using large zone and controlling advertisement message that used for updating service lookup tables, It use multi level zone and specially two-level zones for simplification, for avoiding traffic increasing It reduce advertisement frequency in outer level. This frequency reductions yielded inconsistency in service lookup tables in nodes that located in external zones and for its management we change the border cast protocol in our algorithm. Results show that our algorithm operates better than traditional hybrid service discovery protocol and in spite of service information inconsistency achieve acceptable Hit ratio of successful service delivery.

Hybrid service discovery is introduced as an efficient service discovery protocol in mobile ad-hoc grid witch has a good compromise between response time and network traffic overhead. In this paper we modify the basic idea of this protocol called Zone. We use multi-level

zone in our proposal and called the protocol as multi-level hybrid service discovery protocol. Our algorithm tries to provide the advantage of larger zone with only a little increase of network traffic overhead. We used two levels of zone, inner zone and outer zone which we called internal zone and external zone, respectively. Difference between two zones issued from their advertisement frequency. Simulation results show that our proposed algorithm has better performance in network's traffic and response time than traditional hybrid service discovery protocol. First of all, we must modify service lookup table and advertisement message structure of any node in ad-hoc grid environment. We add a field Zone-type to them. We use this field to distinguish type of the server base on its location in internal zone or external zone. Based on the value of this field, information in service lookup table is divided into two types: 1. Information about the services that belongs to nodes in internal zone, 2. information about the services that belongs to nodes in external zone. Furthermore, we use Hop-count value to limit the extension of advertisement message, the value of Hop count will be set to RI to cover the internal zone, of course, for covering the external zone, in every FI times we will set Hop-count value to RE, that means advertisement messages forwarded out to nodes in external zone. When a neighbor node receives this message should update its own service lookup table based on that message. The receiver node should specify Zone-type and type of server as an external or internal server. If the Zone-type value is Internal, the node doesn't need to do any extra work, but when the Zone-type value is External, the Hop-count field of the message should be evaluated. If $\text{Hop-count} < \text{RI}$, it means that distance between the server and the receiver nodes is more than RI hop, therefore the server is placed in external zone and receiver node sets the Zone-type field of this node by 'External' value in service lookup table. After this, receiver sends the messages to all neighbor nodes. In the following we focused on the condition that the information in external zone is not

always accurate, because advertisement and update frequency in this area are lower than internal zone. To support this condition, the query mechanism of hybrid service discovery protocol must be modified; which is described in the following.

Mobile ad-hoc grid is a computational environment that use parallel and distributed technology. Computing nodes in this system establish on mobile ad-hoc network, so this technology combines capability of traditional grid with flexibility of mobile ad-hoc networks. However, the development of ad-hoc grids entails new challenges compared to traditional wired grids. Resource discovery, power consumption, QoS security and etc, are problems that have still to be solved. In this paper we study in-depth the problem of resource discovery in mobile ad-hoc grids.

Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System

A privacy-preserving location proof updating system called APPLAUS, where collocated Bluetooth enabled mobile devices mutually generate location proofs and upload to the location proof server. We use statistically changed pseudonyms for each device to protect source location privacy from each other, and from the un trusted location proof server. We also develop a user-centric location privacy model in which individual users evaluate their location privacy levels in real time and decide whether and when to accept a location proof exchange request based on their location privacy levels. To the best of our knowledge, this is the first work to address the joint problem of location proof and location privacy. To deal with colluding attacks, we proposed betweenness ranking based and correlation clustering - based approaches for outlier detection. Extensive experimental and simulation results show that APPLAUS can provide real-time location proofs effectively. Moreover, it preserves source location privacy and it is collusion resistant. Today's location-sensitive service relies on user's mobile device to determine the

current location. This allows malicious users to access a restricted resource or provide bogus alibis by cheating on their locations. To address this issue, we propose A Privacy-Preserving Location proof Updating System (APPLAUS) in which colocated Bluetooth enabled mobile devices mutually generate location proofs and send updates to a location proof server. Periodically changed pseudonyms are used by the mobile devices to protect source location privacy from each other, and from the un trusted location proof server. We also develop user-centric location privacy model in which individual users evaluate their location privacy levels and decide whether and when to accept the location proof requests. In order to defend against colluding attacks, we also present between ness ranking-based and correlation clustering-based approaches for outlier detection. APPLAUS can be implemented with existing network infrastructure, and can be easily deployed in Bluetooth enabled mobile devices with little computation or power cost. Extensive experimental results show that APPLAUS can effectively provide location proofs, significantly preserve the source location privacy, and effectively detect colluding attacks.

In APPLAUS, mobile nodes communicate with neighboring nodes through Bluetooth, and communicate with the un trusted server through the cellular network interface. Based on different roles they play in the process of location proof updating, they are categorized as Prover, Witness, Location Proof Server, Certificate Authority or Verifier. Prover: the node who needs to collect location proofs from its neighboring nodes. When a location proof is needed at time t , the prover will broadcast a location proof request to its neighboring nodes through Bluetooth. If no positive response is received, the prover will generate a dummy location proof and submit it to the location proof server. Witness: Once a neighboring node agrees to provide location proof for the prover, this node becomes a witness of the prover. The witness node will generate a location

proof and send it back to the prover. Location proof server: As our goal is not only to monitor real-time locations, but also to retrieve history location proof information when needed, a location proof server is necessary for storing the history records of the location proofs. It communicates directly with the prover nodes who submit their location proofs. As the source identities of the location proofs are stored as pseudonyms, the location proof server is untrusted in the sense that even though it is compromised and monitored by attackers, it is impossible for the attacker to reveal the real source of the location proof. Certificate authority: As commonly used in many networks, we consider an online CA which is run by an independent trusted third party. Every mobile node registers with the CA and pre-loads a set of public/private key pairs before entering the network. CA is the only party who knows the mapping between the real identity and pseudonyms (public keys), and works as a bridge between the verifier and the location proof server. It can retrieve location proof from the server and forward it to the verifier. Verifier: a third-party user or an application who is authorized to verify a prover's location within a specific time period. The verifier usually has close relationship with the prover, e.g., friends or colleagues, to be trusted enough to gain authorization. When a prover needs to collect location proofs at time t , it executes the protocol to obtain location proofs from the neighboring nodes within its Bluetooth communication range. Each node uses its M pseudonyms $PM_i^{1/41}$ as its identity throughout the communication. The prover broadcasts a location proof request to its neighboring nodes through Bluetooth according to its update scheduling. The request should contain the prover's current pseudonym P_{prov} , and a random number R_{prov} . The witness decides whether to accept the location proof request according to its witness scheduling. Once agreed, it will generate a location proof for both prover and itself and send the proof back to the prover. This location proof includes the prover's pseudonym P_{prov} , prover's random number

R_{prov} , witness's current time stamp T_{witt} , witness's pseudonym P_{witt} , and their shared location L . This proof is signed and hashed by the witness to make sure that no attacker or prover can modify the location proof and the witness cannot deny this proof. It is also encrypted by the server's public key to prevent from traffic monitoring or eavesdropping. After receiving the location proof, the prover is responsible for submitting this proof to the location proof server. The message also includes prover's pseudonym P_{prov} and random number R_{prov} , or its own location for verification purpose. An authorized verifier can query the CA for location proofs of a specific prover. This query contains a real identity and a time interval. The CA first authenticates the verifier, and then converts the real identity to its corresponding pseudonyms during that time period and retrieves their location proofs from the server. In order not to expose correlation between pseudonyms to the location server, CA will always collect enough queries from k different nodes before a set of queries are sent out. The location proof server only returns hashed location rather than the real location to the CA, who then forwards to the verifier. The verifier compares the hashed location with the claimed location acquired from the prover to decide if the claimed location is authentic. In order to prevent the CA from knowing locations of a real identity, the location proof server calculates the hash of each location and only sends the hashed locations to the CA. In this way, the following property can be achieved.

Factors Affecting the Online Travel Buying Decision: A Review

It implies that those consumers with online shopping experience have greater intention to search online information, which positively affects intention to purchase online. Further study should research situations where search behavior and the subsequent purchase behavior are performed through different channels(i.e. information search performed in a traditional retail store followed by actual purchase performed online, and vice versa.). The comparison of the

various combinations of situations might produce more fruitful results. Future studies also need to include such stages as problem identification, alternative evaluation, and post-purchase in the purchase decision-making processes in addition to the information search and purchase intention stages, which is the main focus of the present study. Another possible research area is to investigate the effect of other variables such as media attributes, consumer characteristics, product attributes (i.e., search, experience, credence goods), and search conditions as well as the five independent variables (i.e., utilitarian value of information search, hedonic value of information search, perceived benefits of Internet shopping, perceived risk of Internet shopping, purchase experience) employed in our research. The present study also has a limitation in terms of the sample. Subjects were mainly either students or relatively young white-collar office workers residing in the metropolitan area of Seoul with prior online shopping experience. Further research should employ a more representative sample by including older consumers with substantial purchasing power. It focuses on various factors affecting online search intention which has been found to be a key predictor of online purchase intention. Data were collected from a sample consisting of mostly young adults with familiarity of computer use and online shopping experience. A structural equation model was employed to test hypotheses. According to the findings, utilitarian value of Internet information search, hedonic value of Internet information search, perceived benefits of Internet shopping, perceived risk of Internet shopping, and Internet purchase experience predicted online search intention well. The findings also showed that online search intention positively affects online purchase intention.

Tisa: Toward Trustworthy Services in a Service-Oriented Architecture

Verifying conformance to non-functional requirements is important for inspiring client's confidence in remotely-hosted web services. In this work, we proposed a technique, its

implementation, and experimental validation, which serves to verify the integrity of a remotely-hosted requirements monitor. The implementation of the proposed technique was evaluated using the standard web services available with the Apache Axis Distribution. The evaluation demonstrated the feasibility of implementing our technique. It also demonstrated that our technique was effective in monitoring the non-functional requirements of the web services. Our current experimental results have looked at static checksum as a method of ensuring the integrity of the monitor. In the future, besides conducting an extensive evaluation of the overheads associated with this mechanism, we will also explore dynamic mechanisms. Furthermore, we have only informally validated the claims for our approach. In future, we plan to formalize our approach that will allow us to provide more rigorous evaluation. This would include developing a core calculus for the TPM's machine model based on Spi calculus. This semantics would account for the authentication, secrecy, and integrity properties of the TPM. Furthermore, a formal semantics for our approach can be built on top of this core calculus similar to the techniques proposed by Gordon and Pucella. Some of this work is under-way and the reader is encouraged to visit the URL where latest results from the Tisa project are regularly published.

Verifying whether a service implementation is conforming to its service-level agreements is important to inspire confidence in services in a service-oriented architecture. A part of these agreements, in particular those that are functional in nature, can be checked by observing the published interface of the service, but other agreements that are more non-functional in nature, are often verified by deploying a monitor that observes the execution of the service implementation. A key problem is that such a monitor must execute in an untrusted environment (at the service provider's site). Thus, integrity of the results reported by such a monitor crucially depends on its integrity. The key technical contribution of this article is an extension of the

traditional notion of a service-oriented architecture that allows clients, brokers and providers to negotiate and validate the integrity of a requirements monitor. We describe an approach, based on hardware-based root of trust, for verifying the integrity of a requirements monitor executing in an untrusted environment. We make two basic claims: first, that it is feasible to realize our approach using existing hardware and software solutions, and second, that integrity verification can be done at a relatively small overhead. To evaluate our feasibility claim, we present a realization of our approach using a commercial requirements monitor. To measure overhead, we have conducted a case study using a collection of web service implementations available with Apache Axis implementation.

First, hardware protected storage, where TPM is employed to protect sensitive data of the user by encrypting the secret data in such a way that it can only be decoded on a specific hardware that contains the necessary private key. Second, information binding, where critical data is bound to a platform such that it is accessible only if the conditions specified during the binding are met and rendered inaccessible if migrated to a different platform, and third platform authentication, where attestation identity keys are always bound to the platform. These can be used to authenticate the user and the platform. Our technique uses the third model to authenticate the service implementation platform, including the requirements monitor. Critics of TPM claim that TPMs will have a huge impact on user privacy. Service providers with commercial interest will try to misuse the power of TPM by introducing stricter controls and by eliminating user anonymity. Alternatives such as PERSEUS are also proposed. Although the Jury is still out on the social aspects of TPMs, their wide availability and advantages combine to warrant research on the use of these mechanisms for trusted service-oriented architectures. It consists of architectural extensions and algorithms for verifying integrity of a remotely-hosted requirements

monitor. In a spirit similar to the published functional interface for service negotiation, entities in a service-oriented architecture are extended to publish a trust-negotiation and verification interface. New components are added to support the trust-negotiation interface. A trusted platform moduler (TPM) and trust analyzer are added to the service provider and a TPM is added to the broker. The trust analyzer verifies the integrity of the requirements monitor executing in the domain of consists of architectural extensions and algorithms for verifying integrity of a remotely- hosted requirements monitor. In a spirit similar to the published functional interface for service negotiation, entities in a service-oriented architecture are extended to publish a trust-negotiation and verification interface. New components are added to support the trust-negotiation interface. A trusted platform moduler (TPM) and trust analyzer are added to the service provider and a TPM is added to the broker. The trust analyzer verifies the integrity of the requirements monitor executing in the domain.

Existing System

Rajan and Hosamani used an extra monitor deployed at the un trusted vendor's site to guarantee the integrity of the evaluation results.

Wang and Li proposed a two-dimensional trust rating aggregation approach to enable a small set of trust vectors to represent a large set of trust ratings.

Aydey 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.

Douceur indicated that the sybil attacks can compromise the redundancy of distributed storage systems.

Karlof and Wagner showed that the sybil attacks can damage the routing efficiency.

Newsome et al. proposed many defense mechanisms, such as, radio resource testing, key validation for random key pre distribution, and position verification.

In vehicular ad hoc networks, Lu et al. proposed an efficient detection mechanism on double registration, which can be conducted to mitigate the possible sybil attacks.

Disadvantages:

The Sybil attacks in the S-MSNs, where the registered users can legally apply for multiple pseudonyms and alternatively use the pseudonyms for preserving their identity and location privacy. In the meantime, the lack of the in-network third trust authority makes it very difficult to detect the Sybil attacks.

Proposed System

In this paper 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 security analysis and numerical results, it 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.

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.

It 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 SrTSE system.

Advantages:

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 SrTSE to resist the Sybil attacks.

Hardware Requirements

Processor Type	: Pentium IV
Speed	: 2.4 GHZ
RAM	: 256 MB
Hard disk	: 20 GB
Keyboard	: 101/102 Standard Keys

Mouse : Scroll Mouse

Software Requirements

Operating System : Windows 7

Programming Package : Net Beans IDE 7.3.1

Coding Language : JDK 1.7

Modules

S-MSN Formation

Providing Services

Review Generation and Submission

Sybil Attack Detection

S-MSN Formation

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, 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.

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.

It 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.

Providing Services

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.

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.

So, the vendor provide his services to mobile user. Then the mobile user create Reviews and send to the vendor.

Review Generation and Submission

Review generation does not rely on tokens, which gives users flexibility to generate review.

Consider a user u_j who just received a token tok from a nearby user u_w with pseudonym $pid_w, *, *$. It checks if the received tok is valid. This validation step has two perspectives: 1) to ensure that tok is indeed originated from the vendor and has been properly forwarded in the past; 2) to ensure that tok is sent by the user who lastly used it.

The first goal can be realized by using the public key pkt of the vendor and the forwarder information (including secrets, pseudonyms, and time stamps) embedded in tok . The second one

can be achieved by checking if the association (tok,pidw,*,*) exists in the latest TP list provided by the vendor.

During token forwarding, a token is supposed to be passed to only one user that is wishing to submit a review to the same vendor.

When multiple such users are present, a random selection can be made. With the second check on the TP list during token validation, the other users holding the token will find that the token is no longer valid and then try to find a new token to submit their reviews.

Sybil Attack Detection

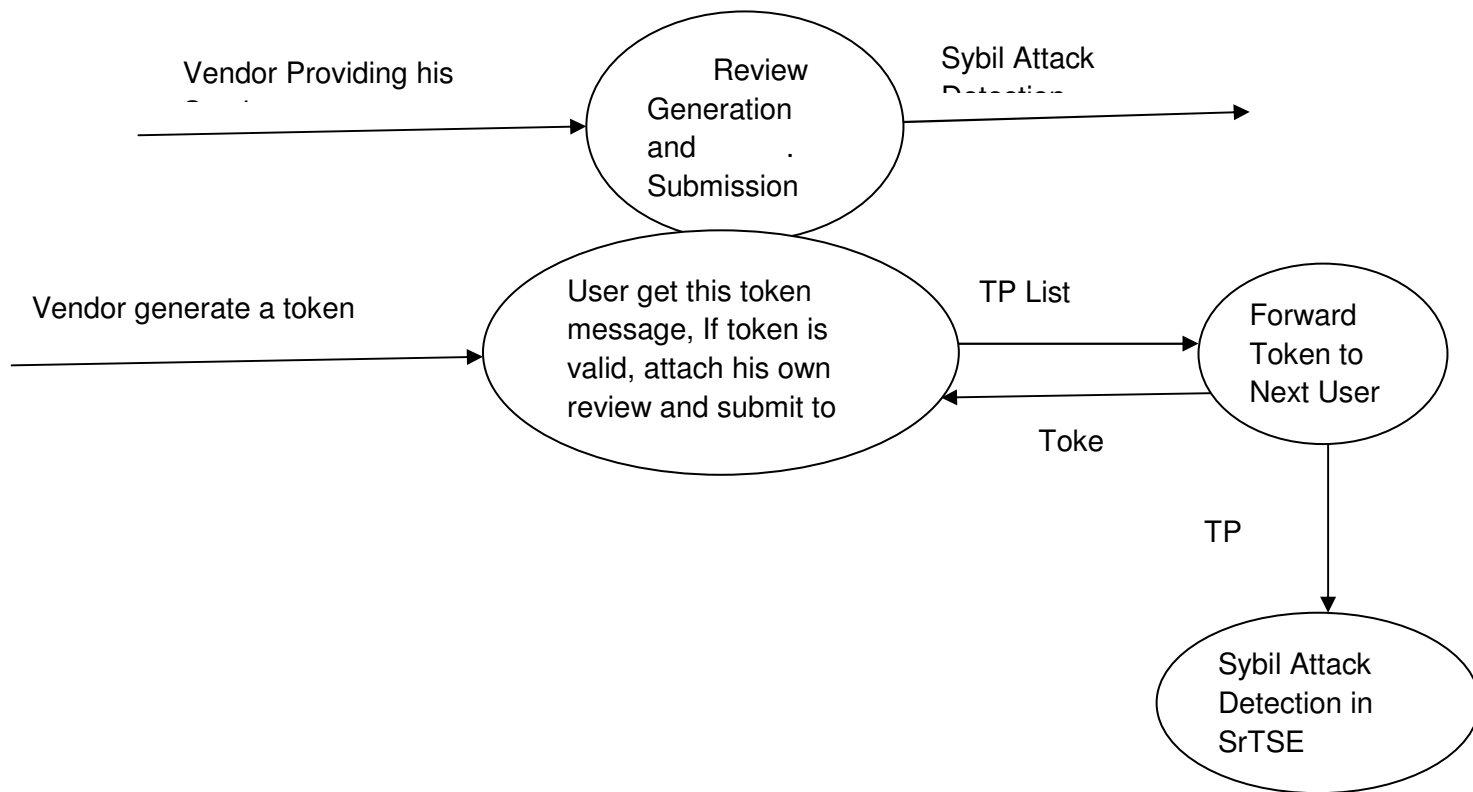
The Sybil attack 1 is launched by a group of registered users. They aim at telling other users the bad service from a vendor while the service of the vendor is good. With the valid registration, these malicious users are able to leave false reviews toward a specific vendor.

Even realizing the reviews are not in accord with the service, the vendor cannot simply delete or reject the reviews. If the vendor does, users will detect such behavior and regard the vendor as a dishonest service provider.

The Sybil attack 2 is launched by a vendor and a group of registered users. They aim at raising the reputation of the service from a vendor while the service of the vendor is not that good. The reviews generated by these malicious users cannot be distinguished from other reviews by well-behaving users.

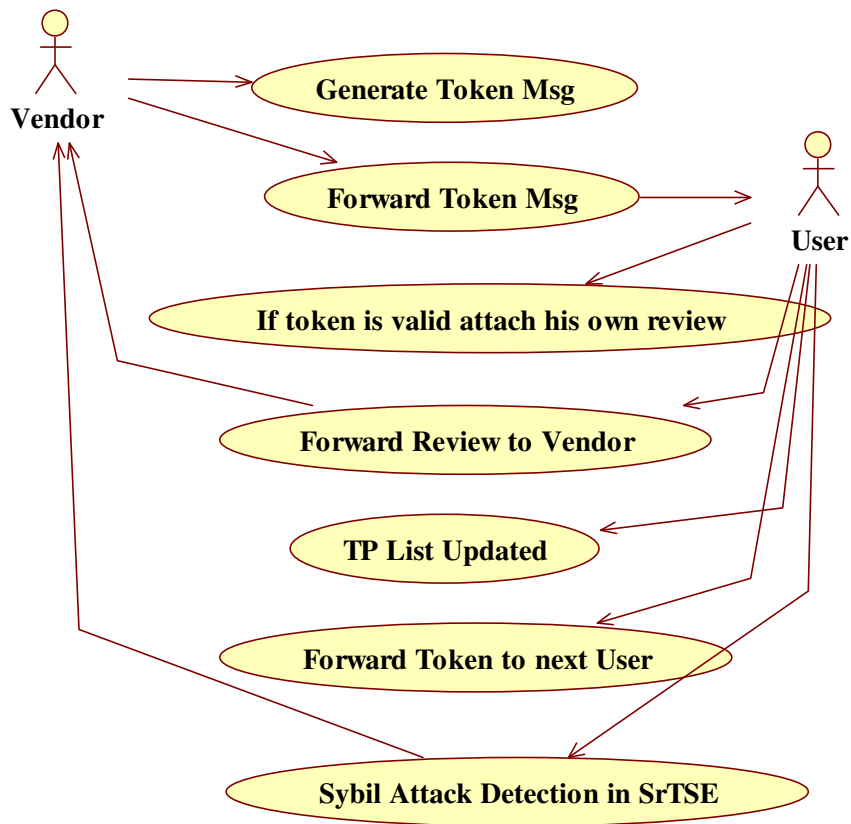
In the SrTSE, we introduce a novel solution to prevent the two Sybil attacks. In the S-MSN, we consider that a user has no need to generate multiple reviews toward a vendor in a short time period.

Data Flow Diagram



UML Diagram

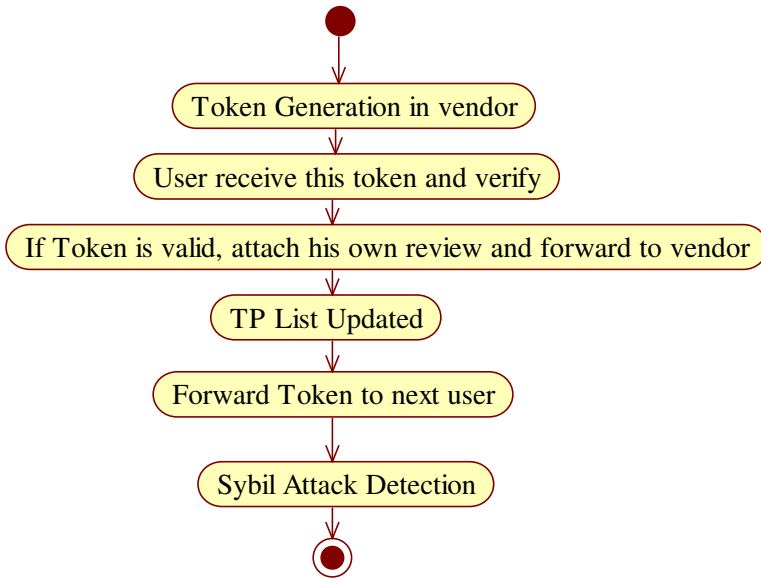
Use Case Diagram



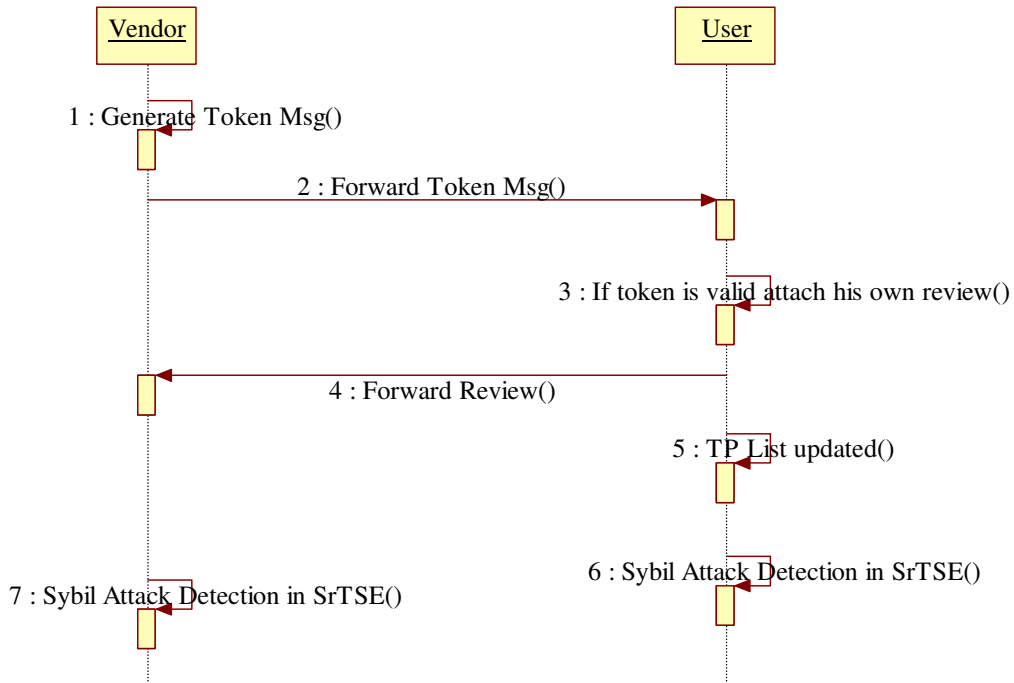
20.2 Class Diagram



20.3 Activity Diagram

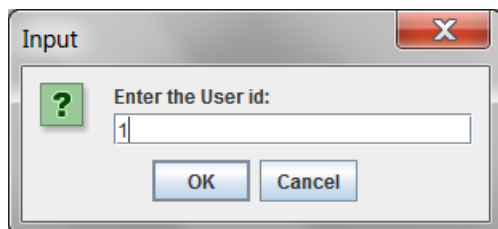
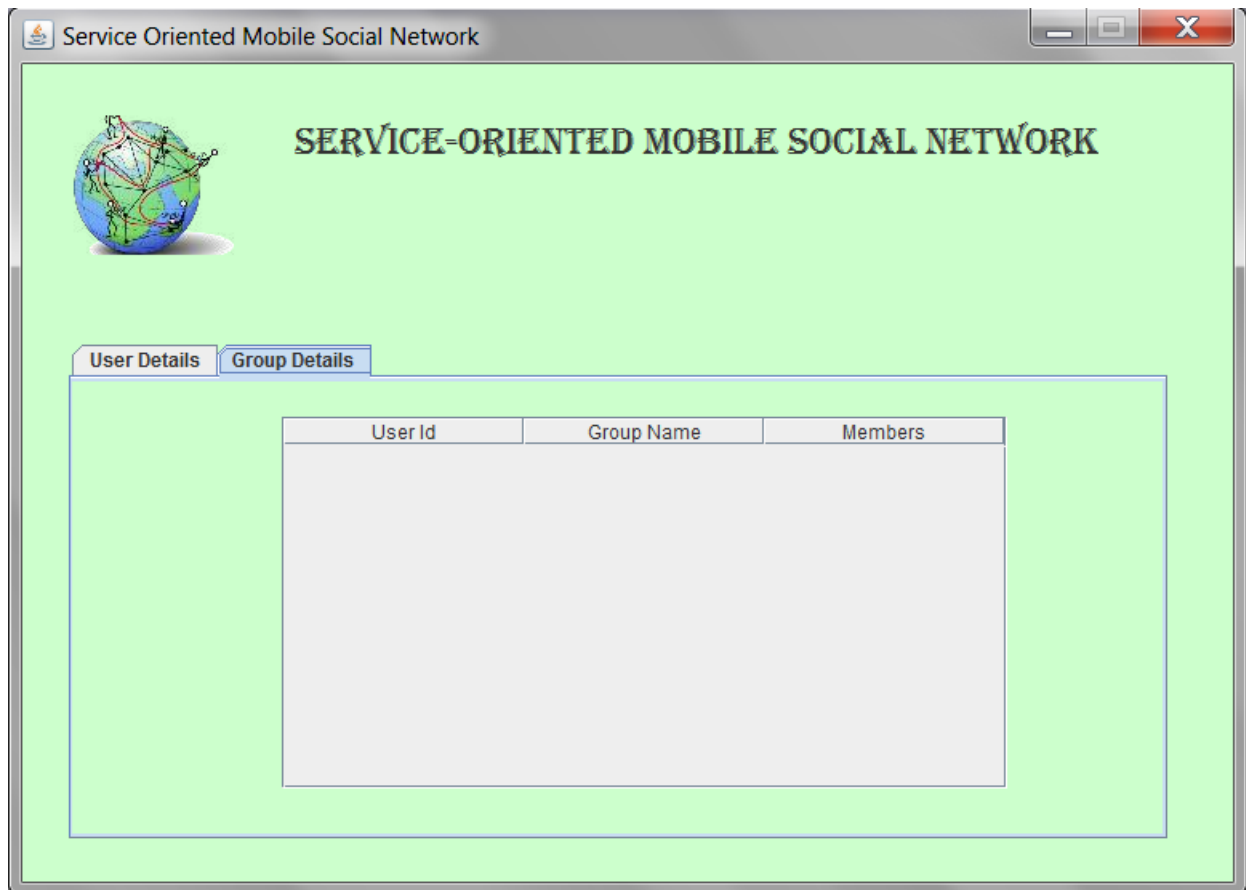


20.4 Sequence Diagram



Screenshots of Execution:






SMSN User Frame-1



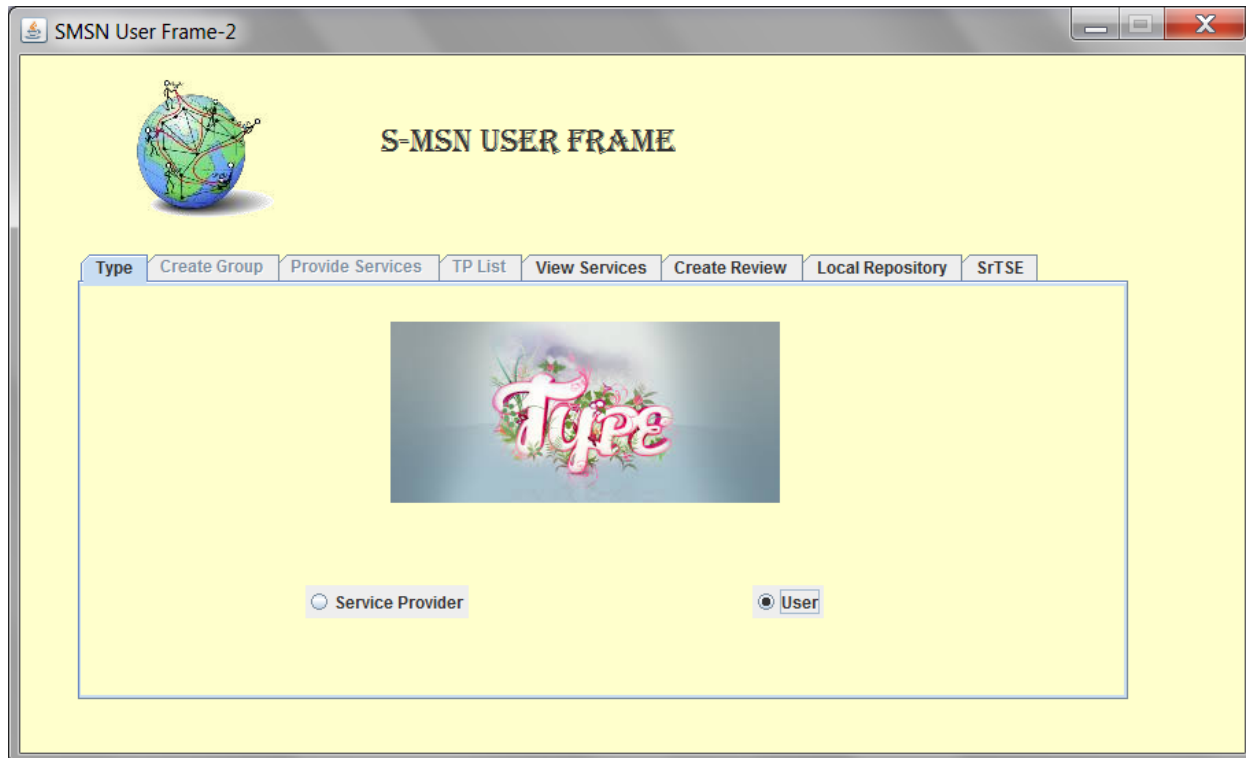
S-MSN USER FRAME

Type Create Group Provide Services TP List View Services Create Review Local Repository SrTSE

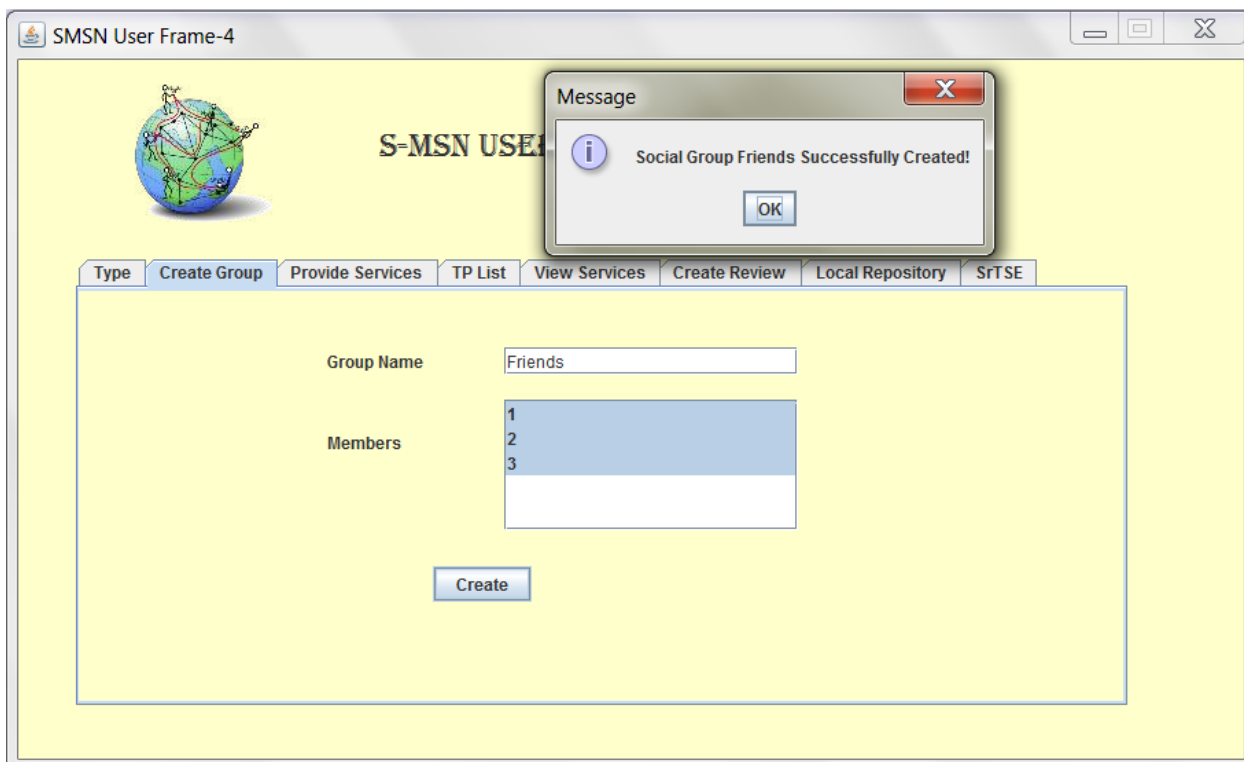
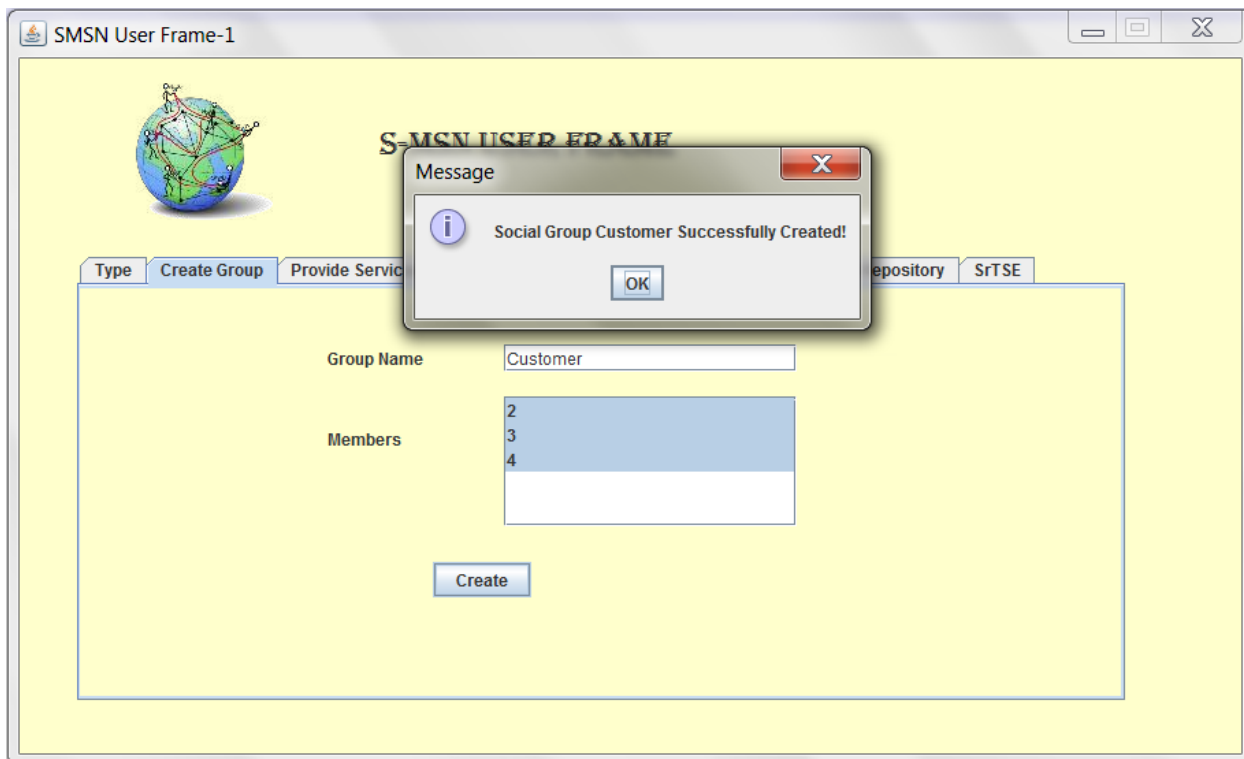


Service Provider User


The image shows a software application window titled "SMSN User Frame-1". The window has a yellow background. At the top left is a globe icon with network connections. In the center, the text "S-MSN USER FRAME" is displayed. Below this is a horizontal menu with several items: "Type", "Create Group", "Provide Services", "TP List", "View Services", "Create Review", "Local Repository", and "SrTSE". The "Type" item is currently selected. Below the menu is a large rectangular area containing a stylized graphic of the word "Type" in pink and white, surrounded by green foliage. At the bottom of this area are two radio buttons: "Service Provider" and "User".







Service Oriented Mobile Social Network




SERVICE-ORIENTED MOBILE SOCIAL NETWORK

User Details **Group Details**

User Id	Group Name	Members
1	Customer	2,3,4
4	Friends	1,2,3

SMSN User Frame-1



S-MSN USER FRAME


Type Create Group **Provide Services** TP List View Services Create Review Local Repository SrTSE

Select Group:

Upload Services:

User id	Acknowledgement
2	ACK
4	ACK
3	ACK

SMSN User Frame-4



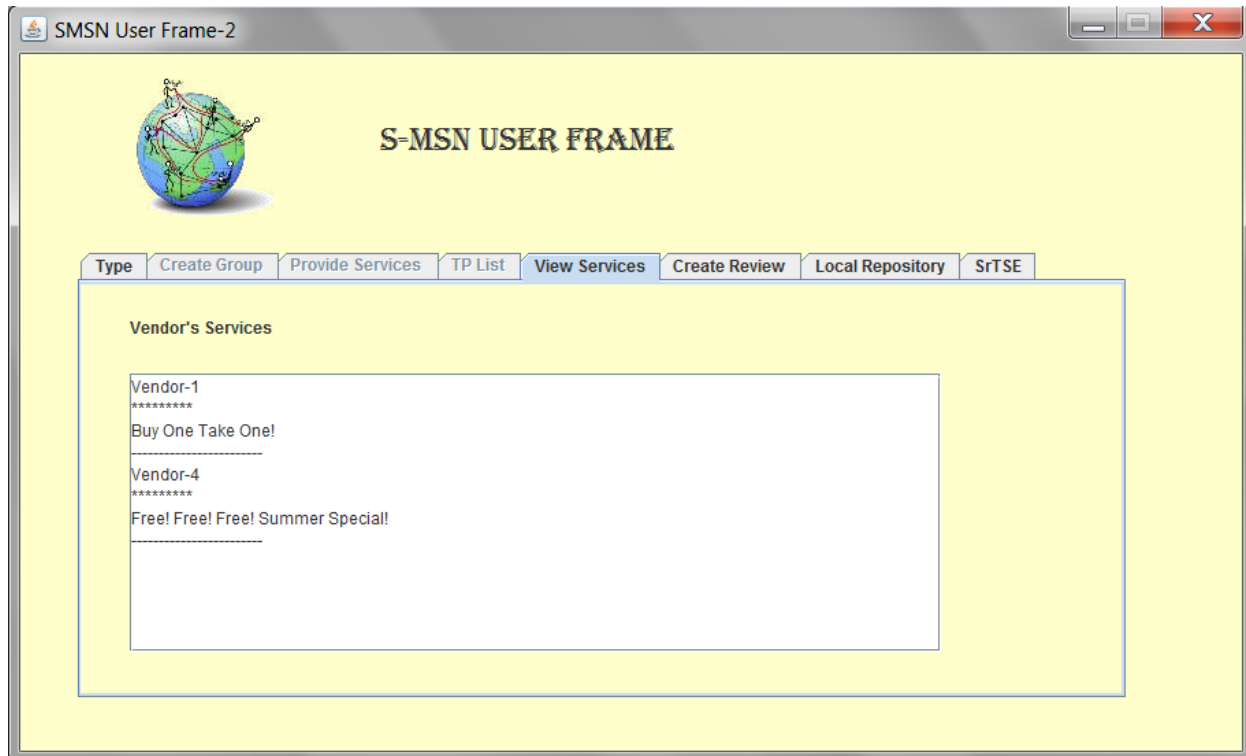
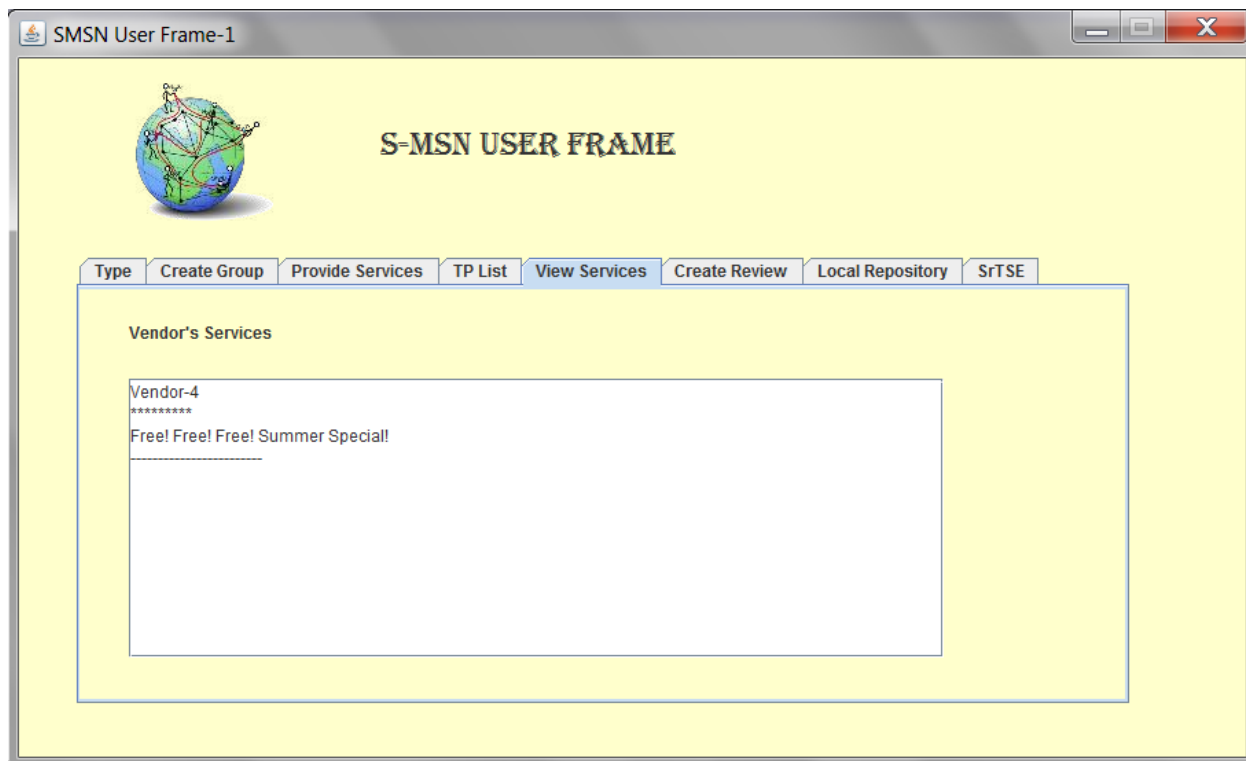
S-MSN USER FRAME

Type Create Group **Provide Services** TP List View Services Create Review Local Repository SrTSE


Select Group:

Upload Services:

User id	Acknowledgement
1	ACK
2	ACK
3	ACK



SMSN User Frame-3



S-MSN USER FRAME

Type Create Group Provide Services TP List **View Services** Create Review Local Repository SrTSE

Vendor's Services

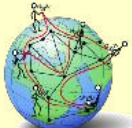
Vendor-1

Buy One Take One!

Vendor-4

Free! Free! Free! Summer Special!

SMSN User Frame-4



S-MSN USER FRAME


Type Create Group Provide Services TP List **View Services** Create Review Local Repository SrTSE

Vendor's Services

Vendor-1

Buy One Take One!

SMSN User Frame-2



S-MSN USER FRAME


Type Create Group Provide Services TP List View Services **Create Review** Local Repository SrTSE

If he is a Malicious User? Yes No

Vendor id

Enter the Reviews

SMSN User Frame-2



S-MSN USER FRAME

Type Create Group Provide Services TP List View Services **Create Review** Local Repository SrTSE

User Id	Vendor Id	Reviews
2	1	Super

SMSN User Frame-3



S-MSN USER FRAME

Type Create Group Provide Services TP List View Services **Create Review** Local Repository SrTSE


If he is a Malicious User? Yes No

Vendor id 1

Enter the Reviews

Good!

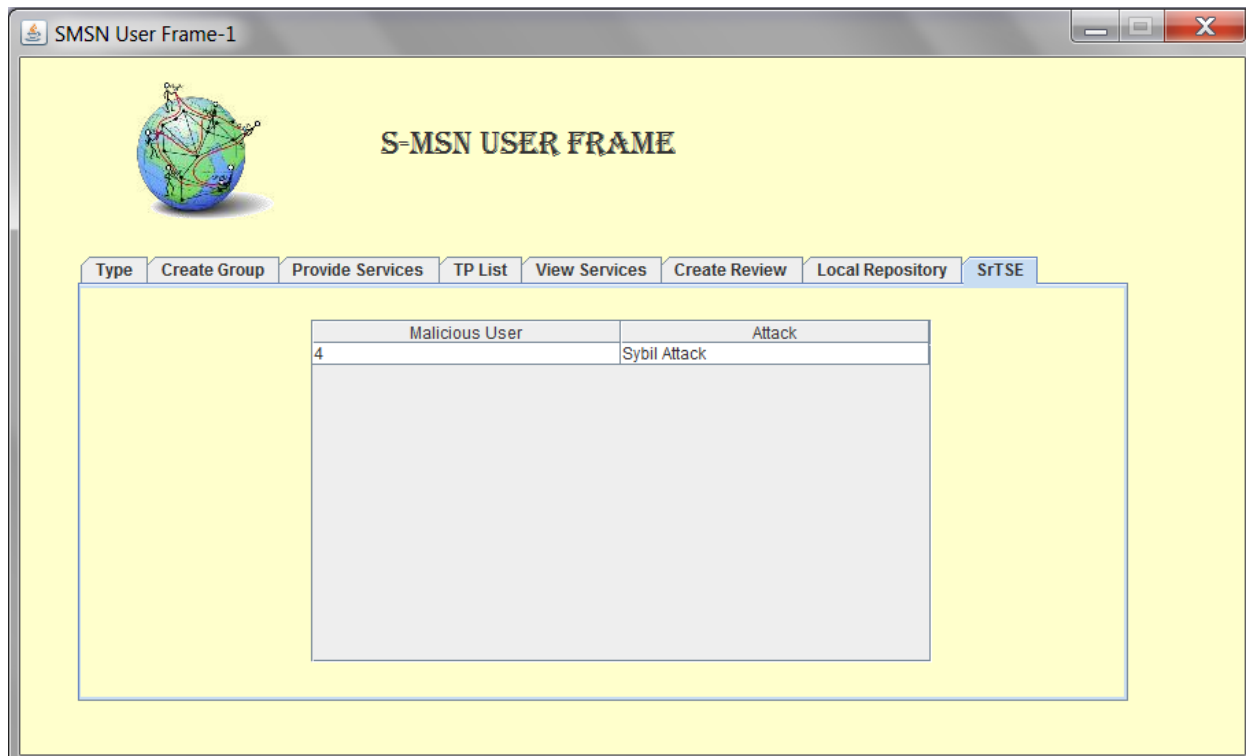
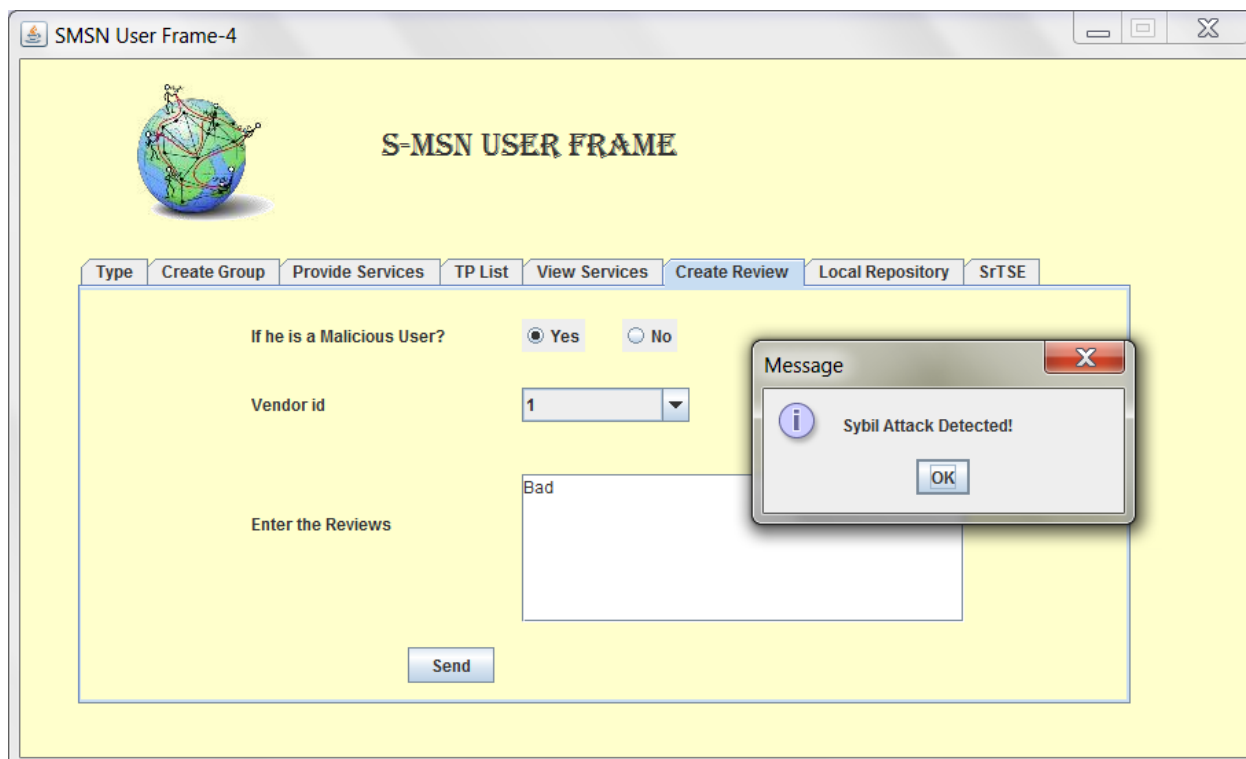
SMSN User Frame-1



S-MSN USER FRAME

Type Create Group Provide Services TP List View Services **Create Review** Local Repository SrTSE

Pseudonym	Token
c81e728d9d4c2f636f067f89cc14862c	Super
eccbc87e4b5ce2fe28308fd9f2a7baf3	Good!



References

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

Luan, L.X. Cai, J. Chen, X. Shen, and F. Bai, "VTube: Towards the Media Rich City Life with Autonomous Vehicular Content Distribution," Proc. IEEE CS Eighth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. Networks (SECON), pp. 359-367, 2011.

J.R. Douceur, "The Sybil Attack," Proc. Revised Papers First Int'l Workshop Peer-to-Peer Systems (IPTPS), pp. 251-260, 2002.

J. Newsome, E. Shi, D.X. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," Proc. Third Int'l Symp. Information Processing in Sensor Networks (IPSN), pp. 259-268, 2004.

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.

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.

H. Rajan and M. Hosamani, "Tisa: Toward Trustworthy Services in a Service-Oriented Architecture," IEEE Trans. Services Computing, vol. 1, no. 4, pp. 201-213, Oct.-Dec. 2008.