Electronic Commerce Research and Applications 12 (2013) 1–13

Contents lists available at SciVerse ScienceDirect

Electronic Commerce Research and Applications

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

An innovative electronic group-buying system for mobile commerce

Jung-San Lee *, Kun-Shian Lin

Department of Information Engineering and Computer Science, Feng Chia University, No. 100, Wunhua Rd., Situn Dist., Taichung City 40724, Taiwan, ROC

ARTICLE INFO

Article history:
Received 22 October 2011
Received in revised form 18 September 2012
Accepted 28 September 2012
Available online 26 October 2012

Keywords:
Mobile commerce
Group-buying
Mutual authentication
BAN logic
Bloom-filter

ABSTRACT

With the benefits of discount and convenience, the group-buying mechanism has become a popular commerce service. Nevertheless, there exist several drawbacks in current group-buying systems. First, the absence of security consideration may reveal the privacy of involved participants. Moreover, buyers must pay money to the initiator in advance. Without a trusted third party to monitor the purchase, the initiator may vanish after collecting the money. To mitigate the risk of the above weaknesses, we propose a new mechanism introducing a group-buying server to secure and monitor the transaction. Because the server acts as a mediator, it can help the buyer and vender to negotiate with each other through a secure channel. Mutual authentication between the buyer and vender is guaranteed under the BAN logic model. In particular, we employ the Bloom filter and XOR operation to reduce the size of the transaction table and the computational cost. Thus, the new method can be implemented in mobile devices.

1. Introduction

Recently, a report of Cable News Network has clearly shown that lots of online shoppers have registered to the group-buying websites in Chinese for purchasing the same thing and negotiating hefty discounts (Cashmore.group.buying, 2010, Chinas-latest-obsession-group-buying, 2011). More precisely, the total number of group-buying users in China, Hong Kong, and Taiwan has reached to 18.75 million in 2010, leading to US$ 260 million in sales. In 2011, the number of users has approached to 42.2 million (Chung and Chen 2012). In particular, the well-known Groupon has realized an annual operating income of US$ 2.0 billion in 2010. It is expected to reach US$ 4.0 billion at the end of 2011 (Song, 2011).

Undoubtedly, the group-buying activity is a pure and successful C2B model which has brought an amazing profit for customers (Song, 2011). The merchant can accordingly earn the outstanding business achievement. This has proved the significance of electronic group-buying system. The conventional group-buying system is shown in (Fig. 1).

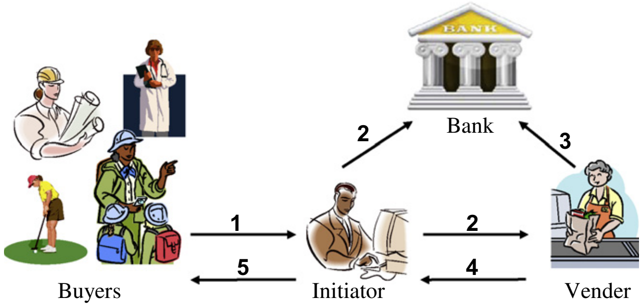
In conventional group-buying systems, an initiator collects money from buyers who want to purchase the same commodities. The initiator pays money to the account of the vender. For a large amount of orders, the vender can offer buyers a discount or provide some additional services, like carriage free. Upon receiving the commodities from the vender, the initiator then forwards the goods to each buyer. Thus, the buyer does not need to visit the store personally or pay a large price to get the commodity. Moreover, the group-buying system provides a platform which allows user to negotiate with other buyers; this can confirm the quality of the commodity and reduce the time of price comparison.

Although the conventional group-buying system is practical, some drawbacks still exist. First, the conventional group-buying system focuses on the convenience of the transaction and the selectivity of payment terms. Even a trusted third party (TTP), i.e. the bank, is introduced to monitor money transfer. The confidentiality of data is seldom considered in the transaction. Since the TTP never checks the integrity of the message, a malicious attacker can intercept and tamper with the message to break the deal. In addition, the group-buying system cannot verify and monitor the transaction procedure. Thus, after buyers pay money to the account of the initiator, they face the risk of the initiator taking the money away. Furthermore, the traditional system does not provide a reliable method to revoke illegal users. If a malicious user joins the buying group, it is infeasible to prevent him from violating the transaction.

To improve the drawback that the TTP does not get involved into the verification, previous study has introduced the concept of key escrow (Long et al., 2005; Youssef, 2010; Ni et al., 2012). The main idea is to authenticate the communications between the sender and receiver according to the TTP. This can achieve the essentials of identity verification and information filtering. Thus, it has been employed to secure dozens of online e-commerce mechanisms. The secret key of a key escrow method is usually separated into two parts. One is kept by the TTP, i.e. the key escrow. Once a user applies the secret key to encrypt the message, the receiver has to cooperate with the TTP to obtain two parts of secret to

* Corresponding author. Tel.: +886 4 24517250x3767; fax: +886 4 27066495.
E-mail addresses: leejs@fcu.edu.tw (J.-S. Lee), logoduo@hotmail.com (K.-S. Lin).

1567-4223/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.elerap.2012.09.005



1. buyers join the group-buying and pay money to initiator
2. initiator sends the purchase order to vender as well as pays money to the account of vender
3. vender checks whether his/her account has received the money or not
4. vender sends the commodity to initiator
5. initiator forwards the commodity to each buyer

Fig. 1. Conventional group-buying system.

reconstruct the secret key. Then the secret key can be used to decrypt messages and verify the involved participant. The main advantage of this mechanism is that the secret key can be well protected and the TTP can help secure the communication. Nevertheless, the key escrow mechanism is constructed according to the asymmetric cryptosystem. The hefty computation and power consumption are not suitable for the mobile commerce. Moreover, the TTP has to record all the corresponding secret keys of involved participants. It has become an additional storage and key management problem. Hence, we aim to develop a more effective solution for securing electronic group-buying system instead of the key escrow method. The overview of the new electronic group-buying system is illustrated in Fig. 2.

We have introduced a fair server as the TTP to help secure the system. So far, the most famous group-buying services are provided by eBay and Google Offers (eBay 2012, Google Offers 2012), in which the complete of a transaction requires the cooperation of the enterprise and venders. Buyers need not to contact with venders directly. All they have to do is to order and pay for what they want via eBay or Google Offers. After that, eBay or Google Offers will contact with venders to finish the deal and send the product to buyers. It is obvious that the website of eBay or Google Offers can serve as the TTP in the novel electronic group-buying system. Since the TTP participates in the purchase, the correctness of transmitted message and the payment can be confirmed. This can secure the transaction from being tampered. Furthermore, we adopt the BAN logic model to ensure the correctness of mutual authentication between buyer and vender (Burrows et al. 1990).

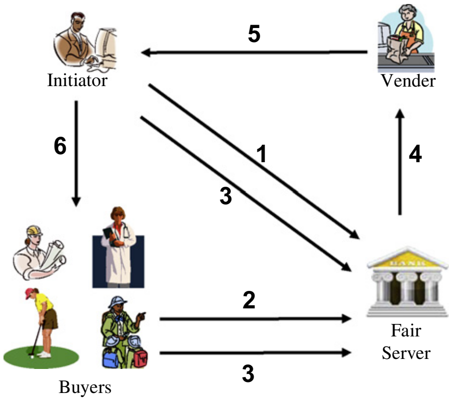
Due to the fact that mobile devices are unable to support the heavy computation of asymmetric/symmetric cryptographic systems such as RSA, ElGaml, DES, and AES (Rivest et al. 1978, ElGamal 1985, Biham and Shamir 1991, Daemen and Rijmen 2002), we apply the XOR operation and one-way hash function to enhance the efficiency of the new mechanism (Exclusive OR 2001, Menezes et al. 1996). In addition, to prevent the server from spending a large amount of storage to keep transaction data and verified tables, we employ the Bloom filter to mitigate the storage consumption (Bloom 1970). This allows the server to support more businesses and enables users to easily check their transaction tables on a mobile device. The advantage of high efficiency and light storage consumption can greatly help carry out the new mechanism.

The rest of this article is organized as follows. In Section 2, we introduce and explain the concept of the Bloom filter. We then specify the new group-buying mechanism in Section 3. The security analyses and performance discussions are presented in Sections 4 and 5, respectively. Finally, we make conclusions in Section 6.

2. Preliminaries of the Bloom filter

In the traditional verification method, if we want to check whether an element is in the set, we need to keep the identification of all elements as a verified table. When the amount of elements is very large, the storage consumption becomes impractical to serve the verification. Hence, B. Bloom has proposed the concept of the Bloom filter, which can solve the predicament of the bulky verified table problem (Bloom 1970). Many studies have researched how to compress the size of verified table and apply it to mobile devices (Bloom 1970, Mitzenmacher 2002, Ren et al. 2009). The architecture of the Bloom filter is shown in Fig. 3.

Bloom used the one-way hash function $h(\cdot)$ to map all elements E_1, E_2, and E_3 into an m bits array, and the initial value of all bits is zero. For each mapped bit, the value will be changed to one. To determine if the element E_1 is correct, a verifier can keep the array as a verified table and use the hash function $h(\cdot)$ to jumble the element and compare it with the one in the table. If the mapped bit is one, E_1 has a high probability to be valid; otherwise, the element must be incorrect. Obviously, we do not need to save all elements but do need to keep the m-bit array; this economizes a lot of storage. However, an extremely low probability of collision still exists. For example, if E_1 and E_2 may be mapped into the same bit, we cannot know which one is correct. Therefore, Bloom employed z different one-way hash functions to address the collision problem. The method is depicted in Fig. 4.



1. Initiator sponsors the purchase request to fair server
2. Buyers join the group-buying
3. After the transaction is established, initiator and buyers pay money to fair server
4. Fair server sends the purchase order to vender as well as transfers money into the account of vender
5. Vender checks the payment and sends the commodity to initiator
6. Initiator forwards the commodity to each buyer

Fig. 2. The overview of novel electronic group-buying system.