Towards Fair and Secure e-Commerce Model In P2P Network

Ji Won Jung*, Chul Sur** and Kyung Hyune Rhee***
* Dept. of Information Security,
**Dept. of Computer Science,
***Devision of Electronic, Computer and Telecommunication Engineering,
Pukyong National University, Busan, 608-737, Korea
E-mail: *forji78@yahoo.co.kr, **kahlil@mail1.pknu.ac.kr, *** khrhee@pknu.ac.kr
Tel : +81-51-620-6395 F ax : +82-51-626-4887

Abstract: In this paper we propose a fair and secure e-commerce model for P2P network, in which communication entities can buy and sell products by P2P contract. In particular, we focus on a fair transaction protocol that is based on a collaboration with distributed communication entities. This feature makes our model very attractive in P2P networking environment which does not depend on any central trusted authority for managing communication entities.

Keywords. P2P, e-Commerce, Fair transaction, Collaboration, Distributed communication

1. INTRODUCTION

Recently Peer-to-Peer(P2P) networking paradigms and its applications offer opportunities for new services over both Internet and Mobile Ad-hoc Networks(MANETs). Specially, mobile devices such as mobile phones and PDAs are already in widespread use, and functionality and performance of these devices are improving day by day. Due to the rapid growth of these technologies, mobile devices are expected to have capability to provide various services beyond the request of desired services. Hence, new services have appeared in P2P network, in which contents are bought and sold among entities by using mobile devices. Moreover, P2P network encourages an efficient contents distribution model among communication entities. Since each communication entity in P2P network does not depend on central trusted authority for management, it is inherently scalable to implement communication models. Therefore, designing an e-commerce model in P2P network is a promising challenge which we have never met before in Internet environment.

However, due to the lack of the central trusted authority, P2P network does not efficiently provide all the services required by e-commerce transaction such as reliability and fairness. In particular, guaranteeing *fairness* is a major challenge in e-commerce model. That is, at the end of exchange, it must be guaranteed that either each entity has received what it expects to receive or neither entity has received anything useful. Moreover, since the dynamic nature of P2P network implies that the consecutive connectivity between communication entities is not provided, it is more difficult to guarantee fairness for e-commerce transaction in P2P network.

In this paper we design a fair and secure e-commerce model for guaranteeing fairness and reliability in P2P network, in which communication entities can buy and sell digital contents by P2P contact. Especially, we focus on a fair transaction protocol based on collaboration with distributed communication entities distinguished from the traditional fair transaction protocol based on the central trusted authority. Moreover, the proposed protocol naturally provides desirable properties such as fault-tolerance and availability for P2P e-commerce model since we design the protocol by using the threshold cryptography.

The rest of the paper is organized as follows. The next section introduces the e-commerce services we have considered and identifies the security requirements in that e-commerce services. Section 3 describes preliminaries to induce the motivation of the paper. We outline our e-commerce model in Section 4. We present a collaborative fair transaction protocol that provides fairness and reliability for our model in Section 5. Finally, in Section 6 we conclude this paper.

2. P2P E-COMMERCE SERVICE AND REQUIREMENTS

P2P e-commerce service have the following features [3][8]. Services are provided by peers, but any peers may not necessarily provide the services. Activities in commercial transactions of the services provided by peers are carried out by entities who play both roles of a buyer and seller, and collaboration among the roles is necessary in commercial transactions. Roles will change dynamically according to the commercial transaction. For example, an entity who performs a buyer role in a commercial transaction might perform a seller role in another transaction.

Also, a peer does not always provide the reliable services, since not all the P2P services are offered with robust central servers. Services among peers are ad-hoc and temporal, and collaboration among peers in P2P commercial transaction is performed under ad-hoc and temporal connection. This characteristics result in formidable challenge as far as providing fair and reliable e-commerce service.

The following requirements are desirable in above P2P e-commerce service:

- Fairness : No entity should be able to interrupt or corrupt the protocol to force an outcome to her advantage. The protocol should terminate with either entity having obtained the desired information, or with neither one acquiring anything useful.
- Authentication : A communication partner is certainly the target partner.
- Confidentiality : The protocol should not need to disclose the message contents to any other entity excepting the communication entities.
- Integrity : In the middle of the protocol, an adversary cannot forge a message.
- Effectiveness : If no messages are lost, both entities behave according to the protocol and do not abandon the exchange, then both entities receive the desired items.
- Timeliness : It guarantees that both entities will achieve their desired items in the exchange within finite time.
- Non-Repudiation : It is impossible for a single entity after the execution of the protocol, to deny having participated in a part of the whole of the communication.

Specially, *fairness* is the most considerable requiremen in e-commerce service. Consequently, it is crucial that th protocol guarantees fairness between communicatio entities in P2P e-commerce model.

3. PRELIMINARIES

3.1. Threshold cryptography

Threshold cryptography distributes the ability to provide a cryptographic service such as signing or decryption. In a t out of n threshold scheme, any subset of greater than or equal to t entities (out of a total of n entities) can compute the desired functionality while any subset of less than t entities cannot. It offers better fault tolerance than non-threshold cryptography: even if some entities are unavailable, others can still perform the desired functionality. Threshold cryptography also provides better security since no single entity is entrusted to perform the desired functionality in its entirety. Consequently, it seems like an ideal choice to provide security services, such as secure, reliable and fair exchange in P2P network.

3.2. Fair Exchange Protocol

A *fair exchange protocol* ensures that, at the end of the exchange, either each entity receives the item it expects or neither entity receives any information about the other's item. The classical solution to the fair exchange problem is based on the idea of *gradually* exchanging small parts of the item. Works in this approach generally rely on the unrealistic assumption that the two entities have equal computational power or require many rounds to execute properly.

The practical approach to resolve the problem is to use a trusted third party (TTP) as arbitrator. Specifically, this approach can be classified as *on-line* protocol and *optimistic* protocol according to their involvement of TTP [1][9][13]. On-line protocol requires the presence of the TTP as a delivery channel, intervening in each transaction. As the TTP is always involved in every transaction, this protocol considerably implies a communication and computation bottleneck. In optimistic protocol the TTP is not used during the transaction when the communication entities behave correctly, but is involved only in case of disputes with one of the entities. Since the TTP is mostly off-line, this protocol reduces the communication and computation overhead of the TTP.

4. SYSTEM MODEL

4.1. System Components and Communication Channel Assumption

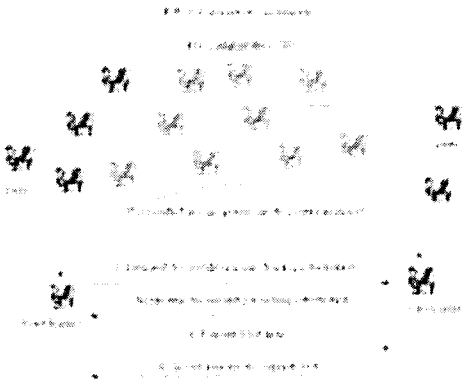

Fig. 1. Fair and Secure P2P e-Commerce Model.

Fig. 1 shows the proposed P2P e-commerce model, in which communication entities can buy and sell their products. The proposed model is consists of peers who play both roles of a seller and a buyer, and CTTP(Collaborative TTP) which manages the service key of peer community. The description of system components is as follows:

- Peer : An entity who plays either role of a seller or a buyer according as the demand that she desires.
- CTTP(Collaborative TTP) : CTTP is composed of a set of n special entities ($n \geq 3t+1$) which is called master peer, each runs on a separate device in a network. Each master peer has the service secret key share ss_i of peer community and performs the threshold cryptographic operations for assuring fairness and reliability between commercial transaction entities in peer community.

In addition to we introduce *an adversary* who can easily steal or otherwise compromise all entities including master peers. Thus our adversary model includes active (or Byzantine) adversary who can compromise some bounded fraction of entities in the network. However, we assume that fewer than 1/3 of the master peers are corrupted or malicious during the entire lifetime of shared service secret key. This means that at least $t+1$ master peers are *available* at any time.
Generally, according to the definition of *Asokan et al.* in [1], an availability of communication channels can be classified as follows:

Definition 1. *A communication channel between two correctly behaving entities is* ***operational*** *if the messages inserted into it by the sender are received by the recipient within a known, constant time interval.*

- **Reliable Channel** : A communication channel between two correctly behaving entities is ***reliable*** if it is guaranteed to be always operational. An adversary will not be able to delay any message in a reliable channel.
- **Resilient Channel** : A communication channel between two correctly behaving entities is ***resilient*** if it is normally operational but an adversary can succeed in delaying messages by arbitrary, but finite amount of time. In other words, a message inserted into a resilient channel will eventually be delivered.
- **Unreliable Channel** : A communication channel between two correctly behaving entities is unreliable if it has no assumptions about the communication channel between the two entities. In other words, a message inserted into a ***unreliable*** channel may be lost or modified.

We assume that communication channel between communication entities who carry out e-commerce transaction is unreliable by the nature of P2P network, and that communication channel between an available master peer and an entity is resilient in order to resolve the dispute. Actually, without resilient communication channel, it is impossible to guarantee fairness between communication entities. By consideration of the nature of P2P network and fairness of communication entities, our assumption is reasonable.
Finally we assume that the communication is carried over confidential and broadcast channels.

4.2. Initialization

We assume that our e-commerce model is based on the existing Public Key Infrastructure (PKI), i.e., every peer who wants to participate in commercial transaction has already its own standard X.509 public key certificate[7] issued by a recognized Certificate Authority (CA).
In the initial phase, a peer(or peers) wants e-commerce transaction of its contents constitutes peer community as virtual market. The high-level description of initialization is as follows:

1. To provide the fairness and reliability for e-commerce transaction, master peers are chosen at the constituting of peer community.
2. Each master peer MP_i obtains her service secret key share ss_i and service public key from a centralized dealer or by collaborative computation among master peers. For example, the threshold scheme described in [4] provides share distribution by collaboration among master peers, while the threshold scheme presented in [12] supports share distribution by trusted dealer.
3. Each master peer publishes the all identities of master peers and the service public key. After obtaining the identities of master peers and the service public key, an entity who wants to buy or sell its own digital contents performs an e-commerce transaction through peer community.

We assume that an entity who plays the role of seller broadcasts the information of its digital contents to all other entities at any time.
Finally, common issues associated with peer community that we have to consider are a peer community policy, an advertisement of digital contents and payment mechanisms. However, it remains beyond the scope of this work.

4.3. Notations

We use the following notations to describe the protocol:

- B,S : the identities of buyer and seller, respectively.
- MP_i : the identity of i-th Master Peer. Where, $1 \quad i \quad n$
- $item_X$: an item of an entity X.
- pay_X : payment information of an entity X.
- $desc_{item_X}, desc_{pay_X}$: the description of the item and the payment of an entity X, respectively.
- t_X : the local timestamp value of an entity X
- com_X : a randomly chosen commitment value by an entity X.
- CTTP : a set of Master Peer's identities.
$$=CTTP: \{MP_i, \cdots, MP_n\}$$
- PH : the protocol header, which contains relevant information such as the identities of the entities involved, the description of the desired item and payment.
$$PH := \{B, S, CTTP, desc_{item_X}, desc_{pay_X}\}$$
- $H(C)$: a collision resistant one-way hash function
- K : a randomly chosen session key for symmetric-key encryption function.
- $E_K()$: a symmetric-key encryption function under session key K.
- $C := E_K(item_X)$: the cipher of $item_X$ under session key K.
- $Sig_X()$: a signature function under X's private key.
- $PU_X()$: an asymmetric-key encryption function under X's public key.

- $PD_X()$: an asymmetric-key decryption function under X's private key.
- $X \rightarrow Y : m$: message m is sent from an entity X to an entity Y.
- $X \rightarrow \forall Y_i : m$: message m is broadcasted from an entity X to every entity Y_i, where $1 \le i \le n$.
- $\forall X_i \rightarrow Y : m$: message m is sent from every entity X_i to an entity Y, where $1 \le i \le n$.

5. A COLLABORATIVE FAIR TRANSACTION PROTOCOL

In this section, we present a *collaborative fair transaction protocol* which is used for guaranteeing fairness and reliability in P2P e-commerce model. In contrast to previously proposed fair exchange protocols [1][2][9][13] that are required the central trusted authority for providing fairness and reliability, our protocol does not require any central trusted authority since it guarantees fairness and reliability through collaboration with distributed community entities. Therefore, the proposed protocol is suitable for P2P e-commerce model.

The proposed protocol is composed of three sub-protocols: *the main protocol, the abort protocol, the recovery protocol.* The main protocol consists of messages exchanged directly between buyer and seller. In case of problems during this main protocol, two possibilities are offered to the entities. Either buyer executes the abort protocol in order to cancel the exchange, or buyer(or seller) launches the recovery protocol to complete the exchange.

5.1. Main Protocol

We assume that a buyer has already obtained the description of the desired item and all entities agree on the **CTTP** to be possibly invoked in case of conflict.

When a buyer wishes to receive the desired item from a seller against a payment of the item, the buyer can launch the main protocol. The detailed step is as follows:

1. A buyer who wants to perform e-commerce transaction constitutes the protocol header PH. The buyer also selects a commitment value com_B and timestamp value t_B, then computes $H(pay_B, com_B)$, $PU_{CTTP}(pay_B)$. The buyer configures a purchasing message including all above parameters and signs the purchasing message, then sends it to seller as [M-1].
$$B \rightarrow S : Sig_B(PH, H(pay_B, com_B), PU_{CTTP}(pay_B)) \quad \text{[M-1]}$$

2. A seller who receives [M-1] checks whether the signature of purchasing message is valid. If the check is invalid, the seller *quits* the exchange. Otherwise the seller constitutes the protocol header $\overline{PH}$, then chooses a random session key K and computes C, $H(item_S, K)$, $PU_{CTTP}(K)$. The seller forms a selling message and signs to it, then sends it to buyer as [M-2].
$$S \rightarrow B : Sig_S(\overline{PH}, H(item_S, K), C, PU_{CTTP}(K)) \quad \text{[M-2]}$$

3. After having checked the validity of the received message in step 2, the buyer sends pay_B, com_B together with the buyer's signature on those information to seller as [M-3]. If the validity of [M-2] is not satisfied, or the buyer gives up receiving the [M-2] message, then the buyer runs *the abort protocol.*
$$B \rightarrow S : Sig_B(pay_B, com_B) \quad \text{[M-3]}$$

4. The seller checks the validity of [M-3]. If the check is valid, the seller obtains the desired payment information pay_B. The seller sends the session key K to the buyer together with its signature. If any problem occurs in above process, the seller may *quit* the protocol.
$$S \rightarrow B : Sig_S(K) \quad \text{[M-4]}$$

5. After receiving the [M-4] message from the seller, the buyer verifies the signature and obtains the desired item by using the session key K. If the validity of the received signature is invalid or the buyer gives up finishing the protocol, then launches *the recovery protocol.*

Remark 1.
The use of the commitment com_B, in steps 1 and 3, prevents a malicious seller from launching the recovery protocol without sending the second message to the buyer. Unless receiving commitment com_B the CTTP does not run the recovery protocol to resolve the conflict.

5.2. Abort Protocol

If the seller does not send the second message of the main protocol, the buyer can collaborate with the CTTP in order to abort the protocol. The detailed step is as follows:

1. The buyer broadcasts an abort request to all the master peers.
$$B \rightarrow \forall MP_i : Sig_B("AbortReq", [M-1]) \quad \text{[A-1]}$$

2. Each master peer verifies the received [A-1]. If [A-1] is correct, each master peer computes partial signature $Sig_{SS_i}("aborted", [M-1])$ with its service secret share ss_i. Then all master peers send their abort confirmation to the buyer.
$$\forall MP_i \rightarrow B : Sig_{MP_i}(Sig_{ss_i}("Aborted", [M-1])) \quad \text{[A-2]}$$

3. To generate a valid signature of CTTP, the buyer needs at least $t+1$ correct partial signatures. Hence, the buyer chooses $t+1$ correct partial signatures, and computes an abort token $Sig_{CTTP}(abort, [M-1])$. This abort token can be used for guaranteeing the fairness in case of potential dispute.

Remark 2.
– Our protocol has been designed considering the threshold RSA scheme because the threshold scheme based on discrete logarithms may require an agreement

upon random number to generate partial signature. Furthermore, the threshold RSA scheme can be applicable to threshold decryption.

- Since the validation of partial signature depends on the underlying threshold scheme, we can check the validation of partial signature by means of applying the threshold RSA schemes that provide the *robustness* [6][12] to our protocol.

5.3. Recovery Protocol

If the seller does not send his final message of the main protocol, the buyer can launch the recovery protocol by means of collaborating with the CTTP, in order to complete the exchange. The detailed step is as follows:

1 The buyer broadcasts the received [M-1], [M-2] and her commitment com_B along with her signature to all the master peers.

$B \rightarrow \forall MP_i$: [M-1],[M-2], Sig_B("RecoverReq",com_B) [R-1]

2 Each master peer checks all the validity of received [R-1]. If the check is valid, each master peer performs the following:

— To complete the exchange for buyer, each master peer generates partial decryption $PD_{ss_i}(PU_{CTTP}(K))$ of the session key with its service secret share ss_i. Then all master peers send to the buyer their recovery information.

$\forall MP_i \rightarrow B : Sig_{MP_i}$("Recovered", $PD_{ss_i}(PU_{CTTP}(K))$) [R-2-B]

— Also, each master peer computes partial decryption $PD_{ss_i}(PU_{CTTP}(pay_B))$ of the payment information with its service secret share ss_i. Then all master peers send corresponding information to the seller.

$\forall MP_i \rightarrow S : Sig_{MP_i}$("Recovered", $PD_{ss_i}(PU_{CTTP}(pay_B))$, com_B) [R-2-S]

3. Finally, Each buyer and seller performs the following, respectively.

— To generate the session key K, the buyer chooses $t+1$ correct partial decryptions, and computes the session key K. Therefore, the buyer can obtain the desired item by using session key K.

— The seller selects t+1 correct partial decryptions, then obtains the desired payment with respect to his item.

Remark 3.
Since the seller does not engage in recovery protocol with the CTTP in main protocol, basically the seller needs not launch the recovery for assuring fairness. However, the seller is able to recognize the activity of recovery caused by receiving [R-2-S] message when the buyer runs the recovery protocol. If the seller receives sufficient information in order to generate the payment information, the seller can obtain the desired payment with respect to his item. Otherwise, the seller can launch the recovery protocol together with commitment com_B within [R-2-S] in order to assure his fairness.

6. CONCLUSION

In this paper we have presented a fair and secure e-commerce model suitable for P2P network. In particular, we have proposed a collaborative fair transaction protocol which is used for guaranteeing the fairness and reliability in P2P e-commerce model.

Compared to the traditional fair exchange protocol based on the central trusted authority, our protocol does not require any central trusted authority.

Consequently, our protocol is attractive in P2P networking environment which does not naturally depend upon any central trusted authority for managing communication entities.

Acknowledgement

This research was supported by the Program for the Training of Graduate Students in Regional Innovation which was conducted by the Ministry of Commerce, Industry and Energy of the Korean Government.

References

[1] N. Asokan, V. Shoup, and M. Waidner, "*Asynchronous protocols for optimistic fair exchange*", in Proceeding of the IEEE Symposium on Research in Security and Privacy, May 1998.

[2] N. Asokan, V. Shoup, and M. Waidner, "*Optimistic fair exchange of digital signatures*", In Proc. Eurocrypt'98 , LNCS 1403, pp. 591-606, 1998.

[3] P. Antoniadis, C. courcoubeits, " *Market models for P2P content distribution*", In Proc. AP2PC'02, 2002.

[4] D. Boneh, M. Franklin, "*Efficient generation of shared RSA keys*", in Proceedings Crypto'97, pp.425-439, 1997.

[5] P. Fouque, J. Stern, "*Fully Distributed Threshold RSA under Standard Assumptions*", In Proc. ASIACRYPT 2001, pp. 310-330, 2001.

[6] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "*Robust and efficient sharing of RSA functions*", In Proc. Crypto'96, LNCS 1109, pp.157-172, 1996.

[7] R. Housley, W. Ford, W. Polk, D.Solo, "*Internet X.509 Public key infrastructure certificate and CRL profile*", RFC 2459. January 1999.

[8] T.Iwao, Y. Wada, S. Yamasaki, M. Shiouchi, M. Okada, M. Amamiya, "*A Framework for the Next Generation of E-Commerce by Peer-to-Peer contact*". IEEE WETICE 2001

[9] O.Markowitch and S.Saeednia, "*Optimistic Fair Exchange with Transparent Signature Recovery*", In Proc. Financial Cryptography 2001, LNCS 2339, pp. 339-350, 2002.

[10] Alfred J. Menezes, Paul C. van Oorshot, Scoot A. Vanstone "*Handbook of Applied Cryptography*", 1997, CRC Press

[11] Tal Rabin, "*A Simplified Approach to Threshold and Proactive RSA*", In H.Krawczyk, editor, Advances in Cryptology-CRYPTO'98, LNCS 1462, pp. 89-104, 1998.

[12] Victor Shoup, "*Practical threshold signatures*", In Proc. Eurocrypt 2000 LNCS 1807, pp.207-220, 2000.

[13] Holger Vogt, "*Asynchronous Optimistic Fair Exchange Based on Revocable Items*", In Proc, Financial Cryptography 2003, LNCS 2851, pp. 193-207, October 2003.