电子证据与反拒认协议及形式化分析

袁 丁[1]，范平志[2]

(1. 西南交通大学移动通信研究所 成都 610031; 2. 四川师范大学计算机科学学院 成都 610066)

【摘要】反拒认是实现电子商务的一个重要前提条件。基于可信的第三方提出了一个面向传输的电子证据与反拒认协议TEENP，解决了收方和发方的拒认问题。扩充了类BAN信任逻辑的语义和逻辑推理规则，并用信任逻辑BAN对其进行了形式化分析。与相关协议相比，本协议是公平的、安全的和高效的。

关 键 词 电子证据; 反拒认; 数字签名; 加密; 网络安全

中图分类号 TP309 文献标识码 A

An Electronic Evidence and Non-Repudiation Protocol and Its Formal Analysis

Yuan Ding[1] Fan Pingzhi[2]

(1. Institute of Mobile Communications, Southwest Jiaotong University Chengdu 610031 ;

2. School of Computer Science , Sichuan Normal University Chengdu 610066)

Abstract Non-repudiation is one of the most important premises to achieve electronic commerce. Based on a trusty third party, this paper proposes a transmission-oriented electronic evidence and non-repudiation protocol transmission-oriented electronic evidence and non-repudiation protocol (TEENP) to resolve the possible repudiation problem both in receiver side and in sender side. We extend the semantics and reasoning rules of the belief logic BAN, and formal analysis of TEENP is presented using logic BAN. The protocol is fair, secure and efficient, compared with the corresponding protocols.

Key words electronic evidence; non-repudiation; digital signature; encryption; network security

随着计算机网络的高速发展，电子商务在全球范围的迅速开展，对网络安全的要求越来越高，网络安全的目的就是使网络上传输数据的机密性、完整性、真实性、有效性和合法性得到充分的保护。反拒认是最重要的网络安全服务之一，目标是保护事务的参与者，以防止不诚实者否认参与了某项事务，从而拒绝承担相应的责任[1]。拒认存在两种可能：发送者拒认和接收者拒认。反拒认协议必须要保证发送者和接收者所处地位是公平的，即协议运行的每一个阶段，发送者和接收者都不比对方更占优势；当协议运行完毕，每方都拥有对方的反拒认证据[2]。

从信息交换的方式来看，网络应用分为2类：1) 是面向连接的应用，即信息交换的双方同时在线并保持网络连接；2) 是面向传输的应用，即信息交换的双方可以不同时在线，而是由第三方对信息进行存储转发，从而达到信息交换的目的。比如，电子邮件就是典型的面向传输的应用。对于网络安全，必须考虑到这两种情况。从反拒认协议的具体实现又可以分为2种形式：1) 不需要第三方参与。其基本思想是交易双方逐渐把秘密泄露给对方[3,4]。该技术要求通信实体间严格的时间同步和相近的计算能力，这在Internet异构网络环

收稿日期：2002 – 12 – 05
基金项目：高等学校博士点基金(20020613020); 国家自然科学基资助项目(69825102)；四川省教育厅重点项目(2003A085)
作者简介：袁 丁(1967 –)，男，博士后，副教授，主要从事信息安全方面的研究.

境中是很难实现的。2) 是借助于可信的第三方参与来实现反拒认，这是一个切实可行的解决思路。

目前，大多数的反拒认协议都有可信的第三方参与并且是面向连接的[1,2,5,6]。其中，文献[5]提出了一个能双向反拒认的协议，能够解决可能发生的争端，但通信量大。文献[2]中的方案只需交互5条信息，但该协议运行结束后，发送者给接收者的信息第三方也能知道，无隐私。文献[6]对文献[2]的方案进行了改进，使协议的运行效率更高，通信双方的隐私也能得到保护。文献[7]提出了一种有可信的第三方参与并且面向传输的反拒认协议CMP，该协议具有如下缺陷：1) 传输的信息无法进行数据的完整性验证，如果传输的信息被攻击者恶意篡改，接收方无法判断，文献[6]也存在类似的问题；2) 由于 EOO 的长度要大于消息 M 的长度，当 M 很大时，协议的每一步传输信息量都很大,非常浪费网络的带宽资源；3) 协议的每一步都要对长度大于消息 M 的长度的数据进行加密运算，尤其是公钥体制下的签名运算，使协议的计算负荷大大增加。本文给出一个新的面向传输的反拒认协议。

1 TEENP协议描述

1.1 TEENP协议的执行过程

本文设计的面向传输的电子证据与反拒认协议 (Transmission-oriented Electronic Evidence and Non-repudiation Protocol, TEENP)与CMP运行步骤一样有4步，如图1所示。参与的实体有：发送方 A，接收方 B，以及可信的第三方 T。T 必须是公平、公正的，这是本协议的基本前提，它的作用相当于电子公告牌。通信实体均拥有一公钥、私钥对，公钥对外公开。L 是本次协议运行的唯一标志，它贯穿于整个协议的运行过程，L 一般是一个大的随机数或是本次协议传递消息 M 的hash函数值 $h(M)$。

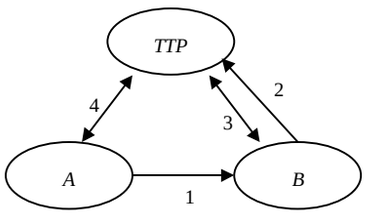

图1 CMP协议

具体协议如下：

1) $A \to B : A, B, L, C, eV_{TTP}\{K_{AB}\}, EOO$，其中对称密钥 K_{AB} 是由 A 产生，用于加密消息 M，密文 $C = eK_{AB}\{M\}$，$EOO = sS_A\{H(A \| B \| L \| C \| eV_{TTP}\{K_{AB}\})\}$ 是 A 发送密文的反拒认证据。式中使用hash运算目的是减少签名时数据的长度。B 用 A 的公钥验证 $H(A \| B \| L \| C \| eV_{TTP}\{K_{AB}\})$ 与 $dV_A(EOO)$ 是否相等。若不等，说明数据的完整性被破坏，则 B 终止协议。B 保留密文 C 和 EOO，由于不知道 TTP 的私钥 S_{TTP} 而无法得到 K_{AB}，所以 B 并不比 A 占优势。

2) $B \to TTP : A, B, L, C, eV_{TTP}\{K_{AB}\}, EOR, EOO$，$EOR = sS_B\{H(A \| B \| L \| C \| eV_{TTP}\{K_{AB}\})\}$ 是 B 接收密文 C 反拒认证据。TTP 验证 $H(A \| B \| L \| C \| eV_{TTP}\{K_{AB}\})$ 与 $dV_B(EOR)$、$dV_A(EOO)$ 是否相等。若等，说明 B 转发给 TTP 的数据确实是 A 发出的。否则，终止协议。

3) $B \leftrightarrow TTP : A, B, L, eV_B\{EOP_1\}$，其中 $EOP_1 = sS_{TTP}\{A, B, L, K_{AB}\}$ 是 A 发送密钥 K_{AB} 的反拒认证据。B 用私钥 S_B 解密 $eV_B\{EOP_1\}$ 得到 EOP_1，用公钥 V_{TTP} 解密 EOP_1 得到 K_{AB}，并用 K_{AB} 解密 C 得到 M。式中用 eV_B 对 EOP_1 加密，目的是防止非法的第三方得到 K_{AB}，从而知晓实体 A、B 之间的通信内容。

4) $A \leftrightarrow TTP : A, B, L, EOR, eV_A\{EOP_2\}$,其中, $EOP_2 = sS_{TTP}\{A, B, L, K_{AB}\}$ 是 B 接收 K_{AB} 的反拒认证据。A 用 S_A 解密 $eV_A\{EOP_2\}$ 得到 EOP_2，保留 EOP_2 和 EOR，当发生争端时，由 A 提交给仲裁机构。

1.2 争端处理

争端1：发送者 A 拒认。如果接收者 B 宣布从 A 处得到消息 M，则仲裁机构要求接收者 B 出示如下证据：$A, B, L, M, C, K_{AB}, EOO, EOP_1$，如果 B 不能提供上述证据或下面的条件之一不成立，则可断定 B 不诚实：1) EOO 是发送者 A 对 $\{A, B, L, C, eV_{TTP}\{K_{AB}\}\}$ 的签名；2) EOP_1 是 TTP 对 $\{A, B, L, K_{AB}\}$ 的签名；3) K_{AB} 是加密信息 M 的密钥，即 $C = eK_{AB}\{M\}$。三个条件成立，则可断定 A 不诚实。

争端2：接收者 B 拒认。如果发送者 A 宣布把 M 发送给了 B，则仲裁机构要求发送者 A 出示如下证据：$A, B, L, M, C, K_{AB}, EOR, EOP_2$，如果 A 不能提供上述证据或下面的条件之一不成立，则可断定 A 不诚实：1) EOR 是接收者 B 对 $\{A, B, L, C, eV_{TTP}\{K_{AB}\}\}$ 的签名；2) EOP_2 是 TTP 对 $\{A, B, L, K_{AB}\}$ 的签名；3) K_{AB} 是加密信息 M 的密钥，即 $C = eK_{AB}\{M\}$。三个条件成立，则可断定 B 不诚实。

2 协议的形式化分析

文献[8]自1989年提出BAN逻辑以来，得到了协议分析者的广泛关注和研究[9~13]。然而，类BAN逻辑不完全适合分析协议的可追究性[13]，为此，本文将扩充BAN逻辑的语义和逻辑推理规则。

2.1 BAN逻辑及其符号表示

以下是类BAN逻辑中的基本概念和符号：

$P|\equiv X$ ：表示P信任X；$P|\sim X$ ：表示P说过X ，即P发送过X；$P\lhd X$ ：表示P见过X；$|\xrightarrow{K}P$ ：表示P有公钥K ，相应的私钥K^{-1}只有P知道 ；

其次，在类BAN逻辑中，增加下列符号定义： $P|\equiv *Q$ ：表示Q是可信任的第三方，即本次协议执行中P相信Q是真实可信的。

类BAN逻辑中的一些相关的推理规则：

签名规则R_1：$\dfrac{P|\equiv \overset{K}{\alpha}\ Q, P\lhd \{X\}_{K^{-1}}}{P|\equiv Q|\sim X}$ ；投影规则R_2：$\dfrac{P|\equiv Q|\sim (X,Y)}{P|\equiv Q|\sim X}$ ；投影规则R_3：$\dfrac{P\lhd (X,Y)}{P\lhd X}$ 。

并增加以下的推理规则：

信任逻辑R_4：$\dfrac{P|\equiv *Q, P|\equiv Q|\equiv X}{P|\equiv X}$ ；杂凑函数不可求逆逻辑R_5：$\dfrac{P|\equiv Q|\sim H(X), P\lhd (X, H(X))}{P|\equiv Q|\sim X}$。

报文发送逻辑R_6：$\dfrac{P|\equiv Q|\sim \{M\}_K, P|\equiv Q|\sim K}{P|\equiv Q|\sim M}$ ；报文接收逻辑R_7：$\dfrac{P|\equiv Q\lhd \{M\}_K, P|\equiv Q\lhd K}{P|\equiv Q\lhd M}$。

2.2 协议的形式化分析

假设J(judge)是仲裁机构。本协议运行完成后希望达到以下目标：

1) 对发送方A的反拒认验证，即 $J|\equiv A|\sim M$ ；

2) 对接收方B的反拒认验证，即 $J|\equiv B\lhd M$ 。

仲裁机构J拥有A,B,TTP的公钥并相信其有效性，TTP是可信任的第三方，则有下列逻辑假设：

(1) $J|\equiv \overset{V_A}{\alpha}\ A$ ；(2) $J|\equiv \overset{V_B}{\alpha}\ B$ ；(3) $J|\equiv \overset{V_{TTP}}{\alpha}\ TTP$ ；(4) $J|\equiv *TTP$ ；(5) $B|\sim \{M\}_{K_{AB}} \Rightarrow B\lhd \{M\}_{K_{AB}}$ ；

(6) $TTP|\sim K_{AB} \Rightarrow TTP|\equiv A|\sim K_{AB}$ ；(7) $TTP|\sim K_{AB} \Rightarrow TTP|\equiv B\lhd K_{AB}$。

当协议执行完成以后，则通信实体A,B分别拥有以下信息：

$A\lhd (A,B,L,M,C,K_{AB},EOR,EOP_2)$ ； $B\lhd (A,B,L,M,C,K_{AB},EOO,EOP_1)$ ，当双方发生争端时，要证明目标1)，B需要把所收到的信息提交给J，即有

$$J\lhd (A,B,L,M,C,K_{AB},EOO,EOP_1) \tag{1}$$

由规则R_3，逻辑假设式(1)，规则R_1，杂凑函数不可求逆逻辑R_5和式(1)可知

$$J|\equiv A|\sim \{A,B,L,C,eV_{TTP}\{K_{AB}\}\} \tag{2}$$

由规则R_2和式(2)可知

$$J|\equiv A|\sim C \tag{3}$$

由规则R_1，R_3，R_4，逻辑假设式(6)可知

$$J|\equiv A|\sim K_{AB} \tag{4}$$

由报文发送逻辑R_6，式(3)、(6)可知： $J|\equiv A|\sim M$ ，目标1)得证。

当双方发生争端时，要证明目标2)，A需要把所收到的信息提交给J，即有

$$J\lhd (A,B,L,M,C,K_{AB},EOR,EOP_2) \tag{5}$$

由规则R_1，R_3，R_5，逻辑假设式(1)、(5)可知

$$J|\equiv B|\sim \{A,B,L,C,eV_{TTP}\{K_{AB}\}\} \tag{6}$$

由规则R_2，逻辑假设式(5)、(6)可知

$$J|\equiv B\lhd C \tag{7}$$

由规则R_1，R_3，R_4，逻辑假设式(7)可知

$$J \mid\equiv B < K_{AB} \tag{8}$$

由报文接收逻辑R_7，式(7)、(8)可知：$J \mid\equiv B < M$，目标2)得证。

3 结 束 语

数字签名技术可以验证发送数据的反拒认性，但很难解决数据接收方的反拒认问题。鉴于此，本文基于可信的第三方提出了一个面向传输的电子证据与反拒认协议TEENP，其目的是为了保证网络上发送、接收数据的机密性、完整性、公正性和有效性。详细比较了TEENP与CMP协议的各项性能指标，本协议在安全性、计算负荷和通信负荷方面均有很大提高。扩充了类BAN逻辑的语义和逻辑推理规则。并使用类BAN逻辑证明了TEENP满足电子证据与反拒认协议中最重要的一个特性可追究性。

参 考 文 献

[1] Zhou J, Gollmann D. Evidence and non-repudiation[J]. Journal of Network and Computer Applications, 1997, 25 (2): 19-25

[2] Zhou J, Gollmann D. A fair non-repudiation protocol[C]. In: Proceedings of 1996 IEEE Symposium on Security and Privacy, California: IEEE Press, 1996. 55-61

[3] Even S, Goldreich O, Lempel A. A randomized protocol for signing contacts[J]. Commun ACM, 1985, 28:637-647

[4] Brickell E, Chaum D, Damgard I, *et al*. Gradual and verifiable release of a secret[C]. In: Advances in Cryptology-Proceedings of CRYPT’ 87, Berlin: Springer-Verlag,1988. 25-30

[5] Coffey T, Saidha P. Non-repudiation with mandatory proof of receipt[J]. Computer Communication Review, 1996, 26 (1): 6-18

[6] 蒋晓宁，叶澄清. 电子证据与反拒认协议[J]，通信学报，2000, 21(7): 76-81

[7] Robert H, Deng L G. Practical protocols for certified electronic mail[J]. Journal of Network Systems Management, 1996, 4(3): 1-6

[8] Burrows M. A logic of authentication[J]. ACM Trans. on Computer System, 1990, 8(1): 18-36

[9]Boyd C, Mao W. On a limitations of BAN logic[C]. In: Lecture Notes in Computer Science, Berlin: Springer-Verlag, 1993. 240-247

[10] Nessett D M. A critique of burrows, abadi and needham logic[J]. Operating System Review, 1990,24(2): 35-38

[11] 宋荣功，胡正名，杨义先. 对BAN逻辑中新鲜子的研究[J]. 电子科学学刊, 2000, 22(3): 505-508

[12] 袁 丁, 范平志. “对BAN逻辑中新鲜子的研究”的注记[J]. 电子与信息学报,2002,24(8): 1 131-1 133

[13] Kailar R. Accountability in electronic commerce protocols[J]. IEEE Transactions on Software Engineering, 1996, 22(5): 313-328

编 辑 孙晓丹