Formal Analysis Of Multi-party Non-repudiation Protocols Without TTP

Xiaoqiong Wang
School of Information
Guizhou institute of Finance and Economics
Guiyang, China 550004
E-mail:125298835@qq.com

Xueming Wang
Computer Science and Information College
Guizhou University
Guiyang, China 550025
E-mail: xmwang1965@163.com

***Abstract*— Non-repudiation service is crucial to electronic commerce. Now multi-party non-repudiation is a new focus of research. This paper presents a multi-party non-repudiation protocol, based on a group encryption scheme. A multi-party non-repudiation problem is defined in this paper. This definition and the resulting protocol are more general than the other comparable work. At last, an example of fair multi-party non-repudiation protocol without a trusted third party (TTP) is given out, which uses formal method of SVO logic to analyze the protocol and prove its correctness.**

Keywords- non-repudiation;multi-party protocol;trusted third party; E-commerce; SVO Logic

I. INTRODUCTION

Non-repudiation service is crucial to electronic commerce. During the last years the impressive growth of the Internet and more generally of open networks has created several security related problems. The non-repudiation and the related fair exchange problem are two of them. Non-repudiation must ensure that no party involved in a protocol can deny having participated in a part or the whole of the protocol. Therefore a non-repudiation protocol has to generate non-repudiation of origin evidences intended to the recipient parties and non-repudiation of receipt evidences destined to the originating parties. In case of a dispute (e.g. an originator denying having sent a given message or a recipient denying having received it), an adjudicator can evaluate these evidences and take a decision in favor of one of the parties without any ambiguity. In fair exchange two parties want to exchange items and the protocol ensures that either both parties receive the desired item, or none of them receives valuable information[1,2].

First solutions to those problems involve a trusted third party (TTP) that acts as an intermediary between the participating entities. The major disadvantage of this approach is the communication bottleneck created at the TTP. Therefore more efficient solutions have been proposed. Two different approaches have been considered: one consists in designing protocols without a TTP, the other tries to minimize its involvement [3].

Most of these protocols have been designed as two-party protocols. In fair exchange first works have been done to generalize them to the case of n participants: Asokan et al., 1996; Asokan et al., 1998; Franklin and Tsudik, 1998; Bao et al., 1999. Considering non-repudiation no investigations towards a generalization have yet been undertaken. The only similar work in the world is the multi-party certified mail protocol proposed by Asokan et al. in Asokan et al., 1998.

Formal methods have been used in the field of security protocols [4] since 1980's. Recent approaches of using formal methods in the design of security protocols include finite-state model checking and belief logics [5]. Belief logics have played a crucial role in the development of protocol analysis as a research topic. BAN logic is simple and elegant and allows for very short abstract proofs. However, it does not allow analysis at the level of sophistication required by some analysts. Accordingly, various other related logics have been developed to fill some of the perceived gaps. Perhaps the most significant of subsequent logics is SVO which aims to efficiently unify previous logics (BAN, GNY, AT and VO). This paper will use SVO logic and its extended as the basis of protocol analysis.

At first, multi-party non-repudiation problem is defined. The requirements of a multi-party non-repudiation protocol shall be defined as well. Then SVO logic, a more sophisticated logic than BAN logic, is initiated to give greater confidence in the analysis of multi-party non-repudiation protocol. At last, an example of a fair multi-party non-repudiation group based on a double group encryption scheme is given out, which uses formal method of SVO logic to analyze the protocol and prove its correctness.

II. MULTI-PARTY NON-REPUDIATION

In literature, different kinds of multi-party fair exchange have been considered. In [6] a classification has been proposed. One can distinguish between single-unit and multi-unit exchanges. Moreover different topologies are possible: [6] and [7] concentrated on a ring topology. Each entity ei($0 \leqslant i \leqslant n-1$) desires an item (or a set of items) from entity ei_1 and offers an item (or a set of items) to entity ei_1, where _ and _ respectively denote addition and subtraction modulo n. Another topology is the more general matrix topology, where each entity may desire items from a set of entities and offer items to a set of entities. Such protocols have been proposed by Asokan et al.

A fundamental difference between non-repudiation and fair exchange protocols is the following. In a fair non-repudiation protocol, the originator sends some data with a

978-0-7695-4260-7/10 $26.00 © 2010 IEEE
DOI 10.1109/ICCIIS.2010.33

non-repudiation of origin evidence to a recipient, who has to respond with a non-repudiation of receipt evidence. The sent data is generally not known to the recipient a priori. In a fair exchange protocol each entity offers a priori known item and receives another item, also known as a priori. In a multi-party fair exchange protocol one can imagine sending an item to one entity and receiving an item from a different one. In non-repudiation it does not make sense that one entity receives some data and a distinct entity sends the corresponding receipt. Thus a ring topology is not sound. The most natural and here considered generalization seems to be a one-to-many protocol, where one entity sends a message to n−1 receiving entities who respond to the sender. Although other possibilities for generalization exist (many-to-one, many-to-many), they seem to be less natural.

The expectations we have towards multi-party non-repudiation protocols are rather similar to the properties required in two-party non-repudiation[9,10]. Particularly, we have to redefine fairness.

Definition 1 A multi-party non-repudiation protocol is said to be viable if, independently of the communication channels quality, there exists an execution of the protocol, where the exchange between all entities succeeds.

Definition 2 A multi-party non-repudiation protocol is said to be fair if at the end of the protocol the sender has got a complete non-repudiation of receipt evidence for a given recipient if and only if this recipient has got the message with a complete corresponding non-repudiation of origin evidence. [8]

Definition 3 A multi-party non-repudiation protocol provides timeliness if each participating entity always has the ability to reach, in a finite amount of time, a point in the protocol, where it can stop the protocol, while preserving fairness.

Definition 4 A multi-party non-repudiation protocol provides confidentiality of the message sent by Alice to a set of recipients, if an intruder, to obtain the message, has to directly receive it from Alice or any of the recipients or has to break the underlying cryptographic primitives used in the protocol.

III. SVO LOGIC

A. SVO Logic Notation

The language of SVO logic consists of the following expressions [11]:

- $P \mid\equiv X$ or P believes X
- $P \ni X$ or P has X
- $P \propto X$ or P received X
- $P \mid\sim X$ or P said X
- $P \mid\approx X$ or P says X
- $P \mid\Rightarrow X$ or P controls X
- $\#(X)$ or fresh(X)
- $P \lhd X$ or P sees X
- P $\xleftrightarrow{k}$ Q: k will never be discovered by any principal but P , Q, or a principal which is trusted by P or Q.

{X}k: This is the notation for encryption of X by key k. It is assumed that encrypted messages are uniquely readable and verifiable by holders of the right keys. Similarly, encrypted messages can only be created by a principal with the appropriate keys.

B. SVO Logic Axioms

When a principal receives a message, the logic provides twenty two axioms that indicate what new beliefs this principal may infer from the message contents. The axioms we need in this paper are as follows.

Belief Axiom

1) (P believes $\varphi \wedge$ P believes $(\varphi \Rightarrow \psi)) \supset$P believes ψ

Source Association Axiom

2) (P $\xleftrightarrow{k}$ *Q* $\wedge$ R received $\{X^Q\}_k$) $\supset$ (*Q said X* $\wedge$ *Q has k*).

Receiving Axioms

3) P received $(X_1,...,X_n) \supset P$ received X_i, for each i$\in${1,...,n}.

4) (P received $\{X\}_k \wedge P$ has *k*) $\supset$P received X.

Possession Axioms

5) P received X $\supset$P has X.

6) P has $(X_1,...,X_n) \supset$P has X_i, for each i$\in${1,...,n}.

Saying Axioms

7) P said $(X_1,...,X_n) \supset$ (P said $X_i \wedge$ P has X_i), for each i$\in${1,...,n}.

8) P says $(X_1,...,X_n) \supset$ (P said $(X_1,...,X_n) \wedge$ P says X_i), for each i$\in${1,...,n}.

See Axiom

9) P received X $\supset$ P sees X

10) P sees $(X_1,\ldots,Xn) \supset$P sees X_i

11) P sees $X_1 \wedge \ldots \wedge$P sees Xn$\supset$P sees $(F(X_1,\ldots,Xn))$

Freshness Axiom

12) fresh(X_i) $\supset$ fresh($X_1,...,X_n$), for any i$\in${1,...,n}.

Jurisdiction Axiom

13) (P controls $\varphi \wedge$ P says $\varphi) \supset \varphi$.

Nonce-Verification Axiom

14) (fresh(X) $\wedge$ P said X) $\supset$P says X.

Symmetric Goodness Axiom

15) P $\xleftrightarrow{k}$ Q $\equiv$ Q $\xleftrightarrow{k}$ P.

IV. FORMAL ANALYSIS OF A FAIR MULTI-PARTY NON-REPUDIATION PROTOCOL WITHOUT TTP

We give an example of fair multi-party non-repudiation protocol without a trusted third party (TTP), and use formal method of SVO logic to analyze the protocol and prove its correctness.

A. Protocol Description

The fair multi-party non-repudiation protocol without a trusted third party (TTP) [12] is description as follows:

(1) $A \Rightarrow B : f_{NRO}, B, S_A(f_{NRO}, B, t_A, E_B(C))$

(2) $B_i \rightarrow A : f_{NRR}, A, S_B(f_{NRR}, A, t_B, PEnc(C, PK_A))$

(3) $A \Rightarrow B' : f_{NRA}, B, S_A(f_{NRA}, B', t_{A_2}, E_{B'}(a))$

(4) $B_i' \rightarrow A : f_{NRF}, A, S_{B_i'}(f_{NRF}, A, PEnc(a, PK_A))$

(5) $A \Rightarrow B'' : f_{NRS}, B'', S_A(f_{NRS}, B'', E_{B''}(K))$

B. Protocol Assumptions

- P0: the execute environment of protocol is not safe
- P1: public-key of each principal which know to all
- P2: private-key of each principal which know itself

C. Goals Of The Protocol Analysis

For reach the fairness and evidence validity of non-repudiation protocol, the goals of the protocol is describe as follows:

GI: $B_i'' \mid\equiv (A \mid\sim M)$ G2: $A \mid\equiv (B_i'' \propto M)$

$B_i'' \in B'' \subseteq B' \subseteq B$

D. Protocol Formal Analysis with SVO logic

From message (1) and Receiving Axiom of SVO logic that:

Dl: $B_i \propto S_A(f_{NRO}, B, t_A, E_B(C))$ $B_i \in B$

From D1 and Source Association Axiom of SVO logic that:

D2: $B_i \mid\equiv A \mid\sim f_{NRO}, B, t_A, E_B(C)$

From D2 and Saying Axiom of SVO logic that:

D3: $B_i \mid\equiv A \mid\sim E_B(C)$

As a result of group encryption technology and $B_i \in B$ that:

D4: $B_i \mid\equiv A \mid\sim C$

From D4 and $B_i'' \in B'' \subseteq B$ that:

D5: $B_i'' \mid\equiv A \mid\sim C$

From message (3) and Receiving Axiom of SVO logic that:

D6: $B_i' \propto S_A(f_{NRA}, B', t_A, E_{B'}(a))$ $B_i' \in B' \subseteq B$

From D6 and Source Association Axiom of SVO logic that:

D7: $B_i' \mid\equiv A \mid\sim f_{NRA}, B', t_A, E_{B'}(a)$

From D7 and Saying Axiom of SVO logic that:

D8: $B_i' \mid\equiv A \mid\sim E_{B'}(a)$

As a result of group encryption technology and $B_i' \in B' \subseteq B$ that:

D9: $B_i' \mid\equiv A \mid\sim a$

From D9 and $B_i'' \in B'' \subseteq B$ that:

D10: $B_i'' \mid\equiv A \mid\sim a$

B_i'' believed A have send the ftp address a of key K.

From message (5) and Receiving Axiom of SVO logic that:

D11: $B_i'' \propto S_A(f_{NRS}, B'', t_A, E_{B''}(K))$ $B_i'' \in B'' \subseteq B' \subseteq B$

From D11 and Source Association Axiom of SVO logic that:

D12: $B_i'' \mid\equiv A \mid\sim f_{NRS}, B'', t_A, E_{B''}(K)$

From D12 and Saying Axiom of SVO logic that:

D13: $B_i'' \mid\equiv A \mid\sim E_{B''}(K)$

As a result of group encryption technology and $B_i'' \in B''$ that:

D14: $B_i'' \mid\equiv A \mid\sim K$

From D5, D14 and Extended Message Sending Axiom of SVO logic that:

D15: $B_i'' \mid\equiv A \mid\sim M$ $B_i'' \in B'' \subseteq B' \subseteq B$

Thus, B_i'' trust A must have received information M.

G1 proved out.

From message (2) and Receiving Axiom of SVO logic that:

D16: $A \propto S_{B_i}(f_{NRR}, A, t_B, PEnc(C, PK_A))$ $B_i \in B$

From D16 and Source Association Axiom of SVO logic that:

D17: $A \mid\equiv B_i \mid\sim f_{NRR}, A, t_B, PEnc(C, PK_A)$

From D17 and Saying Axiom of SVO logic that:

D18: $A \mid\equiv B_i \mid\sim PEnc(C, PK_A)$

From D18, P2 and Message Sending Axiom of SVO logic that:

D19: $A \mid\equiv B_i \mid\sim C$

From D19 and improved Possession Axiom of SVO logic that:

D20: $A \mid\equiv B_i \ni C$

From D20 and non-repudiation based extending axiom of SVO logical that:

D21: $A \mid\equiv B_i \propto C \quad B_i \in B$

From D21 and $B_i'' \in B'' \subseteq B$ that:

D22: $A \mid\equiv B_i'' \propto C \quad B_i'' \in B'' \subseteq B$

From message (4) and Receiving Axiom of SVO logic that:

D23: $A \propto S_{B_i'}(f_{NRR}, A, PEnc(a, PK_A)) \quad B_i' \in B' \subseteq B$

From D23 and Source Association Axiom of SVO logic that:

D24: $A \mid\equiv B_i' \sim f_{NRR}, A, Enc(a, PK_A)$

From D24 and Saying Axiom of SVO logic that:

D25: $A \mid\equiv B_i' \mid\sim PEnc(a, PK_A)$

From D25, P2 and Message Sending Axiom of SVO logic that:

D26: $A \mid\equiv B_i' \mid\sim a$

From D26 and improved Possession Axiom of SVO logic that:

D27: $A \mid\equiv B_i' \ni C$

From D27 and non-repudiation based extending axiom of SVO logical that:

D28: $A \mid\equiv B_i' \propto a \quad B_i' \in B' \subseteq B$

B_i' Received a ftp address a of key K.

From message (5) and D28, $E_{B''}(K)$ can be download from the A release directory:

$B_i' \downarrow E_{B''}(K)$

From the improved FTP access rules of SVO logic that:

D29: $B_i' \propto E_{B''}(K)$

As a result of group encryption technology and $B_i'' \in B''$ that:

D30: $A \mid\equiv B_i'' \ni K$

From D22, D30 and improve cipher text understanding rules of SVO logic:

D31: $A \mid\equiv B_i'' \propto M \quad (B_i'' \in B'' \subseteq B' \subseteq B)$

Thus, A trust B_i'' must have received information M.

G2 proved out.

V. CONCLUSIONS

A multi-party non-repudiation problem is defined in this paper. The requirement of a multi-party non-repudiation protocol has been defined as well. Then SVO logic, a more sophisticated logic than BAN logic, is initiated which is very useful in the formal analysis of multi-party non-repudiation protocol. At last, an example of fair multi-party non-repudiation protocol without a trusted third party (TTP) is given out, which use formal method of SVO logic to analyze the protocol and prove its correctness.

REFERENCES

[1] S. Kremer and O. Markowitch, "A multi-party non-repudiation protocol",Proc.15th International Conference on Information Security, IFIP World Computer Congress (SEC 2000), Aug. 2000, pp.271-280.

[2] S. Kremer and O. Markowitch, "Optimistic non-repudiable information exchange",In J. Biemond, editor, 21st Symp. on Information Theory in the Benelux,Wassenaar (NL), May.2000 pp.139-146.

[3] O. Markowitch and S. Kremer, "A multi-party optimistic non-repudiation protocol",Proc.The 3rd International Conference on Information Security and Cryptology (ICISC 2000), volume 2015 of Lecture Notes in Computer Science, pp 109-122, Seoul, Korea, 2000. Springer-Verlag.

[4] L. Buttyan, "Formal methods in the design of cryptographic protocols (state of the art) ",Technical Report SSC/1999/038, EPFL SSC (1999).

[5] P. Syverson and I. Cervesato, "The logic of authentication protocols", Lecture Notes in Computer Science 2171 (2001), pp. 63-136.

[6] M. Franklin and G. Tsudik, "Secure group barter: Multi-party fair exchange with semi-trusted neutral parties",Lecture Notes in Computer Science, 1465,1998.

[7] F. Bao, R. Deng, K. Q. Nguyen, and V. Vardharajan, "Multi-party fair exchange with an off-line trusted neutral party", Proc.DEXA'99 Workshop on Electronic Commerce and Security, Florence, Italy, Sept. 1999

[8] A. Kremer and O. Markowitch, "Fair multi-party nono-repudiation protocols", Information Security, Jan.2003,pp.223-380.

[9] X.M. Wang and X. Li, "Modeling and Analysis of Multi-party Fair Exchange Protocols", Proc.the 3rd IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM2007), Sep.2007,pp. 2246-2250.

[10] X.M. Wang and X. Li, "Game-base Analysis of Multi-party Non-repudiation Protocols", Proc.2007 International Conference on Computational Intelligence and Security (CIS'2007), Dec.2007,pp. 642-646.

[11] X.M. Wang and X. Li, "Formal Analysis of Multi-party Non-repudiation Protocols",Proc. the 5th International Conference of e-Engineering & Digital Enterprise Technology(e-ENGDET2006), Aug.2006,pp.89-93.

[12] Y.L. Ren and J.Z. Zhang, "A Multi-party Non-repudiation Protocol without TTP", Computer Engineering and Applications.Vol.40, Dec.2004, pp.137-138,232.