一种可靠的多方不可否认协议的逻辑分析方法

苑博奥 刘 军
(陆军工程大学指挥信息系统学院 南京 210007)

摘 要 多方不可否认协议需要满足不可否认性、公平性和时限性三大安全目标,但是现有的对多方不可否认协议的形式化分析方法大多是对两方协议分析方法的简单扩展,单一方法不能完整覆盖所有的安全目标分析;同时,对单一安全目标的分析能力有限,分析结果不可靠。首先,综合比较现有的分析技术,选定SVO逻辑进行扩展,显式引入时间因素,给出对应的语法定义和时间演算公理。然后,对改进逻辑的语义模型进行介绍,并证明了逻辑系统的可靠性,使得改进后的逻辑系统支持对多方不可否认协议三大安全目标的分析。最后,选取一个典型的多方不可否认协议,分别对其时限性和公平性进行分析,发现了其中存在的时限性和公平性缺陷,并给出了对应的攻击方法。其中,公平性缺陷是首次被发现。

关键词 多方不可否认协议,SVO逻辑,时限性,公平性
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.07.024

Reliable Logic Analysis Method of Multi-party Non-repudiation Protocol

YUAN Bo-ao LIU Jun
(College of Command Information Systems, Army Engineering University of PLA, Nanjing 210007, China)

Abstract Multi-party non-repudiation protocol needs to meet three main security goals of non-repudiation, fairness and timeliness, but the existing formal analysis methods for multi-party non-repudiation proctocol are just simple extensions of those applied to two-party protocols. At the same time, each method can not cover all three security goals and has limited ability to analyze one goal with result unreliable. In this paper, the existing analysis methods were compared and the SVO logic was chosen for further study. Time factor was introduced in the logic system with relevant syntax definition and deduction axioms brought in explicitly. Then, the semantic model of the improved logic was stated and the soundness of logic system was proved, causing that the improved logic system can support the analysis of all three security goals of multi-party non-repudiation protocol. In the end, a typical multi-party non-repudiation protocol was analyzed with the improved logic and the defects of timeliness and fairness were found with corresponding attacks stated. Among the defects, the defect of fairness was discovered for the first time.

Keywords Multi-party non-repudiation protocol, SVO logic, Timeliness, Fairness

1 引言

计算机网络技术的发展为人们提供了便捷的通信和资源共享服务,但同时网络中所传输信息的安全问题愈加突出。密码协议(又称安全协议)是为保证信息交互的安全而综合运用密码算法和协议设计技术设计的网络交互协议。冯登国[1]依据密码协议的设计目标将密码协议分为4类:密钥交换协议、认证协议、认证密钥交换协议和电子商务协议。不可否认协议属于电子商务协议,主要用于防止协议的参与方在协议执行后否认自己参与协议的事实而损害其他参与方的利益。多方不可否认协议是指参与方数目多于两个的不可否认协议,协议参与方数目的增多会使协议拓扑结构更加复杂,交互过程更富动态性,同时也会使协议的设计与安全性分析更加困难。

多方不可否认协议的协议设计技术经历了从两方协议阶段[2]、多方单一消息阶段[3-4]到多方多消息阶段[5]的过程,其设计技术已基本满足现有应用领域的功能需求,但不能保证满足其安全需求。多方不可否认协议的设计需要满足3个安全目标:1)不可否认性。这是设计此类协议的初衷,包括消息发送方对发送行为的不可否认和接收方对消息正确接收事实的不可否认。2)公平性。协议执行结束后,消息发送方应获得接收方的接收证据;同时,接收方也必须获得发送方的发送证据。公平性是指协议参与方均获得自己所需的证据项,或者协议参与方均没有获得任何有价值的信息。3)时限性。协议的诚实参与方应在有限的时间内完成协议,并且没有违反公平性。协议的任意参与方都可以在任意时刻终止协议,但前提是这种行为没有损害自身的利益。不满足时限性的协议,协议参与方因无法接收到所需证据项而长久等待下去,无

到稿日期:2017-05-29 返修日期:2017-08-28
苑博奥(1992-),男,硕士生,主要研究方向为安全协议、信息安全,E-mail:yuanboao1201@sina.com;刘 军(1969-),男,教授,主要研究方向为信息安全、软件工程,E-mail:13914735588@139.com(通信作者)。

法正常终止协议。很显然,不满足时限性的协议很有可能同样不满足公平性,但是不能将时限性分析简单归于公平性的分析,协议设计中一些时间因素设置不当也会造成时限性问题,但是简单地对协议的公平性进行分析却容易忽略时间因素的作用,不能发现其中存在的问题。

协议的形式化分析是验证协议是否满足其安全目标的重要方法。现有的对多方不可否认协议的形式化分析方法大多是将两方协议分析方法向多方扩展,这种扩展涉及到密码协议的三大类形式化分析方法,即逻辑方法、模型检测方法和定理证明方法,但是至今仍没有完善的针对多方不可否认协议三大安全目标的形式化分析技术。在对逻辑方法的扩展中[6-7],已有的研究工作通过在原有公式后面附加时间表达式的方式改进了 SVO 逻辑,但是在改进的逻辑系统中并没有给出时间表达式的语法定义和对应的语义解释,因此该系统并不是一个完整的逻辑系统,其时限性分析过程也只是简单的代数运算,无法保证改进后的逻辑系统具有可靠性,从而无法保证通过此逻辑系统得出的结论一定是正确的。在对模型检测方法的扩展中,文献[8]用交替转换系统建模协议,用交替时序逻辑刻画协议的安全属性,并分析了协议的公平性。此种分析方法的局限性表现在分析过程中必须限定协议实例的数量和接收者的数量为有限的常数,否则将出现状态空间爆炸问题,即无法分析参与者数目为 n 的情况;同时,该方法可以发现协议中存在的安全问题,却不能证明正确协议的正确性。在对定理证明方法的扩展中,文献[9]将签名操作加入串空间模型,将公平性表达为串空间中不可否认证据项之间的双向蕴含关系,协议的证明过程较为复杂。该方法可以证明协议的正确性,但是对不能完成证明的协议不能指出其中存在的安全缺陷,对协议设计的指导能力有限。至此,在多方不可否认协议的分析方法中,没有一种分析方法可以同时支持三大安全目标的分析,同时,它们对单一安全目标的分析能力有限,分析结果不可靠。

相比之下,SVO 逻辑属于信念逻辑,便于表达公平性与不可否认性,不存在状态空间爆炸问题,没有对协议参与方的数目进行限制,其证明过程清晰,能够在一定程度上证明协议的正确性,也可通过对证明过程进行分析发现协议中存在的安全缺陷。但是,SVO 逻辑仅能区分过去和现在,对时间的表达能力有限,已有的一些改进停留在语法层面,不能证明逻辑系统的可靠性,破坏了逻辑系统的完整性。本文主要基于 SVO 逻辑做出改进,在逻辑系统中显式地引入时间因素,并对应给出逻辑系统的语法定义和语义解释,证明了逻辑系统的可靠性,并用改进后的逻辑方法分析了一个典型的多方不可否认协议,发现了其中存在的时限性问题和公平性问题。为表述方便,将改进后的逻辑系统简称为 TSVO(Time-SVO)逻辑。

本文第 2 节介绍了 TSVO 逻辑的语法部分及公理系统;第 3 节给出了 TSVO 逻辑的语义模型,并对 TSVO 逻辑系统的可靠性进行证明;第 4 节采用 TSVO 逻辑对典型的多方不可否认协议进行时限性与公平性的分析;最后总结全文。

2 TSVO 逻辑的定义

2.1 语法部分

TSVO 逻辑以 SVO 逻辑为基础,针对多方不可否认协议三大安全目标的分析进行改进,舍弃了与此无关的部分,同时添加了支持时限性分析的相关定义。TSVO 逻辑由以下定义组成。

定义 1(原始项 T) 原始项 T 中包含 3 种符号类型的常量与变量:主体、密钥和时间。

定义 2(消息 M_T) 对消息进行如下归纳:

1)X 是消息,如果 $X\in T$;

2)$F(X_1,\cdots,X_n)$是消息,如果 $X_1,\cdots,X_n$ 是消息,F 为任意函数(包括加密 $\{X\}_k$、组加密 $E_{R'}(X)$、签名 $S_{R_i}(X)$等操作);

3)φ 是消息,如果 φ 是公式。

定义 3(公式 F_T) 对公式进行如下归纳:

1)$R_i\in R$ 是公式,R 为主体的集合,R_i 为特定主体;

2)$PK_\sigma(P,k)$是公式,如果 P 为主体,k 为密钥;

3)$T_y\leqslant T_x$ 和 $T_y=T_x$ 是公式,T_x 和 T_y 是时间常量或变量;

4)$P\ SeesA_{T_x}\ X$,$P\ RcvdA_{T_x}\ X$ 和 $P\ SaidA_{T_x}\ X$ 是公式,如果 P 为主体,X 是消息,T_x 是时间;

5)$P\ BlvsA_{T_x}\ \varphi$ 是公式,如果 P 为主体,φ 是公式,T_x 是时间;

6)$\neg\varphi$ 和 $\varphi\wedge\psi$ 是公式,如果 φ 和 ψ 是公式,$\neg$ 和 $\wedge$ 组成了完备联结词组,可以表示其他命题联结词,如$\rightarrow$等。

2.2 公理系统

TSVO 逻辑的公理系统由两条推理规则、若干公理以及所有谓词逻辑的重言式组成。

1)推理规则

分离规则(MP):$\dfrac{\vdash\varphi,\ \vdash\varphi\rightarrow\psi}{\vdash\psi}$

必然规则(Nec):$\dfrac{\vdash\varphi}{\vdash P\ BlvsA_{T_x}\varphi}$。其中,$P$ 代表任意主体;T_x 为时间变量,代表任意时刻。

2)相信公理

A1 $P\ BlvsA_{T_x}\ \varphi\wedge P\ BlvsA_{T_x}(\varphi\rightarrow\psi)\rightarrow P\ BlvsA_{T_x}\ \psi$

A2 $P\ BlvsA_{T_x}\ \varphi\wedge P\ BlvsA_{T_x}\ \psi\rightarrow P\ BlvsA_{T_x}(\varphi\wedge\psi)$

A3 $P\ BlvsA_{T_x}(\varphi\wedge\psi)\rightarrow P\ BlvsA_{T_x}\ \varphi\wedge P\ BlvsA_{T_x}\ \psi$

3)源关联公理

A4 $PK_\sigma(R_i,k_i)\wedge P\ RcvdA_{T_x}\ S_{R_i}(X)\rightarrow R_i\ SaidA_{T_x}\ X$

4)收到公理

A5 $P\ RcvdA_{T_x}(X_1,\cdots,X_n)\rightarrow P\ RcvdA_{T_x}\ X_i$

A6 $P\ RcvdA_{T_x}\ \{X\}_k\wedge P\ SeesA_{T_y}\ \widetilde{k}\rightarrow P\ RcvdA_{T_z}\ X\wedge(T_z=\max(T_x,T_y))$,$\widetilde{k}$ 为与 k 对应的解密密钥。

A7 $P\ RcvdA_{T_x}\ S_{R_i}(X)\rightarrow P\ RcvdA_{T_x}\ X$

A8 $R_i\ RcvdA_{T_x}\ E_{R'}(X)\wedge R_i\in R'\rightarrow R_i\ RcvdA_{T_x}\ X$

5)看见公理

A9 $P\ RcvdA_{T_x}\ X\rightarrow P\ SeesA_{T_x}\ X$

6)说过公理

A10　$P\ SaidA_{T_x}(X_1,\cdots,X_n)\rightarrow(P\ SaidA_{T_x}\ X_i\wedge P\ SeesA_{T_x}\ X_i)$

7)时间演算公理

A11　$T_x\leqslant T_y\wedge T_y\leqslant T_z\rightarrow T_x\leqslant T_z$

A12　$T_x=T_y\wedge\varphi(T_x)\rightarrow\varphi(T_y/T_x)$,其中 $\varphi(T_x)$为任意带有时间变量 T_x 的公式,$\varphi(T_y/T_x)$为用变量 T_y 替换 T_x 后的公式。

3　TSVO 逻辑的语义

3.1　TSVO 逻辑的语义模型

在给出 TSVO 逻辑的语义之前,首先对其语义模型进行介绍。将协议看作是由有限多个可相互传递消息的主体 $P_1,\cdots,P_n$ 组成的,同时假设存在一个特殊主体 P_e 用于抽象协议的执行环境,其中包括可能的协议攻击者。在协议执行的任意时刻,每个主体均有其本地状态,所有主体的本地状态组成了协议的全局状态,用本地状态的元组$(s_e,s_1,\cdots,s_n)$表示,其中 s_e 为环境 P_e 的本地状态,s_i 为 P_i 的本地状态,主体可以通过执行一定的行为来改变其本地状态。

定义 4(主体的行为)　任意主体 P 可执行的行为如下:

1)$send(X,G)$,P 向主体集合 G 中的主体发送消息 X,并要求主体只能发送它看见的消息;

2)$receive(X)$,P 接收到一个消息 X;

3)$generate(X)$,P 生成了一个新的消息,但该消息只能是原子消息,即 T 中的成员。

定义 5(主体的本地状态)　任意主体 P_i 的本地状态 s_i 包含一个本地历史(主体曾执行的所有行为)及一个密钥集合(主体所拥有的密钥集合)。环境 P_e 的本地状态包含一个全局历史(任意主体执行过的行为序列)、一个密钥集合以及为每个主体 P_i 所准备的消息缓存 X_i(X_i 中包含发给 P_i 但尚未接收的消息)。

定义 6(可能世界)　运行 r 是一个全局状态的无穷序列,表示协议的一种可能的执行轨迹,协议是所有可能运行的集合 $\Re$。在每个运行中,赋予每个全局状态一个整数时间,运行 r 的第一个状态被赋予某一时间值 $T_r\leqslant 0$,第 j 个状态被赋予时间 $T_r+(j-1)$,将零时刻的状态作为当前时段的第一个状态,并称其为初始状态。由运行 r 和时间 τ 组成的元组(r,τ)被称为可能世界,其表示协议的一次执行 r 在时间 τ 时所处的状态。

定义 7(收到的消息集合 $RcvdM$)　定义主体 P 在(r,τ)收到的消息为 P 在(r,τ)为止所显示收到的消息,描述如下:

1)如果 $receive(X)$出现在 P 的本地历史,并且出现在可能世界(r,τ)中或可能世界(r,τ)以前,则 $X\in RcvdM$。

2)如果 $X_i\in RcvdM$ 且 $X_j\in RcvdM$,则 $(X_i,X_j)\in RcvdM$。

3)如果$(X_1,\cdots,X_n)\in RcvdM$,则 $X_i\in RcvdM$。

4)如果$\{X\}_k\in RcvdM$,并且 P 可利用 $\tilde{k}$ 对其实施解密(即 $\tilde{k}$ 在 P 本地状态的密钥集合中,$\tilde{k}$ 为对应于 k 的解密密钥),则 $X\in RcvdM$。如果 P 收到加密消息与获得解密密钥不在同一时刻,则主体会在后一时刻收到解密后的消息。

5)如果 $S_{R_i}(X)\in RcvdM$,则 $X\in RcvdM$,当主体收到对某消息的签名时,主体同时收到了该消息。

6)如果 $E_{R'}(X)\in RcvdM$,并且主体 P 在主体集合 R'中,则 $X\in RcvdM$。当主体收到运用组加密方式加密的消息,且其自身又属于主体集合时,主体可以对加密消息进行解密。

定义 8(看见的消息集合 $SeesM$)　定义主体 P 在(r,τ)看见的消息为到(r,τ)为止显示收到的、生成的或者初始拥有的消息,以及由这些消息通过 P 可计算的递归变形而得到的消息,描述如下:

1)如果 X 属于 P 在(r,τ)收到的消息集合,则 $X\in SeesM$;

2)如果 X 属于 P 到(r,τ)为止生成的消息或初始拥有的消息,则 $X\in SeesM$;

3)如果 $X_1,\cdots,X_n$ 属于消息集合 $SeesM$,则 $F(X_1,\cdots,X_n)\in SeesM$,$F$ 为主体 P 可计算的任意函数(包括加密 $\{X\}_k$、组加密 $E_{R'}(X)$和签名 $S_{R_i}(X)$等)。

定义 9(说过的消息集合 $SaidM$)　定义主体 P 在(r,τ)说过的消息为在(r,τ)之前所发送过的所有消息的说过子消息集合 $SaidSubM$ 的并,主体说过的消息是其看见消息的子集。设 m 为 P 在(r,τ)点发送的消息,则将消息 m 的说过子消息集合 $SaidSubM$ 定义为:

1)$m\in SaidSubM$;

2)若$(X_1,\cdots,X_n)\in SaidSubM$,则$(X_{j1},\cdots,X_{ji})\in SaidSubM$;

3)若$\{X\}_k\in SaidSubM$,并且 P 拥有密钥 k,则 $X\in SaidSubM$;

4)若 $S_P(X)\in SaidSubM$,则 $X\in SaidSubM$。

定义 10(本地理解运行 r_i^*)　在 SVO 逻辑的语义中,曾给出一种消息构造过程[10-11],对于主体 P_i 在(r,τ)世界的任意消息 X,构造过程可以将其转换为消息 $X_i(r,\tau)$,使得消息 $X_i(r_i,\tau)$是主体 P_i 可以理解的消息结构。当消息 X 为 $\{X\}_k$,并且 P_i 没有对应的解密密钥 $\tilde{k}$ 时,P_i 不能理解 X 为 $\{X_i\}_k$ 还是$\{X_j\}_k$,$X_i(r,\tau)$对应变为 $*_x$,若消息 X 为 P_i 所能理解的明文 m,则 $X_i(r,\tau)$仍为明文 m。对于给定运行 r 及主体 P_i,$r_i(\tau)$为 P_i 在 r 中 τ 时的本地状态,本地理解运行 r_i^* 为将任意时刻 τ 中的任意消息 X 替换为 $X_i(r,\tau)$后得到的运行,X 与 $X_i(r,\tau)$之间是一一对应的关系。

定义 11(可达关系 $\sim_i$)　定义主体 P_i 在可能世界(r,τ)与(r',τ')之间是可达的,即$(r,\tau)\sim_i(r',\tau')$,当且仅当对应的本地理解运行 $r_i^*(\tau)$和 $r_i'^*(\tau')$可通过统一替换 $*$ 的下标而相互生成。例如,在 $r_i^*(\tau)$和 $r_i'^*(\tau')$中,当 $*_j$ 在 $r_i^*(\tau)$中出现时,都有对应的 $*_k$ 在 $r_i'^*(\tau')$中出现,除此之外两者都相同。

3.2　公式的真值条件

给定协议 $\Re$,用$(r,\tau)\vdash\varphi$ 表示 φ 在(r,τ)世界成立,$\vdash\varphi$ 表示 φ 是有效的,即在所有可能世界都成立。TSVO 逻辑的语义可以由以下定义的公式的真值条件递归给出。

1)主体

$(r,\tau)\vdash R_i\in R$,当且仅当 R_i 为主体集合 R 中的成员。

2)时间

$(r,\tau)\models T_y\leqslant T_x$,当且仅当对于任意的运行 r',全局状态序列中(r',T_y)出现在(r',T_x)之前;

$(r,\tau)\models T_y=T_x$,当且仅当对于任意的运行 r',全局状态(r',T_y)与(r',T_x)相同。

3)看见

$(r,\tau)\models P\ SeesA_\tau X$,当且仅当 X 属于主体 P 在(r,τ)世界看见的消息集合 $SeesM$。

$(r,\tau)\models P\ SeesA_{T_x} X$,如果 $T_x\leqslant\tau$,则当且仅当$(r,T_x)\models P\ SeesA_{T_x} X$;如果 $\tau\leqslant T_x$,则当且仅当$(r,\tau)\models P\ SeesA_\tau X$。

4)收到

$(r,\tau)\models P\ RcvdA_\tau X$,当且仅当 X 属于主体 P 在(r,τ)世界收到的消息集合 $RcvdM$。

$(r,\tau)\models P\ RcvdA_{T_x} X$,如果 $T_x\leqslant\tau$,则当且仅当$(r,T_x)\models P\ RcvdA_{T_x} X$;如果 $\tau\leqslant T_x$,则当且仅当$(r,\tau)\models P\ RcvdA_\tau X$。

5)说过

$(r,\tau)\models P\ SaidA_\tau X$,当且仅当 X 属于主体 P 在(r,τ)世界说过的消息集合 $SaidM$。

$(r,\tau)\models P\ SaidA_{T_x} X$,如果 $T_x\leqslant\tau$,则当且仅当$(r,T_x)\models P\ SaidA_{T_x} X$;如果 $\tau\leqslant T_x$,则当且仅当$(r,\tau)\models P\ SaidA_\tau X$。

6)密钥

$(r,\tau)\models PK_\sigma(R_i,k_i)$,当且仅当对于所有的 τ',如果$(r,\tau')\models P\ RcvdA_{T_x} S_{R_i}(X)$,那么$(r,\tau')\models R_i\ SaidA_{T_x} X$。

7)相信

$(r,\tau)\models P\ BlvsA_\tau\varphi$,当且仅当对于所有的$(r',\tau')$,如果$(r,\tau)\sim_i(r',\tau')$,则有$(r',\tau')\models\varphi$。

$(r,\tau)\models P\ BlvsA_{T_x}\varphi$,如果 $T_x\leqslant\tau$,则当且仅当$(r,T_x)\models P\ BlvsA_{T_x}\varphi$;如果 $\tau\leqslant T_x$,则当且仅当$(r,\tau)\models P\ BlvsA_\tau\varphi$。

8)逻辑联结词

$(r,\tau)\models\neg\varphi$,当且仅当$(r,\tau)\not\models\varphi$;

$(r,\tau)\models\varphi\wedge\psi$,当且仅当$(r,\tau)\models\varphi$且$(r,\tau)\models\psi$。

3.3 TSVO 逻辑的可靠性

定理 1(TSVO 逻辑的可靠性) TSVO 逻辑是可靠的,如果 $\Gamma\vdash\varphi$,则 $\Gamma\models\varphi$。

证明:为了证明该定理,需要证明其公理是有效的,推理规则是保真的。

A1 假设$(r,\tau)\models P\ BlvsA_{T_x}\varphi\wedge P\ BlvsA_{T_x}(\varphi\rightarrow\psi)$,根据逻辑联结词的真值条件,$(r,\tau)\models P\ BlvsA_{T_x}\varphi$ 且$(r,\tau)\models P\ BlvsA_{T_x}(\varphi\rightarrow\psi)$成立。根据由相信公式的真值条件,对 τ 与 T_x 的大小关系分情况讨论。

1)当 $T_x\leqslant\tau$ 时,由上述假设得$(r,T_x)\models P\ Blvs\ A_{T_x}\varphi$,$(r,T_x)\models P\ BlvsA_{T_x}(\varphi\rightarrow\psi)$;对于任意的可能世界$(r',\tau')$,若有$(r,T_x)\sim_P(r',\tau')$,则有$(r',\tau')\models\varphi$,$(r',\tau')\models\varphi\rightarrow\psi$,从而$(r',\tau')\models\psi$成立;由相信公式的真值条件得$(r,T_x)\models P\ BlvsA_{T_x}\psi$成立,进一步地,$(r,\tau)\models P\ BlvsA_{T_x}\psi$ 成立。A1 得证。

2)当 $\tau\leqslant T_x$ 时,由上述假设得$(r,\tau)\models P\ BlvsA_\tau\varphi$,$(r,\tau)\models P\ BlvsA\tau(\varphi\rightarrow\psi)$;对于任意的可能世界$(r',\tau')$,若有$(r,\tau)\sim_P(r',\tau')$,则有$(r',\tau')\models\varphi$,$(r',\tau')\models\varphi\rightarrow\psi$,从而$(r',\tau')\models\psi$成立;由相信公式的真值条件得$(r,\tau)\models P\ BlvsA_\tau\psi$ 成立,进一步地,$(r,\tau)\models P\ BlvsA_{T_x}\psi$ 成立。A1 得证。

A2 和 A3 的证明与 A1 类似,在此不再赘述。

A4 假设$(r,\tau)\models PK_\sigma(R_i,k_i)\wedge P\ RcvdA_{T_x} S_{R_i}(X)$,根据逻辑联结词的真值条件,$(r,\tau)\models PK_\sigma(R_i,k_i)$且$(r,\tau)\models P\ RcvdA_{T_x} S_{R_i}(X)$。由 $PK_\sigma(R_i,k_i)$公式的真值条件及$(r,\tau)\models P\ RcvdA_{T_x} S_{R_i}(X)$得$(r,\tau)\models R_i\ SaidA_{T_x} X$。A4 得证。

A5 假设$(r,\tau)\models P\ RcvdA_{T_x}(X_1,\cdots,X_n)$。根据收到公式的真值条件,对 τ 与 T_x 的大小关系分情况讨论。

1)当 $T_x\leqslant\tau$ 时,有$(r,T_x)\models P\ RcvdA_{T_x}(X_1,\cdots,X_n)$;由收到公式的真值条件得$(X_1,\cdots,X_n)$属于 P 在(r,T_x)世界收到的消息集合 $RcvdM$,由 $RcvdM$ 的定义可知 $X_i\in RcvdM$,从而$(r,T_x)\models P\ RcvdA_{T_x} X_i$,进一步地,有$(r,\tau)\models P\ RcvdA_{T_x} X_i$。A5 得证。

2)同理可证 $\tau\leqslant T_x$ 的情况。

A6 假设$(r,\tau)\models P\ RcvdA_{T_x}\{X\}_k\wedge PSeesA_{T_y}\tilde{k}$,根据逻辑联结词真值条件,$(r,\tau)\models P\ RcvdA_{T_x}\{X\}_k$,并且$(r,\tau)\models P\ SeesA_{T_y}\tilde{k}$。根据 τ,T_x 和 T_y 的相对大小关系,分情况进行讨论。

1)当 $\tau\leqslant T_x\leqslant T_y$ 时,有$(r,\tau)\models P\ RcvdA_\tau\{X\}_k$,且$(r,\tau)\models P\ SeesA_\tau\tilde{k}$;根据收到公式和看见公式的真值条件可得,$\{X\}_k$ 属于 P 在(r,τ)世界收到的消息集合 $RcvdM$,$\tilde{k}$ 属于 P 在(r,τ)世界看见的消息集合 $SeesM$;根据收到的消息集合 $RcvdM$ 的定义,$X\in RcvdM$,$(r,\tau)\models P\ RcvdA_\tau X$,从而$(r,\tau)\models P\ RcvdA_{T_y}X$,且有 $T_y=\max(T_x,T_y)$。A6 得证。

2)当 $T_x\leqslant\tau\leqslant T_y$ 时,有$(r,T_x)\models P\ RcvdA_{T_x}\{X\}_k$,且$(r,\tau)\models P\ SeesA_\tau\tilde{k}$;由收到公式和看见公式的真值条件可知 $\{X\}_k$ 属于 P 在(r,T_x)世界收到的消息集合,$\tilde{k}$ 属于 P 在(r,τ)世界看见的消息集合;根据收到的消息集合的定义及 T_x 与 τ 发生的先后关系,$\{X\}_k$ 也属于 P 在(r,τ)世界收到的消息集合,即$(r,\tau)\models P\ RcvdA_\tau\{X\}_k$,从而 X 属于 P 在(r,τ)世界收到的消息集合,即$(r,\tau)\models P\ RcvdA_\tau X$,因此有$(r,\tau)\models P\ RcvdA_{T_y} X$,且 $T_y=\max(T_x,T_y)$。A6 得证。

3)当 $T_x\leqslant T_y\leqslant\tau$ 时,有$(r,T_x)\models P\ RcvdA_{T_x}\{X\}_k$,且$(r,T_y)\models P\ SeesA_{T_y}\tilde{k}$;由收到公式和看见公式的真值条件可知 $\{X\}_k$ 属于 P 在(r,T_x)世界收到的消息集合,$\tilde{k}$ 属于 P 在(r,T_y)世界看见的消息集合;根据收到的消息集合的定义及 T_x 与 T_y 发生的先后关系,$\{X\}_k$ 也属于 P 在(r,T_y)世界收到的消息集合,即$(r,T_y)\models P\ RcvdA_{T_y}\{X\}_k$,从而 X 属于 P 在(r,T_y)世界收到的消息集合,即$(r,T_y)\models P\ RcvdA_{T_y} X$,因此有$(r,\tau)\models P\ RcvdA_{T_y} X$,且 $T_y=\max(T_x,T_y)$。A6 得证。

4)$\tau\leqslant T_y\leqslant T_x$,$T_y\leqslant\tau\leqslant T_x$ 和 $T_y\leqslant T_x\leqslant\tau$ 的情况,与上述证明类似,不再赘述。

A7 假设$(r,\tau)\models P\ RcvdA_{T_x} S_{R_i}(X)$,根据收到公式的真值条件,对 τ 与 T_x 的大小关系分情况进行讨论。

1)当 $T_x\leqslant\tau$ 时,有$(r,T_x)\models P\ RcvdA_{T_x} S_{R_i}(X)$,由收到公式的真值条件可知 $S_{R_i}(X)$属于 P 在(r,T_x)世界收到的消息集合 $RcvdM$;由收到的消息集合的定义可知 $X\in RcvdM$,即$(r,T_x)\models P\ RcvdA_{T_x} X$,因此有$(r,\tau)\models P\ RcvdA_{T_x} X$。A7 得证。

2）当 $\tau \leqslant T_x$ 时，有 $(r,\tau) \vdash P\ RcvdA_{\tau}\ S_{R_i}(X)$，与上述证明类似。

A8　由收到公式的真值条件及收到的消息集合 $RcvdM$ 的定义可证。

A9　由收到公式与看见公式的真值条件及看见的消息集合 $SeesM$ 的定义可证。

A10　由收到公式的真值条件及说过的消息集合 $SaidM$ 的定义可证。

A11　由时间公式的真值条件可证。

A12　由公式的真值条件可知，公式的真假取决于协议运行的全局状态，再根据时间公式的真值条件，此公理可得证。

以上证明了 TSVO 逻辑公理系统的有效性，下面说明：如果公式集合 Γ 中的公式均为真，则通过使用 TSVO 逻辑的公理和推理规则得出的公式 φ 仍然为真。对此分情况进行讨论：

1）如果 φ 是一个定理或者 $\varphi \in \Gamma$，那么 $\Gamma \vdash \varphi$ 是显然的；

2）如果 φ 是由分离规则得到的，那么在 φ 之前，一定存在 ψ 和 $\psi \rightarrow \varphi$ 结构为真，则由公式的真值条件可知 $\Gamma \vdash \varphi$；

3）如果 φ 由必然规则得到，那么在 φ 之前，一定有 $\vdash \psi$，并且 φ 具有 $P\ BlvsA_{T_x}\ \psi$ 的形式；根据归纳假设，由 $\vdash \psi$ 可得 $\vdash \psi$，在所有的可能世界 (r,τ) 中，公式 ψ 均为真；依据相信公式的真值条件有 $\vdash P\ BlvsA_{T_x}\ \psi$，从而有 $\Gamma \vdash \varphi$。

至此，定理 1 得证。

4　协议分析

Dolev 和 Yao 于 1983 年提出了 DY 模型，模型中抽象了攻击者所具有的攻击能力：1）攻击者可以获取通过网络的任何消息；2）攻击者可以以合法用户的身份向其他任何用户发起会话；3）攻击者有可能成为任何用户所发送消息的接收者。在该模型下，攻击者对网络具有完全的控制权，可以在协议执行中的任何环节采取多种形式的攻击。逻辑分析方法建立在 DY 模型的基础上，从已知的事实出发，推理得到所需的安全目标或其反面。TSVO 逻辑适用于多方不可否认协议三大安全目标的分析：不可否认性、公平性和时限性。对于不可否认性的分析，其主要证明由协议参与方执行协议收到的证据可以推理得到协议真实发生的事实，已有工作对此进行了深入研究[7,12]。下面主要运用 TSVO 逻辑分析多方不可否认协议的时限性和公平性，以证实逻辑方法的有效性。

4.1　协议描述

Kremer 和 Markowitch 于 2000 年提出了第一个多方不可否认协议[3]，其主要思想是运用组加密技术对两方不可否认协议进行扩展，为表述方便，称此协议为 KM 协议。KM 协议的主要流程如图 1 所示。证实分析方法有效性的普遍方法有两种：1）分析并能够发现协议中存在新的安全问题；2）分析并发现已知的安全问题。KM 协议是多方不可否认协议中的典型协议，许多协议都是在 KM 协议的基础上进行改进设计[13-14]；同时，KM 协议存在已知的时限性问题，便于检验所提分析方法的有效性。因此，本文选定 KM 协议作为分析对象。

1）$O \Rightarrow R: f_{Eoo}, R, l, t, c, Eoo$

2）$R_i \rightarrow O: f_{Eor}, O, R_i, l, Eor_i$ where each $R_i \in R$

3）$O \rightarrow TTP: f_{Sub}, R', l, t, E_{R'}(k), Sub_k$

4）$R_i' \leftrightarrow TTP: f_{Con}, O, R', l, E_{R'}(k), Con_k$ where each $R_i' \in R'$

5）$O \leftrightarrow TTP: f_{Con}, O, R', l, E_{R'}(k), Con_k$

图 1　KM 协议

Fig. 1　KM protocol

对协议中涉及的符号进行说明。

1）协议参与主体：协议涉及 3 类参与主体，即消息发送者 O、消息接收者的集合 R 以及可信第三方 TTP。另外，R' 为向主体 O 发送协议消息 2）（见图 1）的接收者主体集合。

2）协议消息符号：$f_{\{Eoo,Eor,Sub,Con\}}$ 为消息标识，分别预示着消息的目的为源不可否认证据、接收不可否认证据、密钥提交证据和密钥公布证据；l 是一个特殊的标识，$l=h(m,k)$，其中 $h(\cdot)$ 为单向哈希函数，指示着本次协议运行的唯一性；t 为协议运行的时间参数，为 TTP 公布密钥的最后期限；c 为用对称密钥 k 对消息 m 加密的密文；$E_{R'}(k)$ 为运用组加密方式对 k 进行加密的密文，只可以由主体 $R_i \in R'$ 进行解密。

3）证据项及缩写：$Eoo = S_O(f_{Eoo}, R, l, t, c)$，$Eor_i = S_{R_i}(f_{Eor}, O, l, t, c)$，$Sub_k = S_O(f_{Sub}, R', l, t, E_{R'}(k))$ 和 $Con_k = S_{TTP}(f_{Con}, O, R', l, t, E_{R'}(k))$ 均为主体对消息的签名，分别代表了主体 O 对密文 c 的发送不可否认证据、主体 R_i 对密文 c 的接收不可否认证据、主体 O 对密钥 k 的提交不可否认证据和主体 TTP 对密钥 k 的公布不可否认证据。为方便表述，分别以 $Eoop$，Eor_{ip}，Sub_{kp} 和 Con_{kp} 代表主体所签名的消息。

4）消息传递方式：$O \Rightarrow R$ 表示主体 O 向主体集合 R 多播消息；$X \rightarrow Y$ 表示主体 X 向主体 Y 发送消息；$X \leftrightarrow Y$ 表示主体 X 通过 FTP 从主体 Y 处获得消息。

主体 O 首先发起协议，向主体集合 R 中的成员多播消息 1）（见图 1），等待成员回复包含接收证据的消息 2）；随后，主体 O 选择一个合适的时间继续执行协议，即发送消息 3）（见图 1），超过此时间到达的接收证据不再被接收；TTP 收到消息后，验证最后期限 t 的有效性，在 FTP 目录中公布有关解密密钥 k 的消息，如果密钥 k 在时间 t 并没有被公布，则在以后的时间也不会被公布；协议假设主体与 TTP 之间是弹性信道，信道并不总是不可用，即通过此信道发送的消息一定会由对方接收到，假定信道最长的不可用时间为 t_A，TTP 中目录公布的时长为 t_B。

4.2　时限性分析

假定 t_E 是协议终止后协议参与主体向仲裁方提出仲裁的时间。首先给出 KM 协议关于主体密钥的假设：

P1.1　$J\ BlvsA_{t_E}\ PK_{\sigma}(O,k_o)$

P1.2　$J\ BlvsA_{t_E}\ PK_{\sigma}(R_i,k_i)$

P1.3　$J\ BlvsA_{t_E}\ PK_{\sigma}(TTP,k_{TTP})$

关于主体和时间的假设：

P2　$J\ BlvsA_{t_E}(R_i \in R')$

纠纷产生时需要进行仲裁，O 和 R_i 将收集的证据提交给仲裁者 J：

P3　$J\ BlvsA_{t_E}(J\ RcvdA_{t_E}\{Eoo, Eor_i, Con_k\})$

假设 TTP 是称职的，它只有在收到 Sub_k 后才会产生证

据 Con_k，且不会拖延时间：

P4 $J\ BlvsA_{t_E}(TTP\ SaidA_{T_x}\ Con_{kp} \rightarrow TTP\ RcvdA_{T_x}\ Sub_k)$

O 和 R_i 与 TTP 间的信道并非永久不可用，只要 TTP 发布了证据，它们一定能在此后的 t_A 时间内收到：

P5 $J\ BlvsA_{t_E}(TTP\ SaidA_{T_x}\ Con_{kp} \rightarrow (O\ RcvdA_{T_y}\ Con_k \wedge T_x \leqslant T_y \wedge T_y \leqslant T_x + t_A))$

P6 $J\ BlvsA_{t_E}(TTP\ SaidA_{T_x}\ Con_{kp} \rightarrow (R_i\ RcvdA_{T_y}\ Con_k \wedge T_x \leqslant T_y \wedge T_y \leqslant T_x + t_A))$

主体不会做对自己不利的事情，即 R_i 仅在收到 Eoo 后才会发送 Eor_i，O 仅在收到 Eor_i 后才会提交 Sub_k：

P7 $J\ BlvsA_{t_E}(O\ SaidA_{T_x}\ Sub_{kp} \rightarrow (O\ RcvdA_{T_y}\ Eor_i \wedge T_y \leqslant T_x))$

P8 $J\ BlvsA_{t_E}(R_i\ SaidA_{T_x}\ Eor_{ip} \rightarrow (R_i\ RcvdA_{T_y}\ Eoo \wedge T_y \leqslant T_x))$

KM 协议的时限性要求表现为：消息的发送和接收行为应在适当的时间范围内完成。以主体 R_i 为例，其时限性目标为：

G1 $J\ BlvsA_{t_E}(R_i\ RcvdA_{T_x}\ m \wedge R_i\ SaidA_{T_y}\ Eor_{ip} \wedge T_y \leqslant T_x \wedge T_x \leqslant t + t_B)$

目标 G1 说明 R_i 必定是在提交 Eor_{ip}，即接收不可否认证据后，时间 $t+t_B$ 之前获得 Con_k，进而获得明文消息 m。若能证明上述目标，就能说明协议对于主体 R_i 具备时限性。下面对 G1 进行推理证明。

目标 1 G1 $J\ BlvsA_{t_E}(R_i\ RcvdA_{T_x}\ m \wedge R_i\ SaidA_{T_y}\ Eor_{ip} \wedge T_y \leqslant T_x \wedge T_x \leqslant t + t_B)$

证明：

1) $J\ BlvsA_{t_E}(P\ RcvdA_{T_x}(X_1,\cdots,X_n) \rightarrow P\ RcvdA_{T_x}\ X_i)$ {A5,Nec.}

2) $J\ BlvsA_{t_E}(J\ RcvdA_{t_E}\ Con_k)$ {P3,1),A1,MP.}

3) $J\ BlvsA_{t_E}(PK_\sigma(R_i,k_i) \wedge P\ RcvdA_{T_x}\ S_{R_i}(X) \rightarrow R_i\ SaidA_{T_x}\ X)$ {A4,Nec.}

(4) $J\ BlvsA_{t_E}(PK_\sigma(TTP,k_{TTP}) \wedge J\ RcvdA_{t_E}\ Con_k)$ {P1.3,2),A2,MP.}

5) $J\ BlvsA_{t_E}(TTP\ SaidA_{t_E}\ Con_{kp})$ {4),3),A1,MP.}

6) $J\ BlvsA_{t_E}(TTP\ RcvdA_{t_E}\ Sub_k)$ {5),P4,A1,MP.}

7) $J\ BlvsA_{t_E}(PK_\sigma(O,k_o) \wedge TTP\ RcvdA_{t_E}\ Sub_k)$ {P1.1,6),A2,MP.}

8) $J\ BlvsA_{t_E}(O\ SaidA_{t_E}\ Sub_{kp})$ {7),3),A1,MP.}

9) $J\ BlvsA_{t_E}(O\ Rcvd\ A_{T_m}\ Eor_i \wedge T_m \leqslant t_E)$ {8),P7,A1,MP.}

10) $J\ BlvsA_{t_E}(O\ RcvdA_{T_m}\ Eor_i)$ {9),A3,MP.}

11) $J\ BlvsA_{t_E}(PK_\sigma(R_i,k_i) \wedge O\ RcvdA_{T_m}\ Eor_i)$ {P1.2,10),A2,MP.}

12) $J\ BlvsA_{t_E}(R_i\ SaidA_{T_m}\ Eor_{ip})$ {11),3),A1,MP.}

13) $J\ BlvsA_{t_E}(R_i\ RcvdA_{T_u}\ Eoo \wedge T_u \leqslant T_m)$ {12),P8,A1,MP.}

14) $J\ BlvsA_{t_E}(R_i\ RcvdA_{T_u}\ Eoo)$ {13),A3,MP.}

15) $J\ BlvsA_{t_E}(P\ RcvdA_{T_x}\ S_{R_i}(X) \rightarrow P\ RcvdA_{T_x}\ X)$ {A7,Nec.}

16) $J\ BlvsA_{t_E}(R_i\ RcvdA_{T_u}\ Eoop)$ {14),15),A1,MP.}

17) $J\ BlvsA_{t_E}(R_i\ RcvdA_{T_u}\ c)$ {16),{A5,Nec.},A1,MP.}

18) $J\ BlvsA_{t_E}(R_i\ RcvdA_{T_v}\ Con_k \wedge t_E \leqslant T_v \wedge T_v \leqslant t_E + t_A)$ {5),P6,A1,MP.}

19) $J\ BlvsA_{t_E}(R_i\ RcvdA_{T_v}\ Con_k)$ {18),A3,MP.}

20) $J\ BlvsA_{t_E}(R_i\ RcvdA_{T_v}\ Con_{kp})$ {19),15),A1,MP.}

21) $J\ BlvsA_{t_E}(R_i\ RcvdA_{T_v}\ E_{R'}(k))$ {1),20),A1,MP.}

22) $J\ BlvsA_{t_E}(R_i\ RcvdA_{T_x}\ E_{R'}(X) \wedge R_i \in R' \rightarrow R_i\ RcvdA_{T_x}\ X)$ {A8,Nec.}

23) $J\ BlvsA_{t_E}(R_i\ RcvdA_{T_v}\ k)$ {21),P2,A2,MP.,22),A1,MP.}

24) $J\ BlvsA_{t_E}(P\ RcvdA_{T_x}\ X \rightarrow P\ SeesA_{T_x}\ X)$ {A9,Nec.}

25) $J\ BlvsA_{t_E}(R_i\ SeesA_{T_v}\ k)$ {23),24),A1,MP.}

26) $J\ BlvsA_{t_E}(R_i\ RcvdA_{T_r}\ m \wedge T_r = \max(T_u, T_v))$ {17),25),{A6,Nec.},A1,MP.}

27) $J\ BlvsA_{t_E}(T_u \leqslant T_m \wedge T_m \leqslant t_E \wedge t_E \leqslant T_v \wedge T_v \leqslant t_E + t_A)$ {13),9),18){A3,Nec.},{A2,Nec.},A1,MP.}

28) $J\ BlvsA_{t_E}(T_u \leqslant T_v)$ {27),{A11,Nec.},MP.}

29) $J, BlvsA_{t_E}(T_r = T_v)$ {26),28)}

30) $J\ BlvsA_{t_E}(T_m \leqslant T_r)$ {27),29),{A11,Nec.},{A12,Nec.},MP.}

31) $J\ BlvsA_{t_E}(T_r \leqslant t_E + t_A)$ {18),29),{A12,Nec.},MP.}

32) $J\ BlvsA_{t_E}(R_i\ RcvdA_{T_r}\ m \wedge R_i\ SaidA_{T_m}\ Eor_{ip} \wedge T_m \leqslant T_r \wedge T_r \leqslant t_E + t_A)$ {26),12),30),31),{A12,Nec.},MP.}

从证明 32)得到 $T_r \leqslant t_E + t_A$，目标 G1 为 $T_r \leqslant t + t_B$。从证明 5)可得，t_E 为 TTP 公布 Con_k 的时间，由协议的约定，公布时间应不晚于最终期限 t，即 $t_E \leqslant t$，且 $t_E = t$ 是可能的；T_r 为 R_i 在 TTP 处获得 Con_k 的时间，由对弹性信道的假设，$T_r = t_E + t_A$ 是可能的，则必须有 $t_A \leqslant t_B$ 成立，即要求 TTP 公布 Con_k 的时间应长于信道的最长不可用时间，才能保证主体正确获得 Con_k，而这也正是 KM 协议不满足时限性的原因。恶意的 O 在接近最终期限 t 时提交 Sub_k，并在 TTP 公布 Con_k 后干扰 TTP 与 R_i 之间的信道，使得 R_i 因无法检索到 Con_k 而不能正常终止协议。协议中的时限性缺陷导致了协议执行结束后协议发起者 O 获得了接收者 R_i 参与协议的证据，而接收者 R_i 却未能获得发起者 O 参与协议的证据。例如在多方电子商务活动中，商家将商品券发送给客户，当客户凭券去领取商品时，商家却否认曾发送过商品券给客户；同时，客户因没有足够的证据而不能保证自己的权益。

4.3 公平性分析

KM 协议的公平性要求表现为主体提供了相应的消息（证据），同时获得了相应的证据（消息），在对时限性分析过程中，G1 表达了主体 R_i 获得了相应的消息，同时也提供了接收证据。在时限性分析过程中已对此进行了证明，下面针对主体 O 设置公平性目标并加以证明。

目标 2 G2 $J\ BlvsA_{t_E}(O\ SaidA_{T_x}\ m \wedge O\ RcvdA_{T_y}\ Con_k)$

证明：

33) $J\ BlvsA_{t_E}(O\ SaidA_{t_E}\ Sub_{kp})$ {8)}

34) $J\ BlvsA_{t_E}(O\ SaidA_{t_E}\ E_{R'}(k))$
{33),{A10,Nec.},A1,MP.}

35) $J\ BlvsA_{t_E}(J\ RcvdA_{t_E}\ Eoo)$　　{P3,1),A1,MP.}

36) $J\ BlvsA_{t_E}(O\ SaidA_{t_E}\ Eoop)$
{P1.1,35),{A4,Nec.},A1,MP.}

37) $J\ BlvsA_{t_E}(O\ SaidA_{t_E}\ c)$
{36),{A10,Nec.},A1,MP.}

38) $J\ BlvsA_{t_E}(O\ SaidA_{t_E}\ E_{R'}(k) \wedge O\ SaidA_{t_E}\ c)$
{34),37),A2,MP.}

通过证明，可以得到主体 O 的确发送了包含密钥的组加密密文 $E_{R'}(k)$ 和包含明文消息的密文 c，但是无法证明 $E_{R'}(k)$，c 和 m 三者之间的对应关系，无法得到主体 O 的确发送了消息 m 的结论，由此发现一种对协议的新的攻击方式，如图 2 所示。主体 O 同时发起了两个协议会话 $RunA$ 和 $RunB$，两协议各自遵照协议规范与主体 RA 和主体 RB 执行 KM 协议，主体 O 在向可信第三方 TTP 提交解密密钥即消息 3)时，却恶意地交换了 $RunA$ 和 $RunB$ 的消息，使得主体 RA 和主体 RB 无法对应解密运用组加密方式保护的密钥，进而无法获得对应的消息 m，同时，因为主体 O 可以得到两个协议会话 $RunA$ 和 $RunB$ 的不可否认证据，恶意的主体 O 却可以向仲裁机构证实向合法主体发送了消息 m，从而造成协议的公平性缺失。协议中公平性缺陷同样导致协议执行结束时，协议发起者 O 获得了接收者 R_i 参与协议的证据，而接收者 R_i 却未能获得发起者 O 参与协议的证据，主体 O 可以否认参与协议的事实，而主体 R_i 却没有足够的证据保证自己的权益。

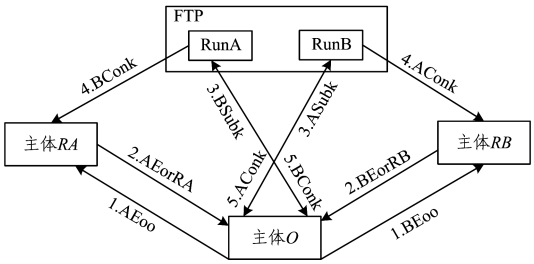

图 2　公平性缺陷

Fig. 2　Defect of fairness

结束语　本文提出了一种适用于多方不可否认协议不可否认性、公平性和时限性三大安全目标的形式化分析方法——TSVO 逻辑。该逻辑系统中显式地引入了时间因素，给出了对应的语法定义，设置了相应的时间演算公理，并对逻辑系统的语义模型进行了介绍，证明了逻辑系统的可靠性；同时对一个典型的多方不可否认协议进行了时限性和公平性分析，分别发现了其中存在的时限性和公平性缺陷，其中公平性问题是首次被发现。另外，TSVO 逻辑也存在着对多协议参与方行为的表达不充分的问题，例如多参与方之间的共谋行为，这是下一步的研究重点。

参 考 文 献

[1] FENG D G, FAN H. Survey on Theories and Methods of Formal Analysis for Security Protocols[J]. Journal of the Graduate School of the Chinese Academy of Sciences, 2003, 20(4): 389-406. (in Chinese)
冯登国，范红. 安全协议形式化分析理论与方法研究综述[J]. 中国科学院研究生院学报，2003，20(4)：389-406.

[2] ZHOU J, GOLLMAN D. A fair non-repudiation protocol[C]// Proceedings of the 1996 IEEE Symposium on Security and Privacy. Oakland: IEEE Computer Society Press, 1996: 55-61.

[3] KREMER S, MARKOWITCH O. A multi-party non-repudiation protocol[C]// 15th International Conference on Information Security (SEC 2000). Beijing: Kluwer, 2000: 271-280.

[4] KREMER S, MARKOWITCH O. Fair multi-party non-repudiation protocols[J]. International Journal of Information Security, 2003, 1(4): 223-235.

[5] ONIEVA J A, ZHOU J, CARBONELL M, et al. A Multi-Party Non-Repudiation Protocol for Exchange of Different Messages [M]. Boston: Springer, 2003: 37-48.

[6] HAN Z G, LUO J Z. Analysis and Improvement of Timeliness of a Multi-Party Non-Repudiation Protocol[J]. Acta Electronica Sinica, 2009, 37(2): 377-381. (in Chinese)
韩志耕，罗军舟. 多方不可否认协议时限性分析与改进[J]. 电子学报，2009，37(2)：377-381.

[7] WANG X, WANG X. Formal Analysis Of Multi-party Non-repudiation Protocols Without TTP[C]// International Conference on Communications and Intelligence Information Security. Nanning: IEEE Computer Society Press, 2010: 96-99.

[8] WANG X M, WENG L C. Analysis and Improvement of A Fair Multi-party Non-repudiation Protocol Based on ATL Logic[J]. Information Security and Technology, 2011, 2(9): 21-25. (in Chinese)
汪学明，翁立晨. 基于 ATL 逻辑的公平多方不可否认协议的分析与改进[J]. 信息安全与技术，2011，2(9)：21-25.

[9] LI L, WANG L, CHEN J, et al. Fairness Analysis for Multiparty Nonrepudiation Protocols Based on Improved Strand Space[J]. Discrete Dynamics in Nature & Society, 2014, 17(1): 1-7.

[10] SYVERSON P F, VAN O P C. A Unified Cryptographic Protocol Logic[R]. Washington: Naval Research Lab, 1996.

[11] LEI X F, XUE R. The Logic Methods of Cryptographic Protocol Analysis[M]. Beijing: Science Press, 2013: 154-159. (in Chinese)
雷新锋，薛锐. 密码协议分析的逻辑方法[M]. 北京：科学出版社，2013：154-159.

[12] WANG Y M. The Application Study on Formalism of Multi-Party Non-Repudiation Protocols on SVO Logic[D]. Guiyang: Guizhou University, 2009. (in Chinese)
王远敏. 基于 SVO 逻辑的多方不可否认协议的形式化分析与研究[D]. 贵阳：贵州大学，2009.

[13] HE B, LI X J, XIA C H, et al. A Fair Multi-Party Non-Repudiation Protocol[J]. Computer Engineering and Applications, 2005, 41(27): 120-122. (in Chinese)
何冰，李肖坚，夏春和，等. 公平的多方不可否认协议[J]. 计算机工程与应用，2005，41(27)：120-122.

[14] HAN Z G, LUO J Z. A Fair Multi-Party Non-Repudiation Protocol[J]. Chinese Journal of Computers, 2008, 31(10): 1705-1715. (in Chinese)
韩志耕，罗军舟. 一个公平的多方不可否认协议[J]. 计算机学报，2008，31(10)：1705-1715.