ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.17, No.7, July 2006, pp.1510−1516
DOI: 10.1360/jos171510

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

不可否认协议时限性的形式化分析*

黎波涛+, 罗军舟

(东南大学 计算机科学与工程系,江苏 南京 210096)

Formal Analysis of Timeliness in Non-Repudiation Protocols

LI Bo-Tao+, LUO Jun-Zhou

(Department of Computer Science and Engineering, Southeast University, Nanjing 210096, China)

+ Corresponding author: Phn: +86-25-83795595, E-mail: leopert@seu.edu.cn

Li BT, Luo JZ. Formal analysis of timeliness in non-repudiation protocols. *Journal of Software*, 2006,17(7): 1510−1516. http://www.jos.org.cn/1000-9825/17/1510.htm

Abstract: While SVO logic has been widely used in the analysis of non-repudiation protocols for its simplicity, its lack of the ability in time description makes it helpless in the analysis of timeliness, which is one of the most important properties of non-repudiation protocols. SVO logic is extended by adding a simple time expression and analysis method into it. Then a widely discussed fair non-repudiation proposed by Zhou and Gollmann in 1996 and one of its improvements are analyzed with the newly extended logic. The result shows that Zhou-Gollmann's fair non-repudiation protocol does not provide timeliness while its improvement does. Therefore, the new logic is able to analyze timeliness of non-repudiation protocols. In addition, the new logic can be used to analyze other time-related properties of cryptographic protocols.

Key words: non-repudiation; timeliness; SVO logic; formal analysis

摘 要: 虽然 SVO 逻辑由于其简单性在对不可否认协议的形式化分析中得到了广泛的应用,但它在时间描述能力上的不足使得它无法分析不可否认协议的时限性.通过向 SVO 逻辑添加一种简单的时间表达和分析方法扩展了 SVO 逻辑,并使用扩展后的逻辑对 Zhou 和 Gollmann 于 1996 年提出的一个公平不可否认协议及其一个改进协议进行了分析.分析结果表明,原协议不具有时限性,而改进协议具有时限性,因此也说明了扩展后的新逻辑能够分析不可否认协议的时限性.另外,新逻辑还能用来分析一般密码协议中的时间相关性质.

关键词: 不可否认;时限性;SVO 逻辑;形式化分析
中图法分类号: TP393 文献标识码: A

不可否认协议能用来防止通信实体对通信事件的抵赖行为,对它的研究在近年来得到了很大的发展,包括对其形式化分析方法的研究.虽然对安全协议进行形式化分析的方法有很多,但目前还没有专门针对不可否认协议的分析方法.通常的做法都是使用现有的安全协议分析方法对不可否认协议进行分析.如:G. Norman 等人

* Supported by the National Natural Science Foundation of China under Grant Nos.90412014, 90604004 (国家自然科学基金); the Jiangsu Provincial High-Tech Research Program under Grant No.BG2004036 (江苏省高技术研究项目); the Jiangsu Provincial Key Laboratory of Network and Information Security under Grant No.BM2003201 (江苏省网络与信息安全重点实验室)

Received 2004-10-22; Accepted 2005-07-11

使用一个概率模型检查器分析了一个概率合同签署协议[1];Levente Buttyun 等人基于博弈论分析了一个理性交换(rational exchange)协议[2];Martín Abadi 等人使用一个基于 prolog 规则的协议验证工具分析了一个挂号邮件协议[3];S. Kremer 等人基于博弈论对几个不可否认协议和公平交换协议进行了分析[4];V. Shmatikov 等人使用有限状态分析工具 Murφ 分析了两个合同签署协议[5].在我国,对不可否认协议形式化分析的研究工作近几年也得到了一定的关注,如:卿斯汉设计了一个不可否认协议并对其进行了形式化验证[6];李先贤和怀进鹏使用 BAN 逻辑对自己设计的不可否认协议进行了形式化验证[7].然而,现有的这些形式化方法往往着重于对协议的认证、机密性及完整性等安全性质的描述和分析,而对可追究性、公平性、时限性等不可否认协议特有的性质的表达和分析能力不够强.因此,它们还无法完全满足不可否认协议形式化分析的需要.

SVO[8]逻辑是 BAN 逻辑[9]的一种扩展,它在不可否认协议的形式化分析方面得到了较多的应用.但这些应用也基本上都是使用 SVO 逻辑分析中一般安全协议的方法进行的,而且 SVO 逻辑本身也存在一些不足.这就使得一些不可否认协议特有的而 SVO 逻辑无法描述的性质得不到分析,其中之一就是时限性.

Zhou J.和 Gollmann D.在 1996 年提出了一个公平的不可否认协议[10](后文称其为 ZG 协议).该协议提出后得到了广泛的讨论和分析.1999 年,K. Kim,S. Park 和 J. Baek 发现 ZG 协议不具有时限性并进行了改进[11](后文称该改进协议为 NZG 协议).很多对 ZG 协议的形式化分析[12−14]都未能发现它的缺陷.

本文通过添加一种简单的时间表达式和时间分析方法对 SVO 逻辑进行了扩展,并使用扩展后的新逻辑对 ZG 协议及 K. Kim 等人改进后的 NZG 协议进行了分析.分析结果表明,ZG 协议不具有时限性,而 K. Kim 等人的改进协议具有时限性.这也说明了新逻辑在时间描述与分析上的能力.

1 扩展 SVO 逻辑

SVO 对时间的描述能力很弱,它只将时间区分为两种:过去和现在.所以它无法区分当前协议运行中各事件发生的不同时间,不可否认协议中影响时限性的正是协议事件(信息的发送和接收)发生的时间.虽然 W. Mao 通过为 SVO 逻辑增加时态逻辑公式增强了其时间描述能力[15],但还是无法满足不可否认协议时限性分析的要求.为此我们在 SVO 逻辑的公式语言的定义中增加一个条件来描述事件发生的时间:

6. P received X at T,P says X at T,P said X at T 是公式,如果 X 是消息,P 是实体且 T 是时间表达式.

这条定义增加了对发送和接收信息的发生时间的描述.设 $I=\{0,1,2,3,\ldots\}\cup\{-1,-2,-3,\ldots\}$,即 I 是整数集,则时间表达式的定义如下:

1. x 是时间常元,如果 $x\in I$;

2. X 是时间变元,如果 X 是一个变域为 I 的变元;

3. $X|TS$ 是时间绑定表达式,如果 X 是时间变元且 $TS\subseteq I$;

4. $[T]$是时间表达式,如果 T 是一个时间绑定表达式.

在后文中,时间常元用带下标的小写字母 t 表示,时间变元则用带下标的大写字母 T 表示.时间绑定表达式 $X|TS$ 为其中的时间变元 X 赋予了一个确定值的时间常元 $t(t\in TS)$.一旦时间变元的值被一个绑定表达式绑定,在绑定值被释放前,该变元的作用就和时间常元相同,不能对其进行再次绑定.这类似于 prolog 语言中变量值绑定的概念.在逻辑公式中,时间表达式$[X|I]$可缩写为$[X]$;而$[X|\{x\}]$可缩写为$[x]$,如果 x 是一个时间常元或一个已绑定值的时间变元.在逻辑公式中,时间变元的值在其按照公式中各操作的运算优先级首次出现时被绑定.

添加了 *at* 操作后,就可以将 SVO 逻辑中相关的公理更改为:

A4. $(PK_\sigma(Q,K)\wedge R$ received $\{X\}_K^{-1}$ at $T)\supset Q$ said X at T

A6. P received $(X_1,\ldots,X_n)$ at $T\supset P$ received X_i at T

A7. $(P$ received $\{X\}_K$ at $T\wedge P$ has $K')\supset P$ received X at T

在不分析事件的时间关系时,上述公理中所有的时间表达式都使用$[X|I]$,这时 at 操作可以省略不写.此时使用的公理就与原逻辑中的公理是一样的了.使用新逻辑对协议进行分析的步骤也相应地扩展为:

(1) 在给出协议的基本假设之前,必须先给出协议推理过程中要用到的所有的时间常元和变元.常量的实

际值可以不给出,但如果不同的时间常元之间存在约束关系(大小关系),则应该指出这种制约关系.在给出协议的基本假设和协议目标时,需要用公式显示地描述协议各事件间的时间依赖关系.例如:J believes (A said M at $[T]$)$\wedge(T\leq t_x)$该公式表达了两部分的内容:第 1 部分是 J 对通信事件的信仰;第 2 部分是事件发生时间满足的条件.

(2) 协议目标证明过程分为两个步骤:第 1 个步骤称为逻辑推理,它证明协议目标的前半部分.该过程就是原 SVO 逻辑中的协议目标证明过程.第 2 个步骤称为时间演算,它证明协议目标的后半部分.该过程的作用是证明逻辑推理中得到的结果公式满足协议目标所规定的时间约束条件.该过程使用的方法完全是代数方程式(组)和不等式(组)的证明方法,因此很容易掌握和使用.

2 ZG 协议的形式化分析

ZG 协议[10]的交互步骤如下:

1. $A\rightarrow B$: f_{NRO},B,L,C,NRO
2. $B\rightarrow A$: f_{NRR},A,L,NRR
3. $A\rightarrow TTP$: f_{SUB},B,L,K,sub_K
4. $B\leftarrow TTP$: f_{CON},A,B,L,K,con_K
5. $A\leftarrow TTP$: f_{CON},A,B,L,K,con_K

$NRO=sS_A(f_{NRO},B,L,C)$; $NRR=sS_B(f_{NRR},A,L,C)$

$sub\_K=sS_A(f_{SUB},B,L,K)$; $con\_K=sS_T(f_{CON},A,B,L,K)$

协议运行完成后,A 收集到的证据是 NRO,NRR 和 con_K;B 收集到的证据是 NRO 和 con_K.如果日后产生争端,它们可以将自己收集到的证据提交给一个权威的仲裁者 J 进行仲裁.仲裁者根据它们提交的证据的有效性得出通信事件是否发生过的仲裁结果.

虽然 Zhou J.和 Gollmann D.声称 ZG 协议是公平的,但下面的分析说明,它仍然缺乏时限性,因而无法达到真正的公平.为了分析过程的可读性和简洁性,定义作了如下缩写:

$C=\{M\}_K$; $NRO_p=\{f_{NRO},B,L,C\}$; $NRO=\{NRO_p\}_{Ka}^{-1}$;

$NRR_p=\{f_{NRR},A,L,C\}$; $NRR=\{NRR_p\}_{Kb}^{-1}$; $sub\_K_p=\{f_{SUB},B,L,K\}$;

$sub\_K=\{sub\_K_p\}_{Ka}^{-1}$; $con\_K_p=\{f_{CON},A,B,L,K\}$; $con\_K=\{con\_K_p\}_{Kt}^{-1}$.

2.1 ZG协议假设集和目标

分析过程中要用到的时间常元有 t_0,t_A 和 t_B,其中 t_0 表示网络不可用的最长时间(因为协议假设网络不是永久不可用的),t_A 和 t_B 则分别表示 A 和 B 在发送完一个协议消息后等待下一个消息的最长等待时间.要用到的时间变元有 $T_s,T_r,T_o,T_A,T_B,T_x,T_y$.

首先给出协议的基本假设中关于实体密钥的假设.每个实体有一个签名私钥,且相应的公钥是公开的:

P1. (1) J believes $PK_\sigma(A,K_a)$ (2) J believes $PK_\sigma(B,K_b)$ (3) J believes $PK_\sigma(TTP,K_t)$

P2. (1) J believes (B has K_a) (2) J believes (B has K_t) (3) J believes (A has K_b)

协议中 TTP 必须是称职的,即它只有在收到 sub_K 后才会产生证据,且 TTP 不会拖延时间:

P3. J believes (TTP said CON_K_p at $[T_x]\supset TTP$ received sub_K at $[T_x\}$])

只要 TTP 发布了证据,B 就一定能在此后一段时间(t_0)内收到证据:

P4. J believes (TTP said CON_K_p at $[T_x]\supset B$ received CON_K at $[T_y|\{x|T_x\leq x\leq T_x+t_0\}]$)

A 和 B 都不会做不利于自己的事:

P5. J believes (A said sub_K_p at $[T_x]\supset A$ received NRR at $[T_y|\{x|x\leq T_x\}]$)

P6. J believes (B said NRR_p at $[T_x]\supset B$ received NRO at $[T_y|\{x|x\leq T_x\}]$)

最后的假设是关于 M 的还原.只要 B 收到了 C 和 K,它就收到了 M:

P7. J believes (B received C at $[T_x]\wedge B$ received K at $[T_y]\supset B$ received M at $[\max(T_x,T_y)]$)

ZG 协议的目标是:

G1. J believes (A said M at $[T_x]\wedge A$ received CON_K at $[T_y]$)$\wedge(T_x\le T_y\le T_x+t_A)$

G2. J believes (B received M at $[T_x]\wedge B$ said NRR_p at $[T_y]$)$\wedge(T_x-t_B\le T_y\le T_x)$

目标 G1 说明:如果 A 收到了 TTP 发布的证据,它一定是在将 sub_K 提交给 TTP 之后有限的时间之内收到该证据的,而不可能是在证据删除之后收到的;目标 G2 也说明了这种时间约束关系.只要能证明上述两个目标,就能说明新 ZG 协议的正确性和时限性.

2.2 ZG协议目标证明

由于目标 G1 没有争议,本文仅对 G2 进行证明.

逻辑推理:	
1. J believes J received con_K	P4,Nec,A1,A6
2. J believes (TTP said con_K_p at $[T_s]$)	1,P1(3),Nec,A1,A4
3. J believes (TTP received sub_K at $[T_s]$)	2, P3,Nec,A1
4. J believes (A said sub_K_p at $[T_s]$)	3,P1(1),Nec,A1,A4
5. J believes (A received NRR at $[T_r\|\{x\|x\le T_s\}]$)	4,P3,A1
6. J believes (B said NRR_p at $[T_r]$)	5,P1(2),Nec,A1,A4
7. J believes (B received NRO at $[T_o\|\{x\|x\le T_r\}]$)	6,P6,A1
8. J believes (B received NRO_p at $[T_o]$)	7,P2(1),Nec,A1,A7
9. J believes (B received C at $[T_o]$)	8,Nec,A1,A6
10. J believes (B received con_K at $[T_B\|\{x\|T_s\le x\le T_s+t_0\}]$)	2,P4,A1
11. J believes (B received con_K_p at $[T_B]$)	10,P2(2),Nec,A1,A7
12. J believes (B received K at $[T_B]$)	11,Nec,A1,A6
13. J believes (B received M at $[\max(T_o,T_B)]$)	9,12,P7,A1
14. J believes (B received M at $[\max(T_o,T_B)]\wedge B$ said NRR_p at $[T_r]$)	6,13,Nec,A1
时间演算:	
令 $T_x=\max(T_o,T_B)$,$T_y=T_r$.现证明 $T_x-t_B\le T_y\le T_x$:	
$T_x=\max(T_o,T_B)$	
$\Rightarrow T_x=T_B$	因 $T_o\le T_r\le T_s\le T_B$
$\Rightarrow T_s\le T_x\le T_s+t_0$	因 $T_B\in\{x\|T_s\le x\le T_s+t_0\}$
$\Rightarrow 0\le T_x-T_y\le T_s+t_0-T_r$	因 $T_r\le T_s$
$\Rightarrow T_x-(T_s+t_0-T_r)\le T_y\le T_x$	
如果能证明 $T_s+t_0-T_r\le t_B$ 就能得到 $T_x-t_B\le T_y\le T_x$.但是 T 和 T_r 之间没有约束关系,因此无论将常元 t_B 的值定义为多大,$T_s+t_0-T_r$ 的值都可能会大于它,所以无法证明 $T_s+t_0-T_r\le t_B$.	

目标 G2 定义的时间约束条件无法得到满足.这是因为 TTP 发布证据的时间(即 A 提交 sub_K 的时间)与 B 发送 NRR 的时间之间没有一种约束关系,致使无论 B 等待的时间 t_B 有多长,A 都可以在它超时之后向 TTP 发送 sub_K 并在 TTP 发布证据之后获得证据证明 B 收到了 M.但 B 因为等待超时已将 C 删除了,因此即使收到了 con_K 并获得密钥 K 也无法进行解密获取 M 了.所以,B 在发送了 NRR 之后,如果一直无法从 TTP 获得 con_K,它也不能删除 NRO,以防止上述情况的发生.

3 NZG 协议的形式化分析

K. Kim 等人通过向协议消息中添加时间限制信息改进了 ZG 协议[11].改进后的协议如下:

1. $A\rightarrow B$: f_{NRO},B,L,T,C,NRO

2. $B\rightarrow A$: f_{NRR},A,L,T_1,NRR

3. $A\rightarrow TTP$: f_{SUB},B,L,T,K,sub_K

4. $B\leftarrow TTP$: $f_{CON},A,B,L,K,T_0,con\_K$

5. $A\leftarrow TTP$: $f_{CON},A,B,L,K,T_0,con\_K$

$NRO=sS_A(f_{NRO},B,L,T,C)$; $NRR=sS_B(f_{NRR},A,L,T_1,C)$;

$sub\_K=sS_A(f_{SUB},B,L,T,K)$; $con\_K=sS_T(f_{CON},A,B,L,T_0,K)$.

在上述步骤中,T 是 A 和 B 能从 TTP 获得 con_K 的最终期限,TTP 会在期限 T 过后将 con_K 从公共目录中删除;T_0 是 TTP 发布 con_K 的时间;T_1 是由 B 规定的 A 必须将 K 发送给 TTP 的最迟时间,因此 T,T_1 和 T_0 之间的关系为 $T_0\le T_1\le T$.协议完成后,A 和 B 收集的证据与 ZG 协议中的相同.

下面开始通过对 NZG 协议进行分析来说明它是如何提供时限性的.先定义如下缩写:

$C=\{M\}_K$; $NRO_p=\{f_{NRO},B,L,T,C\}$; $NRO=\{NRO_p\}_{Ka}^{-1}$;

$NRR_p=\{f_{NRR},A,L,T_1,C\}$; $NRR=\{NRR_p\}_{Kb}^{-1}$; $sub\_K_p=\{f_{SUB},B,L,T,K\}$;

$sub\_K=\{sub\_K_p\}_{Ka}^{-1}$; $con\_K_p=\{f_{CON},A,B,L,T_0,K\}$; $con\_K=\{con\_K_p\}_{Kt}^{-1}$.

3.1 NZG协议假设集和目标

分析过程中要用到的时间常元有 t,t_1,t_0,t_A 和 t_B.其中 t 和 t_1 分别代表协议消息中相应的时间控制信息 T 和 T_1,因此它们满足:$t_1\le t$;t_0 表示网络不可用的最长时间;t_A 和 t_B 则分别表示 A 和 B 在发送完一个协议消息后等待下一个消息的最长等待时间.要用到的时间变元有 $T_s,T_r,T_o,T_A,T_BT_x,T_y$.

NZG 协议的假设集和 ZG 协议基本相同,但需要添加一条用来说明 J 对证据时间关系的检查.

P8. J believes (TTP said $CON\_K_p\supset TTP$ said CON_K_p at $[T_x|\{x|x\le t_1\}]$)

协议目标和 ZG 协议也基本相同,但它有不同的时间约束条件:

G1. J believes (A said M at $[T_x]\wedge A$ received CON_K at $[T_y]$)$\wedge(T_x\le T_y\le t)$

G2. J believes (B received M at $[T_x]\wedge B$ said NRR_p at $[T_y]$)$\wedge(T_y\le T_x\le t_1+t_B\le t)$

G1 说明 A 必须在发送 sub_K 之后,时间 T 之前获得证据 con_K.G2 则说明 B 在发送 NRR 之后还是会等待有限的时间,但等待的时间应该从它自己规定的时间 T_1 开始计算,而不是从发送 NRR 的时间开始;且 B 必须在时间 T 之前获得 con_K.

3.2 NZG协议目标证明

同样,由于 G1 没有争议,也只对 G2 进行证明.

逻辑推理:	
1. J believes J received con_K	P4,Nec,A1,A6
2. J believes (TTP said con_K_p)	P1(3),1,Nec,A1,A4
3. J believes (TTP said con_K_p at $[T_s\|\{x\|x\le t_1\}]$)	2,P8,A1
4. J believes (TTP received sub_K at $[T_s]$)	3,P3,Nec,A1
5. J believes (A said sub_K_p at $[T_s]$)	4,P1(1),Nec,A1,A4
6. J believes (A received NRR at $[T_r\|\{x\|x\le T_s\}]$)	5,P5,A1
7. J believes (B said NRR_p at $[T_r]$)	6,P1(2),Nec,A1,A4
8. J believes (B received NRO at $[T_o\|\{x\|x\le T_r\}]$)	7,P6,A1
9. J believes (B received NRO_p at $[T_o]$)	8,P2(1),Nec,A1,A7
10. J believes (B received C at $[T_o]$)	9,Nec,A1,A6
11. J believes (B received con_K at $[T_B\|\{x\|T_s\le x\le T_s+t_0\}]$)	3,P3,A1
12. J believes (B received con_K_p at $[T_B]$)	11,P2(2),Nec,A1,A7
13. J believes (B received K at $[T_B]$)	12,Nec,A1,A6
14. J believes (B received M at $[\max(T_o,T_B)]$)	10,13,P11,A1
15. J believes (B received M at $[\max(T_o,T_B)]\wedge B$ said NRR_p at $[T_r]$)	7,14,Nec,A1
时间演算:	
令 $T_x=\max(T_o,T_B)$,$T_y=T_r$.现证明 $T_y\le T_x\le t_1+t_B\le t$:	
$T_x=\max(T_o,T_B)$	
$\Rightarrow T_x=T_B$	因 $T_o\le T_r\le T_s\le T_B$
$\Rightarrow T_s\le T_x\le T_s+t_0$	因 $T_B\in\{x\|T_s\le x\le T_s+t_0\}$
$\Rightarrow T_y\le T_x\le T_s+t_0$	因 $T_y=T_r$
$\Rightarrow T_y\le T_x\le t_1+t_0$	因 $T_y=T_r$
因此,只需将时间常元的值定义为:$t_0\le t_B$ 且 $t_1+t_B\le t$,即可得 $T_y\le T_x\le t_1+t_B\le t$.	

从上面的分析可以看出,只要 B 在发送 NRR 时保证 T_1 到 T 之间的时间足够长(长于网络不可用的最长时间),它就可以只等待有限的时间(到时间 T 为止).如果时间 T 过去之后它还没有收到 con_K,它就可以将从 A 收到的 NRO 安全地删除了.因此可以看出,NZG 协议具有时限性.

4 新逻辑的性质

上面对两个协议的分析具体地说明了这种扩展后的逻辑是如何分析不可否认协议中事件间的时间关系的,但这并不足以说明所作扩展是正确和合理的.现在对本文所作的扩展的正确性和特点进行简要的阐述.

4.1 正确性分析

本文对 SVO 逻辑所作的扩展有以下几处:

(1) 为 receive 和 say 添加一个 at 操作以描述这几种事件发生的具体时间;

(2) 为 receive 和 say 相关的公理添加时间表达式以推导事件间的时间关系.

(3) 在证明过程之后添加一个时间演算过程来验证协议是否能保证事件时间关系满足预期的约束条件.

可以从 3 个部分来分析新逻辑的正确性:首先看逻辑推理部分的正确性.本文没有为 SVO 逻辑添加新的公理.从第 2 节、第 3 节的分析中可以看出,如果把分析过程中的 at 操作去除,那么整个分析过程就完全是使用原逻辑进行的分析过程.所以,逻辑推理部分的正确性由原逻辑的正确性决定;其次,本文没有在时间演算部分提出任何新的证明方法,所进行的证明都是基于代数和集合理论进行的.因此,时间演算部分的正确性就得到了保证;最后要考虑的是对 SVO 逻辑公理的扩展是否合理.正如上面所指出的,如果去除 at 操作,那么几个扩展过的公理和原逻辑中对应的公理是相同的.因此,只需确定添加的 at 操作在公式中是否正确.

实际上,公理中 receive 和 say 事件的时间在 SVO 逻辑的基于可能世界的语义中已得到了描述,本文所作的扩展只是将语义用语法进行表达,便于对协议的分析.以 receive 事件为例进行说明:

在 SVO 逻辑的语义[8]中,实体 P_i 在点(r,t)上的已收消息(received messages)的集合包括:(1) 消息 X,这里,$receive(X)$出现在 t 或 t 之前的局部消息历史中;(2) 任何收到的连接消息的子项;(3) 消息 X,这里,$\{X\}_K$是一个已收消息,而且 P_i 持有 K'并进行转换,则 receive 的真值条件为

$$(r,t)\models P \text{ received } X \quad \text{iff} \quad X \text{ 在点}(r,t)\text{上 } P \text{ 的已收消息集合中.}$$

那么,P received X at $[T|TS]$的语义就是:存在 $t\in TS$,使得$(r,t)\models P$ received X.

现在,以公理 A7 为例证明公理的正确性.我们不关心 P has K'的时间,可以认为对所有的 $t\geq 0$ 都有$(r,t)\models P$ has K'.根据 P 的已收消息集合的定义可知,对于任意 t,如果$(r,t)\models \{X\}_K^{-1}\{X\}_{K^{-1}}$ 且$(r,t)\models P$ has K',那么$(r,t)\models P$ received X.所以 A7 是成立的.

4.2 特点与展望

本文扩展后的新逻辑不是一种单纯的逻辑方法,而是一种综合的方法.协议目标证明过程中的逻辑推理部分是基于 SVO 逻辑的证明方法的,但时间演算部分使用的则是代数和集合理论的方法.使用这种综合的方法基于以下几点考虑:

(1) 逻辑方法没有状态爆炸的问题,且容易实现分析过程自动化.

(2) 从 ZG 协议及其扩展可以看出,不可否认协议对协议事件的先后关系,甚至是事件先后间隔的长短都很敏感.使用一般的逻辑方法很难描述并分析时间的数量关系,而使用代数方法来描述和分析则是很简单的.

(3) 在扩展的逻辑中,逻辑方法部分和代数方法是相对独立的两个部分,不会造成不同方法因混合而相互干扰并破坏原有方法的正确性.

因此,本文的扩展既保留了 SVO 逻辑的简单性和正确性,又增强了它的时间描述能力,适于分析不可否认协议的时限性.但本文的扩展是专门针对分析不可否认协议的时限性需要而提出来的,它只考虑到了对信息发送与接收行为的描述,而对逻辑中的其他公式的时间没有进行描述,而且它没有考虑实体本地计算和信道传输信息需要花费的时间.但使用本文的思想是可以对上述的问题进行扩展的.

5 结束语

SVO 逻辑因其简单性在安全协议和不可否认协议的形式化分析中得到了广泛的应用,但它的时间描述能力太弱,无法分析不可否认协议的时限性.本文为 SVO 逻辑添加了一种简单的时间表达式和分析方法,增强了它的时间描述和分析能力.使用新逻辑对 Zhou J.和 Gollmann D.于 1996 年提出的一个不可否认协议和它的一个扩展进行分析的结果表明:原协议不具有时限性,而改进的协议具有时限性.这也说明了扩展后的新逻辑具有分析不可否认协议的时限性的能力.我们进一步的工作是进行第 4.2 节中指出的两个方向的研究工作,将 SVO 逻辑扩展成为一种能够分析各种安全协议时间描述和分析的形式化工具,并为新逻辑的协议理想化工作设计一种形式化的方法以保证分析结果的可靠性.

References:

[1] Norman G, Shmatikov V. Analysis of probabilistic contract signing. In: Proc. of the BCSFACS Formal Aspects of Security (FASec 2002). LNCS 2629, 2002. 81−96. http://citeseer.ist.psu.edu/norman02analysis.html

[2] Buttyun L, Hubaux P, Capkun S. A formal model of rational exchange and its application to the analysis of Syverson's protocol. Journal on Computer Security, 2004,12(3-4):551−587.

[3] Abadi M, Blanchet B. Computer-Assisted verification of a protocol for certified email. In: Cousot R, ed. Static Analysis, the 10th Int'l Symp. (SAS 2003). LNCS 2694, 2003. 316−335.

[4] Kremer S, Raskin JF. A game-based verification of non-repudiation and fair exchange protocols. Journal of Computer Security, 2003,11(3):399−429.

[5] Shmatikov V, Mitchell JC. Finite-State analysis of two contract signing protocols. Theoretical Computer Science, 2002,283(2): 419−450.

[6] Qing SH. A new non-repudiation protocol. Journal of Software, 2000,11(10):1338−1343 (in Chinese with English abstract).

[7] Li XX, Huai JP. A fair non-repudiation cryptographic protocol and its formal analysis and applications. Journal of Software, 2000, 11(12):1628−1634 (in Chinese with English abstract).

[8] Syverson PF, van Oorschot PC. On unifying some cryptographic protocol logics. In: Proc. of the '94 IEEE Computer Society Symp. on Security and Privacy. Oakland: IEEE Computer Society Press, 1994. 14−28.

[9] Burrows M, Abadi M, Needham R. A logic of authentication. ACM Trans. on Computer Systems, 1990,8(1):18−36.

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

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

[12] Zhou J, Gollmann D. Towards verification of non-repudiation protocols. In: Proc. of the 1998 Int'l Refinement Workshop and Formal Methods Pacific. Berlin: Springer-Verlag, 1998. 370−380.

[13] Schneider S. Formal analysis of a non-repudiation protocol. In: Proc. of the 11th IEEE Computer Security Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 1998. 54−65.

[14] Fan H, Feng DG. Formal analysis of a non-repudiation protocol ZG. Journal of Electronics, 2005,1(30):171−173 (in Chinese with English abstract).

[15] Mao W. An augmentation of BAN-like logics. In: Foley S, ed. Proc. of the 8th IEEE Computer Security Foundations Workshop. Dromquinna: IEEE Computer Society Press, 1995. 44−56.

附中文参考文献:

[6] 卿斯汉.一种新型的非否认协议.软件学报,2000,11(10):1338−1343.

[7] 李先贤,怀进鹏.公平的非否认密码协议及其形式分析与应用.软件学报,2000,11(12):1628−1634.

[14] 范红,冯登国.一个非否认协议 ZG 的形式化分析.电子学报,2005,1(30):171−173.

黎波涛(1976－),男,博士生,主要研究领域为网络安全.

罗军舟(1960－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为协议工程,网络安全,网络管理,网格计算.