A STUDY OF MULTI-PARTY ELECTRONIC CONTRACT SIGNING PROTOCOL

Fu-Yao Yang, Department of Marketing Distribution Management, Chien Hsin University of Science and Technology, Taoyuan City, Taiwan, ROC, 886-3-4581196#5521, vipent@uch.edu.tw
Cheng-Yuan Ku, Department of Information Management and Finance, National Chiao Tung University, Hsin-Chu City, Taiwan, ROC, 886-3-5712121#57413, cooper.c.y.ku@gmail.com
Yung-Ting Chuang, Department of Information Management, National Chung Cheng University, Chia-Yi County, Taiwan, ROC, 886-5-2720411#24621, ytchuang@mis.ccu.edu.tw
David C. Yen, Department of Management, Marketing and Information Systems, SUNY at Oneonta, Oneonta, NY 13820, USA, 607-436-3660, David.Yen@oneonta.edu

ABSTRACT

As technology advances, many everyday activities can be implemented on the Internet nowadays. Within a variety of online transactions, electronic contract signing has become the increasingly important one. This paper would like to discuss the related issues regarding the signing interaction. In fact, to exchange digital signatures online and avoid mutual arguments, the operating mechanism shall ensure the fairness, security and timeliness for all of the participants. Therefore, we introduce the two-party protocol first, and then discuss the multi-party protocol. After the detailed review, a draft of cyclic multi-party protocol is proposed. In order to validate the effectiveness of this protocol, its fairness, security and timeliness have been investigated. However, we believe it may be further improved, so the refining work is still on the go.

Keywords: multi-party contract signing protocol, fair exchange, trusted third party (TTP)

INTRODUCTION

Many everyday activities, such as conferencing, business transactions, contracts signing and so on, which require face to face contact previously can be done through the Internet now due to the powerful networking platform. Online applications certainly offer lots of convenience, but also relatively cause many problems. If these problems, for example fairness and security, are not solved, they may discourage people from adopting this new technology.

The traditional contract was signed face to face. Nowadays, increasing many contracts need to be electronically signed on the web due to the consideration of cost and time. Theoretically, if both parties are honest, signing a contract is a thoroughly easy job. However, in real world, there are always some dishonest people, so we can't design a protocol without deliberating the malicious behavior. In general, all these efforts are invested to achieve the expectation of fairness, timeliness and prevention of abuse. Fairness means that if someone signs the contract, then it is guaranteed he/she can also get signed document from the other party. It is because one malicious user may refuse to sign after receiving the signed contracts and this situation causes damage to the other. In the meantime it is very difficult to implement the synchronous transmission of signed document on the Internet to achieve fairness. Therefore, the trusted third party (TTP) is proposed to handle this problem. However, the intervention from TTP may affect the efficiency of the contract signing very much, so TTP should get involved only when a dispute happens.

Because the transactions conducted on the Internet could be delayed by a variety of uncertain factors, some scholars have proposed the necessity of timeliness. If any entity waits for signature from the other more than a specified time, the protocol should be terminated. Timeliness can avoid a party from getting into the endless wait. Very similar to fairness, some researchers have put forward the concept of prevention of abuse. It emphasizes that the result of contract signing protocol cannot be controlled by either party. A protocol may guarantee fairness but cannot prevent the abuse. In this case, one entity can intentionally dominate the success or failure of signing procedure. Therefore, designing a secure contract signing protocol to achieve fairness, timeliness and prevention of abuse is the major objective of this research.

Research on electronic contract agreement involving two parties has been comprehensively studied. Many useful results are published. However only some multi-party electronic contract signing procedures (e.g., mesh, star, ring topologies etc.) have ever been presented and discussed. We believe that it is still possible to raise the efficiency of multi-party protocol. In this paper, a cyclic structure of signing protocol for multiuser is proposed to achieve this purpose. To the best of our knowledge, the cyclic concept has not yet been suggested by other researchers. In the end some preliminary theoretical analyses demonstrate that this efficient signing protocol is secure from a variety of perspectives.

LITERATURE REVIEW

The most important issue regarding the electronic contract signing is how both entities can fairly exchange mutual signatures. The first fair exchange protocol was developed from synchronous secret exchange and the gradual release of secret [7]. However, nobody can guarantee the honesty of two participants, so the introduction of a TTP becomes really necessary. Based on the degree of involvement, TTP could be categorized as the following three types: inline TTP, online TTP and offline TTP.

Coffey-Saidha protocol is the representative one for inline TTP protocols [4]. As for online TTP protocol, Zhou and Gollmann proposed ZG-1996 [14] and then Kim et al. [8] further modified it as Kim protocol. Moreover, ASW [3], GJM [6], and Wang [12] are also some of the important offline TTP protocols. Most researches assume that TTP is honest and fair. Once TTP abuses the transaction or misuses the information, it may cause substantial damage to the involving entities. Therefore Franklin and Reiter [5] proposed the online semi-trusted third party (Online STTP) technology in order to avoid the above-mentioned problem.

In addition to studies regarding two parties, a few researchers also worked on multi-party contract signing. Asokan et al. [2] provided the earlier multiparty-related discussion for electronic contract signing, and they considered a mesh topology. Later on, in another paper, Asokan et al. suggested the star topology and ring topology [1]. Mukhamedov and Ryan proposed MR protocol in 2008 [11]. Recently many scholars used game theory to analyze problem of this type mainly because they would like to tradeoff the efficiency and fairness. The literature in this area is still growing quickly [9-10, 13].

PROPOSED PROTOCOL

In the past, multi-party agreements were suggested to adopt star (1-N) or ring topologies by some scholars. However, we think another new structure - cyclic structure is able to further improve the operation of electronic contract signing. In order to demonstrate the proposed protocol, we first introduce the necessary notations as follows. A: Alice, B: Bob, C: Carol, U: the set of all participants, TTP: trusted third party, P_X: X's intention to sign, S_X: signature of X, RA_X: request of abortion from X, and RR_X: request of recovery from X.

[Main]

(M1) $A \rightarrow B : P_A$ A aborts if times out

(M2) $B \rightarrow C : P_A, P_B$ B aborts if times out

(M3) $C \rightarrow A : P_B, S_C$ C recovers if times out

(M4) $A \rightarrow B : S_A, S_C$ A recovers if times out

(M5) $B \rightarrow C : S_A, S_B$

(M6) $C \rightarrow A : S_B$

[Abortion][A]

(Abortion-A1) $A \rightarrow TTP : RA_A$,
if $Proof = Recovery \vee Abortion$, then
TTP ignores,
else

(Abortion-A2) $TTP \rightarrow U : Abort$, $Proof = Abortion$

[Abortion][B]

(Abortion-B1) $B \rightarrow TTP : RA_B$,
if $Proof = Recovery \vee Abortion$, then
TTP ignores,
else

(Abortion-B2) $TTP \rightarrow U : Abort$, $Proof = Abortion$

[Recovery][C]

(Recovery-C1) $C \rightarrow TTP : RR_C = P_A \| P_B \| S_C$,
if $Proof = Recovery \vee Abortion$, then
TTP ignores,
else

(Recovery-C2) $TTP \rightarrow U : Recovery = S_A \| S_B \| S_C$, $Proof = Recovery$

[Recovery][A]

(Recovery-A1) $A \rightarrow TTP : RR_A = P_B \| S_A \| S_C$,
if $Proof = Recovery \vee Abortion$, then
TTP ignores,
else

(Recovery-A2) $TTP \rightarrow U : Recovery = S_A \| S_B \| S_C$, $Proof = Recovery$

FUTURE WORKS

To verify the security of the proposed protocol, we have already preliminarily examined a variety of possible attacks, including external attacks, insider attacks, internal and external collusion attack, and so on through a series of analyses and evaluations. After having discussed the fairness, safety and timeliness, this mechanism seems to be secure with high probability. However we believe that further analyses are still necessary to complete the design of this multi-party electronic contract signing protocol.

Furthermore some other types of attacks should be thought of and many real-world intervention factors need to be considered in the near future. For example, if the message response time is longer than expected, there could be many possible reasons, such as (1) blocked channel; (2) external attacks; (3) the recipient hesitation or (4) the recipient would like to take advantage of the others. Therefore, a much better construction of the multi-party contract signing protocol is achievable after more of the above-mentioned causes are taken into considerations. Moreover, we also think that our protocol could be extended to *n* entities from three without any problems.

ACKNOWLEDGEMENT

This research is partially supported by MOST 103-2410-H-009-053-MY3 and MOST 104-2410-H-194-090-MY2 of Ministry of Science and Technology, Taiwan, R.O.C.

REFERENCES

[1] Asokan, N., Baum-Waidner, B., Schunter, M. and Waidner, M. (1998). *Optimistic synchronous multi-party contract signing*. Technical Report RZ 3089 (#93135), IBM Zurich Research Laboratory.

[2] Asokan, N., Schunter, M. and Waidner, M. (1996). *Optimistic protocols for multi-party fair exchange*. Technical Report RZ 2892, IBM Zurich Research Laboratory.

[3] Asokan, N., Shoup, V. and Waidner, M. (1998). *Asynchronous protocols for optimistic fair exchange*. Proceedings of the 1998 IEEE Symposium on Security and Privacy, Oakland, CA, USA.

[4] Coffey, T. and Saidha, P. (1996). *Non-repudiation with mandatory proof of receipt*. Computer Communication Review, 26(1), 6-17.

[5] Franklin, M. K. and Reiter, M. K. (1997). *Fair exchange with a semi-trusted third party*. Proceedings of the 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland.

[6] Garay, J. A., Jakobsson, M. and MacKenzie, P. (1999). *Abuse-free optimistic contract signing*. Crypto'99, Lecture Notes in Computer Science, 1666, 449-466.

[7] Goldreich, O. (1983). *A simple protocol for signing contracts*. In D. Chaum (Eds.), Advances in Cryptology: Proceedings of Crypto 83 (pp. 133-136). New York: Plenum Press.

[8] Kim, K., Park, S. and Baek, J. (1999). *Improving fairness and privacy of Zhou-Gollmann's fair non-repudiation Protocol*. Proceedings of 1999 International Workshops on Parallel Processing, Japan.

[9] Kordy, B. and Radomirovic, S. (2012). *Constructing Optimistic Multi-party Contract Signing Protocols*. IEEE 25th Computer Security Foundations Symposium, Cambridge MA, USA.

[10] Li, X. and Zheng, Q. (2010). *Two-round Multi-Party Contract Signing*. Third International Conference on Knowledge Discovery and Data Mining, Phuket, Thailand.

[11] Mukhamedov, A. and Ryan, M. D. (2008). *Fair multi-party contract signing using private contract signatures*. Information and Computation, 206(2-7), 272-290.

[12] Wang, C.-H. (2006). *How to protect exchanged secrets in the fair exchange protocol with off-line TTP*. Computers & Electrical Engineering, 32(5), 364-375.

[13] Zhang, Y., Zhang, C., Pang, J. and Mauw, S. (2010). *Game-based verification of multi-party contract signing protocols*. FAST'09, Lecture Notes in Computer Science, 5983, 186-200.

[14] Zhou, J. and Gollmann, D. (1996). *A fair non-repudiation protocol*. Proceedings of the 1996 IEEE Symposium on Security and Privacy, Oakland, USA.