基于扩展CS逻辑的非否认协议形式化分析方法

王 鹃 刘 珺 张焕国
(武汉大学计算机学院 武汉 430072)

摘 要 将基于知识逻辑的CS逻辑系统用于分析具有时限性的非否认协议,针对非否认协议的性质对CS逻辑进行了扩展,给出了描述和分析非否认性以及公平性的方法,并使用扩展后的逻辑对改进的ZG协议进行了分析。在分析过程中,发现了该协议存在对签名的重放攻击漏洞,不满足强非否认性。验证过程也表明,扩展后的CS逻辑能够有效地描述和分析具有时限性的非否认协议的安全性质。

关键词 非否认协议,CS逻辑,时限性,非否认性,公平性

Extended CS Logic for Analyzing Non-repudiation Protocols

WANG Juan LIU Jun ZHANG Huan-guo
(Computer School, Wuhan University, Wuhan 430072, China)

Abstract This paper presented an extension of CS logic which is a type of knowledge logic and can be used to analyze the properties of non-reputation protocols with timeliness. Using the extended logic, we proved the improved ZG protocol and found a reply attack on signature message of the protocol. As a result, it is not satisfied with non-repudiation property. The example shows the non-reputation protocols with timeliness can be effectively analyzed by the extended CS logic.

Keywords Non-repudiation protocol, CS logic, Timeliness, Non-reputation, Fairness

1 引言

非否认协议是一类通过数字签名技术来防止通信实体对通信事件抵赖行为的协议,可用于认证电子邮件、电子支付和电子合同中,实现非否认服务。非否认协议必须满足两个基本属性:非否认性和公平性,此外,考虑到时间因素对公平性的影响,非否认协议还应具有时限性。

对非否认协议的形式化分析近年来得到了很大发展,但研究工作主要针对无时限性的非否认性协议,对于具有时限性的非否认协议的形式化分析目前还没有很好的方法。主要的工作有:Kudo[1]在Kailar逻辑的基础上,提出时态构造和时限责任问题;梁坚等人[2]指出Kudo方法的一些缺陷,并提出应考虑协议中消息的新鲜性;黎波涛等[3]给出一种基于时间演算的协议时限分析方法。然而,上述方法在描述和分析协议性质时,都是通过在现有BAN类逻辑的推理公式上加入时间条件来描述和分析协议的,如B said NRR at [Tx]⊃B received NRO at [Ty|{x|x≤Tx}]),这使得推理过程冗长而繁琐。此外,BAN类逻辑由于基于主体的信念,而且缺乏时间推理规则,因此无法描述和分析非否认协议的公平性。

CS逻辑[4]是由Coffey和Saidha提出的一种知识逻辑系统,与BAN类逻辑不同,它的推理主要基于主体在某时刻所拥有的知识,进而推理出主体拥有的新知识。CS逻辑在逻辑推理中引入了对时间的推理规则,因此适合分析与时间相关的安全协议的性质。目前CS逻辑仅被用于分析与时间相关的安全协议的秘密性[4-6]。本文针对非否认协议的安全属性,对CS逻辑进行了扩展,使其能够描述和分析具有时限性的非否认协议的非否认性和公平性,并使用扩展后的逻辑对改进的ZG协议进行了分析。在分析过程中,我们发现该协议存在对签名的重放攻击漏洞,不满足强非否认性,同时证明过程和结果也表明,扩展后的CS逻辑能够有效地描述和分析具有时限性的非否认协议的安全性质。

2 CS逻辑

分析安全协议的模态逻辑方法分为信念逻辑和知识逻辑两大类。信念逻辑的典型代表是BAN及BAN类逻辑。知识逻辑的典型代表是CS逻辑和CKT5逻辑[7,8]。CS逻辑在逻辑推理中引入了对时间的推理规则,可用于分析与时间相关的安全协议的性质;CKT5逻辑则侧重于在较低的抽象层次上描述协议相关的一些基本性质,如随机数的新鲜性、角色的行为、密码系统的特性等。

2.1 CS逻辑基本术语

CS逻辑提供了3种运算符K,L和B。K,L表示主体的知识,其中,L表示主体所拥有的客观知识。B表示主体的信仰。3种运算符都以时间做下标索引,表示主体在某时刻的知识或信仰。

CS逻辑的基本术语如下:

到稿日期:2009-06-04 返修日期:2009-09-07 本文受国家自然科学基金(60673071)资助。
王 鹃(1976-),女,博士,讲师,主要研究方向为安全协议分析和设计等,E-mail:jwang@whu.edu.cn;刘 珺(1975-),博士生,主要研究方向为信息安全;张焕国 男,教授,博士生导师,主要研究方向为信息安全。

ϕ 表示任意命题。Σ 表示任意主体。i,j 表示某个协议主体。ENT 表示所有主体的集合；$\{ENT\backslash\Sigma\}$ 表示不包括主体 Σ 的所有主体的集合。

K，知识操作符。$K_{\Sigma,t}\phi$ 表示主体 A 在 t 时刻知道公式 ϕ。

L，知识谓词。$L_{\Sigma,t}X$ 表示主体 Σ 在 t 时刻知道并且能够重新生成对象 X。

B，信念操做符。$B_{\Sigma,t}\phi$ 表示主体 B 在 t 时刻相信公式 ϕ。

$e(x,K_\Sigma)$，用主体 Σ 的公钥对 X 加密。

$d(x,K_\Sigma^{-1})$，用主体 Σ 的私钥对 X 进行签名或解密运算。

$C(x,y)$，表示消息 y 包含在消息 x 中。

$S(\Sigma,t,x)$，主体 Σ 在 t 时刻发送消息 x。

$R(\Sigma,t,x)$，主体 Σ 在 t 时刻接收消息 x。

2.2 CS逻辑推理规则

1. 知识规则和信仰规则

$A1$:(a) $\exists t\exists p\exists q\,(K_{\Sigma,t}p\wedge K_{\Sigma,t}(p\rightarrow q)\rightarrow K_{\Sigma,t}q)$

(b) $\exists t\exists p\exists q\,(B_{\Sigma,t}p\wedge B_{\Sigma,t}(p\rightarrow q)\rightarrow B_{\Sigma,t}q)$

$A2$: $\exists t\exists p(K_{\Sigma,t}\,p\rightarrow p)$

$A1$(a)和 $A1$(b)表明如果主体 Σ 在 t 时刻知道或相信 P，并且由 p 可推出 q，那么主体 Σ 在 t 时刻知道或相信 q。$A2$ 表明了知识和信念的区别：如果一个主体知道一个命题 P，那么 P 在该主体认为的所有可能世界中都为真。而一个主体相信命题 P，命题 P 未必为真。

2. 时间单调性规则

$A3$:(a) $\exists t\exists x\exists i,i\in\{ENT\}(L_{i,t}x\rightarrow\forall t',t'>t\,L_{i,t'}\,x)$

(b) $\exists t\exists x\exists i,i\in\{ENT\}(K_{i,t}x\rightarrow\forall t',t'>t\,K_{i,t'}\,x)$

(c) $\exists t\exists x\exists i,i\in\{ENT\}(B_{i,t}x\rightarrow\forall t',t'>t\,B_{i,t}\,x)$

$A3$ 表明主体的知识和信仰与时间相关的单调增长性，即知识和信念一旦获得就不会丢失。

3. 包含规则

$A4$: $\exists t\exists x\exists y(\exists i,i\in\{ENT\}\ L_{i,t}y\wedge C(y,x)\rightarrow\ \exists j,j\in\{ENT\}\ L_{j,t}x)$

$A4$ 表明如果一个消息由几个数据项组成，那么每个数据项一定被某个主体获知。

4. 发送和接收规则

$A5$: $\exists t\exists x(\ S(\Sigma,t,x)\ \rightarrow\ L_{\Sigma,t}\ x\wedge\ \exists i,i\in\{ENT/\Sigma\}\ \exists t',t\geqslant t'\,R(\ i,t',x)$

$A6$: $\exists t\exists x(\ R(\Sigma,t,x)\ \rightarrow\ L_{\Sigma,t}\ x\wedge\ \exists i,i\in\{ENT/\Sigma\}\ \exists t',t'<t\,S(\ i,t',x)$

$A5$ 和 $A6$ 表明如果一个主体在 t 时刻发送或收到了一个消息，那么在 t 时刻该主体一定已经获知了该消息，并且在此之后或之前一定有一个主体接收或发送了这个消息。

5. 密文获取规则

$A7$:(a) $t\exists x\exists i,i\in\{ENT\}(L_{i,t}x\wedge L_{i,t}x\ K_\Sigma\rightarrow\ L_{i,t}e(x,K_\Sigma))$

(b) $\exists t\exists x\exists i,i\in\{ENT\}(L_{i,t}x\wedge L_{i,t}x\ K_\Sigma^{-1}\rightarrow\ L_{i,t}\,d(x,K_\Sigma^{-1}))$

$A7$(a)和 $A7$(b)表明主体只有知道公钥及其对应的私钥才能进行加密和签名操作。

$A8$:(a) $\exists t\exists x\exists i,i\in\{ENT\}(\neg L_{i,t}\ K_\Sigma\wedge\ \forall t',t'<t\ \neg L_{i,t'}\,e(x,K_\Sigma)\ \wedge\neg(\exists y\,(R(\ i,t,y)\ \wedge C(y,e(x,K_\Sigma)))\rightarrow\neg L_{i,t}\,e(x,K_\Sigma))$

(b) $\exists t\exists x\exists i,i\in\{ENT\}(\neg L_{i,t}\,K_\Sigma^{-1}\wedge\ \forall t',t'<t\ \neg L_{i,t'}\,d(x,K^{-1}{}_\Sigma)\ \wedge\neg(\exists y\,(R(\ i,t,y)\ \wedge C(y,d(x,K_\Sigma^{-1})))\rightarrow\neg L_{i,t}\,d(x,K_\Sigma^{-1}))$

$A8$(a)表明如果主体 i 在 t 时刻不知道密钥 K_Σ，并且在 t 时刻之前不知道密文 $e(x,K_\Sigma)$，且在 t 时刻没有收到包含密文 $e(x,K_\Sigma)$ 的消息，则在 t 时刻，主体 i 不知道密文 $e(x,K_\Sigma)$。

$A8$(b)表明对主体对签名消息的获取能力。

6. 密钥规则

$A9$: $t(i,i\in\{ENT\}\,L_{i,t}\ K_i^{-1}\wedge\ \forall j,j\in\{\{ENT/i\}\rightarrow L_{j,t}\ K_i^{-1})$

$A10$: $\exists t\exists x(\exists i,i\in\{ENT\}L_{i,t}\,d(x,K_\Sigma^{-1}))\rightarrow L_{\Sigma,t}\,x$

$A9$ 表明了主体私钥的私有性。$A10$ 表明私钥的拥有者一定知道用他的私钥进行签名的消息。

3 CS逻辑的扩展

CS逻辑将主体的知识和信仰与时间相关联，适合分析与时间相关的安全协议的性质。但原有的CS逻辑在分析具有时限性的非否认协议中存在着不足，需要进行改进和扩展。

3.1 密文获取规则

CS逻辑主要面向基于公钥的密码协议，没有给出使用对称密钥加密的密文的理解规则，而在非否认协议中，为实现公平性，消息通常需要用对称密钥加密后再发送，因此增加密文获取规则如下：

$A7$:(c) $\exists t\exists x\exists i,i\in\{ENT\}(L_{i,t}e(x,k)\wedge L_{i,t}k\rightarrow L_{i,t}x\ )$

$A7$(c)表明如果主体 A 知道密文 $\{x\}_K$，并且知道加密密钥 k(也是解密密钥)，那么主体 A 知道 x。

3.2 签名验证规则

CS逻辑中的发送和接收规则没有针对签名消息，使得推证签名消息来源的过程非常烦琐。实际上，由于签名具有可验证性，因此可直接通过主体是否拥有对应的公钥来验证签名消息的来源。增加签名规则如下：

$A11$: $\exists t\exists x\,(\,R(\Sigma,t,d(x,K_i^{-1}))\ \wedge L_{\Sigma,t}\ K_i\rightarrow\ K_{\Sigma,t}\ \exists i,i\in\{ENT/\Sigma\}\ \exists t',t'<t\,S(\ i,t',d(x,K_i^{-1}))$

$A11$ 表明如果主体在 t 时刻收到了一个签名消息，并且此时主体拥有签名私钥的对应公钥，那么主体能够验证签名的来源。

3.3 发送规则

在非否认协议中，为实现公平性，不会直接发送明文消息 x，而是先发送加密消息，然后再发送密钥。因此，增加以下推理规则：

$A12$: $\exists x,\exists t',\exists t''\,(S(\Sigma,t',e(x,k))\wedge\ S(\Sigma,t'',k)\rightarrow\ S(\Sigma,t'',x))$

$A12$ 表明对于任意主体 Σ，如果 Σ 在 t' 时刻发送了用 k 加密后的密文 $\{x\}_k$，并且在 t'' 发送了加密密钥 k，那么等价于 Σ 在 t'' 时刻发送了 x。

$A13$: $\exists t\exists x\exists i,i\in\{ENT/\Sigma\}(K_{i,t}(\exists t',t'<tn\,S(\Sigma,t',x)\wedge\forall t'',t''<tm\rightarrow S(\Sigma,t'',x))\rightarrow K_{i,t}\ tm<t'<tn\,S(\Sigma,t',x))$

$A13$ 表明了主体关于发送时间段的推理规则。如果主体 i 知道主体 Σ 在小于 tn 的某时刻发送了消息 x，并且主体 i 知道在 t 小于 tm 所有时间段，主体 Σ 没有发送过 x，那么主体 i 知道主体 Σ 在 tm 和 tn 之间的某一时刻发送了消息 x。

4 分析改进的 Zhou-Gollman 协议

4.1 改进的 Zhou-Gollman 协议

1996 年，Zhou-Gollmann 提出了一种基于 online TTP 的非否认协议(以下简称 ZG 协议)[9]，适用于在信道不可靠的条件下签订电子合同。Zhou-Gollmann 协议简单高效，是基于在线 TTP 非否认协议的典型代表。

Zhou-Gollman 协议的最初版本由于没有考虑时间因素对协议非否认性和公平性的影响，因此存在没有限定 CON_K(用于证明主体收到了密钥 K 的证据)在 TTP 上保存的时间和没有限定主体 A 向 TTP 提交密钥 K 的时间的缺陷。

Kim 等人为解决 ZG 协议存在的时限性问题，对 ZG 协议进行了改进[10](以下简称 ZGK 协议)，在原协议中加入了时间限制。ZGK 协议的描述如下：

$NRO=sS_A(f,B,N,T,C)$

$NRR=sS_B(f,A,N,T1,C)$

$SUB\_K=sS_A(f,B,N,T,K)$

$CON\_K=sS_{TTP}(f,A,B,N,T,T0,K)$

$EOO=\{NRO,CON\_K\}$

$EOR=\{NRR,CON\_K\}$

(1) $A\rightarrow B: f_{NRO},B,N,T,C,NRO$

(2) $B\rightarrow A: f_{NRR},A,N,T1,C,NRR$

(3) $A\rightarrow TTP: f_{SUB},B,N,T,K,SUB\_K$

(4) $A\leftrightarrow TTP: f_{CON},A,B,N,T,T0,K,CON\_K$

(5) $B\leftrightarrow TTP: f_{CON},A,B,N,T,T0,K,CON\_K$

式中，T 是 A 和 B 能获得 K 和 CON_K 的最终期限，TTP 将在期限 T 过后将 CON_K 从目录中删除。如果 B 不同意 A 规定的期限 T，那它在步骤(2)就停止协议的执行。$T1$ 是由 B 规定的 A 必须将 K 发送给 TTP 的最迟时间，一旦 TTP 收到 K，TTP 将 CON_K 放到 FTP 公共目录上，因此如果不考虑网络延迟和消息处理延迟，$T1$ 是 B 规定的 CON_K 放到 FTP 目录上的最迟时间。如果 B 发现 $T1$ 时刻 FTP 目录上还没有 CON_K，它将删除 NRO，并退出协议。这样，可以保证在 $T1$ 和 T 之间有足够长的时间，B 可以获得 CON_K。$T0$ 是 TTP 获得密钥 K 的实际时间。ZGK 协议中的时间参数应满足 $T0<T1<T$。

4.2 非否认性与公平性目标的形式化描述

(1)非否认性

非否认性描述如下：

$G1\ \exists t\, K_{B,t}(\exists t', t0<t'<tn\ S(A,t',M))$

目标 $G1$ 表明 B 知道 A 在本轮协议中发送了 M。其中，$t0$ 表示协议开始时间，tn 表示协议结束时间，$t0<t'<tn$ 表示事件发生在当前协议轮。

目标 $G1$ 的约束条件 $t0<t'<tn$ 表示事件发生在当前协议轮，结合主体的认证性，体现了消息的新鲜性。由于私钥的私有性和签名不能伪造的假设，消息 M 签名的来源只有两种情况：诚实主体在当前协议论发送了签名消息或攻击者重放了签名消息。上述目标表明 B 知道消息 M 是诚实主体 A 在本轮协议中发送的，而不是攻击者重放的，即表明消息 M 是新鲜的。

$G2\ \exists t\, K_{A,t}(\exists t', t0<t'<tn\ L_{B,t}\ M)$

目标 $G2$ 表明 A 知道 B 在本轮协议中得到了 M。

目前 SVO 逻辑和 Kailar 逻辑中将非否认性描述为：A 相信(或能证明)B 收到 M，B 相信(或能证明)A 发送了 M。我们认为这种方法没有考虑对于签名的重放攻击，仅表明了一种弱非否认性。强非否认性应该能够证明：A 相信(或能证明)B 收到了新鲜的 M，B 相信(或能证明)A 发送了新鲜的 M。

本文中给出的非否认目标考虑了重放攻击的可能性，是一种强非否认性。其中，$t0<t'<tn$ 的约束条件表示了消息 M 是在本轮协议中发送的。

(2)公平性

根据强公平性的定义，公平性可以用以下命题表示：

$\forall t,t\in\{Ptime\}\ L_{A,t}EOR\leftrightarrow L_{B,t}EOO$

式中，$\{Ptime\}=\{t_1,t_2,\cdots,t_n\}$ 是一个时间集合，t_1-t_n 是协议各执行步发生的时间。公平性命题表明对于协议的每一步，主体 A 获得了收方非否认证据 EOR 当且仅当主体 B 获得发方非否认证据 EOO。

4.3 证明过程

下面将对 ZGK 协议进行分析，分析之前需要借助于一些假设条件。

1. ZGK 协议的初始假设

(1)有关时间的假设

假设 $t0$ 为协议开始时间，tn 为协议结束时间，$t1,t2,t3,t4,t5$ 分别是协议(1)－(5)发生的时间。很明显协议中的时间满足如下关系：

$t0<t1<t2<t3<\min\{t4,t5\}<tn$

根据协议时限性约束，$T0,T1,T$ 及 $t1-tn$ 应满足如下关系：

$T0<T1<T<tn$，且 $t3<T1,t4<T,t5<T$。

时间集合 $\{Ptime\}=\{t1,t2,t3,t4,t5\}$。

(2)主体初始知识

$I1\ L_{A,t0}(K_B)$

$I2\ L_{A,t0}(K_{TTP})$

$I3\ L_{B,t0}(K_A)$

$I4\ L_{B,t0}(K_{TTP})$

$I5\ K_{A,t0}(\forall i,i\in\{ENT/A\}t,t<t0\rightarrow L_{i,t}\ N)$

$I5$ 表示主体 A 知道随机数 N 的新鲜性。由于 N 是主体 A 产生的协议轮标志，N 是随机数，具有唯一性，因此在协议开始时除了主体 A 之外，其它主体无法获知 N。

(3)针对 ZGK 协议增加的公理

为分析和证明 ZGK 协议，按照协议执行步骤，需要增加以下公理。

$A14: t,t<T1\ (L_{TTP,t}k\rightarrow\exists t', t<t'<T\ (L_{B,t'}\ k\ \wedge L_{A,t'}k)\wedge\exists t'', t''<t\ S(A,t'',k))$

在 ZGK 协议中，由于 TTP 是可信的，并且主体 A,B 可以通过 ftp 方式从 TTP 处得到 k，因此只要 TTP 得到了 k，那么即使信道不可靠，A,B 仍然可以通过多次请求，最终得到 k。但是，密钥 k 在 TTP 上的存放时间不大于 T，而且协议中规定了，主体 A 必须在 $T1$ 时刻之前将 k 发送给 TTP，TTP 才会将 k 存放在 ftp 的公共目录上。$A14$ 描述了协议的上述约定。

2. 对 ZGK 协议的解释如下：

(i)$R(B,t1,C,e((f,B,N,T,C),K_A^{-1}))$

(ii)$R(A,t2,e((f,A,N,T1,C),K_B^{-1}))$

(iii)$R(TTP,t3,e((f,B,N,T,k),K_A^{-1}))$

(iv)$R(A,t4,e((f,A,B,N,T,T0,k),K_{TTP}^{-1}))$

(v)$R(B,t5,e((f,A,B,N,T,T0,k),K_{TTP}^{-1}))$

3. 形式化协议目标

(1)非否认性

$G1\ \exists t\, K_{B,t}(\exists t',t0<t'<tn\ S(A,t',M))$

$G2\ \exists t\, K_{A,t}(\exists t',t0<t'<tn\ L_{B,t}\ M)$

(2)公平性

$t,t\in\{Ptime\}\ L_{A,t}EOR\leftrightarrow L_{B,t}EOO$

4. 逻辑推理过程

(1)假设 A 得到了 EOR 并且 B 得到了 EOO，验证协议的非否认性，如下所示：

由 $R(A,t2,e((f,A,L,T1,C),K_B^{-1}))$ 1)

由 1)，$A3$，初始假设 $I1$ 和 $A11$ 得 $K_{A,t2}(\exists t,t<t2,S(B,t,e((f,A,N,T1,C),K_B^{-1})))$ 2)

由 $I5$，$A3$ 和 $A4$ 得 $K_{A,t2}(\forall i,i\in\{ENT/A\},t,\forall t<t0,\neg L_{i,t}e((f,A,N,T1,C),K_B^{1})))$ 3)

由 3)和 $A5$ 得 $K_{A,t2}(\forall i,i\in\{ENT/A\},\forall t,t<t0,\neg S(i,t,e((f,A,N,T1,C),K_B^{-1})))$ 4)

由 2)，4)和 $A13$ 得 $K_{A,t2}(\exists t,t0<t<t2,S(B,t,e((f,A,N,T1,C),K_B^{-1})))$ 5)

由 5)和 $A5$ 得 $K_{A,t2}(\exists t,t0<t<t2,L_{B,t}e((f,A,N,T1,C),K_B^{-1})))$ 6)

由 6)和 $A10$ 得 $K_{A,t2}(\exists t,t0<t<t2,L_{B,t}C)$ 7)

由 $R(A,t4,e((f,A,B,N,T,T0,k),K_{TTP}^{-1}))$ 8)

由 8)，$A3$，初始假设 $I2$ 和 $A11$ 得 $K_{A,t4}(\exists t,t<t4,S(TTP,t,e((f,A,B,N,T,T0,k),K_{TTP}^{-1})))$ 9)

由 $I5$，$A3$ 和 $A4$ 得 $K_{A,t4}(\forall i,i\in\{ENT/A\},\forall t,t<t0,\neg L_{i,t}\ e((f,A,B,N,T,T0,k),K_{TTP}^{-1})))$ 10)

由 10)和 $A5$ 得 $K_{A,t4}(\forall i,i\in\{ENT/A\},t,\forall t<t0,\neg S(i,t,e((f,A,B,N,T,T0,k),K_{TTP}^{-1})))$ 11)

由 9)，11)和 $A13$ 得 $K_{A,t4}(\exists t,t0<t<t4,S(TTP,t,e((f,A,B,N,T,T0,k),K_{TTP}^{-1})))$ 12)

由 12)和 $A5$ 得 $K_{A,t4}(\exists t,t0<t<t4,L_{TTP,t}\ e((f,A,B,N,T,T0,k),K_{TTP}^{-1})))$ 13)

由 13)和 $A10$ 得 $K_{A,t4}(\exists t,t0<t<T1,L_{TTP,t}k)$ 14)

由 14)，$A14$ 得 $K_{A,t4}(\exists t',t0<t'<T,L_{B,t}\ k)$ 15)

由 7)，和 15)和时间约束得 $K_{A,t4}(\exists t',t0<t'<tn,L_{B,t}\ M)\ G2$

由 $R(B,t1,C,e((f,B,N,T,C),K_A^{-1}))$ 16)

由 16)，$A3$，初始假设 $I3$ 和 $A11$ 得 $K_{B,t1}(\exists t,t<t1,S(A,t,(C,e((f,B,N,T,C),K_A^{-1}))))$ 17)

由 $R(B,t5,e((f,A,B,N,T,T0,K),K_{TTP}^{-1}))$ 18)

由 16)，$A3$，初始假设 $I3$ 和 $A11$ 得 $K_{B,t5}(\exists t,t<t5,S(TTP,t,e((f,A,B,N,T,T0,k),K_{TTP}^{-1})))$ 19)

由 19)，$A5$，$A14$ 得 $K_{B,t5}(\exists t',t'<T1,S(A,t',k))$ 20)

由 17)，20)和 $A12$ 得 $\exists t\, K_{B,t}(\exists t',t'<T1,S(A,t',M))\ G1'$

从推理过程和结果可以看出，协议满足目标 $G2$，但不满足目标 $G1$。原因在于，协议中的 N 是 A 产生的随机数，因此只有 A 知道 N 的新鲜性，而其它主体无法知道。所以，推理的过程中无法利用假设条件 $K_{B,t0}(\forall i,i\in\{ENT/A\},t,t<t0,\neg L_{i,t}\ N)$ 得出主体 B 知道主体 A 在本轮协议中发送了 C 和 k 的结论。由此可知，主体 B 得到的消息 M 有可能是攻击者重放的旧消息，在这样的情况下，主体 A 实际上并没有重新发送 M，而仲裁者却认为主体 A 给 B 发送了 M，从而破坏了协议的非否认性。

从推理步骤中可以看出，协议不满足签名的新鲜性。一个解决的办法是在消息(1)和(3)的签名中加入时间戳。时间戳的新鲜性可定义为：$t+t_F<t_c$。其中 t 为时戳，t_F 为时戳的生存期，t_C 为接收到消息的当前时间。若要满足更强的新鲜性，则可以通过在协议步中加入主体 B 和 TTP 产生的随机数实现。

(2)验证协议的公平性。

协议满足非否认性是其满足公平性的前提，如果协议不满足非否认性，那么主体所获得的证据就毫无意义了，公平性也就失去了意义。因此，以下对于公平性的分析，针对加入了时戳的 ZGK 协议，它满足强非否认性。

由协议执行步骤知，在信道不可靠的条件下，协议第(1)－(3)步是可中断的。分析如下：

当 $t=t1$ 时，由协议步骤(i)$R(B,t1,C,e((f,B,N,T,t,t_F,C),K_A^{-1}))$及 $A6$ 可得：$L_{B,t1}\ NRO$

当 $t=t2$ 时，由协议步骤(ii)$R(A,t2,e((f,A,N,T1,C),K_B^{-1}))$及 $A6$ 可得：$L_{A,t2}NRR$

当 $t=t3$ 时，由协议步骤(iii)$R(TTP,t3,e((f,B,N,T,t,t_F,k),K_A^{-1}))$ 及 $A6$ 可得：$t<T1\ L_{TTP,t3}k$

当 $t=t4\wedge T0<t4<T$，由协议步骤(iv)及 $A6$ 得：$L_{A,t4}CON\_K$

当 $t=t5\wedge T0<t5<T$ 由协议步骤(v)及 $A6$ 得：$L_{B,t5}CON\_K$

由上述分析可得：$\forall t,t\leqslant t3,L_{A,t}\ EOR$ 和 $L_{B,t}\ EOO$ 不成立，故 $L_{A,t}EOR\leftrightarrow L_{B,t}EOO$ 成立。$\forall t,t3<t<T$，根据 $A14$，$t,t<T1\ (L_{TTP,t}k\rightarrow\exists t',t<t'<T\ (L_{B,t'}\ k\ \wedge L_{A,t'}\ k)$，故若 $t,t<T1\ L_{TTP,t}K$，则 $\forall t,t3<t<T,L_{B,t}CON\_K\leftrightarrow L_{A,t}CON\_K$ 成立。综上所述，$L_{A,t}EOR\leftrightarrow L_{B,t}EOO$ 成立。

从证明的过程可以看出，如果 ZGK 协议满足强非否认性，并且满足时间约束关系，即时限性，那么该协议是公平的。

结束语 具有时限性非否认协议的形式化分析需要在验证协议性质的同时，描述和分析时间因素对协议的影响。目前验证此类协议的方法是在现有 BAN 类逻辑的推理公式后加入时间条件来描述和分析协议，这种方法的推理过程冗长而繁琐，并且无法描述和分析非否认协议的公平性。本文将 CS 逻辑用于分析具有时限性的非否认协议，针对非否认协议的性质对 CS 逻辑进行了扩展，给出了描述和分析非否认性以及公平性的方法，并使用扩展后的逻辑对改进的 ZG 协议进行了分析。在分析过程中，发现了该协议存在对签名的重放攻击漏洞，不满足强非否认性。验证过程也表明，扩展后的 CS 逻辑能够有效的描述和分析具有时限性的非否认协议的安全性质。

参 考 文 献

[1] Kudo M. Electronic submission protocol based on temporal accountabil2ity[C]//Proc. of 14th Annual Computer Security Application Conf. Phoenix: ACSA, 1998. 3532363

(下转第 76 页)

的不断增大，虚假文件率基本上没有多少影响。

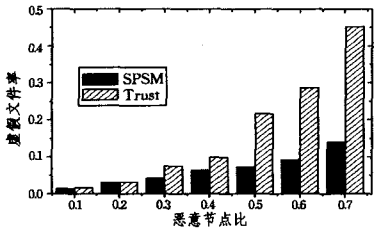

图 4　下载虚假文件率随恶意节点比变化图

SPSM 中虚假文件率更低的原因是系统中采用了举报机制。由于当一个恶意节点为其它节点提供了虚假文件后，该恶意节点会被举报，从而其它节点不会再从该恶意节点进行下载。而本系统中设置了每个节点的最大连接数 Mcn，因此每个恶意节点最多能够提供 Mcn 次虚假文件上传，对于有 N 个节点的网络中，当恶意节点比例为 Mp 时，在该网络中最大的虚假文件上传次数(uploading times of maximum inauthentic files，简写为 $Tmif$)为：

$$Tmif=N*Mp*Mcn \tag{9}$$

而总的下载次数(total downloading times，简写为 Tdt)为：

$$Tdt=N*C \tag{10}$$

因此 SPSM 中最大虚假文件率(inauthentic file ratio，简写为 Ifr)为：

$$Ifr=\frac{Tmif}{Tdt}=\frac{N*Mp*Mcn}{N*C}=\frac{Mp*Mcn}{C} \tag{11}$$

从式(11)可以看出，SPSM 中最大虚假文件率随恶意节点的比例 Mp 的变大而变大，随最大连接数 Mcn 的变大而变大，随轮转周期 C 的变大而变小。从图 4 来看，其 Mcn 为 5，C 为 8。由于 Mp 的量级更小，因此随着 Mp 的变大虚假文件率基本没多大影响。在该系统中，可以通过提高轮转周期数 C 来进一步降低虚假文件率，即在一个长期存在 SPSM 中其虚假文件率可以更低。

总之，SPSM 比基于信誉的系统的虚假文件率更低。

结束语　本文提出的 SPSM(安全 P2P 共享模型)是基于举报机制的，即一经发现恶意节点即对其进行举报，从而避免其它节点向该恶意节点进行下载；同时采取虚拟货币购买文件的方式，以激励网络中节点上传文件；系统中节点通过提供上传文件以挣取 VC，从而保证以后下载文件有足够的虚拟货币。实验显示 SPSM 具有较好的性能。

参 考 文 献

[1] Resnick P, Zeckhauser R. Trust among strangers in internet transactions: Empirical analysis of eBay's reputation system [M]. Advances in Applied Microeconomics, 2002, 11: 127-157

[2] Li N, Mitchell C J, Winsborough W H. Design of a role-based trust management framework [C] // Proc. of the 2002 IEEE Symp. on Security and Privacy. Washington, USA, 2002

[3] Kamvar S D, Schlosser M T, Garcia-Molina H. The EigenTrust Algorithm for Reputation Management in P2P Networks [C]// Proc. of WWW. Budapest, Hungary, 2003

[4] Wang Yao, Vassileva J. Bayesian Network - based Trust Model [C]// Proc. of IEEE/WIC International Conference on Web Intelligence. Halifax, Canada, 2003

[5] Song Weihua, Phoha V V. Neural network-based reputation model in a distributed system [C]// Proc. of IEEE 2004 CEC. San Diego, California, USA, 2004

[6] Stoica I, Morris R, Karger D, et al. Chord: A scalable peer-to-peer lookup service for internet applications[C]// Proc. of SIGCOMM. SanDiego, California, USA, 2001

[7] Bloom B. Space / Time trade - offs in hash coding with allowable errors[J]. Communications of the ACM, 1970, 13(7): 422-426

[8] Mitzenmacher M. Compressed Bloom Filters [J]. IEEE/ACM Transactions on Networking, 2002, 10(5): 604-612

[9] Aguilar-Saborit J, Trancoso P, Muntes-Mulero V. Dynamic Count Filters[C]// Proc. of SIGMOD. Chicago, USA, 2006

[10] Guo Deke, Wu Jie, Chen Honghui, et al. Theory and Network Applications of Dynamic Bloom Filters[C]// Proc. of IEEE INFOCOM. Barcelona, Spain, 2006

[11] Broder AMitzenmacher M. Network applications of bloom filters: A survey[J]. Internet Mathematics, 2005, 1(4): 485-509

[12] peersim [EB/OL]. http://peersim.sourceforge.net/

(上接第 52 页)

[2] 梁坚，敖青云，尤晋元. 安全协议的时限责任分析 [J]. 电子学报，2002，10：35-39

[3] 黎波涛，罗军舟. 不可否认协议时限性的形式化分析[J]. 软件学报，2006，17(7)：1510-1516

[4] Coffey T, Saidha P. Logic for verifying public-key cryptographic protocols[J]. IEEE Proc Computers and Digital Techniques, 1997, 144(1): 28-32

[5] Kudo M, Mathuria A. An Extended Logic for Analyzing Timed-Release Public-Key Protocols[J]. ICICS, 1999: 183-198

[6] 范红，冯登国. 一种分析 Timed-release 公钥协议的扩展逻辑 [J]. 计算机学报，2003，22：832-838

[7] Bieber P. A logic of communication in hostile environment[C]// Proceedings of the Third IEEE Computer Security Foundations Workshop. Franconia, New-Hampshire: IEEE Computer Society Press, 1990: 14-22

[8] 毛晨晓，罗文坚，王煦法. 分析安全协议密码系统相关缺陷的模态逻辑方法[J]. 小型微型计算机系统，2006，27(7)：1223-1228

[9] Zhou J, Gollmann D. A fair non-repudiation protocol[C]// Proc. of the 1996 IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Society Press, 1996: 55-61

[10] Kim K, Park S, Baek J. Improving fairness and privacy of Zhou-Gollmann's fair non-repudiation protocol[C]// Gong K, Niu Z, eds. 2000 IEEE Int'l Conf. on Communication. Beijing: IEEE Computer Society Press, 2000, 3: 1743-1747