密钥链多方非否认协议

李 磊[1,2] 谭新莲[2] 王育民[1]
(西安电子科技大学综合业务网国家重点实验室 西安 710071)[1] (郑州大学信息工程学院 郑州 450001)[2]

摘 要 多方非否认协议通常仅考虑一轮消息交换的情况,很少讨论相同参与方进行多轮消息交换的情况。基于后者对多方非否认协议进行优化,提出了一种利用密钥链实现的多方非否认协议,以有效减轻TTP存储负担。协议由Initialization,Exchange,Abort和Recovery 4个子协议以及争议处理方案组成。分析表明,协议满足公平性、时限性和机密性。

关键词 安全协议,非否认,多方协议,密钥链
中图法分类号 TN918.1 **文献标识码** A

Multi-party Non-repudiation Protocol Using Key Chains

LI Lei[1,2] TAN Xin-lian[2] WANG Yu-min[1]
(National Key Lab. of Integrated Service Networks, Xidian University, Xi'an 710071, China)[1]
(School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China)[2]

Abstract The previous multi-party non-repudiation protocols normally focus on one round message exchange. The multi-round message exchanges within the same participatores are not studied well. For the latter condition, we presented a multi-party non-repudiation protocol using key chains which can reduce the TTP's storage requirements. The protocol consists of a dispute resolution policy and four sub-protocols, i. e., the initialization sub-protocol, the exchange sub-protocol, the abort sub-protocol and the recovery sub-protocol. Technical discussions show that the protocol satisfies fairness, timeliness and confidentiality.

Keywords Security protocol, Non-repudiation, Multi-party protocol, Key chains

非否认协议是实现电子商务的重要基础,它为协议参与方提供非否认服务,包括发方非否认(NRO)和收方非否认(NRR)。根据参与者不同,非否认协议可划分为双方协议和多方协议。双方非否认协议仅有一个发送者和一个接收者,多方非否认协议有一个发送者和多个接收者。非否认协议的研究已经持续多年,文献[1]提出了支持离线TTP的双方非否认协议;文献[2]提出了支持透明TTP的双方非否认协议;文献[3]将密钥链引入非否认协议的研究;文献[4]提出了基于双线性对的双方非否认协议;文献[5]研究了恶意发送者的行为,提出了能抵抗DDoS攻击的非否认协议。在多方非否认协议领域,文献[6,7]首先提出了支持在线和离线TTP的多方非否认协议;文献[8]改进了文献[6,7]的协议,将协议扩展为向多个接收者发送不同消息的协议;文献[9]提出了支持离线TTP的高效多方非否认协议,该协议仅需3次握手;文献[10]对文献[6,7]的缺点进行了细致的分析,在保持原协议特点的基础上,对其进行了优化改进。

在支持离线TTP的非否认协议中,发送方通常用独立的密钥来加密待交换的消息。如果消息交换过程中出现异常,则发送方需要请求TTP中止消息交换或接收方需要请求TTP提供加密密钥。出于容错性的考虑,通常要求TTP对双方的每一次请求都做出响应,因此TTP必须保存加密密钥或者与消息交换相关的一些信息,如参与者标识符、加密消息的Hash函数值或交换的标识符等[11]。在实际应用中,同一组协议参与者经常会进行多轮消息交换,如发送方多次群发邮件给相同接收方。在这种情况下,利用密钥链实现非否认协议,TTP仅需保存密钥链的种子及相关信息,便可有效地降低TTP的存储负担[3]。

就作者所知,仅文献[3]研究了在多轮交换情况下的双方非否认协议。本文旨在提出一个基于密钥链的多方非否认协议,以支持离线TTP,满足公平性、时效性和机密性,在进行多轮交换情况下,可降低TTP的存储负担。

1 基本假定和符号说明

在非否认协议中,有3种典型的通信信道:不可靠信道、弹性信道和可靠信道。在不可靠信道中,消息有可能丢失,因此接收方可能永远无法收到这个消息。在弹性信道中,消息可能被延迟任意长时间,但最终会到达接收方。在可靠信道中,消息会在一个确定的延迟内到达接收方。

较弱的通信信道假定可以使协议适应更多的环境。在本文提出的协议中,假定TTP和协议参与者之间的信道为弹性

到稿日期:2008-11-05 返修日期:2009-01-22 本文受国家自然科学基金(60473027)资助。
李 磊(1974-),男,博士研究生,研究方向为信息安全、电子商务安全,E-mail:ielilei@zzu.edu.cn;谭新莲(1975-),女,讲师,研究方向为计算机网络及安全;王育民(1936-),男,教授,博士生导师,研究方向为编码理论、密码学、信息安全等。

信道，而每个协议参与者之间的信道为不可靠信道。这样的假定比较符合客观情况，也是多数非否认协议采用的通信信道假定。

协议中使用 O、R 和 T 分别代表发送方、接收方和可信第三方 TTP；f_{xxx}：标识消息的目的；$E_k(X)$，$D_k(X)$：用对称密钥 K 对消息 X 加密、解密；$SA(X)$：用户 A 对消息 X 的数字签名；$P_A(X)$：使用用户 A 的公钥对消息 X 加密；$H(X)$：抗碰撞攻击的单向 Hash 函数；$G_R(X)$：用群加密机制[8]对 X 加密，只有 R 的成员才能解密得到 X；$A\rightarrow B$：用户 A 发送一个消息给用户 B；$A\Rightarrow S$：用户 A 广播一个消息给用户集合 S。

2 密钥链多方非否认协议

协议采用双密钥链结构，如图 1 所示。

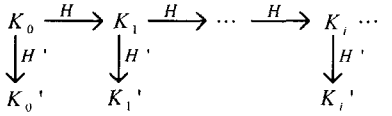

图 1 双密钥链

图中，K_0 为密钥链种子，$K_{i+1}=H(K_i)$，$K_i'=H'(K_i)$；H 和 H' 是两个不可交换的安全 Hash 函数，K_0'，K_1'…用作加密密钥。之所以采用双密钥链结构，是因为若采用单密钥链结构，即使逆向使用密钥链中的密钥进行加密，如果接收方在第 i 轮交换中收到密文后就中止协议，而在第 $i+1$ 轮交换中按协议完成交换，则接收方可自行计算得出第 i 轮交换的加密密钥，使协议失败。

密钥链多方非否认协议包括 Initialization，Exchange，Abort 和 Recovery 4 个子协议以及争议处理方案。

2.1 Initialization 子协议

首先，发送方选择密钥链种子 K_0 和随机数 nc，与参与方标识符一起发送给 TTP。然后 TTP 选择会话标识符 sid，计算 $cert=S_T(O,R,T,sid)$，与 nc 一起发送给发送方 O：

$1^i.\ O\rightarrow T: f_i, P_T(S_A(O,R,K_0,nc))$

$2^i.\ T\rightarrow O: f_{sid}, sid, S_T(nc,cert)$

其中，接收者集合 $R=P_{R_1}(R_1), P_{R_2}(R_2),\cdots$。

T 保存记录$\langle O,R,K_0,sid\rangle$，并保证$\langle O,R,K_0\rangle$在数据库内的唯一性。同时，对应每一条记录，$T$ 维护一个十字链表$\langle j,i,s(j,i)\rangle$，链表元素代表第 j 个接收者 R_j 第 i 轮交换的状态，该链表初始长度为 0。

2.2 Exchange 子协议

每轮交换都有一个交换序号 i，其初值为 0。每轮交换结束后，发方 O 将 i 增 1。第 i 轮交换的协议如下：

$1^e.\ O\Rightarrow R: f_{EOO}, O, R, T, i, sid, H(K_i'), E_{K_i'}(M), EOO, cert$

$2^e.\ R_j\rightarrow O: f_{EOR_j}, EOR_j$

$3^e.\ O\Rightarrow R': f_K, G_{R'}(K_i')$

其中，R'代表将 EOR_j 正确发给 O 的接收者集合；$EOO=S_O(cert,H(K_i'),H(E_{K_i'}(M)),i)$；$EOR_j=S_{R_j}(EOO)$。

2.3 Abort 子协议

如果发方 O 没有收到 R_j 发送的消息 2^e，O 可以将 R_j 加入集合 R''，并启动 Abort 子协议，向 TTP 发起请求，要求中止与 R''中用户的消息交换。Abort 子协议如下：

$1^a.\ O\rightarrow T: f_a, O, R, R'', H(E_{K_i'}(M)), i, sid, abrt$

T：FOR all $(R_j\in R'')$

IF $(s(j,i)=EOR_j)$ THEN retrieves EOR_j

ELSE add R_j into R_i^a；

set $s(j,i)=H(abrt)$

$2^a.\ T\rightarrow O: f_{conf}, conf$, all retrieved EOR_j

$3^a.\ T\Rightarrow R_i^a: f_{abrt}, R'', G_{R_i^a}(abrt)$

其中，$abrt=S_O(f_a,cert,H(E_{K_i'}(M)),i,R'')$，作为中止交换的证据；$conf=S_T(f_a,cert,abrt,R_i^a,i)$；$R_i^a$ 代表在第 i 轮交换中经 TTP 确认与 O 中止交换的用户集合。

Abort 子协议中，T 收到 O 的请求后，对所有属于 R''的用户 R_j，如果 R_j 第 i 轮交换的状态 $s(j,i)=EOR_j$，则说明 R_j 已经通过 Recovery 子协议获得了 K_i'。本轮与 R_j 的交换不能中止，T 在消息 2^a 中把 EOR_j 发给 O，以完成本轮交换；否则，将 R_j 加入集合 R_i^a，并置 $s(j,i)=H(abrt)$，T 保存 $abrt$ 并在消息 3^a 中将中止交换证据 $abrt$ 加密发给 R_i^a。

2.4 Recovery 子协议

如果接收者 R_j 没有收到 O 发送的消息 3^e，R_j 可启动 Recovery 子协议，向 TTP 发起请求，要求协助完成与 O 的消息交换。Recovery 子协议如下：

$1^r.\ R_j\rightarrow T: f_r, O, R, H(K_i'), H(E_{K_i'}(M)), i, sid, EOR_j$

T：IF $(s(j,i)=H(abrt))$ THEN *retrieve abrt*

$2^{r1}.\ T\rightarrow R_j: f_{abrt}, P_{R_j}(abrt)$

T：ELSE *set* $s(j,i)=EOR_j$

$2^{r2}.\ T\rightarrow R_j: f_k, cert, i, P_{R_j}(K_i')$

$3^{r3}.\ T\rightarrow O: f_{EOR_j}, cert, i, EOR_j$

Recovery 子协议中，T 收到 R_j 的请求后，查询 R_j 第 i 轮交换的状态。如果 $s(j,i)=H(abrt)$，则说明 O 已经通过 Abort 子协议中止了与 R_j 本轮的交换，T 在消息 2^{r1} 中将保存的中止交换证据 abrt 发送给 R_j；否则，T 置 $s(j,i)=EOR_j$，将计算密钥 K_i'发送给 R_j，并将 EOR_j 发送给 O。

2.5 争议处理方案

在某些情况下，发方或收方可能要求仲裁机构处理以下两种类型的争议。

(1) 发方不可否认：当发方 O 否认曾发送了某个消息 M 给接收者 R_j 时，R_j 可以向仲裁机构出示 $NRO=(O,R,T,R_j,M,cert,i,K_i',EOO)$，仲裁机构将验证 $cert=S_T(O,R,T,sid)$和 $EOO=S_O(cert,H(K_i'),H(E_{K_i'}(M)),i)$。若两项验证均通过，仲裁机构支持接收者 R_j 的主张，否则拒绝 R_j 的主张。

(2) 收方不可否认：当接收者 R_j 否认曾经收到某个来自发方 O 的消息 M 时，O 可以向仲裁机构出示 $NRR=(O,R,T,R_j,M,cert,i,K_i',EOR_j)$，仲裁机构将验证 $cert=S_T(O,R,T,sid)$和 $EOR_j=S_{R_j}(cert,H(K_i'),H(E_{K_i'}(M)),i)$。

a) 若 R_j 能出示中止交换证据 abrt，且 $R_j\in R''$，仲裁机构拒绝 O 的主张。

b) 若 R_j 不能出示中止交换证据 abrt，且两项验证都通过，仲裁机构支持 O 的主张。

c) 若 R_j 不能出示中止交换证据 abrt，但验证不能通过，仲裁机构拒绝 O 的主张。

3 协议分析

离线 TTP：正常进行信息交换时，发方和收方使用 Ex-

(下转第 97 页)

WLAN 模型和 MANET 模型为无线网络建模与仿真提供了丰富的、多层次的支持。本文详细阐述了这些异常行为对 MANET 网络的影响。仿真实验结果表明本模型较好地刻画了相关威胁的行为。

将来的工作主要集中在进一步研究其他异常行为，如无线被动窃听以及网络灰洞等的建模和仿真；并力求把这些仿真的异常行为模块化，便于移植到真实的系统中应用。

参 考 文 献

[1] Johnson D B, Maltz D A. The dynamic source routing protocol for mobile ad hoc networks. Internet Draft, Mobile Ad Hoc Network(MANET) Working Group, IETF, Version 9, April 2003

[2] Maltz D A, Broch J, Johnson D B. Experiences designing and building a multi-hop wireless Ad hoc network testbed[R]. CMU-CS-99-116. CMU School of Computer Science, March 1999

[3] MANET. Mobile ad hoc networks (MANET) charter WG IETF, 2000

(上接第 90 页)

change 子协议，TTP 不需参与，协议支持离线 TTP。

公平性：以下分 3 种情况分析协议的公平性。

(1) 发方 O 和接收者 R_j 都诚实，则发方和收方都按照 Exchange 子协议交换消息，显然最后 R_j 得到 NRO，且 O 得到 NRR，协议公平。

(2) 发方 O 诚实而接收者 R_j 不诚实，即 R_j 不发送 EOR_j 给 O 或发送错误的 EOR_j 给 O。之后有两种可能：a) R_j 发送正确的 f_r 请求给 TTP，根据 Recovery 子协议，TTP 将发送 K_i' 给 R_j，发送 EOR_j 给 O，协议公平。b) R_j 发送伪造的 f_r 请求给 TTP，由于 EOR_j 中包含 $cert$，R_j 不可能伪造出 $cert$，因而不能发送伪造的 O，R 和 sid；又由于 EOR_j 是对 EOO 的签名，R_j 不可能伪造出 EOO，因而不能发送伪造的 $H(E_{K_i'}(M))$ 和 $H(K_i')$；若伪造 i，则会与 TTP 计算的 $H(K_i')$ 不符。因此，TTP 可以发现伪造的 f_r 请求，中止 Recovery 子协议运行，最终，由于 O 启动 Abort 子协议，R_j 得到 abrt，协议公平。

(3) 接收者 R_j 诚实而发方 O 不诚实。O 的目的是获取有效 NRR 而不提供 M，其可能的欺骗有 3 种：a) 伪造消息 1^e。若 O 伪造标识符 O，R 或 T，接收者将不会响应 O；若 O 伪造 $H(K_i')$，$H(E_{K_i'}(M))$，i 或 $cert$，由于 EOR_j 中包含这些信息，因此 O 得不到有效的接收证据。b) 伪造消息 3^e。由于消息 1^e 中有 $H(K_i')$，R_j 可以辨别出伪造的消息 3^e，转而通过 TTP 获得对称密钥 K_i'，协议公平。c) 不发送消息 3^e，并请求 TTP 中止与 R_j 的交换。根据 Abort 子协议，R_j 将得到 abrt，协议公平。

时限性：协议允许发方 O 启动 Abort 子协议中止交换，允许接收者 R_j 启动 Recovery 子协议通过 TTP 完成交换，且协议的各参与方在任何状态时中止协议运行都不影响协议公平性，因此协议满足时限性。

机密性：(1) Exchange 子协议使用群加密机制发送密钥 K_i'，Recovery 子协议使用接收者公钥加密 K_i' 后发送，所以监听者得不到 K_i'，不能获得 M。(2) 发方和收方与 TTP 通信时，仅发送 $H(E_{K_i'}(M))$ 而没有直接发送密文，虽然 TTP 可以计算出 K_i'，但由于 TTP 没有动机去监听获得的密文，因此 TTP 没有得到 M。(3) R 采用 $(P_{R_1}(R_1), P_{R_2}(R_2), \cdots)$ 的结构，已经获得 M 的 R_i 得不到其他参与方 R_j 的标识符，不能将 M 泄漏给 R_j。(4) 协议采用双密钥链结构，接收者得到第 i 轮交换的密钥 K_i'，不能计算出其它轮的密钥。因此，协议满足机密性。

结束语 本文提出了一种基于密钥链的多方非否认协议。协议采用双密钥链结构，支持离线 TTP，满足公平性、时效性和机密性。在同一组用户进行多轮信息交换时，协议可有效减轻 TTP 存储负担。本文对协议进行了非形式化的分析。下一步的研究，将考虑利用串空间理论或其它工具对非否认协议的安全属性进行形式化分析。

参 考 文 献

[1] Zhou J, Gollmann D. A fair non-repudiation protocol[C]// Proceedings of the 1996 IEEE Symposium on Security and Privacy. Oakland, 1996: 55-61

[2] Wang G. Generic non-repudiation protocols supporting transparent off-line TTP[J]. Journal of Computer Security, 2006, 14(5): 441-467

[3] Cederquist J, Dashti M T, Mauw S. A Certified Email Protocol Using Key Chains[C]// Advanced Information Networking and Applications Workshops(AINAW '07). 21st International Conference. 2007: 525-530

[4] Liang X, Cao Z, Lu R, et al. Efficient and secure protocol in fair document exchange[J]. Computer Standards & Interfaces, 2008, 30(3): 167-176

[5] Permpoontanalarp Y, Kanokkanjanapong J. Dynamic Undeniable Fair Certified Email with DDoS Protection[C]// Advanced Information Networking and Applications. Okinawa, 2008

[6] Kremer S, Markowitch O. A multi-party non-repudiation proto-co[C]//15th International Conference on Information Security. IFIP World Computer Congress. Beijing, China, 2000: 271-280

[7] Markowitch O, Kremer S. A Multi-party Optimistic Non-repudiation Protocol[C]// Information Security and Cryptology-ICISC 2000: Third International Conference. Seoul, Korea: Spinger-Verlag, 2001: 109-122

[8] Onieva J A, Zhou J, Lopez J. Non-repudiation protocols for multiple entities[J]. Computer Communications, 2004, 27(16): 1608-1616

[9] Zhou J, Onieva J, Lopez J. Optimized multi-party certified email protocols[J]. Information Management and Computer Security, 2005, 13(5): 350-366

[10] Wang H, Wang R. Improvement of a multi-party certified email protocol[J]. Chinese Journal of Electronics, 2007, 16(4): 613-616

[11] Gurgens S, Rudolph C, Vogt H. On the security of fair non-repudiation protocols[J]. International Journal of Information Security, 2005, 4(4): 253-262