Chapter 4
Formal Verification of Secure Payment Framework in MANET for Disaster Areas

Shaik Shakeel Ahamad
Majmaah University, Saudi Arabia

V. N. Sastry
Institute for Development and Research in Banking Technology, India

Siba K. Udgata
University of Hyderabad, India

ABSTRACT

In this chapter, the authors propose a secure payment framework in mobile ad hoc network for disaster areas. In order to enable transactions in a disaster area using existing payment systems, we need infrastructure to communicate such as wired networks and base stations for cellular networks which are damaged by natural disasters. The authors propose to use mobile agent technology and digital signature with message recovery (DSMR) mechanism based on ECDSA mechanism to enable transactions in a disaster area using ad hoc networks.

INTRODUCTION

The unprecedented growth of mobile communication technology stimulated by the ever increasing demand for personal mobility in communications has led researchers to develop new technologies. One such recent development is Multi hop Cellular Networks (MCN) which is an integration of Single hop Cellular Networks (SCN) and ad hoc networks. Single hop cellular networks (SCN) is one where a mobile station (MS) communicates with base station (BS) and ad hoc networks are dynamic, decentralized, infrastructure less, self-organizing and easily deployable without any planning. Both the technologies have their own merits and demerits. SCN's performance is reliable and has strong and mature technol-

DOI: 10.4018/978-1-5225-5014-3.ch004

ogy support but the infrastructure is very costly. On the other hand ad hoc networks are very cheap, easily deployable mainly due to the use of unlicensed spectrum of IEEE 802.11. Integration of these two technologies has led to the development of a new technology called Multi hop Cellular Networks (MCN) which provides the merits of both the technologies. The integration of cellular networks with mobile ad hoc networks offers lot of promising applications. Using Multi hop Cellular Networks mobile devices can communicate and access information at any time and everywhere. For any secure electronic payment system to be successful two conditions need to be satisfied a) Need of Public Key Infrastructure (PKI) to provide trust services for the engaging entities (i.e. engaging entities need to prove their credentials with the help of PKI) and b) Need of an online connection with the Bank in order to commit transaction and prevent fraud (double spending and overspending). Satisfying these two conditions is a challenging task in Multi hop Cellular Network environment so we propose to use Digital Signature with Message Recovery (DSMR) based on ECDSA mechanism for satisfying the first condition and Mobile Agent technology in order to satisfy the second condition. DSMR eliminates the need of certificates and removes the hurdle of PKI thereby reducing the consumption of resources. In addition to this DSMR requires smaller band width for data communications in order to achieve confidentiality, integrity, authentication and non-repudiation properties. The authentication of public keys is implicitly being accomplished with DSMR verification. On the other hand Mobile Agent technology has many benefits such as bandwidth conservation, reduction of latency, reduction of completion time, Asynchronous (disconnected) communications. Mobile agent overcomes low bandwidth and disrupted network which is very common in Multi-hop Cellular-Networks. Using mobile agent the client need not be connected during the entire session thereby reducing the consumption of resources which are very scarce in mobile devices. This is achieved by sending an agent to the Issuer's server carrying all the data necessary for the transaction. So by adopting DSMR mechanism and Mobile Agent technology provides an optimal solution for Mobile Payments in Multi hop Cellular Network environment. For reducing the size of messages and for greater efficiency in terms of key sizes and bandwidth we have used DSMR mechanism based on ECDSA. So ECDSA is suitable for resource constrained devices.

A typical scenario applying mobile agents for Mobile Payment framework in Multi hop Cellular Networks (MCN) environment would operate as follows. A Client tries to buy goods/services from merchant through a communication network i.e. internet and the client's platform is mobile phone equipped with UICC (Universal Integrated Circuit Card) as secure element which is tamper resistant. Client cannot tamper the inner working of UICC because of tamper resistant nature of the UICC, the communication channel between UICC and mobile phone is secure and reliable. Mobile agents are created from the tamper resistant UICC which can be used as a communication bridge between the host and the agent so that a malicious host is unable to access the agent directly. UICC launches a smart mobile agent containing all the necessary negotiation and shopping logics to the Internet. The agent shops around and makes decisions based on the contained logics and finally returns the best quote to the UICC. As a result, during the shopping phase, once the agent has been launched only one message must be received and responded to by the UICC. Another advantage of using mobile agent technology is that agent's real-time interaction capability. For many time-critical applications, the mobile agent can make decisions on the spot, without interactively asking for its owner's confirmation. After the agent brings back a Order Information (OI), the UICC verifies the Order Information (OI) and performs the final purchase transaction.