Journal of Network and Computer Applications 34 (2011) 653–667

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Achieving autonomous fair exchange in ubiquitous network settings

Q. Shi [a,*], N. Zhang [b], M. Merabti [a], R. Askwith [a]

[a] School of Computing and Mathematical Sciences, Liverpool John Moores University, Byrom Street, Liverpool L3 3AF, UK
[b] Department of Computer Science, The University of Manchester, Oxford Road, Manchester M13 9PL, UK

ARTICLE INFO

Article history:
Received 23 January 2009
Received in revised form
11 November 2010
Accepted 15 November 2010
Available online 19 November 2010

Keywords:
Ubiquitous networks
Agent systems
Fair exchange
Signatures
Communication protocols

ABSTRACT

This paper addresses the issue of fair (signature or key) exchange in emerging ubiquitous commerce (u-commerce). Such an application poses new security challenges. In particular, it involves distributed and autonomous operations running in a much open, dynamic and resource-diversified networking environment, which makes an exchange highly susceptible to security attacks and system failures. Existing approaches to fair exchange are ineffective in dealing with the new challenges as their design did not envisage such complex operational situations. In this paper, we aim to propose a novel fair exchange protocol specifically for u-commerce in response to the new challenges. The protocol is supported by an integration of several techniques, such as threshold proxy signatures, purpose-restricted encryption key certification and threshold verifiable proxy encryption, to accomplish the fairness of exchange in u-commerce settings. The protocol analysis is also provided for the proof of its fairness.

1. Introduction

Ubiquitous computing utilises wireless technologies to integrate everyday appliances (e.g. networked refrigerators, TVs and cars) together with information suppliers (e.g. the Internet) to greatly enhance the quality of life for individuals and families. This is pushing the frontiers of existing *electronic*/*mobile* (*e*/*m*-) *commerce* further onwards to provide seamless and intelligent business services from anywhere in an integrated digital and physical world at any time, which is called *ubiquitous* (*u*-) *commerce*. Such technology advance is making security research and provision ever more challenging and pressingly important as insecure u-commerce will harm consumer confidence and thus jeopardise the enormous business potential of u-commerce.

A key security issue of existing e/m-commerce applications is concerned about how two parties (e.g. individuals, companies or systems) can exchange valuable/important information through (digital) signatures or (cryptographic) keys over networks such as the Internet. The valuable nature of the exchanged information dictates that the exchange must be fair in the sense that either each party, or neither of them, can get the expected information from the other party at the end of the exchange, which is also called strong fairness. This requirement is essential for preventing frauds committed by one party against the other, e.g. having accepted a digitally signed electronic payment from an on-line customer, an on-line merchant refuses the delivery of the promised and paid digital goods (e.g. a newly released film) to the customer.

The current work on fair exchange normally supposes that a user (or users) involved in an exchange should determine what information to exchange, and employ a computing device with certain trust to perform the exchange. This makes the exchange environment of the user quite simple, so the work can be focused mainly on the issue of how to exchange the agreed information fairly and securely. This approach is suitable for less intelligent existing e/m-commerce applications with pretty static exchange scenarios, relatively simple computing settings and low autonomy activities, although some effort has been made to employ mobile (software) agents to perform exchanges over the Internet (Zhang et al., 2004).

In contrast, the emergence of u-commerce is bringing additional perspectives into studies on fair exchange due to the distinct characteristics of u-commerce applications, including high autonomy, heterogeneity and distributability. This can be demonstrated using an example about a potential u-commerce setting for a user Alice and her networked/smart home, which is shown in Fig. 1, with an application scenario described below:

- Alice is taking a bus to her office in a morning, and her PDA picks up the sale information about a recently released film when the bus passes a shopping centre.
- She decides to purchase the film from the Internet, to invite several close friends to have a dinner in her house in the evening, and then to watch the film on a networked TV together.
- She prepares a request for the purchase of the film, a list of groceries for the dinner, and a name list of the invited friends,

* Corresponding author. Tel.: +44 151 231 2272.
E-mail addresses: Q.Shi@ljmu.ac.uk (Q. Shi), nzhang@cs.man.ac.uk (N. Zhang), M.Merabti@ljmu.ac.uk (M. Merabti), R.J.Askwith@ljmu.ac.uk (R. Askwith).

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.11.002