移动自组网中基于动态第三方的可信公平非抵赖协议

吴呈邑,熊 焰,黄文超,陆琦玮,龚旭东
(中国科学技术大学计算机学院,安徽合肥 230027)

摘 要: 由于移动自组网 Manet(Mobile Ad-hoc Networks)是一个无中心的网络且不存在值得信任的结点,传统的公平非抵赖协议因需要一个固定可信第三方 TTP(Trusted Third Party)而不足以保证 Manet 的高效性和安全性.本文在可信平台模块 TPM(Trusted Platform Module)的安全体系结构基础上提出了一种 Manet 中基于动态第三方的可信公平非抵赖协议,以取代固定 TTP,提高协议效率,并运用 TPM 完整性度量技术和 DAA(Direct Anonymous Attestation)远程认证技术,保证证据可信.最后利用 Event B 对该协议进行形式化建模,证明其有效性和公平性.

关键词: 公平非抵赖; 可信计算; 移动自组网; 动态第三方
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2013) 02-0227-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.02.004

A Trusted Fair Non-Repudiation Protocol Based on Dynamic Third Party in Mobile Ad Hoc Networks

WU Cheng-yi, XIONG Yan, HUANG Wen-chao, LU Qi-wei, GONG Xu-dong
(*School of Computer Science and Technology, University of Science and Technology of China, Anhui, Hefei* 230027, *China*)

Abstract: Traditional fair non-repudiation protocol which need a fixed trusted third party could not assure the high efficiency and security of Manet because the Manet is centralless and no nodes can be trusted. So we propose a fair non-repudiation protocol for Manet based on the secure architecture of trusted platform module, which use dynamic third party instead of traditional fixed trusted third party to improve the efficiency of the protocol, and ensure the evidences is trusted by using the integrity measurement and the interface of direct anonymous attestation based on trusted platform module. Then we modeling the new protocol formally by Event B, and prove the validity and the fairness of the protocol.

Key words: fair non-repudiation; trusted computing; mobile Ad Hoc network; dynamic third party

1 引言

移动自组网 Manet(Mobile Ad-hoc Networks)是由若干带有无线收发器的移动节点所组成的无基站的自治网络,广泛应用于军事、民用、商业等领域.在网上银行、电子商务等商业领域中,为保证其安全性,在交易结束后,交易双方都应得到相应的证据,在出现争议时,仲裁方便能依据双方提供的证据进行仲裁,为此人们提出了公平非抵赖协议.公平非抵赖协议是指当信息传送结束时,信息的发送方能够得到接收方已收到此信息的证据,同时接收方也能得到发送方发送此信息的证据,即双方都不能否认参与本次信息交换.

传统的公平非抵赖协议大多基于可信第三方 TTP (Trusted Third Party),选择一个权威、中立、可信任的第三方节点或组织作为 TTP 来实现证据交换.但是,由于 Manet 的无中心性及拓扑的动态性,传统 TTP 因采用集中服务会带来协议的效率瓶颈,同时 TTP 的崩溃将导致网络中所有节点都无法得到公平非抵赖服务.于是,无需 TTP 的公平非抵赖协议成为研究的重点.文献[1]提出一种公平的交换协议,要求发送方和接受方的计算能力相同,这在实际应用中基本不可能实现.文献[2]提出一种较完整的概率型无需 TTP 的非抵赖协议,文献[3]在其基础上,提出了基于计算能力的无需 TTP 的公平非抵赖协议,但是这两个协议不是完全公平的,有可能出现信息传输双方中只有一方得到证据而另一方得不到证据的情况.而文献[4]证明,在异步通信方式下,无

收稿日期:2012-03-13;修回日期:2012-06-23
基金项目:国家自然科学基金(No.60970128,No.61170233);博士后基金(No.2011M501397)

TTP 参与的协议无法达到完全的公平性.由此可见,现有的公平非抵赖协议都不足以满足 Manet 的安全性和高效性需求.

为此,我们在可信平台模块 TPM(Trusted Platform Module)的安全体系结构基础上提出一种 Manet 中基于动态第三方的公平非抵赖协议,取代传统的固定 TTP,以避免因此带来的效率瓶颈问题,并使用直接匿名认证 DAA(Direct Anonymous Attestation)接口和完整性度量技术对动态第三方进行远程可信认证,最后,进一步利用动态第三方验证协议双方非抵赖证据的可信,从而保证协议的高效和安全.

2 DAA 认证及完整性度量

可信计算的核心是使用可信平台模块 TPM 芯片,将其植入各种平台的计算机中,创建安全体系结构,为应用程序提供安全的计算环境.直接匿名认证 DAA 是可信计算中的一种无需 TTP 的身份认证方案,用于验证计算机是否拥有合法的 TPM 芯片.可信计算的另一个作用是安全的报告平台状态,通过对 TPM 芯片中 PCR(Platform Configuration Register)寄存器所存储的 PCR 值进行比较,能判断平台是否被篡改.

DAA 认证是由 Brickell 等人[6]提出的,利用 DAA 认证,节点可以在不泄露自身私有信息的情况下,证明其自身的 TPM 是合法的.通过对 TPM 芯片中 PCR 值的比较,DAA 认证还可以验证节点平台的完整性,即节点平台是否被篡改过.

DAA 方案中分三个步骤:

(*a*)离线第三方初始化

在网络建立之前,离线可信第三方初始化,生成其公私钥,然后发布公钥,保存私钥.

(*b*)节点获取 DAA 证书

节点在进入网络之前,其 TPM 将私有信息 f 分为 f_0 和 f_1,计算

$$N_1 = \zeta^{f_0 + f_1 2^{l_f}} \bmod \Gamma$$

其中 l_f 为 f 的长度,并将 N_1 发送给离线第三方.离线第三方检查其存储的撤销列表,若存在与 N_1 相等的数值,则说明此节点是恶意节点,中止此协议,否则离线第三方在对节点验证成功后,将资格证书发送给节点.

(*c*)认证过程

当节点 A 要向节点 B 证明身份时,节点 A 利用自身的 TPM 以及获得的资格证书生成 AIK(Attestation Identity Key)公私钥,并用 AIK 私钥签名 PCR 值及存储测量日志 SML(Storage Measurement Log),将签名结果发送给节点 B.节点 B 用节点 A 的 AIK 公钥验证签名结果,并比较接收到的 PCR 值,若相等则说明节点 A 的平台是完整的.若签名结果和 PCR 值都验证成功,则证明节点 A 可信.

DAA 认证签名过程的运行时间过长,在实际应用中严重影响系统效率,为此我们采用文献[7]中提出的优化方法.该方法中,发送方在请求验证前,先生成一个假名,并利用假名实现签名过程,当需要认证时,发送方便将对假名的签名发送给验证方.这个签名可以重复使用,即发送方只需进行一次签名过程,便能被多个验证方验证,解决了签名过程运行时间过长的问题.为防止签名在网络传输中被监听、盗用,发送方可以定时更新假名并生成新假名的签名.

3 可信公平非抵赖协议

本协议分为两个阶段,分别是初始化阶段和证据交换阶段.

本协议要求网络中有一个离线可信第三方,并且网络中所有节点都有 TPM 芯片.

3.1 初始化阶段

在网络建立之前,离线第三方进行初始化;每个节点进入网络之前,与离线第三方进行通信,获得离线第三方颁发的资格证书;进入网络后,节点利用自己的 TPM 生成一个假名并对假名进行签名,节点定时更新假名及相应的签名.流程图如图 1.

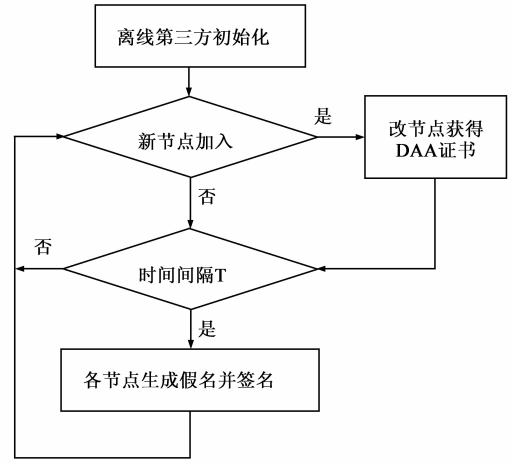


图1 初始化阶段流程图

此后,协议进入发送方和接收方的相互认证阶段.认证过程如图 2.

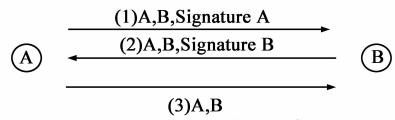


图2 认证阶段示意图

(*a*)当发送方 A 确定要和接收方 B 通信时,向 B 发

送消息(A,B,signature A),其中 signature A 表示节点 A 假名的签名.

(*b*)接收方 B 收到消息后,对 signature A 进行认证,若认证成功,则向 A 发送消息(A,B,signature B);否则中止协议.

(*c*)发送方 A 对接收到的 signature B 进行认证,若认证成功,则向 B 发送消息(A,B),表示双方都认证成功,进入证据交换阶段;否则中止协议.

3.2 证据交换阶段

证据交换阶段,分为 select, *P*step1, *P*step2, *P*step3 四个步骤,其中 select 为选择动态第三方的步骤,*P*step1, *P*step2, *P*step3 则为具体的数据传输步骤.

select 分为以下三步,示意图如图 3:

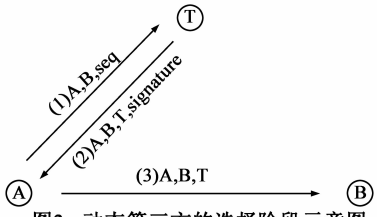


图3 动态第三方的选择阶段示意图

(*a*)发送方 A 随机选择一个邻居节点 T,向其发送消息(A,B,*seq*),请求其作为动态第三方.

(*b*)邻居节点 T 接收到消息,若决定响应该请求,则将其签名发送给 A;否则回到(*a*)步骤.

(*c*)发送方 A 对接收到的签名进行认证,若认证成功,说明邻居节点 T 的 TPM 是合法的且其软件未被篡改,即邻居节点 T 是可信的,则发送消息(A,B,T)给 B;否则回到步骤(*a*).

*P*step1:A 选择一个对称密钥 K 对消息 m 加密,得到密文 C,然后生成 C 的哈希值 $h(C)$,再用 T 的公钥 PK_T 对 K 进行加密,生成 Z_A,将消息(A, B, T, T_A, ID, C, $\{K\}PK\_T$, $e(\{Z\_A\}SK\_A, T\_A, K)$)发送给 B.

*P*step2:B 接收到消息后,决定是否执行协议,若不执行,则中止协议;若执行,则利用从 A 接收到的 C 生成密文 C 的哈希值 $h(C)$,然后生成 Z_B,并对 Z_B 进行签名,将消息(Z_B, $\{Z\_B\}SK\_B$, $\{K\}PK\_T$, $e(\{Z\_A\}SK\_A, T\_A, K)$)发送给 T.

*P*step3:T 接收到以上消息后,验证 B 的签名,通过解密 $\{K\}PK\_T$ 得到 K,利用 K 解密 $e(\{Z\_A\}SK\_A, T\_A, K)$,然后验证 A 的签名,如果验证都成功,那么 T 生成消息(K, $\{K\}SK\_T$)发送给 B,生成消息(Z_T, $\{Z\_T\}SK\_T$)发送给 A.

以上三个步骤的流程图如图 4,其中,

Z_A = A,B,T, T_A, ID, K, $h(C)$,

Z_B = A,B,T, T_B, ID, $h(C)$,

Z_T = A,B,T, T_T, ID, K, $h(C)$.

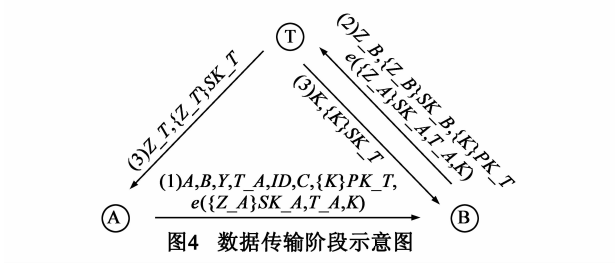


图4 数据传输阶段示意图

在 *P*step2 阶段,由于 A 选择的对称密钥 K 是由 T 的公钥加密的,B 无法得到,故若 B 不将消息($\{K\}PK\_T, e(\{Z\_A\}SK\_A, T\_A, K)$)发送给 T,是无法对 C 进行解密得到 m 的,也得不到所需的证据.在 *P*step3 阶段,T 通过解密得到 Z_A 和 Z_B,比较两者中的 $h(C)$ 是否相等,若相等,则对密钥 K 进行签名,发送给 B,并将证据发送给 A.B 得到对称密钥 K 后,就能够解密 $e(\{Z\_A\}SK\_A, T\_A, K)$,得到证据 $\{Z\_A\}SK\_A$.

4 新协议的形式化分析和证明

我们需要证明新协议的公平性及其证据的有效性.协议的公平性是指在协议的任何一个阶段,只可能有两种情况:发送双方都有证据或双方都没有证据;证据的有效性则是指接收方 B 接收到的证据能证明消息 m 是由发送者 A 发送,A 接收到的证据能证明消息 m 已被 B 接收.

本文使用 Event B 对协议进行形式化证明,Event B 是基于集合理论和逻辑证明的形式化工具,它在 B 方法[8]的基础上改进,并由欧洲委员会信息和通信技术项目组开发[9].Event B 中有两类组件,分别为 Context 和 Machine,其中 Context 描述常量的信息以及关于常量的公理;Machine 则是形式化模型的主体,描述变量的信息以及软件的行为(EVENTS).首先我们对协议进行形式化建模,然后对其进行分析证明.

4.1 形式化建模

4.1.1 模型的初步建立

协议使用 DAA 对机器进行认证,在形式化模型中,给每个参与的机器赋一个常量 signature,若机器认证成功,则其 signature 值为 signed,否则为 unsigned.在证据交换阶段之前,发送方和接收方都已认证成功,即都是可信的,故它们的 signature 值都为 signed.

和协议证据交换阶段的四个步骤相对应,定义四个 EVENT:select, *P*step1, *P*step2, *P*step3.为了能够控制四个 EVENT 的执行顺序,定义控制变量 begin, step1, step2, step3, err, end,它们只有两个值 on 和 off.其流程图如图 5.

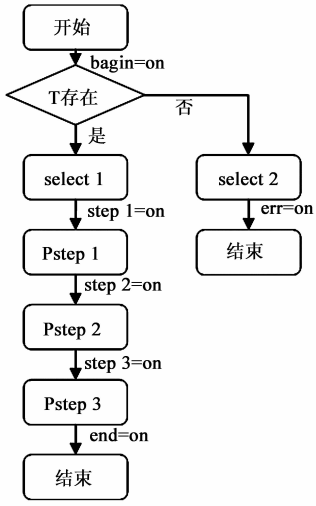


图5 证据交换阶段控制流程图

在初始的形式化模型中,定义 *protocol_ctx*0 和 *protocol_*0 两个组件,其中 *protocol_ctx*0 为 *context* 类型,*protocol_*0 为 *machine* 类型.

在 *protocol_ctx*0 中,定义集合 *ID*, *MESSAGE*, *SIGNATURE*, *FLAG*,其中 *ID* 表示机器的标识,*MESSAGE* 表示消息, $SIGNATURE = \{signed, unsigned\}$, $FLAG = \{on, off\}$.同时定义常量 *pk*, *sk*, *signature*, *a*, *b*, *m*,其中 *a*, *b*, *m* 分别表示协议中的发送方,接收方以及要发送的消息.而 *pk*, *sk*, *signature* 分别满足公式(1)、(2)、(3).

$$pk \in ID \rightarrow MESSAGE \tag{1}$$

$$sk \in ID \rightarrow MESSAGE \tag{2}$$

$$signature \in ID \rightarrow SIGNATURE \tag{3}$$

pk 表示机器的公钥,而 *sk* 表示机器的私钥,为表示各机器的公私钥不相同,在 *protocol_ctx*0 中加上两条公理,即公式(4)、(5).

$$\forall u, v \cdot u \in ID \wedge v \in ID \wedge u \neq v \Rightarrow pk(u) \neq pk(v) \tag{4}$$

$$\forall u, v \cdot u \in ID \wedge v \in ID \wedge u \neq v \Rightarrow sk(u) \neq sk(v) \tag{5}$$

在 *protocol_*0 中,定义控制变量 begin, step1, step2, step3, err, end,它们都是 *FLAG* 类型,即它们只有两个值:on 和 off.在 *EVENT* 中,仅描述控制变量的变化,以保证 select1, select2, *P*step1, *P*step2, *P*step3 按照图 5 的顺序执行,同时为下一步的精化做准备.

4.1.2 模型的精化

在 *protocol_ctx*0 和 *protocol_*0 的基础上,对这两个组件进行精化,得到 *protocol_ctx*1 和 *protocol_*1,其中 *protocol_ctx*1 是 *protocol_ctx*0 的精化,*protocol_*1 是 *protocol_*0 的精化,这四个组件的关系如图 6.

*protocol_*0 对 *protocol_ctx*0 使用 *see* 表示,*protocol_*0 能调用 *protocol_ctx*0 中定义的所有集合、常量以及公理;*protocol_*1 对 *protocol_*0 使用 *refine* 则指,后者是对前者内容的精化.

在 *protocol_ctx*1 中,添加常量 *k*, *hash*, *encrypt* 的定义,其分别满足公式(6)、(7)、(8).

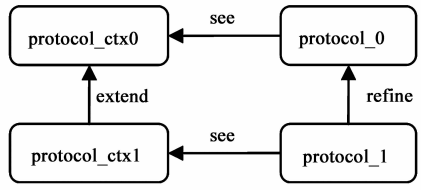


图6 组件关系图

$$hash \in MESSAGE \rightarrow MESSAGE \tag{6}$$

$$encrypt \in MESSAGE \rightarrow (MESSAGE \rightarrow MESSAGE) \tag{7}$$

$$k \in MESSAGE \tag{8}$$

其中 *hash* 表示消息的 *hash* 值;*encrypt* 则是对消息的加密操作,前一个参数是被加密的消息,后一个参数是加密密钥;*k* 是协议中使用的对称密钥.由于密钥也可以被加密,所以也定义为 *MESSAGE* 类型.

为满足对称密钥和非对称密钥的原理,在 *protocol_ctx*1 中加上三条公理,即公式(9)、(10)、(11).

$$\forall x \cdot x \in MESSAGE \Rightarrow encrypt(encrypt(x)(k))(k) = x \tag{9}$$

$$\forall x, y \cdot x \in ID \wedge y \in MESSAGE \Rightarrow encrypt(encrypt(y)(pk(x)))(sk(x)) = y \tag{10}$$

$$\forall x, y \cdot x \in ID \wedge y \in MESSAGE \Rightarrow encrypt(encrypt(y)(sk(x)))(pk(x)) = y \tag{11}$$

第一条表示用对称密钥对任何消息加密两次都将得到消息本身;第二三条则说明用公钥加密可以用私钥解密,反之亦然.

在 *protocol_*1 中,添加变量 *t*, *ma*, *mb*, *mt*,其分别满足公式(12)、(13)、(14).

$$ma \in ID \leftrightarrow MESSAGE \tag{12}$$

$$mb \in ID \leftrightarrow MESSAGE \tag{13}$$

$$mt \in ID \leftrightarrow MESSAGE \tag{14}$$

其中 *t* 表示动态第三方;*ma* 表示发送方 *a* 接收到的消息,它是 *ID* 映射到 *MESSGE* 的关系,*ID* 表示消息的发送方;*mb*, *mt* 类似.

在 *protocol_*1 的 EVENT 中,对各个 EVENT 进行扩充,得到相应的规范.

对于 *select*1, *select*2,若同时满足公式(15)和公式(17),则执行 *select*1,若同时满足公式(16)和公式(17),则执行 *select*2.

$$\exists x \cdot x \in dom(signature) \wedge signature(x) = signed \wedge x \neq a \wedge x \neq b \tag{15}$$

$$\neg(\exists x \cdot x \in dom(signature) \wedge signature(x) = signed \wedge x \neq a \wedge x \neq b) \tag{16}$$

$$begin = on \tag{17}$$

对于 *P*step1,加入公式(18).

$$\begin{aligned}&mb := mb \cup \{a \mapsto encrypt(m)(k)\}\\&\cup \{a \mapsto encrypt(k)(pk(t))\}\\&\cup \{a \mapsto encrypt(encrypt(k)(sk(a)))(k)\}\\&\cup \{a \mapsto encrypt(encrypt(hash(encrypt(m)(k)))\\&\quad (sk(a)))(k)\}\end{aligned} \tag{18}$$

表示发送方 a 向接收方 b 发送了 $encrypt(m)(k)$ 等消息,*P*step2,*P*step3 类似.

*P*step2,加入公式(19).

$$\begin{aligned}&mt := mt \cup \{b \mapsto hash(encrypt(m)(k))\}\\&\cup \{b \mapsto encrypt(k)(pk(t))\}\\&\cup \{b \mapsto encrypt(hash(encrypt(m)(k)))\\&\quad (sk(b))\}\\&\cup \{b \mapsto encrypt(encrypt(k)(sk(a)))(k)\}\\&\cup \{b \mapsto encrypt(encrypt(hash(\\&\quad encrypt(m)(k)))(sk(a)))(k)\}\end{aligned} \tag{19}$$

*P*step3,加入公式(20)和公式(21).

$$mb := mb \cup \{t \mapsto encrypt(k)(sk(t))\} \tag{20}$$

$$\begin{aligned}&ma := ma \cup \{t \mapsto encrypt(hash(encrypt(m)\\&\quad (k)))(sk(t))\}\\&\cup \{t \mapsto encrypt(k)(sk(t))\}\end{aligned} \tag{21}$$

至此,本公平非抵赖协议的形式化模型建立完毕.

4.2　对形式化模型的证明

如上所述,本协议需要证明两项内容,一:A 能收到证据($\{k\}SK\_T$,$\{h(c)\}SK\_T$)且 B 能收到证据($\{k\}SK\_A$,$\{h(c)\}SK\_A$);二:A,B 同时收到证据或同时收不到证据. 由于 *P*step3 步骤中,动态第三方 T 直接将 $\{k\}SK\_T$,$\{h(c)\}SK\_T$ 发送给 A,故这部分不需证明.对第一项,其形式化描述如式(22).

$$\begin{aligned}&encrypt(encrypt(k)(sk(a)))(k)\\&\in ran(mb) \wedge encrypt(encrypt(hash(\\&encrypt(m)(k)))(sk(a)))(k) \in ran(mb) \wedge\\&encrypt(k)(sk(t)) \in ran(mb)\\&\Rightarrow (encrypt(k)(sk(a)) \in ran(mb) \wedge encrypt(hash(\\&encrypt(m)(k)))(sk(a)) \in ran(mb))\end{aligned} \tag{22}$$

上面推出符号的前三项都是 B 接收到的消息,故只需证明前三项能推出后面的结果,即证明了 B 能接收到所需证据.

对第二项,其形式化描述如式(23).

$$\begin{aligned}&(\{t \mapsto encrypt(hash(\\&encrypt(m)(k)))(sk(t))\} \subseteq ma \wedge\\&\{t \mapsto encrypt(k)(sk(t))\} \subseteq ma \wedge\\&\{t \mapsto encrypt(k)(sk(t))\} \subseteq mb) \vee\\&(\{t \mapsto encrypt(hash(\\&encrypt(m)(k)))(sk(t))\} \not\subset ma \wedge\\&\{t \mapsto encrypt(k)(sk(t))\} \not\subset ma \wedge\\&\{t \mapsto encrypt(k)(sk(t))\} \not\subset mb)\end{aligned} \tag{23}$$

将上述两个形式化描述加入 *protocol*_1 的不变式中,前者设为定理,在 Event B 中,定理是必须优先证明的不变式,且能够用来证明其他不变式;后者则为不变式,在每次执行 EVENT 操作前后,都必须满足该条件.我们的最终目的就是证明这两项.

为证明以上两项,我们必须加一些公理:公理一,对任何一个节点,若它拥有消息 m 和密钥 k,则 $encrypt(m)(k)$ 也属于该节点;公理二,对于用私钥加密的消息,任何节点都能够解密.它们的形式化描述为公式(24)和公式(25).

$$\begin{aligned}&\forall x, y, z \cdot x \in ID \leftrightarrow MESSAGE \wedge\\&y \in MESSAGE \wedge z \in MESSAGE \wedge\\&y \in ran(x) \wedge z \in ran(x)\\&\Rightarrow\\&encrypt(y)(z) \in ran(x)\end{aligned} \tag{24}$$

$$\begin{aligned}&\forall x, y, z \cdot x \in ID \wedge y \in MESSAGE \wedge\\&z \in ID \leftrightarrow MESSAGE \wedge\\&encrypt(y)(sk(x)) \in ran(z)\\&\Rightarrow\\&y \in ran(z)\end{aligned} \tag{25}$$

加入以上公理,然后使用 Event B 的交互式证明,对所有证明义务进行证明.

图 7 为 Event B 中组件管理器(Explorer)所显示的视

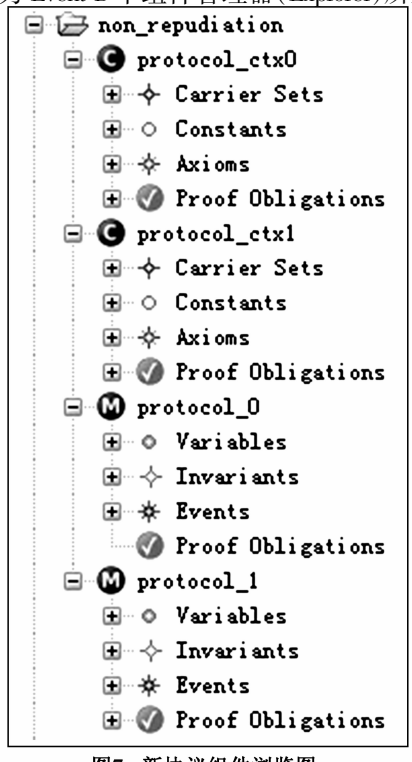


图7　新协议组件浏览图

图,从视图中可以看出,新协议四个组件的证明义务(Proof Obligations)都有✓标志,说明所有组件的证明义务都已证明,即,新协议的公平性及其证据的有效性得到证明.

5 结论

本文在可信平台模块 TPM 的安全体系结构基础上提出了一种 Manet 中基于动态第三方的可信公平非抵赖协议,以取代传统 TTP,解决因其带来的效率瓶颈问题,并使用 DAA 远程认证接口和完整性度量技术,确保协议运行的安全可信,最后使用 Event B 对协议进行形式化建模,证明其公平性及证据的有效性.我们下一步将尝试完全抛弃可信第三方,以进一步提高公平非抵赖协议的效率.

参考文献

[1] T Tedrick. Fair exchange of secrets[A]. Proceedings of CRYPTO 84, Lecture notes in Computer Science[C]. Germany: Springer Verlag, 1985.196:434 – 438.

[2] O Markowitch, Y Roggeman. Probabilistic non-repudiation without trusted third party[A]. Second Conference on Security in Communication Networks 99[C]. Amal Italy: Kluwer Academic, 1999.25 – 36.

[3] 熊焰,张伟超,苗付友,等.一种基于计算能力的无需可信第三方公平非抵赖信息交换协议[J].电子学报,2006,34(3):563 – 566.
Xiong Yan, Zhang Weichao, Miao Fuyou, et al. A fair non-repudiation protocol without TTP based on ent ity′s computing power[J]. Acta Electronica Sinica, 2006, 34(3):563 – 566. (in Chinese)

[4] Pagnia H, Gartner F. On the Impossibility of Fair Exchange Without a Trusted Third Party[R]. Darmstadt, Germany: Darmstadt University of Technology, 1999.

[5] B Meng, Q Xiong. A securely fair non-repudiation protocol with TTP load lightly[A]. The 8th International Conference[C]. Germany: Springer, 2004.2:13 – 17.

[6] E Brickell, J Camenisch, L Chen. Direct anonymous attestation[A]. CCS′04 Proceedings of the 11th ACM Conference on Computer and Communications Security[C]. New York: Association for Computing Machinery, 2004.132 – 145.

[7] Huang Wenchao, Xiong Yan, Chen Depin. DAAODV: A secure ad-hoc routing protocol based on direct anonymous attestation[J]. Computational Science and Engineering, 2009, 2: 809 – 816.

[8] J-R Abrial, 裘宗燕译. B 方法[M].北京:电子工业出版社, 2004.156 – 233.
J-R Abrial, Qiu Trans. B Method[M]. Beijing: Publishing House of Electronics Industry, 2004.156 – 233. (in Chinese)

[9] DEPLOY. Event-B and the Rodin Platform[OL]. http://www.event-b.org/index.html, 2012.

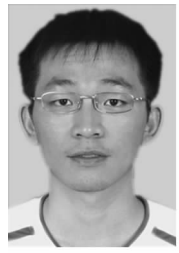
[10] Huang Wenchao, Xiong Yan, Cheng Wenjuan. A formal specification of mobile trusted computing[J]. Chinese Journal of Electronics, 2011, 20(1):11 – 16.

[11] 赵波,严飞,余发江.可信计算[M].北京:机械工业出版社,2009.11 – 245.

作者简介

吴呈邑 男,1987 年出生于江西进贤.2009 年获中国科学技术大学计算机科学与技术系学士学位.现为中国科学技术大学计算机学院在读硕士,从事网络安全、形式化分析以及可信计算方面的研究.
E-mail: wuchengyi@mail.ustc.edu.cn

熊 焰 男,1960 年出生于安徽合肥.中国科学技术大学计算机学院教授,主要研究方向为分布式处理、移动计算、计算机网络和信息安全.
E-mail: yxiong@ustc.edu.cn



黄文超 男,1982 年出生于湖北.中国科学技术大学计算机学院在读博士后,主要研究方向为系统安全、可信计算、形式化分析及计算机网络.