线性拓扑结构的乐观认证邮件

郭利娟 吕晓琳

(西安电子科技大学数学与统计学院 西安 710071)

摘 要 目前的乐观认证邮件大多是环形拓扑结构、星型拓扑结构、网型拓扑结构及这3种拓扑结构的混合结构,在实际应用中会出现需要按顺序接收认证邮件的情况。目前只有Asoken提出的网型拓扑结构的公平交换协议适用于线性拓扑结构的乐观认证邮件。针对这种情况,提出一种新的n方线性拓扑结构乐观认证邮件协议,利用高效的签密方案实现签名和消息认证。本方案在n方都是诚实的情况下仅需传递$4(n-1)$次信息,在最坏情况下需传递$8n-4$次信息,与Asoken线性认证邮件(在n方诚实的情况下需传递$4n(n-1)$次信息,最坏情况下需传递$8n^2-n-10$次信息)相比,效率得到大幅提升。此外,提出通过时间认证来验证消息的新鲜性。分析表明,所提协议具有公平性和不可否认性。

关键词 线性拓扑结构,签密,认证邮件,公平性,不可否认性

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.08.028

Optimistic Certified Email for Line Topology

GUO Li-juan LV Xiao-lin

(School of Mathematics and Statistics, Xidian University, Xi'an 710071, China)

Abstract Most of optimistic certified emails are of ring topology, star topology, mesh topology and the hybrid structure of these three topologies. In practice, the certified email will be collected in order. At present, only the fair exchange protocol for mesh topology put forward by Asoken can be applied to certified email for line topology. Based on this situation, this paper proposed a new multi-party certified email protocol for line topology by using an efficient signcryption scheme for signature and message authentication. The scheme only needs $4(n-1)$ passes in all multi-party honest and $8n-4$ passes in the worst case. The efficiency of scheme is much better than Asoken's certified mail for line topology (the scheme needs $4n(n-1)$ passes in all multi-party honest and $8n^2-n-10$ passes in the worst case). Besides, the freshness of messages can be verified by timestamp. The analysis shows that the protocol is fair and non-repudiation.

Keywords Line topology, Signcryption, Certified email, Fairness, Non-repudiation

1 引言

认证邮件与普通邮件有很大的区别,它是发送方将邮件或邮件相关内容与接收方收到的邮件或邮件相关内容的证据进行交换。认证邮件协议应满足公平性、不可否认性、保密性、有效性和时效性等性质;特别地,为了满足最基本的公平性,协议中基本都会用到可信第三方(TTP)。TTP通常分为在线和离线两种,因为在线TTP参与协议的整个过程,导致计算和通信的复杂度增加,因此大多数认证邮件协议采用离线的TTP[2,4-5,7-13,15-16,18,20],也称乐观TTP,即TTP只在参与方接收发生异常时才将参与协议的认证邮件称为乐观认证邮件。所有参与者线性排列且只能与相邻参与者传递信息的结构被称为线性拓扑结构。按线性结构传递和接收信息的乐观认证邮件被称为线性拓扑结构的乐观认证邮件。

由于认证邮件广泛存在,因此有必要对其进行深入研究,如文献[3]首先针对两个参与者的情况,之后拓展到三方参与者以及多方参与者。Markowith和Kremer首次提出多方认证邮件协议,在文献[19]中使用在线TTP,在文献[20]中使用离线的TTP,但协议的效率均不高。Ferrer-Gomila[7]提出的多方认证邮件协议效率较高,但不能抵抗共谋攻击。Zhou等[11]改进了Ferrer-Gomila的协议,克服了其不能抵抗共谋攻击的缺陷。Min-Hua等[12]提出了一些攻击认证邮件的方式,并提出使用timestamp和加密ID来抵抗这些攻击。当前也有许多对合同签署协议的研究。文献[8]研究了适用于各种拓扑结构的合同签署协议,但由于认证邮件是非对称的,只有当接收方收到邮件或邮件的相关内容后才会给发送方收据,而多方合同签署协议是同时交换信息的,因此大多数的合同签署协议不能直接应用于认证邮件协议中。Asoken等[18]提出了一种网型结构的交换协议,该协议也适用于线性认证邮件,但它的计算量较大,在n方都是诚实的情况下需要传递$4n(n-1)$次信息,在最坏情况下需要传递$8n^2-n-10$次信息。王彩芬等[16]提出星型拓扑结构的多方认证邮件协议,其

到稿日期:2017-01-13 返修日期:2017-03-30

郭利娟(1991-),女,硕士,主要研究方向为信息安全与公平交换协议等,E-mail:lijuanguo16@163.com(通信作者);**吕晓琳**(1990-),女,硕士,主要研究方向为信息安全与基于格的签名等。

利用签密同时实现了加密和签名的功能。文章提出 n 可以是不固定的,但使用广播的方式给接收方发送信息时,网络的延迟是无界的,因此并非所有的接收者都能收到广播的信息,必须请求 TTP,这增加了 TTP 的负担。文献[4]提出一个 3 方的线性拓扑的认证邮件协议,但没有把它拓展为 n 方,导致其应用范围受限。文献[4,7,16,18-20]提出的协议都不具有时间认证性。研究发现,采用组签密可以有效地把 3 方拓展为 n 方,同时满足时间认证性。

本文提出了一个多方线性拓扑结构的认证邮件,方案具有以下特点:1)将文献[4]的 3 方拓展为 n 方,扩大了协议的应用范围,采用组签密方案,实现了加密和签名的功能,相比于文献[4]中使用的签名再加密的方式,计算量更小、效率更高;2)应用于线性认证邮件时,本文协议相比文献[18]提出的网型拓扑结构的交换协议,计算量减小了很多,本文方案在 n 方都诚实且无网络错误的情况下仅需传递 $4(n-1)$ 次信息,在最坏情况下仅需传递 $8n-4$ 次信息;3)本文按顺序传输信息,相比于文献[16]中采用的广播技术,减轻了 TTP 的负担;4)第一轮收到与 m 相关的 M,第二轮解密得到 m,通过验证 $M=hash(m)$是否成立,避免了无法确认收到的 m 的正确性的缺陷;5)所提协议具有时间认证性,参与者能够将收到邮件的时间与发送邮件的时间进行对比,以验证邮件的新鲜性。

2　预备知识

2.1　认证邮件需要满足的性质

公平性:协议结束后,所有参与者都收到渴望的信息,或所有的参与者都没有收到

不可否认性:协议结束后,所有人都不能否认参加了协议,也不能否认发送或接收到邮件。

保密性:只有参加协议的接收方和发送方知道邮件的具体内容(当发生争议涉及 TTP 时,TTP 也知道邮件内容)。

有效性:在认证邮件协议中,所有参与方只要行为正确,都能得到各自想要的信息。

时效性:所有参与者都可以确定协议执行的时间是有限的,且无论协议何时结束,对所有的参与者都是公平的。

时间认证:所有的参与者都能获得邮件发送的时间证据。

2.2　认证邮件的模型和概念

协议中的参与者:邮件的发送者 P,要发送的邮件 m,邮件的接收者 $P_1,P_2,\cdots,P_n$,可信第三方 TTP。其中的 $P,P_1,P_2,\cdots,P_n$ 按顺序接收和传递信息。P 想发送邮件 m 给 P_i,$i\in\{1,2,\cdots,n\}$,而 P_i 想要得到邮件的内容。由于邮件 m 具有很重要的信息,P 需要与 P_i 收到该消息的证据进行交互。为防止敌手拿到信息后可以直接读取,信息都以密文的形式传输,P 收到的收据是对邮件相关信息的签名。发送者和接收者或许是诚实的,他们都能正确执行协议;或许是不诚实的,会背离协议。假设参与者和参与的顺序是提前固定的,所有的参与者都知道其他参与者的公钥。

对通信信道做一般性假设:由于异步通信模型不需要相同的全球钟,假设 P 与 P_1,P_i 与 P_j 之间的通信信道是异步信道,通信过程中会由于网络故障或敌手的攻击而丢失信息;假设 P 与 TTP,P_i 与 TTP 之间的通信信道是弹性信道,即信息经过有限时间的延迟后,最后都到达接收者;在异步信道,敌手能够窃取并篡改信息。

本文使用到线性拓扑结构:发送者 P 开始发送一个或多个信息给 P_1,P_1 将信息顺序发送给 $P_2,\cdots,P_{n-1},P_n$,P_n 按相反的顺序将信息发送给 $P_{n-1},\cdots,P_1,P$。线性拓扑结构如图 1 所示。

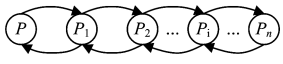

图 1　线性拓扑结构

Fig. 1　Line topology

乐观认证邮件协议由 3 部分组成:交换协议,Abort 子协议和 Recovery 子协议。如果发送者和接收者都正确执行协议且没有网络错误,此时只需要执行交换协议,不涉及可信第三方 TTP。当发送者没有收到信息或收到的信息不能通过验证时,可以请求 Abort 子协议;当接收者没有收到信息或收到的信息不能通过验证时,可以请求 Recovery 子协议。我们的协议满足认证邮件需要满足的性质:公平性、不可否认性、保密性、有效性、时效性和时间认证性。

协议中假设签名是不可伪造的,同时是基于离散对数困难问题的。约定以下符号:p 表示大素数;q 表示 $p-1$ 的大素因子;g 表示 z_p^* 中阶为 q 的元;$hash$ 表示单向 hash 函数;KH 表示有钥的单向 hash 函数;(E,D)表示对称加、解密算法;$sign_i(\cdot)$表示接收方 P_i 对信息的签名;$sign_T(\cdot)$表示可信第三方 TTP 对信息的签名;$sign_P(\cdot)$表示发送者 P 对信息的签名;y_a,x_a 分别表示 P 的公钥和私钥,满足 $y_a=g^{x_a} \bmod p,x_a,y_a\in Z_q^*$;$y_i,x_i$ 分别表示 P_i 的公钥和私钥,满足 $y_i=g^{x_i} \bmod p,x_i,y_i\in Z_q^*$;$y_T,x_T$ 分别表示 TTP 的公钥和私钥,满足 $y_T=g^{x_T} \bmod p,x_T,y_T\in Z_q^*$;$m$ 是发送的邮件,$M=hash(m)$。

签密过程:

P 做如下计算:

随机选取 $x\in z_q^*$,$k_i=hash(y_i^x \bmod p)$,$k_T=hash(y_T^x \bmod p)$,$r_i=KH_{k_i}(c_i,M)$,$c_i=E_{k_i}(M)$,$m'=E_{k_i}(m,timestamp)$,$m''=E_{k_T}(m,timestamp)$,$s=x/(r_1r_2\cdots r_n+x_a)$。$P$ 发送$(c_1,\cdots,c_n,r_1,\cdots,r_n,s,M)$给 P_1。

P_i 做如下计算:

$y=(y_ag^{r_1r_2\cdots r_n})^s \bmod p$,$k_i=hash(y^{x_i} \bmod p)$,$M=D_{k_i}(c_i)$,$m=D_{k_i}(m')$

P_i 接收签名当且仅当:

$r_i=KH_{k_i}(c_i,M)$,$hash(m)=M$

TTP 做如下计算:

$y=(y_ag^{r_1r_2\cdots r_n})^s \bmod p$,$k_T=hash(y^{x_T} \bmod p)$,$m=D_{k_T}(m'')$

3　线性结构的异步乐观认证邮件

该协议是将一份邮件发送给多个接收者的认证邮件协议。在第一轮中,发送者给接收者发送信息,接收者按特定的顺序传递信息。在每一次传递中,每一个参与者利用后面相邻者的公钥加密信息,同时用自己的私钥对 $timestamp$ 签名;接收者能够验证消息是谁传递的,同时能将解密后的 $timestamp$ 与当前的时间进行比较,还能够验证信息的发送方是否为 P。在第一轮,发送方 P 收到每个接收方对信息 M 和 $timestamp$ 的签名,说明每个接收者都愿意参与协议,接收方 P_i 收到与邮件 m 相关的消息 M。在第二轮,P 收到想要的目

标收据，P_i 得到邮件内容，且能够利用 M 验证收到的邮件内容是否真实。理想情况下，线性拓扑结构的乐观多方认证邮件的交换协议如下所示：

$r=1$

$P\rightarrow P_1$

$E_{y_1}(c_1,\cdots,c_n,r_1,\cdots,r_n,s,M,sign_P(timestamp))$

$P_i\rightarrow P_{i+1}$

$E_{y_{i+1}}(c_1,\cdots,c_n,r_1,\cdots r_n,s,M,sign_i(timestamp))$

$P_n\rightarrow P_{n-1}$

$sign_n(M,timestamp)$

$P_{i+1}\rightarrow P_i$

$sign_{i+1}(M,timestamp),\cdots,sign_n(M,timestamp)$

$P_1\rightarrow P$

$sign_1(M,timestamp),\cdots,sign_n(M,timestamp)$

$r=2$

$P\rightarrow P_1$

$E_{y_1}(m'=E_{k_i}(m,sign_P(timestamp)))$

$P_i\rightarrow P_{i+1}$

$E_{y_{i+1}}(m'=E_{k_i}(m,sign_i(timestamp)))$

$P_{i+1}\rightarrow P_i$

$sign_{i+1}(m',timestamp),\cdots,sign_n(m',timestamp)$

$P_1\rightarrow P$

$sign_1(m',timestamp),\cdots,sign_n(m',timestamp)$

由于网络问题或敌手窃取并篡改信息，参与者可能接收不到信息或收到的信息不能通过验证。为了保证每个参与者的利益，P 接收不到信息或收到的信息不能通过验证时，请求 Abort 子协议；P_i 接收不到信息或接收到的信息不能通过验证时，请求 Recovery 子协议。

3.1 P 的 Abort 子协议

原则 1　在第一轮，P 如果决定终止协议，则向 TTP 发送 $Abort,sign_P(timestamp)$。TTP 验证消息，若验证通过，则发送 $Abort,sign_T(timestamp)$给 P 和 P_i；若不能通过验证，则要求重发或忽略。

原则 2　在第一轮，P 如果未收到 P_1 的消息，则向 TTP 发送$(c_1,\cdots,c_n,r_1,\cdots,r_n,s,M),sign_P(M,timestamp)$。TTP 验证消息，若验证通过，则进行检索，若检索到 $P_i(i\in\{1,2,\cdots,n\})$对 M 的签名，则发送 $sign_1(M,timestamp),\cdots,sign_n(M,timestamp),sign_T(M,P,timestamp)$给 P；若未检索到所有的 $P_i(i\in\{1,2,\cdots,n\})$对 M 的签名，则发送 $Abort,sign_T(timestamp)$给 P 和 P_i。

原则 3　在第二轮，P 如果未收到 P_1 发送的消息，则向 TTP 发送 $m'=E_{k_i}(m,timestamp),m''=E_{k_T}(m,timestamp),(c_1,\cdots,c_n,r_1,\cdots,r_n,s,M),sign_p(m',timestamp)$。TTP 验证并计算 m 与 M 是否匹配，若验证和匹配通过，则进行检索，若检索成功，则发送 $sign_1(m',timestamp),\cdots,sign_n(m',timestamp),sign_T(m',P,timestamp)$给 P；若未检测到所有的收据，则发送 $sign_i(m',timestamp),sign_j(m',timestamp),sign_n(m',timestamp),sign_T(m',P,\{P_k\},k\neq i,\cdots,j,timestamp)$给 P；若 TTP 验证和匹配均不成功，则要求重发或忽略信息。

原则 4　在第一轮，若 P 收到的信息不能通过验证，则 P 向 TTP 请求终止协议。在第二轮，若 P 收到 P_1 的消息，但有的消息未通过验证，则 P 发送未通过验证的收据 $sign_i(m',timestamp),\cdots,sign_j(m',timestamp),sign_P(m',timestamp)$给 TTP，若仍未通过 TTP 的验证，则 TTP 发送 $sign_T(P_i,\cdots,P_j,P,timestamp)$给 $P(P_i,\cdots,P_j$ 表示收据未通过验证的接收者)。

3.2 P_i 的 Recovery 子协议

原则 1　在第一轮，P_1 如果未收到 P 的信息，则向 TTP 发送请求 $sign_1(timestamp)$。TTP 验证消息，若验证通过，则发送 $Abort,sign_T(timestamp)$给 P 和 P_i；若验证不能通过，则要求重发或忽略。

原则 2　在第一轮，P_i 如果未收到 P_{i-1} 的消息，则向 TTP 发送 $sign_i(timestamp)$。TTP 验证消息，若验证通过，则检索并发送$(c_1,\cdots,c_n,r_1,\cdots,r_n,s,M),sign_T(timestamp,P_i,M)$给 P_i；若检索不成功，则发送 $Abort,sign_T(timestamp)$给 P 和 P_i。若验证不能通过，TTP 要求重发或忽略。

原则 3　在第二轮，P_i 如果未收到 P_{i-1} 的消息，则向 TTP 发送$(c_1,\cdots,c_n,r_1,\cdots,r_n,s,M)$。$sign_i(M,timestamp)$，TTP 验证收到的消息，若验证通过，则检索并发送 $m'=E_{k_i}(m,timestamp),sign_T(m',P_i,timestmp)$给 P_i；若验证不能通过，TTP 要求重发或忽略。

原则 4　若 P_1 收到 P 的信息，但未通过验证，则 P_1 要求 P 重发或忽略；若 P_i 收到 P_{i-1} 的信息，但未通过验证，在第一轮，P_i 要求 P_{i-1} 重发或忽略，在第二轮，P_i 向 TTP 发送$(c_1,\cdots,c_n,r_1,\cdots,r_n,s,M),m'=E_{k_i}(m,timestamp),sign_i(m',timestmp)$，TTP 验证消息，若验证仍未通过，则 TTP 检索信息，并发送 $m'=E_{k_i}(m,timestamp),sign_T(m',P_i,timestmp)$给 P_i。

4 安全性分析

4.1 公平性分析

如果协议中各参与方都诚实，则只需要执行交换协议，在交换协议中 P 得到目标收据，P_i 得到邮件的内容。即使敌手窃取到信息，由于第一轮传送的 $E_{y_{i+1}}(c_1,\cdots,c_n,r_1,\cdots,r_n,s,M,sign_i(timestamp))$和第二轮传送的 $E_{y_{i+1}}(m'=E_{k_i}(m,sign_i(timestamp)))$都是密文，敌手也无法获得邮件内容；同时基于假设，签名是不可伪造的，敌手无法冒充 P 和 P_i 发送消息，这对所有参与者都是公平的。

对于发送者，若 P 在第二轮试图欺骗，发送的消息与真实的邮件内容 m 不同，如发送 $m_1'=E_{k_i}(m_1,timestamp)$给 P_1，但 P_1 验证时发现 $hash(m_1)\neq M$，则 P_1 拒绝接收信息。对于其他的接收者 $P_i,i\in\{2,3,\cdots,n\}$，若请求 TTP，由于检索得到的邮件内容仍为 $m_1'=E_{k_i}(m_1,timestamp),P_i,i\in\{2,3,\cdots,n\}$，因此 TTP 拒绝接收信息。最后，发送方 P 没有得到收据，接收方没有得到邮件内容，满足公平性。

若 P 与敌手 C(参与者之外的人)合谋试图欺骗 P_i，C 充当发送者来骗取接收者的收据，由于参与者固定，接收者对接收到的信息仍使用 P 的公钥进行验证，此时不能通过验证，P_i 拒绝接收信息，则 P 得不到收据，P_i 得不到邮件内容，满足公平性。

若 P 与接收者合谋，如果 P 与 P_1 合谋，不发送信息给 P_2，则 TTP 检索不到$(c_1,\cdots,c_n,r_1,\cdots,r_n,M)$或 $m'=E_{k_i}(m,timestamp)$，此时其会发送 $Abort,sign_T(timestamp)$给 P 和 P_i；如果 P 与 P_1 合谋发送错误的信息$(c_1',\cdots,c_n',r_1',\cdots,$

r_n',s,M)或 $m_1'=E_{k_i}(m_1,timestamp)$给 P_2,则 P_2 因消息不能通过验证而拒绝接收。如果 P 与 P_i 合谋不发送信息给 P_{i+1},由于协议的执行时间有限,正常情况下 P_{i+1}会在某时间段 t 内收到信息,但若经过时间 $2t$ 后仍未收到发送的信息,则可以请求 TTP。P_{i+1} 的请求通过验证后,TTP 检索得到(c_1,…,c_n,r_1,…,r_n,s,M)或 $m'=E_{k_i}(m)$,会发送(c_1,…,c_n,r_1,…,r_n,s,M),$sign_T(M,P_i,timestamp)$或 $m'=E_{k_i}(m,timestamp)$,$sign_T(m',P_i,timestamp)$给 P_{i+1};如果 P 与 P_i 合谋发送错误的信息(c_1',…,c_n',r_1',…,r_n',s,M)或 $m'=E_{k_i}(m_1,timestamp)$,$m_1'=E_{k_i}(m1,timestamp)$给 P_{i+1},则 P_{i+1}因消息不能通过验证而拒绝接收。因此,如果发送方 P 与 P_1 合谋,P 得不到收据,接收方 P_i 也得不到邮件内容,满足公平性;如果 P 与 P_i 合谋不发送信息给 P_{i+1},P_{i+1}通过请求 TTP 可以得到邮件内容;若合谋发送错误的信息,P 得不到目标收据,P_{i+1}得不到邮件内容,即或者都能得到各自想要的信息,或者都得不到,满足公平性。

对于接收者,若接收者 P_i 与敌手 C(参与者之外的人)合谋试图欺骗,P_i 接收到(c_1,…,c_n,r_1,…,r_n,s,M)或 $m'=E_{k_i}(m,timestamp)$后不再执行协议,将信息(c_1,…,c_n,r_1,…,r_n,s,M)或 $m'=E_{k_i}(m,timestamp)$发送给 C,此时 C 充当 P_i 执行协议。若 C 发送错误的信息(c_1',…,c_n',r_1',…,r_n',s,M)或 $m_1'=E_{k_i}(m_1,timestamp)$,后面的接收者收到的信息不能通过验证,拒绝接收信息;若 C 发送正确的(c_1,…,c_n,r_1,…,r_n,s,M)或 $m'=E_{k_i}(m,timestamp)$,后面的接收者收到的信息可以通过验证,但 P 收到 C 对 M 或 m'的签名后,不能通过验证,P 请求 TTP 取消协议,或 P 请求 TTP,得到 TTP 的签名,满足公平性的要求。

若接收者 P_i,P_j 合谋,例如 P_2,P_3 合谋,若在第一轮中 P_2 接收到信息后 P_3 拒绝执行协议,则后面的接收者可以通过请求 TTP 得到(c_1,…,c_n,r_1,…,r_n,s,M),$sign_T(timestamp,P_i,M)$。若 P 没有收到 P_3 对 M 的签名请求 TTP,TTP 由于检索不到 P_3 的签名,因此给所有的参与者发送 $Abort$,$sign_T(timestamp)$。若在第二轮,P_2 接收到信息后 P_3 拒绝执行协议,后面的接收者则可以通过请求 TTP 得到 $m'=E_{k_i}(m,timestamp)$,$sign_T(m',P_i,timestamp)$。若 P 没有接收到 P_3 对 m'的签名请求 TTP,TTP 检索不到 P_3 的签名,发送 $sign_T(P,\{P_3\},m',timestamp)$给 P,P 得到 TTP 的证据,证明 P_3 获得了邮件的内容,满足公平性的要求。

Zhou 等[11]提出接收者找不到 TTP 的攻击,而本文方案能够有效抵抗这种攻击。第一轮,若某个接收者收不到信息或收到的信息不能通过验证,因为找不到 TTP,发送者得不到该接收者对 M 的签名,同时发送者也无法确定该接收者是否愿意参与协议;第二轮,若某个接收者收不到信息或收到的信息不能通过验证,因为找不到 TTP,发送者也无法得到该接收者的收据,这对接收者是公平的。

4.2　不可否认性分析

若 P 否认发送过邮件 m,但接收者 $P_i(i\in\{1,\cdots,n\})$声称接收到了 P 发送的邮件 m,此时 P_i 发送(c_1,…,c_n,r_1,…,r_n,s,M),$m'=E_{k_i}(m,timestamp)$,$sign_P(timestamp)$或(c_1,…,c_n,r_1,…,r_n,s,M),$m'=E_{k_i}(m,timestamp)$,$sign_T(m',P_i,timestamp)$,$sign_P(timestamp)$给仲裁,仲裁验证。

1)m 是否与 M 匹配为 $M=hash(m)$。

2)验证签名 $sign_P(timestamp)$是否为 P 的签名,并检验 $sign_P(timestamp)$,$m'=E_{k_i}(m,timestamp)$的时间是否为一前一后。

3)签名对信息的签名(m',P_i,$timestamp$)是否为 TTP 的签名。若验证通过,则 P_i 获胜,说明 P 试图欺骗,反之亦然。若 P 声称收到 $P_i(i\in\{1,\cdots,n\})$的收据,但 P_i 否认接收到邮件,P 发送(c_1,…,c_n,r_1,…,r_n,s,M),$m'=E_{k_i}(m,timestamp)$,$sign_i(M,timestamp)$,或涉及到第三方时还需要验证 $sign_T(M,P,timestamp)$,$sign_T(m',P,timestamp)$或者 $sign_T(m',\{P_k\},k\neq i,\cdots,j,timestamp)$给仲裁,仲裁验证。

①m 是否与 M 匹配为 $M=hash(m)$。

②验证签名 $sign_i(M,timestamp)sign_i(m',timestamp)$是否为 P_i 签名,且两次的签名是否是同一个人,并且对比两次签名的时间是否为一前一后。

③验证对信息 $M,timestamp,m',timestamp,m',\{P_k\},k\neq i,j,timestamp$ 的签名是否为 TTP 的签名,且为同一个 TTP,并对比两次签名的时间是否为一前一后。

4.3　其他性质的分析

保密性:整个协议中的信息是以密文的形式传输的,参与者通过解密能得到各自想要的信息,敌手即使窃取得到信息,也无法解密得到邮件内容。当涉及 TTP 时,TTP 也知道邮件的内容,可验证 m 与 M 是否满足 $M=hash(m)$。除此之外,无人知晓邮件的内容。

有效性:协议中只要所有参与者的行为正确,即使网络传输出现问题,参与者也可以通过请求可信第三方来得到各自想要的信息。

时效性:所有参与者都知道协议执行的时间是有限的,正常情况下诚实者会在某时间段 t 内收到信息,但若经过时间 $2t$ 后仍未收到发送的信息,则可以请求 TTP 得到想要的信息。

时间认证性:协议中所有的参与者在发送信息时都会发送对时间戳的签名,接收者利用收到的对时间戳的签名来验证信息是否新鲜。

4.4　效率分析

在应用线性结构认证邮件时,Asoken 的协议在 n 方都诚实的情况下需传递 $4n(n-1)$次信息,在最坏情况下需传递 $8n^2-n-10$ 次信息;本文方案在 n 方都诚实的情况下只需执行交换协议,传递 $4(n-1)$次信息,在最坏情况下每一轮每一个参与者都与 TTP 接触,需传递 $8n-4$ 次信息。此外,本文采用了签密方法,同时实现了加密和验证,减少了计算量,提高了效率。

结束语　认证邮件协议是一种公平交换协议,设计高效且安全的认证邮件协议在实际应用中具有非常重要的意义。本文采用文献[6]的组签密方案,提出 n 方线性拓扑结构的乐观认证邮件协议。在较弱通信信道的假设条件下,所提协议能够抵抗共谋攻击、重放攻击和接收者找不到 TTP 的攻击等;同时,该协议有较高的效率,在实际应用中适用于任何一对多按顺序发送信息的情况。但该协议不满足参与者匿名的性质,而且在交易过程中参与者需要进行多次签名和对协议做进一步的优化,未来将改进基于签密的拓扑结构的公平交换协议,尝试将多种密码协议和各种拓扑结构相结合,以提高协议的效率,同时拓宽拓扑结构认证邮件在实际生活中的应用范围。

(下转第 173 页)

田鹤，赵海. 基于软件加权网络的软件结构复杂性度量[J]. 计算机科学，2016，43(S2)：506-508.

[4] WANG L，WANG Z，YANG C，et al. Linux kernels as complex networks：A novel method to study evolution[C]// IEEE International Conference on Software Maintenance. IEEE，2009：41-50.

[5] VASA R，SCHNEIDER J G，NIERSTRASZ O. The inevitable stability of software change[C]// IEEE International Conference on Software Maintenance. DBLP，2007：4-13.

[6] SHEN P T，CHEN L Y. Complex network analysis in Java application systems[J]. Journal of East China Normal University Natural (Natural Science)，2017(1)：38-51. (in Chinese)
沈娉婷，陈良育. Java 应用系统的复杂网络分析[J]. 华东师范大学学报(自然科学版)，2017(1)：38-51.

[7] MYERS C R. Software systems as complex networks：structure，function，and evolvability of software collaboration graphs[J]. Physical Review E，2003，68(4)：046116.

[8] BARABÁSI A L，ALBERT R. Emergence of scaling in random networks[J]. Science，1999，286(5439)：509-512.

[9] 汪小帆，李翔，陈关荣. 网络科学导论[M]. 北京：高等教育出版社，2012：81-293.

[10] NEWMAN M E J，WATTS D J. Renormalization group analysis of the small-world network model[J]. Physics Letters A，1999，263(4-6)：341-346.

[11] CLAUSET A，SHALIZI C R，NEWMAN M E J. Power-Law distributions in empirical data[J]. Siam Review，2007，51(4)：661-703.

[12] WATTS D J，STROGATZ S H. Collective dynamics of 'small-world' networks[J]. Nature，1998，393(6684)：440-442.

[13] LOVROŠUBEL J，BAJEC M. Software systems through complex networks science：review，analysis and applications[C]// International Workshop on Software Mining. 2012：9-16.

(上接第 159 页)

参 考 文 献

[1] ALOIS P，TATJANA W. A universal system for fair n-onrepudiable certified mail without a trusted third party [J]. Computers & Security，2013，32(1)：207-218.

[2] GAO Y X，PENG D Y，YAN L L. Design and formal analysis of a new fair multi-party certified mail protocol[C]// Proeedings of the Ninth International Conference on Machine Learning and Cybernetic. 2010：3101-3106.

[3] EVEN S，GOLDREICH O，LEMPEL A. A randomized protocol for signing contacts[J]. Communications of the ACM，1985，28(6)：637-647.

[4] YOSHIAKI S，MASAKATU M，MASAMIM，et al. At-hree-party optimistic certified email protocol using very-fiably encrypted signature scheme for line topology[C]// IEEE 2nd International Conference on Cyber Security and Cloud Computing. 2015.

[5] KYIKYI M，EIEI K. A fair certified email protocol with message confidentiality[C]// International Conference on Advances in Engineering and Technology(ICAET'2014). 2014：29-30.

[6] SEO M，KIM K. Electronic funds transfer protocol using domain verifiable signcryption scheme[C]// Proceedings of Information Security and Cryptology. Springer Berlin Heidelberg，2000：269-277.

[7] FERRER-GOMILA J L，PAYERAS-CAPELLÁ M，HUGUET-ROTGER L，et al. A realistic protocol for multi-party certified electronic mail[C]// Proceedings of 2002 Information Security Conference. 2002：210-219.

[8] DRAPER-GILL G，FERRER-GOMILA J L，HINAREJOS M F，et al. On the efficiency of multi-party contract signing protocols [M]// Information Security. Springer International Publishing，2015：227-243.

[9] HANDAN K，ALPTEKIN K. Optimally efficient multi-party fair exchange and fair secure multi-party computation[C]// Cryptographers' Track at the RSA Conference. Springer，Cham，2015：330-349.

[10] ONIEVA J，ZHOU J Y，LOPEZ J. Enhancing certified email service for timeliness and multicast[C]// 4th International Network Conference. Plymouth，UK，2004：327-336.

[11] ZHOU J Y. On the security of a multi-party certified e-mail protocol[C]// 2004 International Conference on Information and Communications Security. Malaga，Spain，2004：1040-1052.

[12] SHAO M H，WANG G L，ZHOU J Y. Some common attacks against certified mail protocol and the Countermeasures[J]. Computer Communications，2006，29(15)：2759-2769.

[13] HWANG R J，LAI C H. Provable fair document exchange protocol with transaction privacy for e-commerce [J]. Symmetry，2015，7(2)：464-487.

[14] CORETTI S，GARAY J，HIR T M，et al. Constant-round asynchronous multi-party computation based on one-way functions [C]// International Conference on the Theory & Application of Cryptology & Information Security. 2016：998-1021.

[15] GAO Y X，PENG D Y，TANG P Z. A formal analysis method for optimistic fair exchange protocol [J]. International Journal of Convergence lnformation Technology，2013，8(3)：35-46.

[16] WANG C F，JIA A K，LIU J L，et al. Mult-iparty certified mail protocol based on signcryption[J]. Electronic Journal，2005，33(11)：2070-2073. (in Chinese)
王彩芬，贾爱库，刘军龙，等. 基于签密的多方认证邮件协议[J]. 电子学报，2005，33(11)：2070-2073.

[17] GAO Y X，PENG D Y，YAN L L. Security analysis and improvement of certified email protocol [J]. Journal of University of Electronic Science and Technology of China，2013，42(2)：300-305. (in Chinese)
高悦翔，彭代渊，闰丽丽. 认证邮件协议的安全性分析与改进[J]. 电子科技大学学报，2013，42(2)：300-305.

[18] ASOKAN N，SCHUNTER M，WAIDNER M. Optimistic protocols for multi-party fair exchange [J]. Biotechniques，1996，37(1)：72-88.

[19] KREME R，MARKOWITCHOS. A multi-party onrepu-diation Protocol[C]// 15th IFIP International Information Security Conference. 2000：271-280.

[20] MARKOWITCHO，KREMER S. A multi-party optimistic non-repudiation protocol[M]// Information Security and Cryptology—ICISC 2000. 2000：109-122.