一个公平不可抵赖协议及其形式化分析

刘　敬,周明天
(电子科技大学计算机学院,四川成都 610054)

摘　要:　不可抵赖作为基本的网络安全服务之一,必须提供不可抵赖证据的产生、收集和维护机制以防止交易的任何一方试图对交易中已发生的特定事件或行为的欺诈性抵赖.另外,公平性也是一个必须考虑的因素,它保证交易的任何一方都不可能因为过早地退出交易或在交易中作弊而取得事实上凌驾于另一方的优势地位.本文针对目前 ISO/ IEC 13888 的不可抵赖机制因为不公平性而存在的严重缺陷:选择性收据问题,提出了一个公平不可抵赖协议 FNORP,并通过严格的形式化分析证明了 FNORP 具有不可抵赖性、公平性和适时中止性.

关键词:　不可抵赖;公平性;适时中止性;离线 TTP
中图分类号:　TP309　　**文献标识码**:　A　　**文章编号**:　0372-2112 (2003) 09-1422-04

A Fair Non-Repudiation Protocol and Its Formal Analysis

LIU Jing, ZHOU Ming-tian
(*School of Computer S&E, University of Electronic Science and Technology of China, Chengdu, Sichuan* 610054, *China*)

Abstract:　Non-repudiation, as one of the basic network security services, must provide mechanisms in which evidence will be generated, collected and maintained to protect the transacting parties against any false denial in which a particular event or action has taken place. In addition, fairness is a desirable requirement such that neither party can gain an advantage by quitting prematurely or otherwise misbehaving during a transaction. Aiming at solving a serious bug: the selective receipt problem in the current ISO/ IEC 13888 non-repudiation mechanism, which is induced by unfairness, this paper presents a Fair non-repudiation protocol FNORP and through a strict formal analysis. We show that FNORP possesses the capabilities of non-repudiation, fairness and timely-termination.

Key words:　non-repudiation; fairness; timely termination; off-line TTP

1　引言

不可抵赖服务就是防止交易的任何一方试图对交易中已发生的特定事件或行为的欺诈性抵赖,为此不可抵赖服务提供不可抵赖证据的产生、收集和维护机制,用以对日后可能产生的法律纠纷进行仲裁.基本的不可抵赖服务是:

(1) 发信不可抵赖 (Non-repudiation of Origin,简称 NRO):为消息接收方提供发信的证据,防止发信方试图否认曾经发送过消息.证据的提供者是发信方;

(2) 接收不可抵赖 (Non-repudiation of Receipt,简称 NRR):为发信方提供消息已接收的证据,防止接收方试图否认曾经收到消息.证据的提供者是接收方.

除了上述两种基本的不可抵赖服务外,ISO/ IEC 13888 系列标准[3~5]还定义了另外两种不可抵赖服务:提交不可抵赖和发送不可抵赖.这两种服务在发送代理 (Delivery Agent) 参与交易时才涉及.

2　利用离线 TTP 适时中止的公平不可抵赖协议 FNORP

ISO/ IEC13888 系列标准[3~5]中提供的不可抵赖机制存在选择性收据问题[7].它的造成是由于协议存在不公平性,协议的一方可以谋得凌驾于另一方的优势地位[7].针对选择性接收问题,我们提出了一个利用离线 TTP 的适时中止的公平不可抵赖协议 FNORP (Fair NOn-Repudiation Protocol).首先给出公平性和适时中止性的准确定义.

定义 1　不可抵赖协议被称为是公平的.如果满足以下两个条件:

(1) 在协议结束时,能够分别给发信方和接收方提供有效的 NRR 和 NRO 证据;

(2) 协议中止在任何阶段时,不会造成任何一方处于较另一方更为优势的地位,或者说协议双方要么得到了各自期望

收稿日期:2002-05-27;修回日期:2003-04-27
基金项目:国防科工委跨行业基金 (No. 51415010101DZ02)

的东西,要么都得不到任何有利信息.

定义 2　不可抵赖协议如果在不失公平性的前提下,能够保证协议的任何一方可以单方地促使一个交易结束,那么这个不可抵赖协议就是适时中止的.

除了文[1]的基本记号外,我们将用到如下记号:

$T_{sb\_what} = sS_{TTP}(t_{sb\_what})$:在 sb 产生 what 证据时,TTP 为 sb 生成的时间戳依据(由于篇幅所限,本文省略了 TTP 时间戳服务的细节).

$EOO\_C = sS_A(f_1, B, L, C, T_{A\_EOO\_C})$:对密文 C 的发信证据(Evidence of Origin).

$EOR\_C = sS_B(f_2, A, L, H(C), eP_{TTP}(eP_B(K)), T_{B\_EOR\_C})$:对密文 C 的收信证据(Evidence of Receipt).

$EOO\_K = sS_A(f_3, B, L, eP_B(K), T_{A\_EOO\_K})$:对密钥 K 的发信证据(Evidence of Origin).

$EOR\_K = sS_B(f_4, A, L, K, T_{B\_EOR\_K})$:对密钥 K 的收信证据(Evidence of Receipt).

$sub\_K = sS_A(f_5, B, L, eP_B(K), H(C), T_{A\_sub\_K})$:$A$ 提交 K 的证明.

$con\_K = sS_{TTP}(f_6, A, B, L, eP_B(K), T_{TTP\_con\_K})$:TTP 发布的对 K 的确认证据(Evidence of Confirmation).

$abort = sS_{TTP}(f_8, A, B, L, T_{TTP\_abort})$:TTP 发布的对一个交易的中止证据(Evidence of Abort).

FNORP 协议包括:交换子协议,中止子协议,决议子协议.

交换子协议如下:

(1) $A \rightarrow B: f_1, f_5, B, L, C$, TTP, $eP_{TTP}(eP_B(K))$, EOO_C, sub_K(msg1)

IF B 未收到 msg1 THEN 导致 A 等待响应超时,A 执行中止子协议

ELSE IF B 放弃 THEN 导致 A 等待响应超时,A 执行中止子协议 ELSE goto2

(2) $B \rightarrow A: f_2, A, L, EOR\_C$(msg2)

IF A 未收到 msg2 THEN A 执行中止子协议 AND 导致 B 等待响应超时,B 执行决议子协议

ELSE IF A 放弃 THEN 导致 B 等待响应超时,B 执行决议子协议 ELSE goto3

(3) $A \rightarrow B: f_3, B, L, eP_B(K), EOO\_K$(msg3)

IF B 未收到 msg3 THEN B 执行决议子协议 AND 导致 A 等待响应超时,A 执行决议子协议

ELSE IF B 放弃 THEN 导致 A 等待响应超时,A 执行决议子协议 ELSE goto4

(4) $B \rightarrow A: f_4, A, L, EOR\_K$(msg4)

IF A 未收到 msg4 THEN A 执行决议子协议 ELSE 交换子协议结束

中止子协议如下:

(1) $A \rightarrow$TTP: $f_7, B, L, sS_A(f_7, B, L)$

IF resolved THEN

(2) $A \leftarrow$TTP: $f_2, f_6, A, B, L, eP_B(K), con\_K, EOR\_C$

ELSE

(3) $A \leftarrow$TTP: f_8, A, B, L, abort

决议子协议如下,当中的 U 可以是 A 或 B.

(1) $U \rightarrow$TTP: $f_2, f_5, A, B, L, eP_{TTP}(eP_B(K)), H(C), sub\_K, EOR\_C$

IF aborted THEN

(2) $U \leftarrow$TTP: f_8, A, B, L, abort

ELSE

(3) $U \leftarrow$TTP: $f_2, f_6, A, B, L, eP_B(K), EOR\_C, con\_K$

整个交易的流程如图 1 所示. 详细描述参见定理 1,2 和 3 的证明过程.

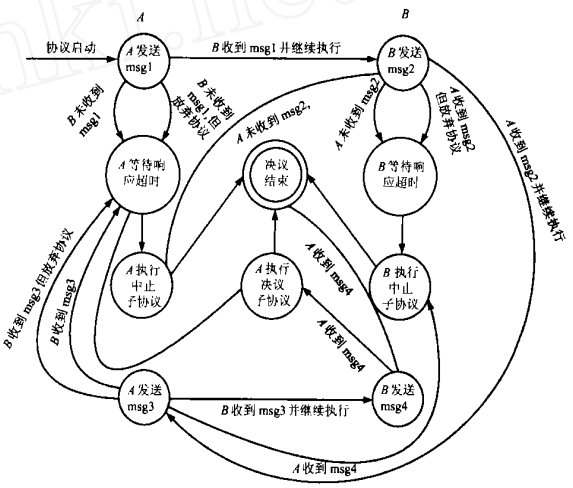

图 1　交易状态变迁图

3　FNORP 协议分析

我们将证明 FNORP 协议具有公平性、适时中止性(见定义 1 和 2)和不可抵赖性.

在进行定理 1 的证明之前,首先简要介绍 SVO 逻辑[6]. SVO 逻辑是一种模态逻辑,可以用来验证不可抵赖协议. 它有两个推理准则和 20 个公理. 在这里我们简要描述两个推理准则和将要使用到的公理.

推理准则

MP:从 φ 和 $\varphi \supset \psi$ 推出 ψ.

Nec:从 $\rightarrow\varphi$ 推出 $\rightarrow P$ 相信 φ.

下面是我们列出将用到的 SVO 公理,具体说明见文[6]:

相信 —A1. (P 相信 $\varphi \wedge P$ 相信 $(\varphi \supset \psi)$) $\supset P$ 相信 ψ

源联系 —A4. ($PK_\sigma(Q, K) \wedge R$ 收到 $X \wedge SV(X, K, Y)$) $\supset Q$ 说过 Y

收到 —A7. P 收到 $(X_1, \cdots, X_n) \supset P$ 收到 X_i

说话 —A14. P 说过 $(X1, \cdots, X_n) \supset (P$ 说过 $X_i \wedge P$ 看见 $Xi)$

定理 1　如果 TTP 和每一个交易方(A 和 B)之间的通信信道是可复原的,那么 FNORP 协议性满足不可抵赖性.

证明　分两步:首先我们陈述需要用到的前提;然后使用这些前提和上述的公理和逻辑规则对定理给予证明. 要证明 FNORP 协议满足不可抵赖性等价于要证明下面两个命题同

时满足:

命题 1 NRO 发信不可抵赖:J 相信(A 说过 M)

命题 2 NRR 接收不可抵赖:J 相信(B 收到 M)

其中 J 为第三方仲裁者(机构).作为仲裁者,J 拥有 A,B 和 TTP 的公钥并确信这些密钥的有效性(从他们各自的 X.509 数字证书中获得).这样就有:

$P1$. J 相信 $PK_\sigma(A, V_A)$; $P2$. J 相信 $PK_\sigma(B, V_B)$; $P3$. J 相信 $PK_\sigma(\mathrm{TTP}, V_{\mathrm{TTP}})$

在 A 执行中止子协议后:A 收到 $(f_8, A, B, L, M, C, eP_B(K), \mathrm{abort})$;$B$ 收到 $(f_1, f_8, A, B, L, C, EOO\_C, \mathrm{abort})$;双方都没有得到有用的信息,交易及时中止.

交易成功包括两种情形:

情形 ①顺利执行完交换子协议,整个交易正常完成:

A 收到 $(f_2, f_4, A, B, L, M, C, eP_B(K), EOR\_C, EOR\_K)$;

B 收到 $(f_1, f_3, A, B, L, C, eP_B(K), EOO\_C, EOO\_K)$;

情形 ② A 或 B 执行完决议子协议,整个交易决议完成:

A 收到 $(f_2, f_6, A, B, L, M, C, eP_B(K), EOR\_C, con\_K)$;

B 收到 $(f_1, f_6, A, B, L, C, eP_B(K), EOO\_C, con\_K)$;

为了证明命题 1,B 应该把他收到的信息提供给 J.为证明命题 2,A 应该把他收到的信息提供给 J.即:

$P4$. J 收到 $(f_1, f_3, A, B, L, C, eP_B(K), EOO\_C, EOO\_K)$(情形 ①)

或 $(f_1, f_6, A, B, L, C, eP_B(K), EOO\_C, con\_K)$(情形 ②);

$P5$. J 收到 $(f_2, f_4, A, B, L, C, eP_B(K), EOR\_C, EOR\_K)$(情形 ①)

或 $(f_2, f_6, A, B, L, C, eP_B(K), EOR\_C, con\_K)$(情形 ②);

使用 A,B 和 TTP 的公钥,J 能够验证他收到的签名信息的有效性.即:

$P6$. J 相信 $SV((f_1, B, L, C, EOO\_C), V_A, (f_1, B, L, C))$

$P7$. J 相信 $SV((f_3, B, L, eP_B(K), EOO\_K), V_A, (f_3, B, L, eP_B(K)))$

$P8$. J 相信 $SV((f_2, A, L, H(C), eP_{\mathrm{TTP}}(eP_B(K)), EOR\_C), V_B, (f_2, A, L, H(C), eP_{\mathrm{TTP}}(eP_B(K)))$

$P9$. J 相信 $SV((f_4, A, L, K, EOR\_K), V_B, (f_4, A, L, K))$

$P10$. J 相信 $SV((f_6, A, B, L, eP_B(K), con\_K), V_{\mathrm{TTP}}, ((f_6, A, B, L, eP_B(K)))$

以上这 10 个前提很容易由 SVO 逻辑推导得出.

对情形 ②,当 TTP 收到 $eP_B(K)$ 和 con_K(来自 A 或 B),TTP 将会检查 A 或 B 的请求然后生成元组 $(f_2, f_6, A, B, L, eP_B(K), con\_K)$,最后通过类似 FTP 的服务公之于众.因为我们假定通信信道是可复原的,所以 A 或 B 总可以从 TTP 处检索到该信息.即有:

$P11$. TTP 说过 $(A, B, L, eP_B(K)) \supset A$ 说过 $(A, B, L, eP_B(K)) \wedge B$ 收到 $(A, B, L, eP_B(K))$

$P12$. B 说过 $(f_2, A, B, L, C) \supset B$ 收到 (f_2, A, B, L, C)

由于消息 M 实际上被分为两个部分分别传送,即 $C(=eK(M))$ 和被加密的密钥 $eP_B(K)$.唯一的标签 L 将 C 和 $eP_B(K)$ 联系在一起以唯一确定消息 M.即:

$P13$. A 说过 $(A, B, L, eK(M)) \wedge A$ 说过 $(A, B, L, eP_B(K)) \supset A$ 说过 M

$P14$. B 说过 $(A, B, L, eK(M)) \wedge B$ 说过 $(A, B, L, eP_B(K)) \supset B$ 说过 M

下面开始验证不可抵赖性(NRO 和 NRR).简洁起见,在验证过程中我们忽略了使用 $A1$,Nec 和 MP 的推理步骤.

证明命题 1. NRO 发信不可抵赖:J 相信(A 说过 M)

情形 ①

(1) J 相信 J 收到了 $(f_1, f_3, A, B, L, C, eP_B(K), EOO\_C, EOO\_K)$:由 $P4$

(2) J 相信 A 说过 (f_1, A, B, L, C) 及 $(f_3, A, B, L, eP_B(K))$:由(1),$P1$,$P6$,$P7$,$A4$

(3) J 相信 A 说过 $(A, B, L, eK(M))$ 及 $(A, B, L, eP_B(K))$:由(2),$A14$

(4) J 相信(A 说过 M):由(3),$P13$. 得证命题 1.

情形 ②

(1) J 相信 J 收到了 $(f_1, f_3, A, B, L, C, EOO\_C)$:由 $P4$ 和 $A7$

(2) J 相信 A 说过 (f_1, A, B, L, C):由(1),$P1$,$P6$,$A4$

(3) J 相信 A 说过 $(A, B, L, eK(M))$:由(2),$A14$

(4) J 相信 J 收到 $(f_6, A, B, L, eP_B(K), con\_K)$:由 $P4$ 和 $A7$

(5) J 相信 TTP 说过 $(f_6, A, B, L, eP_B(K))$:由(4),$P3$,$P8$ 和 $A4$

(6) J 相信 TTP 说过 $(A, B, L, eP_B(K))$:由(5),$A14$

(7) J 相信 A 说过 $(A, B, L, eP_B(K))$:由(6),$P11$

(8) J 相信(A 说过 M):由(3),(7),$P13$. 得证命题 1.

证明命题 2. NRR 接收不可抵赖:J 相信(B 收到 M)

情形 ①(上接证明命题 1 的情形 ①的第(4)步)

(5) J 相信 J 收到 $(f_2, f_4, A, B, L, C, eP_B(K), EOR\_C, EOR\_K)$:由 $P5$

(6) J 相信 B 说过 (f_2, A, B, L, C) 及 $(f_4, A, B, L, eP_B(K))$:由(5),$P2$,$P8$,$P9$,$A4$

(7) J 相信 B 收到 (A, B, L, C) 及 $(A, B, L, eP_B(K))$:由(6),$P12$

(8) J 相信(B 收到 M):由(7),$P14$. 得证命题 2.

情形 ②(上接证明命题 1 的情形 ②)

(9) J 相信 J 收到 (f_2, A, B, L, C, EOR_C):由 $P5$ 和 $A7$

(10) J 相信 B 说过 (f_2, A, B, L, C):由(9),$P2$,$P8$,$A4$

(11) J 相信 B 收到 (A, B, L, C):由(10),$P12$

(12) J 相信 B 收到 $(A, B, L, eP_B(K))$:由(6),$P11$

(13) J 相信(B 收到 M):由(11),(12),$P14$. 得证命题 2.

综上,FNORP 协议满足不可抵赖性.证毕.

定理 2 如果 TTP 和每一个交易方(A 和 B)之间的通信信道是可复原的,那么 FNORP 协议满足公平性.

证明 首先考虑 A 可能遭遇的不公平情形.

(1) 在交换子协议中,A 在发送 msg1 后,没有收到响应信息.这时,A 启动中止子协议保证交易在有限时间内完成.如

果 B 没有执行决议子协议,TTP 在以后也不会执行决议子协议,这样 B 不会得到 $eP_B(K)$,即 K,从而他也得不到 M. 如果 B 已经执行了决议子协议,A 将会从 TTP 那里得到 EOR_C 和 con_K,它们将可以用来证明 R 收到了 M;

(2)在交换子协议中,A 在发送 msg3 后没有收到 EOR_K. 这时,A 启动决议子协议以从 TTP 得到 con_K, con_K 将代替 EOR_K 来证明 B 收到了 $eP_B(K)$,即 K.

B 可能遭遇的不公平情形只可能是在它发送了 msg2 之后没有收到 $eP_B(K)$ 和 EOO_K. 这时 B 启动决议子协议以从 TTP 得到 $eP_B(K)$ 和 con_K. 因此,从 A 和 B 的两个角度来看,协议是满足公平性的. 证毕.

定理 3　如果 TTP 和每一个交易方(A 和 B)之间的通信信道是可复原的,那么 FNORP 协议满足适时中止性.

证明　我们首先分析 A 可能结束交易的可能方式

(1)在交换子协议中,在发送了 msg4 后交易正常结束;

(2)在交换子协议中,在发送 msg3 之前的任何时候启动中止子协议;

(3)在交换子协议中,在收到了 msg2 后的任何时候启动决议子协议.

由于我们假定 TTP 和每一个交易方(A 和 B)之间的通信信道是可复原的,由 A 启动的中止子协议和决议子协议确保交易在有限时间内结束. 这样在任何时候,A 总有办法适时地结束交易.

B 可能结束交易的可能方式:

(1)在交换子协议中,在发送了 msg4 后交易正常结束;

(2)在交换子协议中,在发送 msg2 之前的任何时候退出;

(3)在交换子协议中,在收到 msg1 之后的任何时候启动决议子协议.

同样,对 B 而言,交易总可以通过上述方式适时地结束. 综上所述,FNORP 协议满足适时中止性. 证毕.

总之,FNORP 协议具有不可抵赖性、公平性和适时中止性.

4　结论

指出了 ISO/IEC 13888 系列标准中提出的不可抵赖机制存在严重缺陷:选择收据问题. 这个问题是由于协议存在的不公平性导致的. 为此,我们提出了一个利用离线 TTP 的适时中止的公平不可抵赖协议 FNORP,并通过对协议进行严格的形式化分析证明了 FNORP 协议具有不可抵赖性、公平性和适时中止性.

致谢　感谢审稿专家给本文提出了宝贵的修改意见.

参考文献:

[1] J Zhou, D Gollmann. An efficient non-repudiation protocol[A]. Proceedings of 10th IEEE Computer Security Foundations Workshop[C]. Rockport, Massachusetts: IEEE Computer Society Press, June 1997. 126 - 132.

[2] ISO 7498-2, Information Processing Systems - Part2: Security Architecture[S]. International Organization for Standardization, 1989.

[3] ISO/IEC 13888-1, Information Technology-Security Techniques-Non-Repudiation-Part1: General[S]. International Organization for Standardization, 1997.

[4] ISO/IEC 13888-2, Information Technology-Security Techniques-Non-Repudiation-Part2: Mechanisms Using Symmetrical Techniques[S]. International Organization for Standardization, 1998.

[5] ISO/IEC 13888-3, Information Technology-Security Techniques-Non-Repudiation-Part3: Mechanisms Using Asymmetrical Techniques[S]. International Organization for Standardization, 1997.

[6] P F Syverson, P C van Oorschot. On unifying some cryptographic protocol logics[A]. Proceedings of the 1996 IEEE Symposium on Security and Privacy(S & P'96)[C]. Los Alamitos, CA: IEEE Computer Society Press, May 1996. 62 - 72.

[7] J Zhou, D Gollmann. Observations on non-repudiation[A]. K Kim, T Matsumoto. Advances in Cryptology| ASIACRYPT'96: International Conference on the Theory and Applications of Cryptology and Information Security, volume 1163 of Lecture Notes in Computer Science Series[C]. Berlin: Springer-Verlag, November 1996. 133 - 144.

作者简介:

刘 ▒　男,1972 年 2 月生于四川绵阳,1998 年获成都电子科技大学应用数学专业理学硕士学位,现为成都电子科技大学计算机学院在读博士生,主要研究领域为网络与信息系统安全、分布对象技术,在国内外学术刊物和学术会议上发表论文 14 篇.

周明天　男,1939 生于广西容县,1962 年毕业于哈尔滨工业大学电机系,1981 年到 1983 年在美国加州伯克利大学(UC, Berkeley)的 EECS 系当访问学者,现为成都电子科技大学计算机学院教授,博士生导师,主要研究领域为计算机网络、分布对象技术、并行分布处理和网络与信息系统安全,主持过多项"六五"、"七五"和"八五"国家重点科技攻关项目,先后获国家科技进步三等奖 2 次,电子工业部和四川省科技进步一等奖 5 次,二等奖 1 次,1992 年起享受国家特殊津贴待遇,出版发行著作 10 本,其中《TCP/IP 网络原理与技术》获电子工业部优秀教材一等奖,1985 年以来在国内外学术刊物和学术会议上发表论文 136 篇.