Payment Scheme for Multi-Party Cascading P2P Exchange

Yichun Liu and Zemao Zhao
Hangzhou Dianzi University
Hangzhou 310018, China
liuyichun@126.com

Abstract. As a decentralized technology, P2P architecture arises as a new model for distributed computing and transaction in the last few years, consequently there is a need for a scheme to incorporate payment services to enable electronic commerce transaction via P2P systems. In this paper, the cascading sale model is described for multi-party P2P transaction, an efficient pricing and routing scheme is proposed for multi-party P2P transaction, and a new onion payment scheme is proposed, which can ensure that each middleman and digital content owner can obtain the payments due to them.

1 Introduction

P2P systems are network where peer nodes communicate and transport information directly each other. Unlike the conventional client-server model, a peer node of P2P network may act as both a client and a server simultaneously to share files or computing powers. It can request, serve, or relay services as needed. A major differentiating factor of P2P from traditional models is the lack of central management and control. This very important characteristic offers the ability to create efficient, scalable, and persistent services by taking advantage of the fully distributed nature of the systems.

In traditional electronic commerce transaction, some parties serve as vendors, who only sell goods, and the others act as buyers, who only purchase goods. However, in P2P transaction environment, peers serve as both vendors and buyers. A peer who has bought digital content might sell it to other for earning middleman commission.

Most of the current e-commerce researches are based on simple electronic transaction model. This is quite a distance away from what an electronic marketplace is envisioned to be. Nowadays, most of them are limited to simple exchange of funds and merchandise, and not sufficient for the complex transaction scenarios. Electronic commercial exchanges may be stymied because of a lack of a proper transaction model or protocol.

In this paper, we aim to propose a cascading transaction model for electronic commerce, in which multiple brokers relay the goods and payment between the goods owner and consumer according to the chained path. The related works are introduced in the next section; the cascading transaction model is described in section 3; the policy for transaction chain and price negotiation is discussed in section 4; the cascading payment model is proposed in section 5.

2 Related Work

A number of research projects have engaged in P2P computing and most have been focused on efficient resource location and load balancing; very few have addressed the need of payments in P2P environment.

An early P2P payment scheme is provided in [1], which relies on a fully trusted on-line escrow server. In this scheme, an escrow server is used as trusted thirty parties, which deal with the protocol commitment, transmission of decryption key and payment. The escrow server bearing too much burden will be inefficient and it might become the bottleneck of payment system, so the scheme has poor scalability.

Another P2P payment system is provided in [2], where a stamped digital note is introduced as token of transaction. The digital note is produced by the specific vendor and is stamped by the broker, and it can only be received and cashed by its issuer, so the scheme has still poor scalability.

The P2P payment scheme provided in [3] inherits the idea of the stamped digital note and delegates the vendor role to the agent during the payment phase, where the buyer peer does not need special digital notes for each vendor peer. Instead, he can buy digital goods from several vendor peers by interacting with only one agent who represents these vendor peers. In the scheme, the stamped digital note can only be used by a few vendors and an on-line third party is introduced, who is a heavy server in fact.

In the P2P payment protocol provided in [4], the buyer obtains the broker coin from the broker, and the vendor coin is produced by the vendor. The buyer and the vendor exchange their digital coins, and then buyer pays vendor coins to buy the goods from the vendor. The protocol is anonymous and secure, but it is neither practical nor convenient that the buyer must obtain special coin from different vendor before per transaction.

Ppay is a micropayment scheme for P2P environment [5], which presents the concept of floating and self-managed currency to greatly reduce broker involvement. The currency is allowed to float from one node to another without involving a centralized broker, and all security related to a coin, except for when the coin is first created or cashed. This currency is practical and efficient, but the related payment protocol is not presented.

Some complex transaction models are provided in [6], where the multi-party cascading transaction model is described as a transaction tree. The paper proposed some important requirement for complex transaction model, but the payment scheme has not been presented.

3 Cascading Transaction

With the globalization of economy, the commodity manufacturers wish selling their products over the world. It is necessary that goods producers sell their goods with the help of the middlemen. Usually, the hierarchical sale system includes the following levels: the manufacturer, the general agents, the district agents, the wholesalers, and the retailers. In the traditional chained model, the broker nodes are distributed in term of directed tree structure, and each node has only parent node. The traditional hierarchical sale model is described as Figure1.

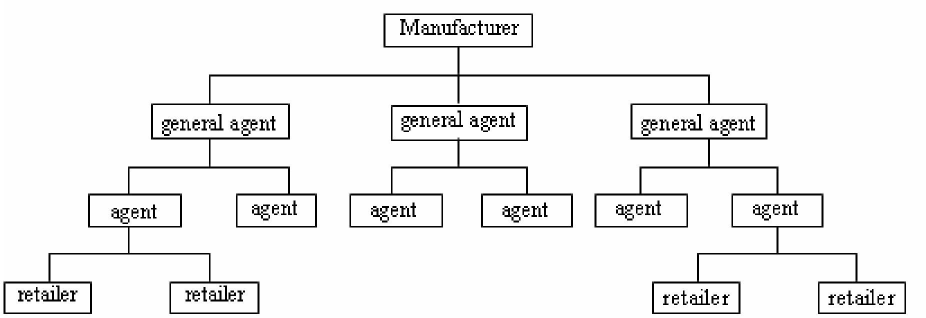

Fig. 1. Traditional Model for Multi-Party Cascading Sale

In the P2P cascading model, the broker nodes are peer-to-peer, and distributed in term of mesh structure, in which there are multiple path between any two nodes. In this model, theoretically unlimited parties can participate in the whole transaction. Among these parties, there should be a customer who is an end buyer and a supplier who is an end seller. The other parties are brokers who buy and resell the products.

The P2P model for multi-party cascading transaction is described as Figure2.

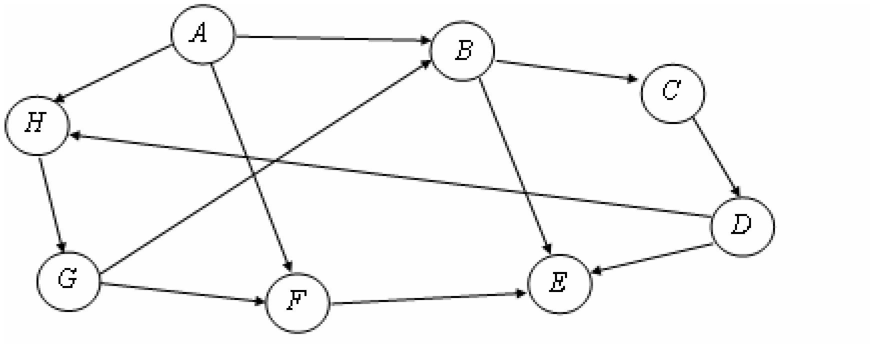

Fig. 2. Traditional Model for Multi-Party Cascading Sale

In the transaction shown as Figure2, the goods owner *A* might sell its goods along the path *A*→*B*→*C*→*D*→*E*, and it might also sell the goods along the path *A*→ *H*→*G*→*F*→*E*, the path *A*→*B*→*E*, or the path *A*→*F*→*E*. The node *B* might obtain goods from *A* and might obtain other goods from *G*. The P2P members choose the path for obtaining suitable goods by considering the goods price and the trust of other peers, instead of regular hierarchical relation in traditional model.

In traditional commerce model, the customers only contact with the retailers, instead of contacting with the original goods owner. Usually, the items of P2P exchange are digital contents, which are easy to be duplicated and counterfeited. The P2P members are dynamical and changeable, so the payments should be distributed among both middle agent and goods owner, and it should be avoided that one party take the payment illegally which belongs to the others. In a P2P transaction, it should be guaranteed that the goods owner can obtain the royalties and the middleman brokers should get the commissions.

4 Exchange Chain And Price Negotiation

In multi-party cascading transaction, the goods price depends on the exchange chain that the goods and payment is transferred. Optimal exchange chain should be determined before the scheme is designed for P2P multi-party cascading transaction, so that the customers pay out at the lowest price.

When a P2P member wants to buy goods, it will send the purchase request to its neighbour node for searching the vendors. Each node which has received the request will relay the purchase message to their neighbour, until the goods owner receives the request. A larger P2P system has a mesh-like topological structure, in which there are many chain from a customer node to a merchant node, and it is possible that several merchant node have the requested goods.

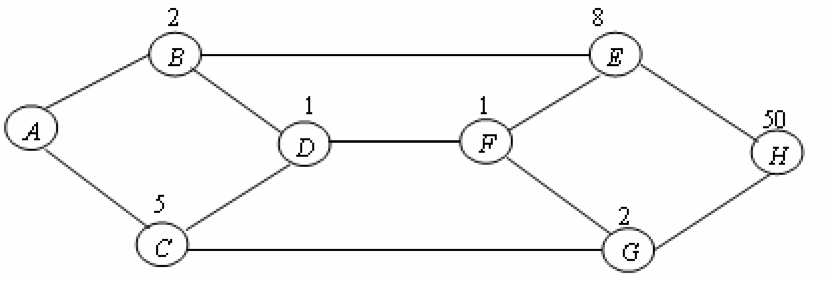

Fig. 3. Node Path of P2P Exchange

An example of multi-party P2P transaction is shown as Figure3. The nodes *A*, *B*, *C*, *D*, *E*, *F*, *G and H* denote the P2P members. *A* is an end buyer and *H* is the owner of the goods in the example. The weight on the node *H* denotes the royalty of the owner, and the weight on other nodes denotes the commissions of middleman agents. *A*'s exchange cost can be expressed the sum of the weight on nodes along a path from *A* to *H*. There are different paths from *A* to *H* as follows: the sum of weight is 60 on the path $A \to B \to E \to H$; the sum of weight is 57 on the path $A \to C \to G \to H$; the sum of weight on the path $A \to B \to D \to F \to E \to H$ is 62; the sum of weight on the path $A \to C \to D \to F \to G \to H$ is 59; the sum of weight on the path $A \to B \to D \to F \to G \to H$ is 56; the sum of weight on the path $A \to C \to D \to F \to E \to H$ is 65. The path is shortest and *A* pay at lowest cost when the route $A \to B \to D \to F \to G \to H$ is selected. Selecting the shortest exchange path means selecting the lowest price. A famous method is Dijkstra algorithm for computing the shortest path.

In the P2P multi-party transaction, the disclosure of exchange information might lead to the broker's loss. The middle brokers don't wish that their exchange information and its neighbour nodes are not known by other parties in the same chain. It would be possible in Figure 3 that *B* contacts with *F* directly instead of node *D* for obtaining more commissions if *B* learns that *D* would get the goods from *F*.

This problem can be resolved efficiently by the aid of public key cryptography. A customer *C* selects a public/private key pairs, and then multicasts the purchase request and digital certificate to its neighbor nodes. The request receivers will relay the received messages on and on, until the original goods owner *O* receives the purchase request and digital certificate.

There are multiple routes from the customer *C* to the goods owner *O*. If a route is $C \to A_m \to A_{m-1} \to \ldots \to A_1 \to O$, here A_i is the *i*-th middle broker between *O* and *C*, *O* sends its royalty to the adjacent broker node A_1.

$O \to A_1 : PK_C(O, [royalty]_O)$

A_1 send its commission information $commission_1$ and the message from *O* to A_1.

$A_1 \to A_2 : \quad PK_C(A_1, [commission_1]_{A_1}, PK_C(O, [royalty]_O))$

Similarly, each A_i sends the message from A_{i-1} and A_i 's commission information $commission_i$ to A_{i+1}.

$A_i \rightarrow A_{i+1}$: $PK_C(A_i, [commission_i]_{A_i}, PK_C(A_{i-1}, [commission_{i-1}]_{A_{i-1}}, \ldots PK_C(O, [royalty]_O)\ldots))$, i=1~m-1

At last, the vendor A_m sends the price list *price_list* to the buyer *C*.

$A_m \rightarrow C$: $price\_list = PK_C(A_m, [commission_m]_{A_m}, PK_C(A_{m-1},[commission_{m-1}]_{A_{m-1}}, \ldots, PK_C(O, [royalty]_O)\ldots))$

The item PK_X (*message*) denotes the encryption of the message *message* with *X*'s public key. $[message]_X$ includes two parts, the message *message* and the digital signature on it with *X*'s private key.

The customer *C* decrypts the price list with its private key and obtains the nodes information on each path $\{A_m, A_{m-1}, \ldots, A_1, O\}$, the commission information $\{commission_m, commission_{m-1}, \ldots, commission_1\}$ for every brokers, and the royalty information *royalty*. *C* can calculates the shortest path from *C* to *O* and obtain the optimal scheme for selecting the exchange path and pricing the exchange.

In the above negotiation process, RSA algorithm is recommended for the encryption and signature algorithm. DSA is an alternative algorithm for message signature. When the secure algorithms such as RSA or DSA are adopted, the malicious could not decode encrypted message or counterfeit valid signature.

5 Cascading Payment Model

A typical multi-party cascading payment system includes multiple parties: a customer *C*, a goods owner *O*, multiple intermediary peers A_1, A_2, A_3, $\ldots A_{m-1}$, A_m. The intermediaries buy the goods and sell it for obtaining the commissions.

The payments shall be distributed among peers (on a royalty-commission basis), where the content owner receives a fixed amount of the payment value. To ensure only the owner can claim payment for royalty, the payment for royalty shall be encapsulated for the owner at the payment origin. Content needs to be tagged with the owner's identity to enable this. Also, only payment meant for a peer may be redeemed by that peer, this requires the use of encryption techniques being applied. This enables the payments meant for content owners to be stored on other peers without them being wrongly redeemed.

We propose a new onion payment scheme to ensure that a goods owner can receive the royalty and all intermediaries can receive the commissions. In this scheme, the buyer peer encapsulates the payments for royalty and commissions into an onion payment package, and then transfers it to goods owner along the selected exchange path. Each intermediary peers on the exchange path strips the skin of onion payment package and gets its commission, until the owner obtain its royalty. The onion payment can be taken as a kind of onion route with payment information.

Let A_0 denotes the owner *O*, and $payment_i$ denotes the payment for the commission of each intermediary peer A_i for i=1~m. When the payment is transferred along the path $C \rightarrow A_m \rightarrow A_{m-1} \rightarrow \ldots \rightarrow A_1 \rightarrow O$, the onion payment package is as following:

$Onion\_Payment_0 = PK_{A_0}(payment_0)$

$Onion\_Payment_i = PK_{A_i}(payment_i, A_{i-1}, Onion\_Payment_{i-1})$, i=1,2, …, m

The customer C encapsulate the onion payment package $Onion\_Payment_m$ and sends it to vendor A_m.

$C \rightarrow A_m$: $Onion\_Payment_m = PK_{A_i}(payment_m, A_{m-1}, Onion\_Payment_{m-1})$

A_m strip the exterior layer of onion payment package and get the payment for its commission $payment_i$ and the identifier of next broker A_{m-1}. Similarly, each A_i gets its payment $payment_i$ and then sends the onion payment message $Onion\_Payment_{i-1}$ to A_{i-1}.

$A_i \rightarrow A_{i-1}$: $Onion\_Payment_{i-1} = PK_{A_{i-1}}(payment_{i-1}, A_{i-2}, Onion\_Payment_{i-2})$
$i = m \sim 2$

At last, A_1 send the payment $payment_0$ for royalty to the owner O.

$A_1 \rightarrow O$: $PK_{A0}\ (payment_0)$

By using onion payment package with public key cryptography system, each exchange party can obtain its due, and no one can intercept the payment for other party.

The onion payment technology can guarantee the anonymity of payment information. By using onion payment technology for exchange payment, each broker can only get and learn its own payment information but it can’t obtain the other’s payment information by unpacking the payment package. The onion payment is efficient for multi-party cascading payment in complex exchange environment.

6 Conclusion

Nowadays most of researches on electronic commerce are focused on the simple exchange mode. Multi-party cascading exchange is a typical model of electronic commerce transaction. In this paper, the cascading exchange mode is described for multi-party P2P transaction, a new optimum strategy is presented for pricing and routing in multi-party P2P transaction, and the onion payment scheme is proposed so that the goods owner can obtain its royalty and each middleman broker can obtain its due commission in the complex multi-party transaction. By introducing public key cryptography system, our scheme is secure, and no one can illegally decode and counterfeit the confidential information or intercept the payment due to other peers.

Acknowledgments

This research was supported by the the Scientific Research Fund of Zhejiang Provincial Education Department under Grant No. 20060239.

References

1. B. Horne, Escrow Services and Incentives in Peer-to-peer Networks, Proceedings *of the 3rd ACM conference on Electronic Commerce*, 85-94 (2001).

2. L. Anantharaman, *An Efficient and Practical Peer-to-peer E-payment System*, Manuscript(2002).

3. J. A. Onieva, *Practical Service Charge for Peer-to-peer Content Distribution*, Springer-Verlag ,112-123 (2003).

4. P. Daras, A Novel Peer-to-peer Payment Protocol, *Proceedings of the EUROCON '2003,* 2-6 (2003).

5. B.Yang, Ppay: micropayments for peer-to-peer systems, *Proceedings of the 10th ACM conference on Computer and communication security*, 300 – 310 (2003).

6. G. Wang, Models and protocol structures for software agent based complex e-commerce transactions, *Springer-Verlag* , 121−131(2001).