# 多方不可否认协议时限性分析与改进

韩志耕, 罗军舟
(东南大学计算机科学与工程学院, 江苏南京 210096)

摘 要: 时限性是实用的不可否认协议必须具备的一个基本性质. 形式化分析典型的多方不可否认协议时发现其存在未公布的时限性缺陷. 本文通过向协议消息中添加额外时间控制信息和改变协议交互步骤的办法对该缺陷进行了改进.

关键词: 多方不可否认; 形式化分析; 时限性
中图分类号: TN91 文献标识码: A 文章编号: 0372-2112 (2009) 02-0377-05

# Analysis and Improvement of Timeliness of a Multi-Party Non-Repudiation Protocol

HAN Zhi-geng, LUO Jun-zhou
(*School of Computer Science and Engineering, Southeast University, Nanjing, Jiangsu 210096, China*)

**Abstract:** Timeliness is a key security property of practical non-repudiation protocols. This paper analyzed an existing representative multi-party non-repudiation protocol using formal method and found that it lacks the support for timeliness. Then an improved protocol was proposed which fixes the flaw by both adding extra time limit information into protocol messages and modifying the sequence of protocol steps.

**Key words:** multi-party non-repudiation; formal analysis; timeliness

## 1 引言

不可否认服务主要用于收集、维护、验证与一个事件或行为相关的不可抵赖证据,以便解决有关该事件或行为是否发生的争端[1]. 不可否认协议作为一种具体的实现技术,必须具备不可否认性、公平性和时限性; 其中时限性主要用于确保诚实的协议实体在协议执行的任何阶段都能采取措施在有限时间内结束协议运行,避免其在不知道协议是否已结束的情况下无限期地维持协议轮状态以确保获取公平[2].

所有的不可否认协议中, Zhou 等人于 96 年提出的公平不可否认协议[3] (ZG 协议) 得到了最广泛的研究,出现过多种形式化验证[4] 和多个协议变体[5]. ZG 的致命缺陷是不具备时限性,诚实的接收者无法在有限的时间内结束协议运行. 对此缺陷, 文献[3] 提出一种通过添加时间限制信息到协议消息中的改进办法. 文献[6] 指出文献[3] 改进后的协议仍然存在与原协议同样的问题,本质上协议运行仍由发送者控制,某些情况下其会阻止接收者收集有利证据. 该文给出的改进协议中发送者与接收者都有能力控制协议运行. 文[7] 指出文[6] 中协议虽解决了时限性问题,但部署困难: 协议运行要求全局时钟同步. 该文基于相对时钟的思想重新改进了 ZG,协议运行时无需全局时钟同步. 需要指出的是,在已有的形式化分析中,除文[8] 成功检测出 ZG 存在时限性缺陷外,其他分析如文[9, 10] 使用 SvO 逻辑、文[11] 使用秩函数方法、文[12] 使用定理证明器 Isabelle、文[13] 使用异步积自动机(APA) 都没能发现该缺陷.

为使 ZG 具备多方参与的能力, 文[14] 将其扩展成多方不可否认协议(KM 协议). KM 为此类协议的设计提供了极好的思路,有必要通过严格的形式化技术来验证其安全性; 但截至目前,对 KM 的讨论仅有文献[15] 对其进行过功能扩充,并没出现针对协议性质,如时限性是否满足的讨论.

## 2 时限性分析方法

时限性要求协议结束后实现的公平性级别不低于实体开始结束协议时的公平性级别. 目前还不存在多方不可否认协议时限性的明确定义, 本文基于文献[14] 给出如下定义:

定义 1 多方不可否认协议时限性: $Entity_i$ 是多方

收稿日期: 2007-08-28; 修回日期: 2008-10-20
基金项目: 国家自然科学基金会重大研究计划项目(No. 90604004, No. 60773103); 江苏省自然科学基金重点项目(No. BK2007708, BK2008030); 江苏省"网络与信息安全"重点实验室(No. BM2003201); 计算机网络和信息集成教育部重点实验室项目(No. 93K-9); 科技部国际科技合作项目

不可否认协议 *MPRP* 的任意协议实体, *Run* 代表*MPR* 的单个协议轮, *Tr* 是 *Run* 开始时间. *MPRP* 具有时限性, 当且仅当对于任意 *Run* 都有: 任意时刻 $T(T \geqslant Tr)$, 诚实的 $Entity_i$ 都可在 $T+t(0<t<+\infty)$ 之前结束 *Run*, 并且 $Entity_i$ 在 $T+t$ 时获得的公平性级别不会低于其在 $T$ 时获得的公平性级别.

不可否认协议时限性分析的主要任务是考察协议实体数量增加时, 某些实体的欺骗行为能否影响到诚实的实体在不丢失公平的前提下安全地终止协议执行. 虽然可用于该类协议分析的方法有很多, 但能描述与分析时限性的却极少; 仅有的包括文[8]使用扩展 SvO 逻辑方法分析过 ZG 的时限性, 以及文[16]基于博弈论分析过拥有一个发送者、两个接收者的多方乐观不可否认协议的时限性. 多方协议分析的难点在于确定合理的最小协议实体数量, 既能使模型最小化又能充分说明协议性质; 实体过多会造成模型的状态空间急剧膨胀, 甚至无法分析; 实体过少则无法充分分析协议性质. 本文之所以选用文[8]提出的基于推理结构性(逻辑)方法, 主要考虑到其在分析大系统时不会产生状态爆炸, 简化分析的复杂性.

扩展 SvO 逻辑方法将时限性目标描述为对通信事件的信仰和协议事件发生时间应满足的约束. 证明过程包括逻辑推理和时间演算. 下文需采用的扩展公理介绍如下:

Nec 规则: 由 $\vdash \varphi$ 有 $\vdash P$ believes $\varphi$;

A1. $P$ believes $\varphi \wedge P$ believes$(\varphi \supset \psi) \supset P$ believes $\psi$;

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

A6. $P$ received $(X_1, \cdots, X_n)$ at $[T] \supset P$ received $X_i$ at $[T]$;

A7. $(P$ received$\{X\}_K$ at $[T_1] \wedge P$ has $K'$ at $[T_2]) \supset P$ received $X$ at $[\max(T_1, T_2)]$;

## 3 分析 KM 协议时限性

KM 将待发送信息分为两部分: 密文和密钥. 协议执行由两阶段完成: 前一阶段发送者与接收者集合中的成员交换密文以及与密文相关的发送/接收证据. 后一阶段发送者将密钥以及由其所确定的合法接收者集合提交给 *TTP*(*Trusted Third Party*), 此后 *TTP* 通过公共目录将密钥及相关证据同时提供给相关协议实体. 交互步骤描述如下:

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

(2) $Bi \rightarrow A: f_{EOR}, A, Bi, L, EOR_i$ where $Bi \in B$ and $i \in \{1, \cdots, |B|\}$;

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

(4) $B'j \leftarrow TTP: f_{Con}, A, B', L, E_{B'}(K), Con_K$ where $B'j \in B'$ and $\forall j: 1 \leqslant j \leqslant |B'|$;

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

Where $L = h(M, K)$; $EOO = S_A(f_{EOO}, B, L, T, h(C))$; $EOR_i = S_{Bi}(f_{EOR}, A, L, T, C)$; $Sub_K = S_A(f_{Sub}, B', L, T, E_{B'}(K))$; $Con_K = S_{TTP}(f_{Con}, A, B', L, T, E_{B'}(K))$.

$T$ 是 $A$ 及 $B'$ 中成员获得 $K$ 和 $Con_k$ 的最终期限. 若 $B$ 中成员 $Bi$ 不同意 $A$ 规定的期限 $T$, 它可在步骤 2 停止协议执行. 协议执行后, $A$ 收集到证据$\{EOR_i, Con_K\}$, $B'$ 成员 $B'j$ 收集到证据$\{EOO, Con_K\}$. 若日后产生纠纷: (1) $B'j$ 接收到了 $A$ 发送的 $M$, 但 $A$ 否认发送过 $M$; (2) $A$ 发送了 $M$ 给 $B'j$, 但 $B'j$ 否认接收过 $M$. 它们可将自己收集到的证据提交给仲裁者 $J$ 进行仲裁, $J$ 根据相应证据的有效性给出通信事件是否发生过的仲裁结果. 为确保分析过程的简洁性, 给出如下缩写:

$C = \{M\}_K$; $EOO_p = \{f_{EOO}, B, L, T, h(C)\}$; $EOO = \{EOO_p\}_{KA}^{-1}$; $EOR_{ip} = \{f_{EOR}, A, L, T, C\}$; $EOR_i = \{EOR_{ip}\}_{KB_i}^{-1}$; $Sub_{K_p} = \{f_{Sub}, B', L, T, E_{B'}(K)\}$; $Sub_K = \{Sub_{K_p}\}_{KA}^{-1}$; $Con_{Kp} = \{f_{Con}, A, B', L, T, E_{B'}(K)\}$; $Con_K = \{Con_{K_p}\}_{KT}^{-1}$.

用到的时间常元有: $t$, $t_0$, $t_A$ 和 $t_{Bi}$, 其中 $t$ 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(协议假设网络非永久不可用), $t_A$ 和 $t_{Bi}$ 表示 $A$ 和 $Bi$ 在发送完协议消息后等待下一消息的最长时间. 时间变元有: $T_s$, $T_r$, $T_o$, $T_A$, $T_{Bi}$, $T_x$, $T_y$. 分析中 $i(1 \leqslant i \leqslant |B|)$ 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 $j(B'j)$.

首先给出 KM 关于实体密钥的假设. 实体拥有签名私钥, 且相应公钥公开:

**P1.** (1) $J$ believes $PK_\sigma(A, KA)$; (2) $J$ believes $PK_\sigma(Bi, KBi)$; (3) $J$ believes $PK_\sigma(TTP, KT)$;

**P2.** (1) $J$ believes ($Bi$ has $KA$); (2) $J$ believes ($Bi$ has $KT$);

纠纷产生时需要进行仲裁, $A$ 和 $B'j$ 将收集的证据提交给仲裁者 $J$:

**P3.** $J$ believes $J$ received $\{EOO, EOR_i, Con_K\}$;

*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.** $J$ believes (*TTP* said $Con_{Kp}$ at $[T_x] \supset TTP$ received $Sub_K$ at $[T_x]$);

$A$ 和 $B'j$ 与 *TTP* 间网络非永久不可用, 只要 *TTP* 发布了证据, 它们一定能在此后 $t_0$ 时间内收到:

**P5.** $J$ believes (*TTP* said $Con_{Kp}$ at $[T_x] \supset A$ received $Con_K$ at $[T_y | \{x | T_x \leqslant x \leqslant T_x + t_0\}]$);

**P6.** $J$ believes (*TTP* said $Con_{Kp}$ at $[T_x] \supset B'j$ received $Con_K$

at $[T_y|\{x|T_x \leqslant x \leqslant T_x + t_0\}]$);

实体不会做对己无利的事: $Bi$ 仅在收集到 $EOO$ 后才发送 $EOR_i$, $A$ 仅在收集到自己所关心的 $EOR_i$ 后才提交 $Sub_K$:

**P7.** $J$ believes ($A$ said $Sub_{Kp}$ at $[T_x] \supset A$ received $EOR_i$ at $[T_y|\{x|x \leqslant T_x\}]$);

**P8.** $J$ believes ($Bi$ said $EOR_{ip}$ at $[T_x] \supset Bi$ received $EOO$ at $[T_y|\{x|x \leqslant T_x\}]$);

最后是关于 $M$ 的还原: 只要 $B'j$ 收到/$A$ 发送了 $C$ 和 $K$, 它就收到/发送了 $M$:

**P9.** $J$ believes ($A$ said $C$ at $[T_x] \wedge A$ said $K$ at $[T_y] \supset A$ said $M$ at $[\max(T_x, T_y)]$);

**P10.** $J$ believes ($B'j$ received $C$ at $[T_x] \wedge B'j$ received $K$ at $[T_y] \supset B'j$ received $M$ at $[\max(T_x, T_y)]$);

根据定义 1, KM 协议的时限性目标为:

**G1.** $J$ believes ($A$ said $M$ at $[T_x] \wedge A$ received $Con_K$ at $[T_y]) \wedge (T_x \leqslant T_y \leqslant t)$;

**G2.** $J$ believes ($B'j$ received $M$ at $[T_x] \wedge B'j$ said $EOR_{ip}$ at $[T_y]) \wedge (T_x - t_{Bi} \leqslant T_y \leqslant T_x \leqslant t)$;

目标 **G1** 说明 $A$ 必定是在提交 $Sub_K$ 后, 时间 $T$ 之前获得 $Con_K$; 目标 **G2** 也说明了这种约束关系. 若能证明上述两个目标, 就能说明该协议具备时限性. 由于 **G1** 是无争议的, 下面仅证明 **G2**.

逻辑推理:

(1) $J$ believes $J$ received $Con_K$ {P3, 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), P4, Nec, A1};

(4) $J$ believes ($A$ said $Sub_{Kp}$ at $[T_s]$) {(3), P1(1), Nec, A1, A4};

(5) $J$ believes ($A$ received $EOR_i$ at $[T_r|\{x|x \leqslant T_s\}]$) {(4), P7, A1};

(6) $J$ believes ($B'j$ said $EOR_{ip}$ at $[T_r]$) {(5), P1(2), Nec, A1, A4};

(7) $J$ believes ($B'j$ received $EOO$ at $[T_o|\{x|x \leqslant T_r\}]$) {(6), P8, A1};

(8) $J$ believes ($B'j$ received $EOO_p$ at $[T_o]$) {(7), P2(1), Nec, A1, A7};

(9) $J$ believes ($B'j$ received $C$ at $[T_o]$) {(8), Nec, A1, A6};

(10) $J$ believes ($B'j$ received $Con_K$ at $[T_{Bi}|\{x|T_s \leqslant x \leqslant T_s + t_0\}]$) {(2), P6, A1};

(11) $J$ believes ($B'j$ received $Con_{Kp}$ at $[T_{Bi}]$) {(10), P2(2), Nec, A1, A7};

(12) $J$ believes ($B'j$ received $K$ at $[T_{Bi}]$) {(11), Nec, A1, A6};

(13) $J$ believes ($B'j$ received $M$ at $[\max(T_o, T_{Bi})]$) {(9), (12), P10, A1};

(14) $J$ believes ($B'j$ received $M$ at $[\max(T_o, T_{Bi})] \wedge B'j$ said $EOR_{ip}$ at $[T_r]$) {(6), (13), Nec, A1}.

时间演算:

令 $T_x = \max(T_o, T_{Bi})$, $T_y = T_r$. 现证明 $T_x - t_{Bi} \leqslant T_y \leqslant T_x \leqslant t$:

由逻辑推理中第(5)、(7)、(10)三步, 得 $T_o \leqslant T_r \leqslant T_s \leqslant T_{Bi}$, 因此有式(1): $T_x = \max(T_o, T_{Bi}) = T_{Bi}$; 由逻辑推理中第(10)步 $T_{Bi} \in \{x|T_s \leqslant x \leqslant T_s + t_0\}$, 结合式(1)得式(2): $T_s \leqslant T_x \leqslant T_s + t_0$; 由逻辑推理中第(5)步, 有 $T_y = T_r \leqslant T_s$, 结合式(2)得 $0 \leqslant T_x - T_y \leqslant T_s + t_0 - T_r$. 即 $T_x - (T_s + t_0 - T_r) \leqslant T_y \leqslant T_x$. 故若有 $T_s + t_0 - T_r \leqslant t_{Bi}$ 就可得 $T_x - t_{Bi} \leqslant T_y \leqslant T_x$. 但 $T_s$ 和 $T_r$ 间无约束关系, 故无论将常元 $t_{Bi}$ 的值定义为多大, $T_s + t_0 - T_r$ 的值都可能会大于它, 故无法保证 $T_x - t_{Bi} \leqslant T_y \leqslant T_x \leqslant t$ 成立.

目标 G2 定义的时间约束条件无法得到满足. 这是因为 $A$ 提交 $Sub_K$ 的时间与 $B'j$ 发送 $EOR_i$($i$ 与 $j$ 满足前面给出的映射)的时间之间无约束关系, 使得恶意 $A$ 完全有能力在期限 $T$ 快要到时才提交 $Sub_K$, 并在 $TTP$ 发布证据之后获得证据证明 $B'j$ 收到了 $M$. 由于 $TTP$ 会在 $Con_K$ 发布不久就将其删除, 迫使 $B'j$ 必须在 $T$ 附近不断检索 $TTP$ 公共目录; 而 $A$ 此时可干扰 $B'j$ 所在网络或计算机系统, 阻止其收集 $Con_K$, 最终导致 $B'j$ 因无法检索 $Con_K$ 而不能正常终止本协议轮. 故 KM 协议不具有时限性, 对 $B'j$ 不公平.

## 4　改进 KM 协议时限性

KM 不具备时限性的原因在于协议实体地位不等, 发送者可利用时间限制信息控制协议执行. 本节通过交换协议交互步骤和向协议消息中添加时间限制信息的办法对其进行改进, 确保原本处于弱势地位的实体也能控制协议执行. 为使新协议能够实用, 一方面, 鉴于真实环境中实体时钟间差异不会太大, 设计中引入时间段机制[7], 确保协议实现无需全局时钟同步. 其中时间点($T$)为时间轴上的一点; 如果 $T_x$ 和 $T_y$ 是时间点, 那么 $t_{xy} = |T_x - T_y|$ 就是时间段($t$). 另一方面, 引入证据链技术[17], 确保协议实现时能对证据实施高效管理. 新协议仍假设 $TTP$ 与协议实体间为弹性信道, 实体相互间为不可靠信道. 新协议采用的基本符号同文献[14, 15], 此外还有:

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

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

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

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

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

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

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

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

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

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

需要说明的是, 时间段 $t_A$ 由 $A$ 定义, 表示 $TTP$ 在私有目录中保存 $Sub_K$ 过了 $t_A$ 个时间单位后若还没收到任一 $Bi$ 提交的 $EOR_i$, 就将 $Sub_K$ 删除. $t_{Bi}$ 是由 $Bi$ 定义的时间段, 表示 $TTP$ 在私有目录中保存 $EOR_i$ 过了 $t_{Bi}$ 个时间单位后若还没收到 $A$ 提交的 $Sub_K$, 就将 $EOR_i$ 删除. $T$ 为 $TTP$ 在公开发布 $Con_K$ 的时间点. 协议各步解释如下:

(1) $A \rightarrow Bi: f_{EOO}, Bi, t_A, l_i, c_i, x_i, uBi, EOO_i$. 若 $Bi$ ($1 \leqslant i \leqslant |B|$) 未收到 $EOO_i$, 其不会产生 $EOR_i$, 故 $A$, $Bi$ 都无法从 $TTP$ 处获得证据.

(2) $A \rightarrow TTP: f_{Sub}, B, t_A, L, E_B(K), EOO, Sub_K$. $A$ 无需等待 $Bi$ 确认就可向 $TTP$ 提交 $Sub_K$. $TTP$ 收到 $Sub_K$ 后, 若私有目录中已有某些 $EOR_i$, 也不可立即产生 $Con_K$, 而须继续等待所有可能的 $Bi$ 发送 $EOR_i$, 等待最长时间为 $t_A$ 个时间单位(基于 $TTP$ 时钟, 计时起点为 $TTP$ 收到 $Sub_K$). 每当收到新的 $EOR_i$, $TTP$ 就须将相应的实体标识 $Bi$ 添加到集合 $B'$ (初值为时间段 $t_A$ 计时前已提交 $EOR_i$, 且 $EOR_i$ 仍保存在 $TTP$ 处的那些实体标识) 中; 若在 $t_A$ 内某些时间段 $t_{Bj}$ ($1 \leqslant j \leqslant |B'|$) 已超时, 则 $TTP$ 须将 $Bj$ 从 $B'$ 中移除. 若到 $t_A$ 即将超时为止 $B'$ 仍为 $\Phi$, 则 $TTP$ 可将 $Sub_K$ 安全删除, 不会引发纠纷.

(3) $Bi \rightarrow TTP: f_{EOR}, A, l_i, x_i, uBi, t_{Bi}, EOO_i, EOR_i$. $Bi$ ($1 \leqslant i \leqslant |B|$) 收到 $EOO_i$ 后, 若不同意 $t_A$ 或不关心 $M_i$, 可不提交 $EOR_i$ 给 $TTP$, 不会产生任何纠纷. 时间段 $t_A$ 并非限制 $Bi$ 一定要在 $t_A$ 内执行此协议步, 而是提醒 $Bi$ 密钥 $ki$ 将在 $t_A$ 超时后被删除. 即使 $Bi$ 过了 $t_A$ 个时间单位后才提交 $EOR_i$, 协议也还是有可能顺利完成的, 因为 $A$ 有可能在步骤 3 之后再执行步骤 2.

证据 $Con_K$ 的生成: 上述 3 步完成后, $TTP$ 收集到 $Sub_K$ 和 $EOR_j$ ($1 \leqslant j \leqslant |B'|$). 接着 $TTP$ 将 $EOR_j$ 中 $EOO$ 和 $Sub_K$ 中 $EOO$ 逐一比较, 若任意两个不等, 不产生 $Con_K$. 为防止无限期保存证据, $TTP$ 可预先定义时间段 $t_0$, 表示 $Con_K$ 发布了 $t_0$ 个时间单位后将被删除. 因 $TTP$ 与协议实体间采用弹性信道, 故信道受到干扰的时间是有限的(设最长为 $t_d$ 个时间单位); 只要 $TTP$ 将 $t_0$ 定义为 $t_d + x\ (x > 0)$, $A$ 和 $Bj$ 总能从 $TTP$ 处检索到 $Con_K$.

(4) $A \leftrightarrow TTP: f_{Con}, A, B', L', T, t_A, tSet_{B'}, \varphi_{B'}(E_B(K)), EOR, Con_K$. $A$ 提交 $Sub_K$ 后, 就可以不断检索 $TTP$ 是否发布了 $Con_K$, 若直到时间段 ($t_A + t_0$) 超时后还没检索到 $Con_K$, $A$ 可确信 $B' = \Phi$, 并停止检索证据, 不会产生纠纷. 若其检索到 $Con_K$, 它能证明 $Bj$ ($1 \leqslant j \leqslant |B'|$) 必在时刻 $T$ 与 $T + t_0$ 间从 $TTP$ 处检索到 $lj$. $A$ 须保存 $EOO$、$EOR$ 和 $Con_K$, 以防日后纠纷.

(5) $Bi \leftrightarrow TTP: f_{Con}, A, B', L', T, t_A, tSet_{B'}, \varphi_{B'}(E_B(K)), EOR, Con_K$. $Bi$ ($1 \leqslant i \leqslant |B|$) 提交 $EOR_i$ 后, 也需不停地检索 $Con_K$. 若直到时间段 ($t_{Bi} + t_0$) 超时后还没检索到 $Con_K$, $Bi$ 可确信 $TTP$ 未收到 $Sub_K$, 并可停止检索, 不会引发纠纷. 若 $Bi$ 检索到 $Con_K$, 其也未必能获得 $ki$, 因 $Bi$ 可能由于时间段 $t_{Bi}$ 超时而被 $TTP$ 从 $B'$ 中移除. $B'$ 中成员需保存 $EOO$、$EOR$ 和 $Con_K$ 以便日后纠纷解决.

新协议的时限性目标与 KM 基本相同, 但需满足不同的时间约束:

**G1.** $J$ believes ($A$ said $M_i$ at $[T_x] \wedge A$ received $Con_K$ at $[T_y]) \wedge (T_x \leqslant T_y \leqslant T_x + t_A + t_0)$;

**G2.** $J$ believes ($B'j$ received $M_i$ at $[T_x] \wedge B'j$ said $EOR_{ip}$ at $[T_y]) \wedge ((T \leqslant T_x \leqslant T + t_0) \wedge (T_x - t_{B'j} - t_0 \leqslant T_y \leqslant T_x))$.

此处时间常元 $T$, $t_A$, $t_{B'j}$, $t_0$ 都由协议信息中相应字段确定. 与第 3 节不同, $i$ ($1 \leqslant i \leqslant |B|$) 与 $j$ ($1 \leqslant j \leqslant |B'|$) 映射定义为: 若集合 $B$ 中标号为 $i$ 的实体 ($Bi$) 最终被 $TTP$ 添加到集合 $B'$ 中, 则其在 $B'$ 中的标记为 $j$ ($B'j$).

目标 G1 说明如果 $A$ 收到了 $TTP$ 发布的证据, 那么它一定是在将 $Sub_K$ 提交给 $TTP$ 之后有限的等待时间之内收到该证据, 而不可能在证据被删除后收到; 目标 G2 也说明了类似的时间约束关系. 按照上面的思路, 容易验证两目标成立, 故新协议具备时限性, 弥补了 KM 的时限性缺陷.

## 5 结束语

利用形式化方法发现 KM 协议无法满足时限性, 同时给出了相应的改进. 当然, 协议运行环境的多样化特征通常会导致理论上具备时限性的协议在实际运行时不能很好地满足该要求. 鉴于时间参数的引入会对协议有效性产生一定的影响, 进一步的研究包括: 其一, 通过实验方法评估协议待运行的实际环境(诸如网络响应速度、$TTP$ 特性以及实体数量和自身能力等的超时等); 其二, 引入容错设计对协议实体行为、消息延迟和节点可靠性等要素进行控制, 弱化环境对协议运行造成的影响. 此外, 本文所使用的形式化方法虽能检测出时限性缺陷, 但其抽象程度高, 描述能力弱, 无法精确描述协议结构(尤其是协议事件间关联和协议实体间协作)、消息和交换项、安全目标等; 彻底解决时限性问题需要首先研制出相关的形式化模型, 然后利用完备的模型指导协议时限性分析与设计.

参考文献:


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

[2] Kremer S, Markowitch O, Zhou J. An intensive survey of non-repudiation protocols[J]. Computer Communications, 2002, 25(17): 1606-1621.

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

[4] Pancho-Festin S, Gollmann D. On the formal analyses of the Zhou-Gollmann non-repudiation protocol[A]. Dimitrakos T, et al. FAST'05[C]. Berlin Heidelberg: LNCS 3866, Springer Verlag, 2006. 5-15.

[5] Louridas P. Some guidelines for non-repudiation protocols[J]. ACM SIGCOMM Computer Communication Review, 2000, 30(1): 29-38.

[6] Kim K, Park S, Baek J. Improving fairness and privacy of Zhou-Gollmann's fair non-repudiation protocol[A]. Proc of the 1999 ICPP workshop on Security (IWSEC)[C]. Aizu, Japan: IEEE Computer Society, 1999. 140-145.

[7] Li Botao, Luo Junzhou. On timeliness of a fair non-repudiation protocol[A]. Proceedings of the 3rd international conference on Information security (InfoSecu'04)[C]. Shanghai, 2004. 99-107.

[8] 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.
Li Botao, Luo Junzhou. Formal analysis of timeliness in non-repudiation protocols[J]. Journal of Software, 2006, 17(7): 1510-1516. (in Chinese)

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

[10] 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.
Fan Hong, Feng Dengguo. Formal analysis of a non-repudiation protocol ZG[J]. Acta Electronica Sinica, 2005, 33(1): 171-173. (in Chinese)

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

[12] Bella G, Paulson L C. Mechanical proofs about a non-repudiation protocol[A]. Proceedings of the 14th International Conference on Theorem Proving in Higher Order Logics[C]. Edimburgh, UK: LNCS 2152, Springer-Verlag, 2001. 91-104.

[13] Gürgens S, Rudolph C. Security analysis of (un-)fair non-repudiation protocols[A]. In: Proceedings of the Conference on Formal Aspects of Security (FASec'02)[C]. London, UK: LNCS 2629, December 16-18, 2002. 97-114.

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

[15] Onieva J A, Zhou J, Lopez J. Non-repudiation protocols for multiple entities[J]. Computer Communications, 2004, 27(16): 1608-1616.

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

[17] You C, Zhou J, Lam K. On the efficient implementation of fair non-repudiation[J]. ACM Computer Communication Review, 1998, 28(5): 50-60.


作者简介:

韩志耕　男, 1976 年生于江苏东台, 东南大学计算机科学与工程学院博士生, 研究方向为网络安全. E-mail: hanzgnit@seu.edu.cn

罗军舟　男, 1960 年生于浙江宁波, 博士, 教授, 博士生导师, 东南大学计算机科学与工程学院院长, 江苏省网络与信息安全重点实验室主任, 研究方向为下一代网络体系结构、协议工程、网络安全与管理、网格计算.