A Privacy based Web Services Application for Secure Routing in Mobile Ad Hoc Networks

Sesha Bhargavi Velagaleti

Assistant Professor, IT Departmnet, GNITS, Shaikpet, Hyderabad, India.
b.velagaleti@gmail.com

Dr.M.Seetha
Professor, CSE Departmnet, GNITS, Shaikpet, Hyderabad,India
smaddala2000@yahoo.com

Dr.S.Viswanadha Raju
Professor, CSE Departmnet, JNTUK, Hyderabad, India.
viswanadha_raju2004@yahoo.co.in

Abstract

In the today's competitive world, necessity of fast and convenient ways of communication was increasing day by day, which significantly had influenced the computer networking field. This has led to many notable changes in the area of mobile communications and in particular when users want to share their data securely, security in the routing process has become one of the fundamental requirements of today's routing algorithms for wireless mobile ad hoc networks. Our work mainly focuses on several security challenges faced and an efficient secure scheme has been proposed, which effectively addresses the privacy related issues in any Web Services network.

I. Introduction

The term ubiquitous computing was coined by Mark Weiser to describe a state of computing in which users are no longer aware of computation being done [1]. The emergence of smart environments, where devices are embedded pervasively in the physical world, has sparked many new research areas and represents a step towards ubiquitous computing. To this end, researchers have begun to outline plans to achieve ubiquitous computing. For example, Basu et al. [2] advocate the vision of power-up-n-play for smart environments in which no pre-defined infrastructures are installed and, when powered up, the devices "intelligently" configure and connect themselves to other devices. Bhagwat et al. [3] also focus on the interoperability of sensor devices and present three research issues: (1) distributed algorithms for self-organizing devices, (2) packet forwarding, and (3) Internet connectivity. Mobile ad-hoc network (MANET) routing protocols play a fundamental role in a possible future of ubiquitous devices. Current MANET commercial applications have mainly been for military applications or emergency situations. However, we believe that research into MANET routing proto- cols will lay the groundwork for future wireless sensor networks and wireless plug-n-play devices. The challenge is for MANET routing protocols to provide a communication platform that is solid, adaptive and dynamic in the face of widely fluctuating wireless channel characteristics and node mobility.

DOI : 10.5121/ijitcs.2012.2206

A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes (hosts) which are capable of independent operation and operates without a base station, in which nodes cooperate to provide interconnectivity and cooperate among themselves to provide services to the users. MANETS are mainly used for disaster recovery services ,in metropolitan area networks, enhanced cellular networks and also provide a wide range of delay-tolerant networking applications. Performance of a MANET is generally measured in terms of data throughput, route latency, overhead cost, route optimality etc.,

Several techniques have been proposed to detect and alleviate the effects of such selfish nodes in MANETs [7]-[12]. In [7], two techniques were introduced, namely watchdog and path rater,to detect and mitigate the effects of the routing misbehavior, respectively. The watchdog technique identies the misbehaving nodes by overhearing on the wireless medium. The pathrater technique allows nodes to avoid the use of the misbehaving nodes in any future route selections. The watchdog technique is based on passive overhearing.

II. Related Work

Recently, TCP performance in ad hoc wireless networks has become an active research field. Link failures due to mobility have been identified as one of the major factors degrading TCP performance . To combat this problem, Holland and Vaidya et al proposed Explicit Link Failure Notification (ELFN) scheme whereby the intermediate nodes notify the TCP sender when a link failure happens. This is a scheme similar to the Explicit Congestion Notification (ECN) technique originally proposed in the wired networks. With the help of ELFN, TCP senders can tell whether a packet loss is caused by link breakage or congestion. Thus, it could properly response to different kinds of packet losses. In TCP-F (TCP-Feedback), Chandran and Prakash et al proposed a scheme, very similar to the ELFN scheme, by asking the intermediate node to notify TCP sender about the network condition. When one intermediate node detects a route failure, it explicitly sends a route failure notification (RFN) to the TCP sender. The difference between TCP-F and ELFN is the response of route failures. TCP-F relies on the intermediate node to send a route reestablishment notification (RRN) to notify that the path is back up. In ELFN, the TCP sender must send probing packet periodically to detect the route recovery.

Another more serious problem that link failures may cause to TCP performance is unnecessary exponential backoff of the retransmission timeout (RTO) interval. In the conventional TCP protocol, when a retransmission timeout happens, TCP sender retransmits the lost packet and doubles the RTO. This procedure is repeated until the lost packet is acknowledged. Such an exponential backoff of the RTO helps TCP react to congestion gracefully. However, when link failure happens, TCP tends to increase the RTO rapidly even there is no congestion. Wrongly applied exponential backoff significantly degrades the TCP performance since in the ad hoc wireless networks, the TCP congestion window size is usually small and the RTO plays an important role. Dyer and Boppana et al proposed a mechanism called fixed-RTO to repair this problem. When the retransmission timeout happens consecutively, the authors think it is mainly due to route break, not congestion. Thus, after retransmitting the lost packet, fixedRTO will freeze the RTO value utile the route is reestablished. Through simulation experiments, the

authors show that with fixed-RTO, TCP can achieve throughput comparable to that of the ELFN mechanism. However, ELFN requires support from the intermediate nodes, while fixed-RTO is pure end-to-end mechanism. The above related work mostly focuses on letting TCP detect route failures and react to them in a proper way.

III. Implementations and Validations

Privacy is a well recognized sticking point in the Web Services network. In this case study implementation, we explore privacy protection which brings about many new security challenges. Web Services extended Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. Here data (i.e., message/file) is transferred between the sender and the receiver in an extensively secure manner. Hence the communication between the sender and receiver is guaranteed by the Third Party Auditor (TPA).The software is designed in such a way that the user can easily interact with the screen because they are GUI and screen has several buttons with captions indicating the functionality like Sender details, message typed, searching for a file, keys and signatures generated, shows the encrypted data, verification of data, system name details, Receiver details. Business layer of this application are to be developed in such a way they must be easily maintainable and extensible. Software developed will able to do any type of data transfer between sender and receiver in an authenticated, privacy of data contents. The Figures 1, 2 & 3 provides the class diagram, sequence diagram and execution screen shot respectively of the privacy web services application implemented.

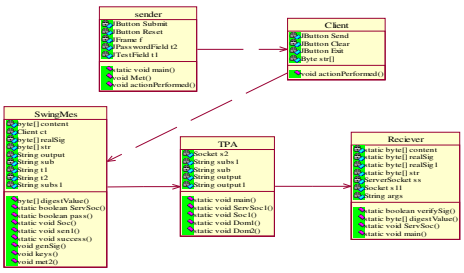

Figure 1. Class diagram of the Privacy Web Services application with an extension to Web Services Cloud

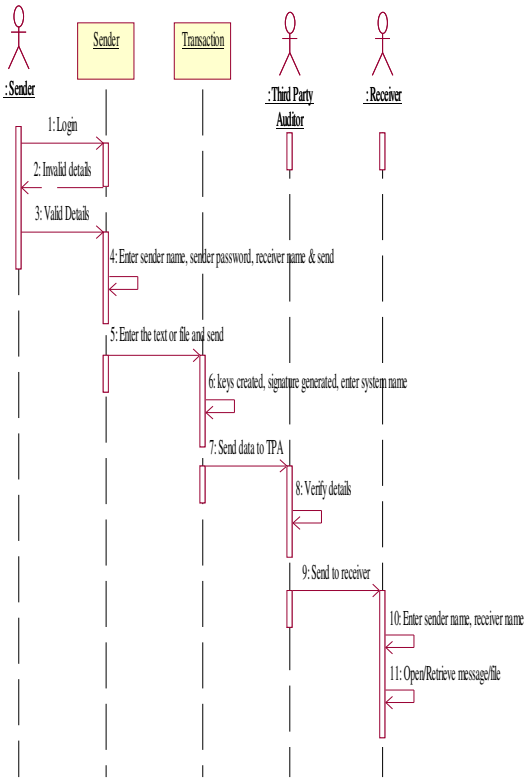

Figure 2. Sequence diagram of Privacy Web Services application with an extension to Web Services Cloud

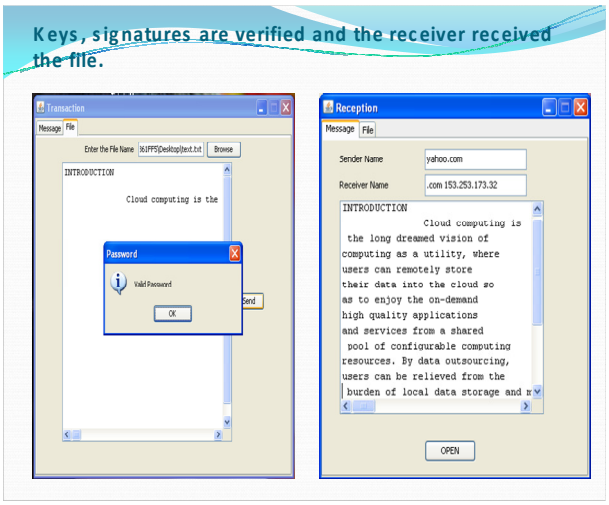

Figure 3. Execution Screen shot of Privacy Web Services application with an extension to Web Services Cloud

IV. Conclusions

In this paper, we try to explore the privacy of web services applications which will address many security challenges. Using this approach, the data is securely sent between the sender and the receiver. Privacy of the contents transferred is also maintained with the use of this web services application. Data is transferred in a very authenticated way between the sender and the receiver , with an extension to a web services cloud. Hence the proposed scheme is very much secure compared to many of the existing security schemes.

V.References

[1] “Implementation Experience with MANET Routing Protocols” Kwan-Wu Chin, John Judge, Aidan Williams and Roger Kermode,Sydney Networks and Communications Lab.

[2] “Task-based self-organisation in large smart spaces:issues and challenges”. P. Basu and T. D. C. Little , In DARPA/NIST/NSF Workshop on Research: Issues in Smart Computing Environment, Atlanta, USA, 1999.

[3] “Smart connectivity for smart spaces.” , P. Bhagvat, C. Bisdjikian, P. Kermani, and M. Naghshineh. In DARPA/NIST/NSF Workshop on Research: Issues in Smart Computing Environment, Atlanta, USA, 1999.

[4] “An Acknowledgment-based Approach for the Detection of Routing Misbehavior in
MANETs “ Kejun Liu, Jing Deng, Pramod K. Varshney, and Kashyap Balakrishnan

[5] H. Miranda and L. Rodrigues,Preventing selshness in open mobile ad hoc networks,” in Proc. of the Seventh CaberNet Radicals Workshop, October 2002.

[6] L. Buttyan and J-P. Hubaux,Security and cooperation in wireless networks,available at http://secowinet.ep.ch/.

[7] L. M. Feeney and M. Nilsson,Investigating the energy consumption of a wireless network interface in an ad hoc networking environment,” in IEEE INFOCOM, 2001.

[8] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in Proc. of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom), August 2000.

[9] L. Buttyan and J-P. Hubaux,Enforcing service availability in mobile ad-hoc WANs, in Proc. of First IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHoc), Boston, MA, USA, August 2000.

[10] J-P. Hubaux, T. Gross, J-Y. Le Boudec, and M. Vetterli,Toward self-organized mobile ad hoc networks: The terminodes project,” in IEEE Communications Magazine, January 2001.

[11] S. Buchegger and J-Y. Le Boudec,Performance analysis of the CONFIDANT protocol: Cooperation of nodes, fairness in dynamic ad-hoc networks,” in Proc. of MobiHoc'02, June 2002.

[12] S. Zhong, J. Chen, and Y. R. Yang,Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks, in Proc. of Infocom'03, San Francisco, CA, USA, March 30 - April 3 2003.

[13] M. Jakobsson, J-P. Hubaux, and L. Buttyan, A micropayment scheme encouraging collaboration in multi-hop cellular networks, in Proc. of Financial Crypto 2003, January 2003.

[14] TCP Performance over Multipath Routing in Mobile Ad Hoc Networks Haejung Lim
Telecommunication Network Division Samsung Electronics,Seoul,Korea,Kaixin Xu, Mario Gerla Computer Science Department, UCLA Los Angeles, CA 90095, USA Email: fxkx, gerlag@cs.ucla.edu