Expert Systems with Applications 38 (2011) 11048–11054

Contents lists available at ScienceDirect

Expert Systems with Applications

journal homepage: www.elsevier.com/locate/eswa

Adaptation of agent-based non-repudiation protocol to mobile digital right management (DRM)

Chung-Ming Ou [a,*], C.R. Ou [b]

[a] Department of Information Management, Kainan University, Luchu 338, Taiwan
[b] Department of Electrical Engineering, Hsiuping Institute of Technology, Taichung 412, Taiwan

ARTICLE INFO

Keywords:
Mobile agent
Non-repudiation
PKI
Digital right management
Proxy certificate

ABSTRACT

Non-repudiation of a mobile digital rights management (DRM) ensures that when a user (*U*) sends some message to a rights issuer (RI), neither *U* nor RI can deny having participated in this transaction. An evidence of a transaction is generated by wireless PKI mechanism such that *U* and RI cannot repudiate sending and receiving the message respectively. *U* generates a mobile agent which carries encrypted payment information to RI. This mobile agent is also issued a proxy certificate by *U*; this certificate guarantees the binding relationship between them. One trusted third party acts as a lightweight notary for evidence generation. One advantage of this agent-based non-repudiation protocol is to reduce inconvenience for mobile clients such as connection time; it causes difficulty for fair transaction for mobile DRM.

1. Introduction

Recently, varied concepts of intelligent agents are experienced growing applications in many areas related to network management. Grossklags and Schmidt introduced software agents with market efficiency (Grossklags & Schmidt, 2006). Wang proposed an agent-based control of traffic management system (Wang, 2005). Hamdi proposed a multiagent-based approach to information customization (Hamdi, 2006), etc. On the other hand, agent-based E-commerce systems provide some advantages over the conventional client and server-based E-commerce systems; it is also a promising architecture for peers to peers (P2P) E-commerce systems and cloud computing. According to Borrell, Robles, Serra, and Riera (1999), they reduce network traffics, provide efficient resource access and dynamic system adaptations, and particularly support mobile transactions. The agent-based system is becoming a framework for both E-commerce and mobile commerce (M-commerce).

Wireless devices which communicate with application servers over the air are highly exposed to potential security threats. They require enhanced security and authenticity services for mobile transactions which are not properly supported by the original GSM and UMTS security mechanisms. For example, Stach, Park, and Makki (1999) proposed an enhanced GSM protocol supporting non-repudiation of services. Moreover, as M-commerce applications increases, further sensitive services such as payment and billing are needed. Tseng, Yang, and Su (2004) proposed a PKI-based protocol of authentication and billing for WLAN and 3G integrations. This scheme can provide non-repudiation billing service based on digital signatures. According to M'Raihi and Yung (2001), smart cards (SIMs for GSM and USIMs for UMTS) are crucial in allowing safe operations for these mobile telecom applications. Dispute of mobile transactions is a common problem that could jeopardize the mobile commerce (Zhou, Deng, & Bao, 1999). The purpose of non-repudiation is to collect, maintain, make available and validate irrefutable evidence concerning a claimed event or action in order to resolve disputes on the occurrence or non-occurrence of the event or action (ITU-T., 1996; Li & Luo, 2004). Any evidence has to be verified by some fair arbitrator once dispute arises.

One motivation for this paper is the mobile TAIWAN project (mTAIWAN). Since 2005, mTAIWAN is one major nation-wide project of establishing seamless and ubiquitous wireless infrastructure. This next generation communication network combines mobile communication systems such as 2G (GSM), 2.5G (GPRS), 3G (UMTS), wireless network systems such as WiFi and WiMAX technologies. One major goal for mTAIWAN project is to promote the ubiquitous mobile applications using varied mobile devices such as mobile phone, PDA, laptop PC, etc. Combining these motivations, we propose an agent-based architecture and protocol to implement the non-repudiation mechanism over the mobile application systems, which includes the digital right management (DRM); this will also improve the security mechanisms of those existing electronic invoice systems. On the other hand, mobile

* Corresponding author.
E-mail addresses: cou077@mail.knu.edu.tw (C.-M. Ou), crou@mail.hit.edu.tw (C.R. Ou).

0957-4174/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.eswa.2011.02.149

applications need to be user-friendly and convenient for mobile clients via their mobile handsets; this investigation leads to the research of agent-based mobile applications.

DRM is a technology to solve the issues of transferring copyright-protected information. Many multimedia contents are distributed without any copyright protection via digitalization and communication network. Among them, medical data from unauthorized peers, copyright-protected music or books, must be only consumed by users who paid for it (Onieva, Lopez, Roman, Zhou, & Gritzalis, 2007). In this paper, we show how to establish a simple agent-based protocol integrated existing DRM architecture based on the OMA (open mobile alliance) DRM specification 2.0. This protocol provides the secure mechanism between the mobile user and the right issuer (RI) through the mobile network provider, while they are exchanging a right object (RO) according to agreed purchase order. Non-repudiation services must ensure that when mobile consumer *U* sends some content right request to rights issuer RI over a network, neither *U* nor RI can deny having participated in a part or the whole of this transaction. The basic idea is the following: an evidence of origin (*EOO*) is generated for *U* and an evidence of receipt (*EOR*) is generated for RI. In general, evidences are generated via PKI-based digital signatures. Disputes arise over the origin or the receipt of messages. For the case of origin dispute, *U* denies sending message while RI claims having received it. As for the receipt dispute, RI denies receiving any message while *U* claims having sent it.

Many non-repudiation protocols have been proposed in a so-called "wrapper context", for example, the one proposed by Zhou and Gollman (Zhou & Gollmann, 1996). In this situation, a party *A* wants to send a message *M* to *B* to enforce non-repudiation on *M*; namely, non-repudiation is enforced for one message (*M*). Stach et al. (1999) focus on non-repudiation of GSM service based on one-way hash function in order to preventing mobile subscribers from denying initiating this GSM service. However, this is more authentication rather than non-repudiation from applications point of view. Liew, Ng, Lim, Tan, and Ong (1999) proposed a non-repudiation protocol for communication sessions rather than messages in an agent-based E-commerce system. Their protocol is a general-purposed one for any E-commerce system. Lee and Yeh (Lee & Yeh, 2005) proposed a delegation-based authentication protocol for mobile devices; it is achieved by utilizing proxy signatures which basically delegates signing power to other end-entities.

Mobile agents are considered to be an alternative to client and server-based mobile commerce where mobile devices have limited computing resource. A mobile agent of the host is a set of code and data which can execute codes with data as parameter in some trusted processing environment (TPE) or on some merchant hosts. However, there are several issues related to security and trust while considering mobile agent-based E-commerce (Esparza, Munoz, Soriano, & Forne, 2003; Pagnia, Vogt, Gartner, & Wilhelm, 2000; Wilhelm, Staamann, & Buttyan, 1998), such as the non-repudiation. We consider brokerage rather than TPE in our mobile DRM. One advantage of adopting this mobile agent architecture to non-repudiation protocol is the following: Mobile devices simply send their agents with (digital) right request to the broker; they need not to connect to specific application servers throughout the whole transacting activity. The wireless public key infrastructure (WPKI) adoptable for this non-repudiation mechanism relies on some trusted third party (*TTP*) which generates the final evidence for digital right request. The identity binding of a mobile agent and its owner is a major security concern from M-commerce point of view; this issue can be reasonably solved by using proxy certificates within the WPKI. Mobile agent systems provide platforms allowing mobile agents autonomously migrating between different hosts. While migrating between hosts, these agents are under security threats with different scenarios. Borrell et al. (1999) proposed a PKI-based cryptographic solution with some trusted authority (TA) launching agents. Bamasak and Zhang (Bamasak & Zhang, 2005) have proposed a distributed reputation management scheme to reduce the risk of malicious hosts. We propose a revocation mechanism of host certificates to help brokers from sending agents to malicious hosts.

The arrangement of this paper is as follows. In Section 2, we introduce the architecture of an agent-based mobile application system. In Section 3, we propose an agent-based non-repudiation protocol suitable for mobile digital right management; we also analyze security mechanisms of this agent-based non-repudiation protocol, namely, dispute resolutions.

2. Preliminary knowledge

An efficient and fair non-repudiation protocol was proposed by Zhou and Gollmann where *TTP* acts as a lightweight notary (we name it ZGP) (Zhou & Gollmann., 1996). This protocol is suitable for 3G communication by analyzing the capability of implementing cryptographic operations such as digital signature, symmetric key encryption/decryption, hash function and random number generations (WPKI., 2004). According to this investigation, we design a non-repudiation protocol adaptive to agent-based mobile digital right management systems.

2.1. Basic structure for 3G mobile digital right management services

DRM is defined as a set of technologies and systems that can collectively support the entire life cycle (creation, manipulation, distribution and consumption) of contents by preventing illegal copying (Onieva et al., 2007).

The architecture for mobile digital right management system is composed of the following entities: a user represented by mobile equipment (ME), WPKI, a content provider and corresponding (digital) rights issuer, a bank and a broker, see Fig. 1. These entities are also issued certificates by some certification authority (CA) within this WPKI. ME utilizes the USIM (Universal Subscriber Identity Module) to store mobile client's information such as IMSI (International Mobile Subscriber Identity) and WPKI components. ME is capable of verifying digital signatures to authenticate other entities, if necessary. We also deploy a middleware called the broker to help ME authenticate the merchant server such that attackers cannot impersonate this seller. Merchant servers can perform PKI operations for evidence generations.

2.2. WPKI

The WPKI is the core cryptographic mechanism for non-repudiation protocol; it consists of two parts, one is the operation; the other is the entity. WPKI entities must contain at least two public–private key pairs for encryption/decryption and signature generation/verification, respectively. These key pairs are generated by some CAs whose major task is to bind public key, private key and entity together. The public key will be stored in some certificate field; CA will issue (subscriber) certificates and server certificates to buyers and varied servers, respectively, see Fig. 2. Users may issue proxy certificates to their mobile agents for transaction delegations. The digital signature of a message is generated by using the private key of message owner and some hash function. Without loss of generality, we may assume that one of the standard hash function is applied, which is denoted by *H*.

2.2.1. WPKI operations

Major WPKI operation in our non-repudiation protocol is the digital signature-based evidence generation and verification. Let