International Journal of Computer Networks & Communications (IJCNC) Vol.4, No.4, July 2012

A Review of Fair Exchange Protocols

Abdullah AlOtaibi and Hamza Aldabbas

Software Technology Research Laboratory (STRL)
De Montfort University, Leicester, United Kingdom

Otaibi_as@hotmail.com and hamza@dmu.ac.uk

ABSTRACT

Recently, the Internet has become an essential business platform, aiding trading, distribution and sales between organisations, consumers and even between consumers themselves. This technology revolution has brought e-commerce to an entirely new level, which therefore has raised some new security issues. Security protocols in e-commerce are required to manage the transactions between buyers and sellers. In order to engage customers in e-commerce, these protocols should be well formulated and secured; they should protect both parties from fraudulent users and subsequently promote the growth of e-commerce. There are some protocols, known as fair exchange protocols, in e-commerce that are designed to guarantee fairness between the customer and the merchant so that neither party gains any advantage over the other. Therefore, in this paper, we review these protocols in detail. In addition, we present a survey of three fair exchange protocols based on online TTP from different application areas. In particular, we review these protocols with regard to certain properties, namely, fairness, correctness of product, customer's anonymity, timeliness and channel requirement.

KEYWORDS:

E-commerce, Fair exchange protcocol, TTP (Trusted Third Party)

1. INTRODUCTION

The amount of business directed electronically has grown notably, in concert with the rapidly increasing use of the Internet, because e-commerce has recently become the standard platform for streamlining business flows and trading between organizations and consumers [1]. Nowadays, without any doubt, the development of information and communication technology is playing an enormous part in making individuals' lives easier than before. Due to the rapid growth of e-commerce in recent years, much business today is conducted online. In other words, more businesses than ever before are using the Internet to sell their commodities to people all over the world. The Internet provides them with a platform for selling their items to all kinds of people without the restrictions of geographical borders. Customer choice in buying goods and services has been greatly enhanced by this growth of e-commerce. For various reasons, many customers opt to buy their items through the Internet; firstly, they have the convenience of making purchases from the comfort of their homes without going to shopping centres or suffering the hassles of traffic jams. Secondly, customers have the opportunity to quickly compare the prices of various traders. Thirdly, goods and services are delivered to the customer's home. Lastly, customers are able to buy products at any time, from anywhere in the world.

DOI : 10.5121/ijcnc.2012.4420

In traditional commerce, customers do not have to worry that they will be given the product that they paid for. This is because the customer goes to a shop, selects a product, pays for it and takes it away. Customers also do not have to worry that their financial data will be revealed to a third party, as they make payment in cash. In addition to the above points, customers can also remain anonymous and avoid the merchants tracing their buying habits by making their payments in cash. However, in e-commerce, these factors in traditional commerce can become a major concern for customers. Through online payment, personal data and financial information that is not encrypted might be revealed to fraudulent persons.

There must be trust between the buyer and the seller, but in e-commerce, customers are worried that dishonest dealers might send them the wrong product. There must be a system in place to ensure that the data being sent through any secure means are heavily protected. There is no doubt that e-commerce has made the exchange of goods and services easier but it also poses risks to both the customer and the merchant, in terms of security, safeguarding users' privacy, trust and anonymity [2, 3]. The threat of e-crime is real risk, and conducting commercial activities over the Internet is still highly risky. This high risk is mainly becausethe Internet being an open and insecure environment. Performing fraud over the Internet is relatively easy; attacks can be performed from distant peer and can be executed automatically,entities may easily act under false identities and then become extinctafter the transaction. Also, dispute resolution over the Internet can be fairly difficult or even impossible at some points;especially inthese countrieswhere they do not have enough legal e-commerce regulations.

This has resulted in the threat of e-crime becoming even bigger than from traditional robberies. Securing e-commerce should therefore facilitate the reliable execution of business transactions over unreliablecommunications, where transactions may be revealed by external or internal attacks. Generally, an e-commerce means an exchange of items. For example, software, music, films, video games, utility bills, electronic newspapers, magazines and journals, etc.E-purchase represents physical or electronic exchange; paying a utility bill electronically is an exchange of an e-payment for a receipt acknowledging the payment. It is very important to ensure that such exchanges are fair. Fair exchange is a security service that assures that, at the end of an exchange process, either all entities receive the items they expect, or none of them receives anything. In order to address these issues and to promote fair exchange of trade through the Internet, there is a real need for e-commerce protocols [4].

2. FAIRNESS IN ELECTRONIC COMMERCE

According to Asokan [5], a fair system refers to a system "that does not discriminate against a correctly behaving player. As long as a player behaves correctly, a fair system must ensure that other players will not gain any advantage over the correctly behaving players." In a fair exchange scenario, the transacting parties, for example X and Y, follow a fair exchange process. This process must not allow a situation where X can obtain Y's items while Y cannot obtain X's items. A process that involves a fair exchange protocol between X and Y must fulfil three conditions:

1. **Effectiveness:** If the protocol is executed correctly and the parties X and Y honourtheir commitment, then both parties will have each other's items.
2. **Timeliness:** The protocol will be finally executed within an acceptable timeframe.

3. **Fairness:** There are two types of fairness:

    - *Strong fairness*: This means that at the end of the protocol, either eachparty obtains the expected item from the other, or no party obtains the expected item. This means that a party who behaves correctly does not suffer any disadvantage. For example, both parties shouldreceive the expected items, or none do so.

    - *Weak fairness*: This means that at the end of the exchange, either strongfairness is achieved, or the correctly behaving party thatdoesnot receive the expected item can prove to a third partthat Y has received (or stillcanreceive) X's item, without anymore involvement from X (regardless of whether Y behaves correctly or not), and vice versa. Although strong fairness isdesirable, sometimes it is very expensive or impossible to guarantee, that is why the two forms of fairness exist[23].

Weak fairness is important because it provides a platform for dispute resolution. The disadvantaged party can seek a dispute resolution outside the system. The party that suffered a disadvantage can achieve strong fairness by using an external dispute resolution system, such as a court of law, provided it can prove that it was treated unfairly. There are a number of fair exchange protocols that can ensure strong fairness by using a trusted third party. Most of these protocols, apart from Burk and Pfitzmann [6], refer to the fairness definition of Asokan [5].

Other protocols (such as those of Jakobsson, Pagnia and Jansen [7] and Sandholmand Lesser [8]) are difficult to juxtapose, as they do not precisely define the kind of fairness that has been attained. The Asokanas [9] definition of fairness will be used as a foundation for the formalization in the sections below, as other explanations of fairness (such as the notions of money atomicity and goods atomicity of Tygar [2]), have not been exactly defined.

3. A TRUSTED THIRD PARTY (TTP)

Any nonpartisan party or impartial intermediary used in fair exchange protocols is the entity whose role is to ensure that each party receives the item it expects, or that none do. It is assumed that the TTP is neutral, available and trusted by all groups. Sometimes, more than one TTP might be involved in a transaction. Hence, the TTP carries out all or some of the roles shown below [4]:

- Ensures fair exchange of items.
- Acts as an agent of delivery,for example, gives items to the concerned parties.
- Acts as a reliable and trusted agent for the transacting parties.
- Solves problems between the parties in case of disputes.
- Validates items and gives certificates.

The role of fair exchange protocols is to ensure that both parties involved in the transaction are exchanging the items fairly. Often, transactions occur between parties who are not familiar with one another and (or) may not trust one another. Thus, to facilitate fair exchange and to protect both parties, fair exchange protocols have been designed. The objective of the protocols is to ensure (at the end of the exchange) that both parties receive each other's items, or that none do.

4. CLASSIFICATION OF FAIR EXCHANGE PROTOCOLS

There are many different contexts where the importance of fair exchange protocols is apparent. These contexts may include certified e-mail, contract signing, certified delivery and fair purchase. All parties aim to exchange the items fairly without any party suffering from the dishonest behaviour of the other. These contexts mainly depend on the items that the two parties will exchange and can be summarized as follows [10].

1. **Certified email:** In certified email fair exchange protocols, the parties involved in the transaction exchange the receipt and the email. In other words, when the sender transmits an email there should be a receipt from the recipient of the message to prevent any claim that an email was not delivered to the recipient's mail box.
2. **Certified delivery:** Certified delivery fair exchange protocols and certified email fair exchange protocols are almost the same. The distinction between the two is that the item received (and to be certified) is any digital product or payment, but not an email.
3. **Contract signing:** In contract signing fair exchange protocols, the signatures of the transacting parties to a contract are the commodities to be traded between the parties during the transaction. If there is a contract to be signed by the two parties, each party will receive a contract signed by the other party.
4. **Fair purchase:** Fair purchase exchange protocols deal with the trading of payments and digital products. In other words, one party (such as the customer) has the payment while the other party (such as the merchant) has the digital product. The role of the fair purchase exchange protocol is to guarantee that both parties exchange the payment and the digital product fairly.

5. TYPES OF FAIR EXCHANGE PROTOCOLS

Fair exchange protocols (whether they are for certified email, certified delivery, contract signing or fair purchase) may be classified into two main types, depending on the use of the TTP. Those protocols that do not involve the use of a TTP are the first type, while those protocols that involve the use of a TTP form the second type [4, 7, 10].

5.1 Protocols that involve a TTP

The protocols that involve the use of a TTP can be divided into three types, which are as follows [11]:

5.1.1 Protocols that are based on inline TTP.

Inline TTP-based protocols use the TTP for sending the traded commodities to the respective parties. This means that the TTP receives the items from each party, authenticates them and delivers them to the respective parties. For example, if there is a customer and a merchant in a transaction, then the two parties will exchange items such as a digital product (held by the merchant) and a payment (held by the customer). The protocol is then carried out in the following way. Both the customer and the merchant send their items to the TTP. The customer sends the payment while the merchant delivers the digital product. Then, the TTP authenticates the received items and after approving them, it delivers the payment to the merchant and the

digital product to the customer. Figure 1 illustrates a model of a fair exchange protocol that involvesan inline TTP.

We realize in this protocol that the TTP is involved actively in the exchange of items between the transacting parties. Involving the TTP in this type of protocol guarantees that the parties involved in the transaction exchange their items fairly. Direct contact between the transacting parties is not normally necessary in inline TTP-based protocols.

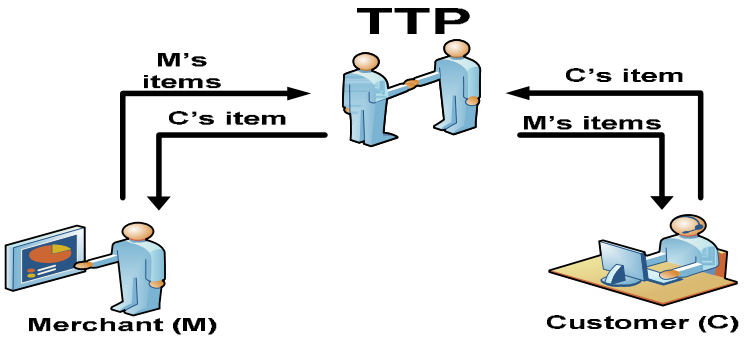

Figure 1: Inline TTP-based fair exchange model

The protocols that use an inline TTP guarantee fairness for all parties involved in the transaction because the TTP will deliver the respective items to the parties;however, they have some drawbacks. Firstly, it is expensive to run inline TTP protocols, asthey require the availability of the TTP during the execution of the protocol, which will lead to extra costs [12]. Secondly, in this type of protocol, the TTP may become the source of a communication bottleneck, hence leading to performance problems [5, 7, 13, 14] and[5, 5]. This is because the items to be exchanged must pass through the TTP. Thirdly, in the case of a crash at the TTP, the protocol will not be carried out and the parties will not be able to receive the items that they expect. Lastly, in the case of an attack, the TTP will be the main target [13].

Burk and Pfitzmann [6] suggestedan inline TTP-based fair exchange protocol that allows the transacting parties (where the parties are the customer and the merchant, and the items are the payment and the digital product) to reach an agreement on the items to be exchanged. Both parties then communicate with the TTP to confirm the contract that they have agreed upon. The payment is then sent to the TTP by the customer.

Upon receiving the payment, the TTP then confirms and verifies whether or not the payment is according to the agreement between the parties. After verifying that the payment is according to the agreement, the TTP sends a message to the merchant confirming that the correct payment from the customer has been received. After that, the digital product is sent to the TTP by the merchant. When the digital product is received by the TTP from the merchant, the TTP confirms and verifies whether or not the product certifies the agreement made by the two parties. If the digital product is in line with the description of the customer and fulfils the agreement between the two parties, the TTP then delivers the digital product and the payment to both the customer and the merchant, respectively.

5.1.2 Protocols that are based on online TTP

Protocols that make use of an online TTP involve less participation on the part of the TTP. In such a protocol, the TTP will not be used during the protocol run for delivering the parties' items but rather, verifying the items, and generating and/or storing proof of exchange of the items [4]. The figure below illustrates the use of online TTP in fair exchange protocols. If the commodities to be traded between the transacting parties are a digital product and a payment, the customer starts the exchange, and when the payment is received by the merchant from the customer, then the merchant verifies it with the TTP (a bank for example) before sending the digital product to the customer.

The TTP must therefore be online for the exchange process to be completed and should be contacted in case there is any dispute. Figure 2 illustrates a model of a fair exchange protocol that is based on an online TTP. There is minimal involvement on the part of the TTPin this type of protocol, but the TTP must be available during the exchange process. This can be viewed as a drawback because the TTP may become the source of a communication bottleneck. In addition, the TTP might be targeted by dishonest users.

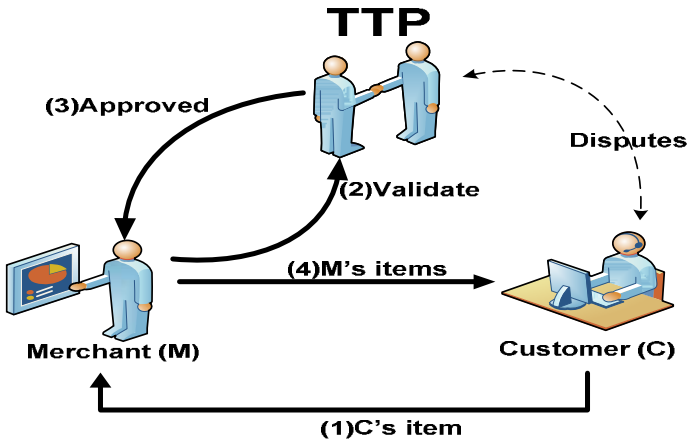

Figure 2: Online TTP-based fair exchange model

Zhang *et al*.[15, 16] suggested a fair exchange protocol that uses an online TTP. This protocol is for the exchange of an item, such as a physical product, and a payment. The customer makes an online payment (i.e. via the protocol messages) to the merchant, where a delivery agent is used to deliver the product to the customer, which means that the product is not transmitted electronically. The protocol is based on the theory of cross validation [17]. In this protocol, the customer first begins the process by ordering a product from the merchant. The merchant then sends the invoice to the customer. Once the customer is happy with the invoice, then they first send a coded payment to the merchant and secondly to the TTP (the bank). It is taken for granted that the merchant can download the coded payment (that was sent by the customer to the TTP) from the TTP (the bank). The merchant then makes a comparison of the two encrypted payments (i.e. the one received from the customer and the one downloaded from the TTP). If the merchant is satisfied that the encrypted messages compare, it means that the payment is valid. The merchant then delivers the product to the delivery agent after confirming the coded payment. The customer then takes the product from the delivery agent and after

confirming that the right product has been sent, they send the decryption key to the merchant, who will then decode the coded payment.

5.1.3 Protocols that are based on offline TTP

In offline TTP protocols, the transacting parties exchange their commodities directly without the use of the TTP unless a problem occurs. Such type of protocols is also known in the literature as "Optimistic fair exchange protocols". These protocols will thus be called optimistic fair exchange protocols. The example below illustrates how optimistic fair exchange protocols work if the commodities to be traded between the transacting parties are a payment and a digital product. The two parties directly trade their items, and in case of any problem, the TTP will be involved to mediate between the parties. Figure 3 illustrates a model of a fair exchange protocol that uses an offline TTP (optimistic fair exchange protocol).

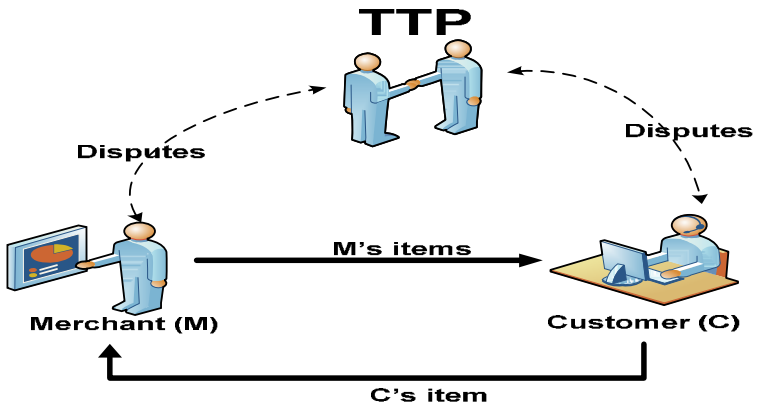

Figure 3: Offline TTP-based fair exchange model

In the optimistic fair exchange protocol, the role of the offline TTP is greatly reduced because the TTP is not involved in every exchange. As a result, the issue of the TTP being the source of a communication bottleneck, which is found in protocols that involve inline and online TTPs, is greatly reduced, as the parties exchange their items directly and rarely use the TTP.

The other advantage of these protocols is that the issue of having the TTP as the only source of failure is decreased, as the TTP will not be involved in the transaction unless there is a dispute. In addition to the above advantages, it will be less costly to run the TTP, as it will not be actively involved in the exchange process.

Zhang *et al.*[15] suggested an optimistic fair exchange protocol for trading two valuable documents (the two documents can be a payment and a digital product) between two parties; Party A and Party B (the two parties can be a customer and a merchant).The process of exchanging the items in Zhang's protocol consists of four messages to be exchanged between Party A and Party B. Party A begins the exchange process by transmitting the first message to Party B with the coded document of Party A together with the coded key that decodes the decrypted document. After receiving the first message, Party B verifies its authenticity and, if

satisfied, then transmits the second message to Party A together with the coded document of Party B and the encrypted key that decodes it.

Upon receiving the second message, Party A verifies its validity and, if approved, then transmits to Party B the third message with the decoding key. After receiving the decoding key, Party B then uses it to decode the decrypted document that was obtained in the first message. After that, Party B transmits the fourth message with the decoding key to Party A. After receiving the decoding key, Party A then uses it to decode the coded document that was obtained in the second message. In case of any problem, the TTP will be involved.

5.2 Protocols that do not involve a TTP

In this type of protocol, the two parties involved in the transaction exchange their items without the involvement of a TTP.

5.2.1 Gradual Exchange Protocols

Gradual exchange protocols [18, 19] can be used when the commodities to be exchanged can be partitioned into a number of parts. The gradual exchange protocol is based on the principle of having several rounds to complete the process of exchanging items between the transacting parties. The parties exchange some items in every round and it is ensured that the number of rounds is equivalent to the number of parts into which the commodities are divided. The process of exchanging commodities continues until the transaction is completed and every party receives what it expects. In each round, both the customer and the merchant send part of their commodity and also receive part of the other party's commodity (see Figure 4). The number of parts delivered to each party is almost the same at any given time [14].

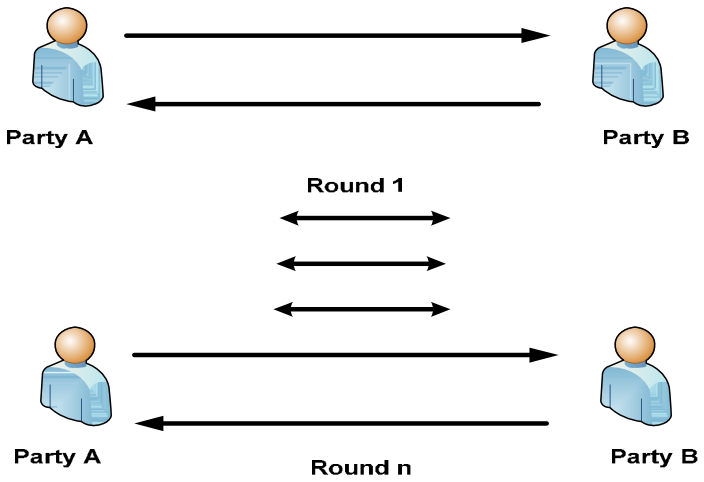

Figure 4: Gradual exchange protocols.

The major drawback of the gradual exchange protocol is that several rounds are needed to complete the exchange process. If there are many rounds to be made, a number of

communication steps are required, which can heavily load the communication channel to be used between the two parties. It is actually taken for granted that the items to be traded between the transacting parties have the same size [11]. As a result, this type of protocol does not support items of different sizes. Gradual exchange protocol lacks the involvement of a TTP, which makes it problematic,as it is impossible to guarantee fairness for both parties without a TTP who can mediate and solve problems.

Jakobsson [20] suggested a new way of fair exchange for a digital product and a payment without the use of a TTP. The protocol is based on the principle of dividing the payment into two parts. The two parts are then combined before the full payment can be realized, i.e. the first part of the payment cannot be used without the second part, and vice versa.

In the Jakobsson protocol [20], the first part of the payment is sent to the merchant by the customer. The merchant then submits the digital product to the customer after receiving the first initial payment. The customer then submits the second part of the payment to the merchant upon receiving the digital product. The merchant then combines the first and the second parts of the payment to construct the total payment. This protocol does not necessarily provide fairness for the two parties because the customer can vanish after receiving the digital product without sending the payment of the second part. Fairness is not guaranteed in this transaction, as the customer received the digital product while the merchant did not receive the second part of the payment,i.e. the total payment could not be constructed.

6. ANALYSIS OF PROTOCOLS

An important requirement in e-commerce protocols is fairness, as defined in Section 1. The objective of fairness is to ensure that, during the exchanges, all the parties receive their expected items, or none do. Here, we describe the four fair exchange protocols from different areas of applicability.

Zhou and Gollmann proposed a non-repudiation protocol that uses an online TTP [21]. The objective of this protocol is to minimize the role of the TTP, to provide the originator and the intended recipient with evidence after an execution of the protocol (without any party having an unfair advantage), and during the execution to divide the message M into two parts: a commitment C and a key K. The commitment is transmitted from the originator A to the recipient B, and then the key is lodged with the trusted third party TTP. Both parties must acquire the confirmed key from the TTP, as part of the non-repudiation proof needed in resolving a dispute.

During the protocol, if an invalid message is received or if an awaited message does not arrive, the prospective recipient terminates the protocol. In such a case, the following proofs are revealed: proof of origin, evidence of delivery, evidence of submission, and evidence of confirmation. The protocol is outlined as follows: the message to be sent consists of two parts,where one is the encrypted text C and the other is a key K. The sender A sends his digital signature and the encrypted text C to the intended recipient B. A begins the protocol by transmitting the cipher, using a session key k, of the message he needs to transmit to B, a tag that marks the protocol session, a time-out value before which the session key should be sent to the TTP and after which it can be consulted, as well as the signed non-repudiation of origin evidence for the ciphered message.

A suggests a consultation time-out and if B agrees, he transmits his signed non-repudiation of receipt evidence for the ciphered message. After receiving it, A then transmits to the TTP a signed copy of the session key. The TTP only receives one submission from a party in the course of a protocol session. The TTP then confirms the validity of A's signature and whether the time-out is exceeded or not. After the time-out, B may obtain the session key and the non-repudiation of origin evidence for this session key issued by the TTP. This evidence is required when making a full non-repudiation of origin evidence for the message that A submits to him. Similarly, A completes the non-repudiation of receipt evidence for the message by consulting with the TTP. The two parties, A and B, will then request the session key and the related evidence for this key from the TTP.

For Party B, the proof or evidence is an indication of origin, and for party A, the evidence proves that B can access the key. Both parties can access, at the right time, a read-only public directory controlled by the TTP. If the gathered evidence cannot be obtained by one party, that party will lose any potential dispute on the issue. In this case, the role of the TTP is minimized by obviating the obligation to acquire the data (controlled by the TTP) on the parties. A resilient communication channel between the TTP and the parties is necessary for the proper functioning of the protocol. If the channels of communication between the TTP and respectively A and B are resilient, the protocol is fairly strong and upholds the timeliness feature.

In a fair non-repudiation protocol, the execution of the protocol should make sure that the Non-Repudiation of Delivery Token and the Non-Repudiation of Origin Token are accessible to both the originator and the intended recipient, respectively. In addition, the protocol should be fail-safe. In other words, an incomplete execution of the protocol will not lead to a scenario where the NRDT is accessible to the originator but the NROT is not accessible to the intended recipient, or vice versa.

According to the definition of fairness, the protocol is not fair. This is because if B gives up after B finishes the first step, B does not know the subject matter of the message, but he receives the Non- Repudiation of Delivery Token. Besides, the protocol is designed to transport more messages when running and it includes C in the evidence, which increases the amount of data transport. The correctness of the product property is not considered in this protocol. Also, the protocol does not ensure the customer's anonymity, as it starts with a message sent by A, which discloses the customer's true identity. A secured channel is proposed to ensure confidentiality; also, timeliness is a strong property in this protocol.

Devane *et al*.[8] suggested a fair exchange protocol that can be used for buying items online. This protocol enforces the fair exchange of a payment from a customer and a digital product from a merchant. However, in this protocol, a bank acts as an online TTP, in which both the customer and the merchant have accounts. In Devane's protocol, there are seven messages that are exchanged by the transacting parties and the TTP (which is the bank during the exchange phase).

The protocol begins by the customer sending the first message with a signed purchase order. Upon receiving the first message, the merchant authenticates it and after approval, submits the second message with a signed invoice together with the coded digital commodity to the customer. After receiving the second message, the customer confirms and authenticates the

signed invoice and, if contented, sends the third message to the merchant, which contains a signed payment. After receiving the third message, the merchant confirms and authenticates it and, if contented, sends the fourth message to the bank with the decoding key for the digital commodity together with the third message that was sent by the customer and signed by the merchant (i.e. the merchant signs the signed payment by the customer and sends it to the bank).

Upon receiving the fourth message, the bank authenticates it and, if it is approved, then the bank submits the fifth message to the merchant with the bank's signature on the signed payment and the decoding key. After receiving the fifth message, the merchant then forwards it to the customer.

After receiving the sixth message, the customer receives the decoding key and decrypts the encrypted digital product that was delivered in the second message. The customer submits the seventh message to the bank after approving that the decrypted digital product is the one that was described in the first message. The seventh message contains the customer's approval of the digital product. Upon receiving the seventh message, the bank then finalizes the transaction by deducting the payment from the customer's account and transferring it to the merchant's account.

We observe a limitation in the fairness of the protocol; the merchant will receive the payment only after the customer has confirmed the items but there is no guarantee that the customer will make the payment after acquiring the items. The customer is certainly in an advantaged position. A secured channel is proposed to ensure confidentiality. Also, timeliness is a strong property in this protocol. The protocol takes into account the accuracy of the commodity property. The protocol does not ensure the customer's anonymity.

In Zhang *et al*.[16], we observe a limitation in the fairness of the protocol. If the merchant claims that he received an incorrect decryption key for the payment token or did not receive one at all, the third party (bank) will provide the K1-1 after asking the customer if he is satisfied. The third party (bank) will also provide the K1-1 if the customer is not traceable. However, if the customer is not intentionally untraceable and also does not have the required product, then by having the K1-1 from the third party, the merchant is certainly in an advantage. The fairness of the protocol is based on the theory of cross-validation, which proceeds via a number of process steps that take into account the accuracy of the commodity property. According to this protocol, the product information is not revealed to both the third party and the merchant in order to safeguard the customer’s anonymity. A secured channel is proposed in this protocol to ensure confidentiality. Also, timeliness is a strong property in this protocol.

7. CONCLUSION

In this paper, fair exchange protocols have been reviewed. These protocols are intended to ensure fairness for both parties involved in a transaction. Fairness in the context of the fair exchange protocols between the merchant and the customer is achieved in the transaction if, at the end of the protocol execution, each party involved in the exchange receives the item of the other party, or none do.

A number of different fair exchange protocols have been reviewed in this paper, which can be categorized into two types; the ones that do not involve the use of a TTP, and the ones that involve the use of a TTP. The former allows the parties to exchange their items gradually, bit by bit, until the whole item is exchanged fairly. The latter is divided into three types. The first type involves the use of the TTP for delivering the items to the parties involved in the exchange, for example, inline TTP-based fair exchange protocols. The second type uses an online TTP, where there is minimum involvement on the part of the TTP. The third type uses an offline TTP (optimistic fair exchange protocols). In the optimistic fair exchange protocols, the involvement of the TTP is only initiated if there is a problem during the protocol execution. We then described three published fair exchange protocols and discussed their properties, and individually analysed these fair exchange protocols, assessing their strengths and weaknesses.

References

[1] M. Alshehri, H. Aldabbas, J. Sawle and M. A. Baqar. "Adopting E-commerce to user's needs". *International Journal of Computer Science & Engineering Survey (IJCSES), vol 3, no.1,* February 2012.

[2] A. Alaraj and M. Munro, "An efficient e-commerce fair exchange protocol that encourages customer and merchant to be honest," *Computer Safety, Reliability, and Security,* pp. 193-206, 2008.

[3] H. Aldabbas, T. Alwada'n, H. Janicke and A. Al-Bayatti, "Data Confidentiality in Mobile Ad hoc Networks", *International Journal of Wireless & Mobile Networks (IJWMN),* vol. 4, no. 1, February 2012.

[4] A. Nenadic, *A Security Solution for Fair Exchange and Non-Repudiation in e-Commerce,* 2005.

[5] N. Asokan, M. Schunter and M. Waidner, "Optimistic protocols for fair exchange," in *Proceedings of the 4th ACM Conference on Computer and Communications Security,* pp. 7-17, 1997.

[6] H. Bürk and A. Pfitzmann, "Value exchange systems enabling security and unobservability," *Comput. Secur.,* vol. 9, pp. 715-721, 1990.

[7] I. Ray, I. Ray and N. Natarajan, "An anonymous and failure resilient fair-exchange e-commerce protocol," *Decis. Support Syst.,* vol. 39, pp. 267-292, 2005.

[8] S. Devane, M. Chatterjee and D. Phatak, "Secure E-commerce protocol for purchase of e-goods-using smart card," in *Information Assurance and Security, 2007. IAS 2007. Third International Symposium on,* pp. 9-14, 2007.

[9] G. Ateniese, B. de Medeiros and M. T. Goodrich, "TRICERT: A distributed certified e-mail scheme," in *ISOC 2001 Network and Distributed System Security Symposium (NDSS'01),* 2001.

[10] M.Schunter :*Optimistic fair exchange*. PhD Thesis, University of Saarland, Germany, 2000.

[11] S. Kremer, O. Markowitch and J. Zhou, "An intensive survey of fair non-repudiation protocols," *Comput. Commun.,* vol. 25, pp. 1606-1621, 2002.

[12] S. Micali, "Simple and fast optimistic protocols for fair electronic exchange," in *Proceedings of the Twenty-Second Annual Symposium on Principles of Distributed Computing,* pp. 12-19, 2003.

[13] P. Liu, P. Ning and S. Jajodia, "Avoiding loss of fairness owing to process crashes in fair data exchange protocols," in *Dependable Systems and Networks, 2000. DSN 2000. Proceedings International Conference,* pp. 631-640, 2000.

[14] V. Shmatikov and J. C. Mitchell, "Analysis of a fair exchange protocol," in *Proceedings of the Seventh Annual Symposium on Network and Distributed System Security (NDSS 2000),* 2000.

[15] N. Zhang, Q. Shi, M. Merabti and R. Askwith, "Practical and efficient fair document exchange over networks," *Journal of Network and Computer Applications,* vol. 29, pp. 46-61, 2006.

[16] Q. Zhang, K. Markantonakis and K. Mayes, "A practical fair-exchange e-payment protocol for anonymous purchase and physical delivery," in *Computer Systems and Applications. IEEE International Conference*, pp. 851-858, 2006.

[17] I. Ray and H. Zhang, "Experiences in developing a fair-exchange e-commerce protocol using common off-the-shelf components," *Electronic Commerce Research and Applications,* vol. 7, pp. 247-259, 2008.

[18] M. Blum, "How to exchange (secret) keys," *ACM Transactions on Computer Systems (TOCS),* vol. 1, pp. 175-193, 1983.

[19] S. Even, O. Goldreich and A. Lempel, "A randomized protocol for signing contracts," *Commun ACM,* vol. 28, pp. 637-647, 1985.

[20] M. Jakobsson, "Ripping coins for a fair exchange," in *Advances in Cryptology—EUROCRYPT'95,* pp. 220-230, 1995.

[21] J. Zhou and D. Gollman, "A fair non-repudiation protocol," in *Security and Privacy, 1996. Proceedings, 1996 IEEE Symposium*, pp. 55-61, 1996.

[22] A. Alaraj,*Enforcing Honesty in E Commerce Fair Exchange Protocols*. PhD Thesis, University of Durham, UK, 2008.

[23] F. Gartner, H. Pagnia ,H. Vogt," Approaching a Formal Definition of Fairness in Electronic Commerce "Proceedings of the 18th IEEE Symposium on Reliable Distributed Systems . USA,1999.