doi:10.3969/j.issn.1000-436x.2012.z2.026

多方不可否认协议的增广 CSP 建模与分析

韩志耕[1]，陈耿[1]，罗军舟[2]
(1. 南京审计学院 信息科学学院，江苏 南京 211815；2. 东南大学 计算机科学与工程学院，江苏 南京 211189)

摘 要：基于逆向工程的思想，使用前期工作中提出的面向两方不可否认协议分析的增广 CSP 方法，对典型的 Kremer-Markowitch 多方不可否认协议的安全性进行了探索性建模与分析。借助该分析成功发现此协议在满足不可否认性和公平性的同时却不具备时限性。这表明在适用于两方不可否认协议安全性验证的同时，增广 CSP 方法也可作为多方不可否认协议安全性验证的新方法。

关键词：形式化分析；多方不可否认；时限性；增广 CSP 方法
中图分类号：TP393 **文献标识码**：B **文章编号**：1000-436X(2012)Z2-0189-07

Modeling and analysis of multi-party non-repudiation protocols with extended-CSP approach

HAN Zhi-geng[1], CHEN Geng[1], LUO Jun-zhou[2]
(1. School of Information Science, Nanjing Audit University, Nanjing 211815, China;
2. School of Compute Science and Engineer, Southeast University, Nanjing 211189, China)

Abstract: Follow with the methodology of reverse engineering, an exploratory modeling and analysis of security of the typical Kremer-Markowitch multi-party non-repudiation protocol were carried out with a novel method named extended-CSP approach which had been proposed for two-party non-repudiation protocol in preliminary work. With the analysis, the inherent fact that this protocol statisfies not timeliness but non-repudiality and fairness was found successfully. The result of the analysis indicates that, as applying to two-party non-repudiation protocols, the extended-CSP approach can also be a new method for security verification of multi-repudiation protocols.

Key words: formal analysis; multi-party non-repudiation; timeliness; extended-CSP approach

1 引言

作为国际标准化组织定义的 5 项安全服务之一，不可否认服务通过收集、维护和验证与一个事件及行为相关的不可抵赖证据，以解决相关事件或行为是否发生的纠纷[1]。该服务近年来在电子商务[2]、合同签名[3]、签收邮件[4]、公平交换[5]、审计取证[6]和云存储完整性[7]等众多领域取得广泛应用。为确

收稿日期：2012-11-06
基金项目：国家自然科学基金资助项目(71271117, 70971067, 61272074)；江苏省高校自然科学基金资助项目(12KJB520005, 12KJD410001)；江苏省网络与信息安全重点实验室基金资助项目(BM2003201)；江苏省高校科研成果产业化推进工程基金资助项目(JHB2012-20)；江苏省六大人才高峰基金资助项目(07-E-025)；南京审计学院人才引进基金资助项目(NSRC10033)
Foundation Items: The National Natural Science Foundation of China (71271117, 70971067, 61272074); The Natural Science Foundation of Jiangsu Educational Committee(12KJB520005, 12KJD410001); Jiangsu Provincial Key Laboratory of Network and Information Security (BM2003201); The Scientific Research Promotion Industrialization Project of Jiangsu Educational Committee (JHB2012-20); The Jiangsu Provincial Six Talents Peak Project (07-E-025); Nanjing Audit University Talent Introduction Project (NSRC10033)

保不可否认服务的有效性，首先需要确保不可否认协议的安全性[8]。

形式化分析是确保不可否认协议安全性的常用方法，但目前并没有研制出针对不可否认协议分析的专用方法。所有的分析都是借助于已有的密码协议分析技术进行。以著名的 Zhou-Gollmann 两方不可否认协议[9]为例，Zhou 等人[10]和冯登国等人[11]使用 SVO 逻辑、Schneider[12]使用进程代数 CSP、Bella 等人[13]使用定理证明器 Isabelle、Kremer 等人[14]使用博弈论及模型检测工具 Mocha、Ġurgens 等人[15]使用异步积自动机(APA)及简单同态验证工具(SHVT)、罗军舟等人[16]使用有色 Petri 网、Wei 等人[17]使用有限状态工具 PVS 和 FDR、Armando 等人[18]使用带弹性信道编码的 LTL、Klay 等人[19]使用扩展 AVISPA、Mayla Brusò等人[20]使用进程演算工具 LYSA 和控制流分析等诸多技术对该协议及其变体的部分安全性质进行了满足性分析。

在形式化分析研究上，虽然目前针对两方不可否认协议的研究有很多，但以多方不可否认协议为目标的讨论却极少。有代表性的研究包括，1）在状态检测方面，采用有限状态工具 Mocha，2003 年 Kremer 等人[21]分析过 Markowitch-Kremer 多方不可否认协议的时限性；2004 年 Chadha 等人[22]分析过 2 个多方合同签名协议(Garay-MacKenzie 及 Baum-Waidner)的公平性。2）在定理证明方面，2005 年 Mukhamedov 等人[23]使用串空间模型分析过 Franklin-Tsudik 多方公平交换协议及其变体协议(Gonzalez-Markowitch)的公平性。3）在逻辑推理方面，2009 年韩志耕等人[24]利用扩展 SVO 逻辑方法分析过 Kremer-Markowitch 多方不可否认协议的时限性。

多方不可否认协议分析研究进展缓慢的原因在于，与两方不可否认协议相比，多方不可否认协议的实体数目和消息数量要大很多，其所需要满足的安全性质更难于描述与分析。其一，以状态检测类分析而言，模型选择太小会导致安全性质得不到充分分析；模型选择过大会导致状态空间爆炸。其二，多方不可否认协议实体行为复杂，逻辑推理类描述的高层抽象性无法准确地从事件层面上对实体行为序列进行准确描述。其三，多方不可否认协议事件具备时间敏感性，如何使用定理证明类技术对该类协议时限性进行建模与分析并没有出现公开讨论。其四，多方不可否认协议基本性质之间彼此关联：一方面，不可否认性是目标，公平性和时限性是达成目标的重要手段；另一方面，时限性的满足情况会对真公平和强公平的实现形成制约；这使得只有采取统一的框架方法对 3 个基本性质进行整体分析，才能有效避免传统的利用不同方法建模分析不同安全性质所带来的力度差异性。从目前研究来看，除笔者以两方不可否认协议为目标进行过前期预研外[25]，并没有发现其他的公开讨论。

考虑到目前的趋势是综合利用多种手段，取长补短，以期发现更多的协议缺陷，达到更好的分析效果。本文基于逆向工程思想，利用前期工作中提出的增广 CSP 方法对典型的多方不可否认协议进行了探索，尝试性建模与分析，以期为该类协议的安全性形式化分析提供一种新方法。

2 理论准备

2.1 基本安全性质

实用的多方不可否认协议必须具备不可否认性、公平性和时限性等基本安全性质。然而，截至目前仍不存在针对上述性质的形式化定义，考虑到下文建模与分析的方便性，此处基于文献[26,27]提供的定义，给出一对多通信拓扑（应用最多）下多方不可否认协议的基本性质。

设 A 为发送实体，B_i 为接收实体集 B 中成员，$Evidence\_A_i$ 和 $Evidence\_B_i$ 为 A 和 B_i 交互中收集到的证据，$Message_i$ 为它们间的交互数据。

定义 1 多方不可否认协议具备发送不可否认性，当且仅当，对于任意的协议执行均有：1) 协议执行前：A 持有 $Message_i$，B_i 不持有 $Evidence\_B_i$ 和 $Message_i$；2) 协议执行后：B_i 持有 $Message_i$ 和 $Evidence\_B_i$；3) 若 B_i 持有 2) 中数据，则 A 发送过 $Message_i$。

定义 2 多方不可否认协议具备接收不可否认性，当且仅当，对于任意的协议执行均有：1) 协议执行前：A 持有 $Message_i$ 且 A 不持有 $Evidence\_A_i$，B_i 不持有 $Message_i$；2) 协议执行后：B_i 持有 $Message_i$ 且 A 持有 $Evidence\_A_i$；3) 若 A 持有 $Evidence\_A_i$，则 B_i 接收过 $Message_i$。

定义 3 多方不可否认协议具备不可否认性，当且仅当该协议满足发送不可否认性和接收不可否认性。

定义 4 多方不可否认协议具备公平性，当且仅当，对于任意的协议执行均有：1) 协议执行前：

A 持有 $Message_i$ 且 A 不持有 $Evidence\_A_i$，B_i 不持有 $Evidence\_B_i$ 和 $Message_i$；2) 协议执行后：A 持有 $Evidence\_A_i$ 且 B_i 持有 $Message_i$ 和 $Evidence\_B_i$，或 A 不持有 $Evidence\_A_i$ 且 B_i 不持有 $Evidence\_B_i$ 和 $Message_i$；3) 若 A 持有 $Evidence\_A_i$，则 B_i 持有 $Message_i$；若 B_i 持有 $Evidence\_B_i$ 和 $Message_i$，则 A 持有 $Message_i$。

定义 5　多方不可否认协议具备时限性，当且仅当，对于任意的协议执行均有：给定协议执行开始后的任意时刻 T，诚实的协议实体均可在时刻 T' ($T<T'$)之前结束协议执行，且其在时刻 T'持有的公平性级别不低于其在时刻 T 持有的公平性级别。

2.2　增广 CSP 方法

为确保能够在统一的方法框架内对两方不可否认协议的基本安全性质进行同粒度分析，文献[25]以秩函数理论为基础，通过扩展进程代数 CSP（communicating sequential processes）提出了一种适用于两方不可否认协议建模与分析的新方法—增广 CSP 方法。该方法将时间维添加到传统的 CSP 事件定义，即 $event = c.\ i.\ j.\ m.\ T$，其中，$new\_event$ 为协议事件，c 为信道、i 为信源、j 为信宿、m 为信息和 T 为协议事件发生的具体时间（时间表达式）。

增广 CSP 方法对两方不可否认协议的分析遵循如下 4 步。第 1 步给出时间常元和变元；第 2 步建立增广 CSP 模型，包括协议整体模型、实体模型，以及信道模型等；第 3 步描述协议安全性质，其中安全规约作为迹谓词给出，活性规约作为失效谓词给出；并在规约中建立协议事件间的时间约束关系目标；第 4 步验证协议性质是否满足，其中安全性和活性主要依靠秩函数和组件活性来保证。在对时间敏感性质进行分析时，需要另外增加一个时间演算，负责对事件之间的时间约束关系进行满足性推演。

为检验增广 CSP 方法的有效性，文献[25]利用该方法成功检测到 Zhou 和 Gollmann 于 1996 年提出的 Zhou-Gollmann 公平不可否认协议固有的时限性缺陷，同时还首次形式化证明了 Kim-Park-Baek 变体协议[28]通过向协议消息中添加时间限制信息的办法的确弥补了原协议存在的这个缺陷。在此基础上，该文进而从语义的正确性（依据：源于进程语法上的显式表达，没有破坏 CSP 原始语义）、非时间敏感性质分析的正确性（依据：基于秩函数理论）、时间敏感性质分析的正确性（依据：源于初等代数和集合理论的正确性）3 个方面对增广 CSP 方法的正确性进行了讨论。

3　Kremer-Markowitch 协议分析

3.1　协议描述

Kremer-Markowitch 协议是 Zhou-Gollmann 协议的多方扩展[26]。T 是 A 及 B'中成员获得 K 和 Con_k 的最终期限，TTP 在期限 T 过后将 Con_k 从公共目录中删除。如果 B 中成员 B_i 不同意 A 规定的期限 T，它可在步骤 2 就停止协议执行。协议交互步骤如下。

$Bi \in B$ *and* $i \in \{1,\cdots,|B|\}$

$B' \subseteq B$

$B'j \in B'$ and $\forall j: 1 \leqslant j \leqslant |B'|$

$L=h(M, K)$

$EOO=S_A(f_{EOO}, B, L, T, h(C))$

$EOR_i=S_{Bi}(f_{EOR}, A, L, T, C)$

$Sub_K=S_A(f_{Sub}, B', L, T, E_{B'}(K))$

$Con_K=S_{TTP}(f_{Con}, A, B', L, T, E_{B'}(K))$

1) $A \Rightarrow B$: f_{EOO}, B, L, T, C, EOO;

2) $Bi \rightarrow A$: f_{EOR}, A, Bi, L, EOR_i;

3) $A \rightarrow TTP$: $f_{Sub}, B', L, T, E_{B'}(K), Sub_K$;

4) $A \leftrightarrow TTP$: $f_{Con}, A, B', L, E_{B'}(K), Con_K$;

5) $B'j \leftrightarrow TTP$: $f_{Con}, A, B', L, E_{B'}(K), Con_K$。

协议成功执行后，B'中成员 $B'j$ 及 A 将分别收到有关 M 的发送不可否认证据 $NRO=(EOO, Con_K)$ 和接收不可否认证据 $NRR_i=(EOR_i, Con_K)$。

3.2　协议建模

考虑到多方不可否认协议分析的重点是实体数目增大时，一个实体的欺骗行为对其他实体造成的影响。借鉴两方不可否认协议扩展为多方不可否认协议的思想[26]，可将通信拓扑为 1 对 n 的多方不可否认协议等价为 n 个并发执行的共享同一个发送源的通信拓扑为 1 对 1 的两方不可否认协议。基于上述思想，在不考虑发送方与特定的接收方共谋欺骗其他接收方，以及接收方共谋共同欺骗发送方的这两个前提下，多方不可否认协议的形式化分析可以由 n 例 2 方不可否认协议分析组成。

文献[25]中对 Zhou-Gollmann 协议的建模过程，此处定义时间常元：t_g 表示协议消息中时间控制信息 T，t_0 表示网络不可用的最长时间，t_A 和 $t_{B'j}$ 表示 A 和 $B'j$ 在发送完协议消息后等待下一消息的最长时间。其余符号（T 加下标）为时间

变元。分析中 $i(1\leqslant i\leqslant\leqslant|B|)$与 $j(1\leqslant j\leqslant|B'|)$存在如下映射：若集合 B 中标号为 i 的实体(Bi)最终被实体 A 添加到集合 B' 中，则该实体在 B' 中的标记为 j ($B'j$)。

一方面，Kremer-Markowitch 协议步骤中的接收方集合中的单个成员 Bi 等价于 Zhou-Gollmann 两方协议中的接收方 B，从这个角度来讲，前者的单个实体行为模型与后者的实体模型相同；另一方面，Kremer-Markowitch 协议在扩展 Zhou-Gollmann 时没有改变其信道模型和 *TTP* 行为模型；基于上述两方面考虑，文献[25]建模时给出的引理 1 到引理 6 和推论 1 对于本文 Kremer-Markowitch 协议模型仍然适用。

3.3 不可否认性分析

Kremer-Markowitch 协议运行后引发的纠纷包括：发送方否认，$B'j$ 接收到 A 发送的 M，但 A 否认发送过 M；接收方否认，A 发送 M 给 $B'j$，但其否认接收过 M。下面对这 2 个无否认的满足性进行验证。

1) 发送不可否认

协议目标 1：

$NRO\ (tr)\square evidence.B'j.EOO.[T_{B'j}]$ in $tr\ \wedge$ $evidence.\ B'j.\ Con_K.\ [T_{B'j}]$ in $tr \Rightarrow A$ sent EOO at $[T_x|\{x|\ x\leqslant T_{B'j}\}]\ \wedge\ A$ sent Sub_K at $[T_y|\{x|\ x\leqslant T_{B'j}\}]$。下面验证 *NETWORK* sat *NRO* (*tr*)是否成立。

证明 依次应用文献[25]中引理 4、引理 6 和推论 1，容易验证该“sat”关系成立。

2) 接收不可否认

协议目标 2：

$NRR\ (tr\ X)\ \square evidence.\ A.\ EOR_j.\ [T_A]$ in $tr \wedge$ $evidence.\ A.\ Con_K.\ [T_A]$ in $tr \Rightarrow B'j$ sent EOR_j at $[T_x|\{x|\ x\leqslant T_A\}]\wedge ftp.\ B'j.\ TTP.\ Con_K.\ [T_y]\notin X$。下面验证 *NETWORK* sat *NRR* (*tr X*)是否成立。

证明 依次应用文献[25]中引理 4、引理 1 引理 6 和引理 3，很容易验证上述“sat”关系成立。

3.4 公平性分析

分析公平性中需要注意到 Kremer-Markowitch 协议蕴含这样的事实：其一，作为理性实体，发送方和接收方均不会做对自己无利的事情，否则在日后的纠纷中将处于劣势。其二，协议实体 A 和 $B'j$ 仅在遵循协议规程 $PROT_A$ 和 $PROT_{B'j}$ 时才能确保自身的公平性。

1) 公平的消息接收

协议目标 3：

$FAIR1(tr\ X)\ \square\ evidence.\ B'j.\ M.\ [T_{B'j}]$ in $tr \Rightarrow ftp.\ A.\ TTP.\ Con_K.\ [T_A]\notin X\ \vee (evidence.\ A.\ EOR_j.\ [T_A]\notin X\ \wedge\ evidence.\ A.\ Con_K.\ [T_A]\notin X)$。需要验证 $((PROT\_AGENT_A\ |||\ (|||_{i\neq A}\ AGENT_i))\ |[ftp]|\ TTP\ )\ |[trans\ rec]|\ MEDIUM$ sat $FAIR1(tr\ X)$是否成立。

2) 公平的证据获取

其一，发送不可否认证据方面。

协议目标 4：

$FAIR2(tr\ X)\ \square\ evidence.\ A.\ Con_K.\ [T_A]$ in $tr \wedge$ $evidence.\ A.\ EOR_j.\ [T_A]$ in $tr \Rightarrow ftp.\ B'j.TTP.\ Con_K.[T_{B'j}]\notin X\ \vee\ (evidence.\ B'j.\ EOO.[T_{B'j}]\notin X\ \wedge$ $evidence.\ B'j.\ Con_K.[T_{B'j}]\notin X)$。需要验证 $((PROT\_AGENT_{B'j}|||\ (|||_{p\neq B'j}\ AGENT_p))\ |[ftp]|\ TTP\ )\ |[trans\ rec]|\ MEDIUM$ sat $FAIR2(tr\ X)$是否成立。

其二，接收不可否认证据方面。

协议目标 5：

$FAIR3(tr\ X)\ \square\ evidence.B'j.Con_K.[T_{B'j}]$ in $tr \wedge$ $evidence.B'j.EOO.[T_{B'j}]$ in $tr \Rightarrow ftp.A.TTP.\ Con_K.[T_A]\notin X\ \vee (evidence.A.\ EOR_j.\ [T_A]\notin X \wedge evidence.\ A.\ Con_K.\ [T_A]\notin X)$。需要验证 $((PROT\_AGENT_A\ |||\ (|||_{i\neq A}\ AGENT_i))\ |[ftp]|\ TTP\ )\ |[trans\ rec]|\ MEDIUM$ sat $FAIR3(tr\ X)$是否成立。

借助文献[25]中引理和推论容易验证上述 3 个“sat”关系成立，略。

3.5 时限性分析

1) 发送方 A 能否在不丢失公平性的前提下正常终止协议轮。

协议目标 6：

$TIMELINESS1(A)\ \square\ A$ sent M at $[T_x] \Rightarrow A$ received Con_K at $[T_y|\{x|T_x\leqslant x\ \leqslant T_x+t_A\leqslant\ t_g\}]$。需要验证 $((PROT\_AGENT_A\ |||\ (|||_{i\neq A}\ AGENT_i))\ |[ftp]|\ TTP)\ |[trans\ rec]|\ MEDIUM$ sat $TIMELINESS1(A)$ 是否成立。

2) 接收方 $B'j$ 能否在不丢失公平性的前提下正常终止协议轮。

协议目标 7：

$TIMELINESS2(B'j)\ \square\ B'j$ received M at $[T_x] \Rightarrow B'j$ sent EOR_j at $[T_y|\{x|\ T_x-t_{B'j}\leqslant x\leqslant T_x\leqslant t_g\}]$。需要验证 $((PROT\_AGENT_{B'j}|||\ (|||_{p\neq B'j}\ AGENT_p))\ |[ftp]|\ TTP\ )\ |[trans\ rec]|\ MEDIUM$ sat $TIMELINESS2(B'j)$是否成立。

对时限性分析由定理证明和时间演算 2 步完

成。以协议目标 7 为例，进行证明。

其一，定理证明。

据文献[25]中相关引理容易验证 $((PROT\_AGENT_{B'j} ||| (|||_{p\neq B'j} AGENT_p)) |[ftp]| TTP) |[trans\ rec]| MEDIUM$ sat $B'j$ received $M \Rightarrow B'j$ sent EOR_j 成立，下面验证 $T_x - t_{B'j} \leqslant T_y \leqslant T_x \leqslant t_g$ 是否成立。

其二，时间演算。

$PROT_{B'j} = rec.B'j?\ A?\ (S_A(f_{EOO}, \{Bi\}, l, t_g, h(C))).\ [T_o] \rightarrow trans.\ B'j!\ A!\ (S_{B'j}(f_{EOR}, A, l, t_g, C)).\ [T_r\ |\{x|\ x \geqslant T_o\}]$(理性实体 $B'j$ 仅在收到 EOO 后才发送 EOR_j) $\rightarrow ftp.\ B'j.\ TTP?\ (S_{TTP}(f_{Con}, A, \{B'j\}, l\ t_g, E_{\{B'j\}}(k))).\ [T_{B'j}|\{x|\ T_s \leqslant x \leqslant T_s + t_0\}]$(源自文献[25]中引理 2，此处 T_s 为实体 A 向 TTP 提交密钥的时间) $\rightarrow FINISHED_{B'j}(S_A(f_{EOO}\ \{Bi\}\ l\ t_g\ h(C))\ S_{TTP}(f_{Con}\ A\ \{B'j\}\ l\ t_g\ E_{\{B'j\}}(k)))$ at $[T_{FB'j}\ |\{x|\ x \geqslant T_{B'j}\}]$

协议目标 7 中的 T_x 为实体 $B'j$ 接收到消息的时刻，即为实体接收到密文和密钥的时刻，依据 $PROT_{B'j}$ 定义，可令 $T_x = max(T_o\ T_{B'j})$。

协议目标 7 中 T_y 为实体 $B'j$ 提交证据 EOR_j 的时刻，依据 $PROT_{B'j}$ 定义，有 $T_y = T_r$。

$B'j$ 是理性实体，不会做对自己无利的事情，故有 $T_o \leqslant T_r \leqslant T_s \leqslant T_{B'j}$ 又因为 $T_s \leqslant T_{B'j} \leqslant T_s + t_0$ 故有 $T_s \leqslant T_x \leqslant T_s + t_0$。考虑到 $T_x - (T_s + t_0 - T_r) \leqslant T_y \leqslant T_x$，若能保证 $T_s + t_0 - T_r \leqslant t_{B'j}$ 就能有 $T_x - t_{B'j} \leqslant T_y \leqslant T_x$。但 T_s 与 T_r 间并无约束关系，故 $T_s + t_0 - T_r \leqslant t_{B'j}$ 非横成立，即协议目标 7 中的时间约束关系无法得到满足。

所以，Kremer-Markowitch 协议不具有时限性。$B'j$ 无法在不丢失公平性的前提下正常终止协议轮。

4　进一步讨论

4.1　协议改进及验证

为使 Kremer-Markowitch 协议具备时限性，本文在文献[29]中通过添加时间限制信息和交换协议步的方法对其作如下改进，变体协议描述如下。

$l_i = h(A, Bi, TTP, h(c_i), h(K))$

$EOO_i = S_A(f_{EOO}, Bi, l_i, x_i, uBi, t_A, h(c_i))$

$L = \{ l_i \mid Bi \in B \ \wedge\ 1 \leqslant i \leqslant |B| \}$

$EOO = \{EOO_i \mid Bi \in B \ \wedge\ 1 \leqslant i \leqslant |B| \}$

$Sub_K = S_A(f_{Sub}, B, L, t_A, E_B(K), EOO\ Count_A)$

$EOR_i = S_{Bi}(f_{EOR}, A, l_i, x_i, uBi, t_{Bi}, c_i, EOO\ Count_{Bi})$

$L' = \{l_i \mid Bi \in B' \ \wedge\ 1 \leqslant i \leqslant |B'| \}$

$EOR = \{EOR_j \mid Bj \in B' \ \wedge\ 1 \leqslant j \leqslant |B'| \ \wedge B' \subseteq B \}$

$tSet_{B'} = \{t_{Bj} \mid 1 \leqslant j \leqslant |B'| \}$

$Con_K = S_{TTP}(f_{Con}, A, B', L', T, t_A, tSet_{B'}, \varphi_{B'}(E_B(K)), EOO, EOR)$

1) $A \rightarrow Bi$: $f_{EOO}, Bi, t_A, l_i, c_i, x_i, uBi, EOO_i$;

2) $A \rightarrow TTP$: $f_{Sub}, B, t_A, L, E_B(K), EOO\ Count_A\ Sub_K$;

3) $Bi \rightarrow TTP$: $f_{EOR}, A, l_i, x_i, uBi, t_{Bi}, EOO_i\ Count_{Bi}\ EOR_i$;

4) $A \leftrightarrow TTP$: $f_{Con}, A, B', L', T, t_A, tSet_{B'}, \varphi_{B'}(E_B(K)), EOR, Con_K$;

5) $Bi \leftrightarrow TTP$: $f_{Con}, A, B', L', T, t_A, tSet_{B'}, \varphi_{B'}(E_B(K)), EOR, Con_K$。

其中，时间段 t_A 和 t_{Bi} 分别由 A 和 Bi 定义，用于限定标识 TTP 存储 Sub_K 和 EOR_i 的最终期限；T 是 TTP 发布 Con_K 的时间点。

该变体协议具备不可否认性、公平性是无可非议的，但需要检验其是否满足时限性。依据 Kremer-Markowitch 协议要达成的协议目标，该变体的时限性规约构建如下。

协议目标 8：

$TIMELINESS1'(A)$ □ A sent M_i at $[T_x] \Rightarrow A$ received Con_K at $[T_y\ |\{x|T_x \leqslant\ x\ \leqslant T_x + t_A + t_0\}]$

协议目标 9：

$TIMELINESS2'(B'j)$ □ $B'j$ received M_i at $[T_x|\{x|\ T \leqslant\ x\ \leqslant\ T + t_0\}] \Rightarrow B'j$ sent EOR_j at $[T_y\ |\{x|\ T_x - t_{B'j} - t_0 \leqslant\ x\ \leqslant\ T_x\ \}]$

应用文献[25]中相关引理容易验证下列 sat 关系成立(略)。

1) $((PROT\_AGENT_A ||| (|||_{i\neq A} AGENT_i)) |[ftp]| TTP) |[trans\ rec]| MEDIUM$ sat $TIMELINESS1'(A)$。

2) $((PROT\_AGENT_{B'j} ||| (|||_{p\neq B'j} AGENT_p)) |[ftp]| TTP) |[trans\ rec]| MEDIUM$ sat $TIMELINESS2'(B'j)$。

4.2　分析技术比较

与现有技术相比，增广 CSP 方法在分析多方不可否认协议上具备如下优势，如表 1 所示。

5　结束语

基于逆向工程的思想，通过使用增广 CSP 方法对现有典型的 Kremer-Markowitch 协议进行建模与分析，为多方不可否认协议的形式化分析找到了一种新方法。然而，一方面，本文分析并没有考虑到

表 1　　**新方法与已有方法对比**

多方不可否认协议分析典型方法	状态爆炸	事件描述	基本安全性质分析
逻辑推理类（如扩展 SvO）[24]	不存在	能力弱	不适合建模与分析公平性
状态检测类（如 Mocha）[21]	存在	能力中	未见关联分析
定理证明类（如串空间模型）[23]	不存在	能力强	时限性分析未见讨论
增广 CSP 方法	不存在	能力强	可关联分析

接收者共谋，以及发送者与特定接收者共谋的情况；另一方面，本文分析侧重于在线 online TTP 协议，对目前讨论也较多的 offline TTP 协议并没有讨论。对上述 2 个方面情况下的多方不可否认协议建模与分析，需要引入新的增广 CSP 语义模型，这将是笔者下一步的工作重点。

参考文献：

[1] ISO/IEC JTC1 Information Technology-Open Systems Interconnection-Security Frameworks in Open Systems Part 4: Non-repudiation[S]. ISO/IEC DIS 10181-4, 1995.

[2] MILDREY C, JOSE M S, JAVIER L. Secure multi-party payment with an intermediary entity[J]. Computers & Security, 2009, 28(5):289-300.

[3] SJOUKE M, SASA R, MOHAMMAD T D. Minimal message complexity of asynchronous multi-party contract signing[A]. Proc of 2009 IEEE Computer Security Foundations Symposium[C]. New York, USA, 2009. 13-25.

[4] ARNE T. A survey of certified mail systems provided on the internet[J]. Computers & Security, 2011, 30(6/7):464-485.

[5] HUANG X Y, MU Y, WILLY S, *et al*. Optimistic fair exchange with strong resolution-ambiguity[J]. IEEE Journal on Selected Areas in Communication, 2011, 29(7):1491-1502.

[6] HUANG X Y, MU Y, WILLY S, *et al*. Preserving transparency and accountability in optimistic fair exchange of digital signatures[J]. IEEE Trans on Information Forensics and Security, 2011, 6(2):498-512.

[7] FENG J, CHEN Y, KU W S, *et al*. Analysis of integrity vulnerabilities and a non-repudiation protocol for cloud data storage platforms[A]. Proceeding of 39th International Conferena on Parallel Processing (ICPP 2010)[C]. San Diego, USA, 2010.

[8] KREMER S, MARKOWITCH O, ZHOU J. An intensive survey of non-repudiation protocols[J]. Computer Communications, 2002, 25(17): 1606-1621.

[9] ZHOU J, GOLLMANN D. A fair non-repudiation protocol[A]. Proceedings of the IEEE Symposium on Research in Security and Privacy[C]. Oakland, CA, USA, 1996. 55-61.

[10] ZHOU J, GOLLMANN D. Towards verification of non-repudiation protocols[A]. Proc of Int Refinement Work and Formal Methods Pacific[C]. Canberra, Australia, 1998. 370-380.

[11] 范红, 冯登国. 一个非否认协议 ZG 的形式化分析[J]. 电子学报 2005, 33(1): 171-173.
FANG H, FENG D G. Formal analysis of a non-repudiation protocol ZG[J]. Acta Electronica Sinica, 2005, 33(1): 171-173.

[12] SCHNEIDER S. Formal analysis of a non-repudiation protocol[A]. Proc of The 11th Computer Security Foundations Work[C]. USA, 1998. 54-65.

[13] BELLA G, PAULSON L C. Mechanical proofs about a non-repudiation protocol[A]. TPHOLs 2001[C]. Edinburgh, Scotland, UK, 2001. 91-104.

[14] KREMER S, RASKIN J F. A game-based verification of non-repudiation and fair exchange protocols[A]. CONCUR 2001[C]. Aalborg, Denmark, 2001. 551-565.

[15] GURGENS S RUDOLPH C. Security analysis of efficient (Un-)fair non-repudiation protocols[J]. Formal Aspects of Computing, 2005, 17(3):260-276.

[16] 黎波涛，罗军舟. 不可否认协议的 Petri 网建模与分析[J]. 计算机研究与发展，2005, 42(9):1571-1577.
LI B T, LUO J Z. Modeling and analysis of non-repudiation protocols by petri nets[J]. Journal of Computer Research and Development, 2005, 42 (9): 1571-1577.

[17] WEI K, HEATHER J. A theorem-proving approach to verification of fair nonrepudiation protocols[A]. FAST 2006[C]. Hamiltor Ontario, Canad, 2007. 202-219.

[18] ARMANDO A, CARBONE R, COMPAGNA L. LTL model checking for security protocols[A]. 20th IEEE Computer Security Foundations Symp. CSF[C]. Venice, Italy, 2007, 385-396.

[19] FRANCIS K, LAURENT V. Automatic methods for analyzing non-repudiation protocols with an active intruder[A]. Formal Aspects in Security and Trust (FAST 2008)[C]. Malaga, Spain, 2009. 192-209.

[20] MAYLA B, AGOSTINO C. Non-repudiation analysis with LYSA[A]. IFIP Advances in Information and Communication Technology Emerging Challenges for Security Privacy and Trust[C]. Pafos, Cyprus, 2009. 318-329.

[21] KREMER S, RASKIN J F. A game-based verification of non-repudiation and fair exchange protocols[J]. Journal of Computer Security, 2003, 11(3):399-429.

[22] CHADHA R, KREMER S, SCEDROV A. Formal analysis of multi-party contract signing[A]. Proceedings of the 17th IEEE

Computer Security Foundations Workshop (CSFW'04)[C]. Ztaly, 2004. 266-279.

[23] MUKHAMEDOV A, KREMER S, RITTER E. Analysis of a multi-party fair exchange protocol and formal proof of correctness in the strand space model[A]. Financial Cryptography 2005[C]. Ztaly, 255-269.

[24] 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.
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.

[25] 韩志耕, 罗军舟, 王良民. 不可否认协议分析的增广 CSP 方法[J]，通信学报，2008, 29(10): 8-18.
HAN Z G, LUO J Z, WANG L M. Extended-CSP based analysis of non-repudiation protocols[J]. Journal on Communications, 2008, 29(10): 8-18.

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

[27] ONIEVA J, ZHOU J, LOPEZ J. Multi-party non-repudiation: a survey[J]. ACM Computing Surveys, 2008, 41(1): 1-43.

[28] KIM K, PARK S, BAEK J. Improving fairness and privacy of zhou-gollmann's fair non-repudiation protocol [A]. Proc of ICPP workshop on Security(IWSEC)[C]. Wakamatsum, Japan, 1999. 140-145.

[29] 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.
HAN Z G, LUO J Z. A fair multi-party non-repudiation protocol[J]. Chinese Journal of Computers, 2008, 31(10):1705-1715.

作者简介：

韩志耕（1976-），男，江苏东台人，博士，南京审计学院讲师，主要研究方向为网络安全与管理，信息系统安全与审计。

陈耿（1965-），男，江苏无锡人，博士，南京审计学院教授，主要研究方向为数据挖掘、信息系统安全与审计。

罗军舟（1960-），男，浙江宁波人，博士，东南大学教授、博士生导师，主要研究方向为下一代网络体系结构、协议工程、网络安全、网格与云计算、无线局域网。