文章编号:1001 - 9081(2009)09 - 2432 - 03

知性 Cord 逻辑:验证 Ad Hoc 网络匿名路由协议

李 沁[1,2],曾庆凯[1,2]
(1. 南京大学 软件新技术国家重点实验室,南京 210039; 2. 南京大学 计算机科学与技术系,南京 210039)
(zqk@nju.edu.cn)

摘 要:为形式化验证移动自主网的匿名路由协议,提出了基于知性 Cord 逻辑的模块化验证方法。首先将协议分解为针对不同子安全功能的组件,然后分别利用知性 Cord 逻辑证明是否满足安全属性的规范。在这个框架下路径匿名的安全属性得到了规范。

关键词:匿名;移动自主网;知性 Cord 逻辑;模块化;形式化方法
中图分类号: TP393 **文献标志码**:A

Epistemic Cord logic: verifying anonymous routing protocols in Ad Hoc network

LI Qin[1,2], ZENG Qing-kai[1,2]
(1. *State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing Jiangsu* 210093, *China*;
2. *Department of Computer Science and Technology, Nanjing University, Nanjing Jiangsu* 210093, *China*)

Abstract: For verifying Ad Hoc anonymous routing protocols, a modular method was proposed, which was based on epistemic Cord logic. This method decomposed a protocol into several components according to different security sub-function, and then proved whether these components satisfied their specifications of security properties. The security property of path anonymity was defined and was specified by this logic.

Key words: anonymity; Ad Hoc network; Epistemic Cord Logic (ECL); modularity; formal method

0 引言

当移动自主网络被布置在敌方战场中时,匿名路由协议对于网络的正常工作有着极其重要的意义。如果没有匿名保护,敌方可以通过被动监听网络通信并发现和定位那些隶属于高级指挥人员的设备,从而可以发动精确打击。近几年研究人员已经提出了一些匿名协议[1-3],这些协议着重于保证在为上层协议栈提供路由服务的同时避免路由参与节点身份的泄露。然而这些协议仅仅被非正式地证明,没有用更为严格形式化方法证明。

匿名路由协议的形式化验证有别于传统因特网安全协议的验证,相比而言更为复杂。其难点在于匿名的安全需求同时包含了不同却相互依赖的安全属性,比如发送匿名(Sender anonymity)、接收匿名(Recipient anonymity)和关系匿名(Relation anonymity)。另一方面,协议运行的环境对验证结果的影响也很大。例如,验证时需要考虑一个有多少节点的网络才能确保验证结果是可信赖的?此类问题的存在源于在实现匿名时必须考虑基于统计的攻击方式。我们必须回答在已有的验证方法下这样的问题能否被验证。

本文提出了一种验证方法学,其主要思想是把协议分解为若干个分量,每一个分量实现某一个特定的安全需求同时又简单到可以被一些既有的验证方法所验证。这个思想来源于协议组合逻辑(Protocol Composition Logic, PCL)[4-5]。就我们所知,这是此类逻辑首次被应用于匿名路由协议的形式化验证。我们对 Cord 演算[4]做了两个扩展。首先是通过在 Cord 空间中增加知识集使其成为认知 Cord 空间(Epistemic Cord Space, ECS),它提供了一个语义模型使我们可以定义判定攻击者是否能够区分来自不同节点消息的谓词;其次,我们在 ECS 上附加了一个拓扑限制用来定义一些谓词:两节点是否可以直接通信以及某一消息是否曾经在这两个节点间传递。

如前所述,匿名路由包含发送匿名、接收匿名以及路径匿名。这些属性均有它们各自的实现并且按照一定关系组合在一起。由于移动自主网的特点,这些属性往往都有一些事实上标准的实现方法。例如,笔名(Pseudonymity)是匿名协议运行的前提;全局后门(Global trapdoor)则是实现发送匿名和接收匿名的常用机制;洋葱路由(Onion routing)以不同的表现方式作为路径匿名的实现机制。在已经提出的匿名路由方案中这些目的各异的实现机制以各种形式组合在一起。基于此,在扩展的 PCL 框架之下,我们把各匿名属性的规范和验证统一地以知性 Cord 逻辑(Epistemic Cord Logic, ECL)的形式表达。

1 ECL 的逻辑与语义模型

1.1 Epistemic Cord 空间

Cord 空间与观察等价的概念可分别参见文献[5-6]。

ECS 是一个由 Cord 空间与函数 $E_{r,G_0}:(\mathbf{N}\times\Lambda)\to\Psi$ 构成的二元组,r 指某次运行,$\mathbf{N}$ 是自然数的集合,Λ 是名字的集合,Ψ 是知识集的集合。每个知识集以项为元素,它表示在协议运行时特定角色掌握的信息。给定初始格局 G_0,$E_{r,G_0}(i,X)$ 指运行 r 中在第 i 次反应后节点 X 所掌握的信息。如果 i 不变,$E_{r,G_0}(i,X)$ 则是一个将名字 X 映射至某个知识集的一元函数,简写为 E_r^i。特别地,E_r^0 表示协议初始状态下各角色掌握的初始信息。

收稿日期:2009 - 03 - 23;**修回日期**:2009 - 05 - 18。 **基金项目**:国家自然科学基金资助项目(60773170;60721002;90818022);国家 863 计划项目(2006AA01Z432);高等学校博士学科点专项科研基金资助项目(200802840002)。

作者简介:李沁(1976 -),男,安徽芜湖人,博士研究生,主要研究方向:信息安全、形式化方法; 曾庆凯(1963 -),男,安徽来安人,教授,博士生导师,博士,主要研究方向:信息安全、分布式系统。

ECS 中的运行 r_e 形如 $\{E_r^0, a_0, E_r^1, a_1, \cdots, a_{n-1}, E_r^n\}$ 的序列,a_i 是介于 G_{i-1} 与 G_i 之间的反应(后文中的运行均指在ECS中的运行)。序列长度 $|r_e| = n$。$E_r^i(X)$ 是一个集合,由闭包算子[6]71 $S \mapsto \bar{S}$ 作用于集合 $E_r^{i-1}(X)$ 和角色 X 由于反应 a_i 而新得项集的并生成。直观地说,此闭包算子包含两步操作。

首先将新的项分解至原子项,然后基于所有已知原子项与项代数的基调(signature)迭代地生成新的组合项。R_{G_0,E^0} 是所有可能的运行构成的集合,这些运行始于初始格局 G_0 并具有相同的 E^0。

运行受拓扑(Top)的限制,此限制决定了实例化角色之间的连通性,使反应仅仅发生在那些可以相互连通的 Cord 之间。Top 是元组 $\{V,E\}$,V 是节点集,E 是边集。

1.2　ECL 语法

逻辑的常元符号包括名字的可数集 Λ,由 $A,B,C,\cdots$ 表示;数项(numerals);密钥符号,由 k_X, k_X^{-1} 或 k_{XY} 表示。它还包括 E,一个由名字对构成的集合。函词符号包括 $\$\overline{XY}: \Lambda \times \Lambda \to E$ 以及操作符号"$'$"(元组),hash(哈希),enc(加密)等。

逻辑的合式公式 φ 的定义如下:

$$\varphi ::= Sent(X,T) \mid Has(X,T) \mid Endof(X,\overline{XY}) \mid Originates(X,T,T',K) \mid Adjoined(\overline{XY},\overline{YZ}) \mid Occur(T,\overline{XY}) \mid t_1 \cong_X t_2 \mid \neg\varphi \mid \forall X.\varphi \mid \Diamond\varphi \mid \odot\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi$$

X 和 T 分别是名字和项。在证明过程中形如 $[P]_X\varphi$ 的式子表示在 X 执行行为 P 之后的状态下 φ 为真;$\varphi_1[P]_X\varphi_2$ 表示 φ_1 在 P 执行前成立而在其后 φ_2 成立。$After(a,b)$ 是代表 $\Diamond(b \wedge \odot\Diamond a)$ 的语法糖,a,b 指诸如 $Sent(X,T)$,$Occur(T,\overline{XY})$ 以及 $Originates(X,T,T',K)$ 之类的谓词。合式公式的语义见 1.3 节。

1.3　ECL 的语义模型

ECL 的语义由解释 I 定义,I 把常元名字符号映射至协议参与者名字;如果 X 与 Y 在 Top 中相邻则将 $\overline{XY}$ 映射至拓扑边集;将 T 映射至项集。

在协议的一次运行中公式可以为真或假。语义关系 $P, r_e \vDash \varphi$ 读作"φ 在协议 P 的运行 r_e 中成立"。r_e 可以是完全或不完全的运行。以下给出形式语义,关系对不含自由变量的 φ,$P, r_e \vDash \varphi$ 的归纳定义如下。

$P, r_e \vDash Send(A,t)$,如果 $\exists i \leqslant |r_e| - 1, a_i$ 为一个反应,参与反应的协议参与者 $I(A)$ 的动作是发送消息 $\langle t\rangle$,此公式指协议参与者 $I(A)$ 发送消息 t。

$Has(A,t)$,如果 $\exists i \leqslant |r_e| - 1, t \in E_r^i(A)$,此公式指在协议运行中协议参与者 $I(A)$ 可以构造消息 T。

$P, r_e \vDash Originates(A,t,t_1,k)$,如果 $P, r_e \vDash Send(A,t\_1)$,$enc(t,k) \subset t_1$,$\neg\ \exists X \in \Lambda_r - \{A\}.\ Send(X,\hat{t})$,$\hat{t} \subset t$,$\Lambda_r$ 是运行 r 中牵涉到的所有名字。关系 $\subset$ 是定义在 T 上的子项关系。此公式指协议参与者 $I(A)$ 第一个发出包含加密新鲜值 $enc(t,k)$ 消息 t_1。

$P, r_e \vDash Endof(Z,\overline{XY})$,若协议参与者 $I(Z)$ 位于 $I(\overline{XY})$ 一端。

$P, r_e \vDash Adjoined(\overline{XY},\overline{ZW})$,如果 $I(\overline{XY}), I(\overline{ZW}) \in E$ 共享一个端点。

$P, r_e \vDash Occur(T,\overline{XY})$,如果 $\{Sent\}(X,T)$ 或 $Sent(Y,T)$,且 $\overline{XY} \in I^{-1}(E)$。

$P, r_e \vDash \forall X.\varphi$,如果 $\forall A \in \Lambda_{r_e}.P, r_e \vDash \varphi[A/X]$。此公式指对 φ 在其中包含的变量替换为协议中牵涉之名字后仍成立。

$P, r_e \vDash \neg\varphi$ 如果 $P, r_e \vDash \varphi$ 不成立。

$P, r_e \vDash \varphi_1 \vee \varphi_2$ 如果 $P, r_e \vDash \varphi_1$ 或 $P, r_e \vDash \varphi_2$。

$P, r_e \vDash \varphi_1 \wedge \varphi_2$ 如果 $P, r_e \vDash \varphi_1$ 和 $P, r_e \vDash \varphi_2$。

$P, r_e \vDash t_1 \cong_X t_2$,如果存在一个重解释 π 在 $E_r^i(X), i \leqslant |r_e|$ 下同时满足 $\pi(t_1) = t_2$ 和 $\pi^{-1}(t_2) = t_1$。

$P, r_e \vDash \Diamond\varphi$,如果 $P, r_e \vDash \varphi, r'_e$ 是 r_e 的前缀(可能相同)。此公式指在过去的某一状态 φ 为真。

$P, r_e \vDash \odot\varphi$,如果 $P, r_e \vDash \varphi, r'_e, r_e = r'_e.a$。此公式指在前一状态 φ 为真。

2　ECL 的证明系统

2.1　公理和推理规则

表 1 列出了关于拓扑环境(Top1 ~ Top4)的公理和关于时序(T1 ~ T3)的公理。Top1 ~ Top3 的意义显然,Top4 指如果一跳(hop)的一端发送过消息,那么此则消息在此跳上发生。

表 1　拓扑与时序的公理

公理名	公理
Top1	$Endof(X,\overline{XY})$
Top2	$Adjoined(\overline{XY},\overline{YZ})$
Top3	$\overline{XY} = \overline{YX}$
Top4	$Sent(X,t) \wedge Endof(X,\overline{XY}) \supset Occur(t,\overline{XY})$
T1	$\Diamond(\varphi \wedge \psi) \supset (\Diamond\varphi \wedge \Diamond\psi)$
T2	$\odot(\varphi \wedge \psi) \supset (\odot\varphi \wedge \odot\psi)$
T3	$\odot\neg\varphi \leftrightarrow \neg\odot\varphi$

表 2 是关于协议行为的公理。公理 AM 是关于协议角色的静态变量的绑定。公理 AA 是关于行为的效果。公理 AN,AS 和 AR 分别是关于生成新鲜值、发送以及接收消息。K1 ~ K6 是关于监听者的推理能力,K6 指监听者是全局的。

表 2　协议行为的公理

公理名	公理
AM	$(x_1, x_2, \cdots, x_n)[]_X \wedge_{i\in[1,n]} Has(X, x_i)$
AA	$\varphi[a]_X\psi \supset \Diamond(\psi \wedge \odot\Diamond\varphi)$
AN1	$[(\nu m)]_X Has(X, m)$
AN2	$[(\nu m)]_X \forall T, k.\ Originates(X, m, T, k)$
AN3	$[(\nu m)]_X Has(Y, m) \supset Y = X$
AS1	$[\langle m\rangle]_X Sent(X, m)$
AS2	$Sent(X,(t_1,t_2)) \supset Sent(X,t_1) \wedge Sent(X,t_2)$
AR1	$[(m)]_X \exists Y.\ Sent(X, m)$
AR2	$[(m)]_X Has(X, m)$
K1	$Has(X,t_1) \wedge Has(X,t_2) \supset Has(X,(t_1,t_2))$
K2	$Has(X,(t_1,t_2)) \supset Has(X,t_1) \wedge Has(X,t_2)$
K3	$Has(X,t) \wedge Has(X,k) \supset Has(X,enc(t,k))$
K4	$Has(X,enc(t,k)) \wedge Has(X,k^{-1}) \supset Has(X,t)$
K5	$Has(X,t) \supset Has(X,hash(t))$
K6	$\forall X.\ Sent(X,m) \supset Has(M,m)$
SRC	$Originates(X,T,T',k) \wedge Has(Z,T) \wedge Z \neq X \supset \exists Y.\ Has(Y,k^{-1})$
EU1	$\forall X.\ t_1 = t_2 \supset t_1 \cong_X t_2$
EU2	$\forall X.\ Has(X,t) \wedge Has(X,k_1) \wedge Has(X,k_2) \supset enc(t,k_1) \cong_X enc(t,k_2)$
EU3	$\forall X.\ Has(X,enc(t,k_1)) \wedge Has(X,k_1^{-1}) \wedge Has(X,k_2) \supset enc(t,k_1) \cong_X enc(t,k_2)$
EU4	$\forall X.\ Has(X,t) \wedge Has(X,hash(t)) \supset t \cong_X hash(t)$
HON	$Has(Y,k_X^{-1}) \supset X = Y$
SYM	$Has(Z,k_{XY}) \supset Z = X \vee Z = Y$

公理 EQU 指当 X 拥有相应的密钥时，能够识别两则消息。HON 指正常参与者的私钥不会泄漏。最后一则指对称密钥仅属于两个拥有它的参与者。

表3是 ECL 的推理规则。一般规则与谓词逻辑无异。Preservation 规则指协议参与者的知识不会随着协议的执行而减少。其中 $Persist \in \{Has, Sent, Originates\}$，$a \in \{(\nu x), \langle T \rangle, (x), (u/q(x))\}$。

表3 推理规则

规则名	规则
G1	$\frac{[P]_X\varphi_1 \quad [P]_X\varphi_2}{[P]_X\varphi_1 \wedge \varphi_2}$
G2	$\frac{[P]_X\varphi_1 \supset \varphi_2 \quad [P]_X\varphi_1}{[P]_X\varphi_2}$
G3	$\frac{\varphi}{[P]_X\varphi}$
G4	$\frac{\varphi}{\neg \odot \neg \varphi}$
P	$\frac{[P]_X Persist(X, T, \cdots)}{[P < a >]_X Persist(X, T, \cdots)}$

2.2 系统的可靠性证明

定理1 可靠性。如果 $P, r_e \vDash \varphi$，则 $P, r_e \vDash \varphi$。

证明 定理的证明与文献[5]中的证明类似。主要的区别来自新增的公理。所以我们仅证明了这些新增的公理的可靠性，其余的证明可参见文献[5]。

首先，对公理 K1，…，K6，我们以证明 K1 为例：如果 $Has(X, t_1)$ 及 $Has(X, t_2)$ 成立，说明运行 r 中存在状态 i，其中项 t_1 和 t_2 属于集合 $E_r^i(X)$。因为集合 $E_r^i(X)$ 是对于元组操作来说是封闭的，所以项 (t_1, t_2) 也一定属于此集合，从而 $Has(X, (t_1, t_2))$ 成立。

其次，我们考虑公理 EQU1，EQU2，EQU3 以及 EQU4。EQU1 显然成立。EQU2 的证明如下：如果 $Has(X, t)$，$Has(X, k_i)$，$i = 1, 2$ 成立，则存在状态 i，使 $t, k_1, k_2 \in E_r^i(X)$。根据观察等价的定义，在集合 $E_r^i(X)$ 下存在一个在 $enc(t, k_1)$，$enc(t, k_2)$ 之间的重解释，所以 $enc(t, k_1) \cong_X enc(t, k_2)$ 成立。其余两则的证明是类似的。

最后，对于有关拓扑的公理，显而易见它们反映了拓扑的自然几何关系。

3 路由匿名的规范

我们认为路由匿名的属性规范在移动自主网中的含义为在路由形成的过程中对监听者来说没有发现这样事件的可能：在两个相邻的跳上存在两对观察等价且有时序关系的消息。在 ECL 中路由匿名可规范为：

$$\varphi_{route} \equiv \neg \exists T_1, T_1', T_2, T_2'. ((T_1 \cong_M T_1') \wedge (T_2 \cong_M T_2') \wedge After(Occur(T_1, \overline{XY}), Occur(T_1', \overline{XY})) \wedge After(Occur(T_2, \overline{WZ}), Occur(T_2', \overline{WZ})) \wedge Adjoined(\overline{XY}, \overline{WZ}))$$

4 相关工作

在过去的20年中匿名协议的形式化验证主要集中在 Web 服务和 P2P 网络中运行的匿名协议。文献[7]提出基于 CSP 的匿名协议验证框架，主要着重于形式化发送者和接收者之间的不可连接性。文献[8]利用函数视图的概念建模匿名属性。Halpern 在文献[9]中提出了多代体系统的框架，在这个框架中可以规范各种不同的匿名需求。Syverson 和 Stubblebine 提出了基于认知逻辑的方法[10]。一些研究工作侧重于匿名强度的量化。匿名集的概念首先出现于文献[11]。匿名协议在文献[12]中被当作噪声信道。信息论的方法分别在文献[13－14]中被独立地提出。

5 结语

本文提出了一个以验证 Ad Hoc 匿名路由协议为目的的组合式逻辑 ECL。分别在逻辑和证明系统中引入了一些表达网络拓扑、通信事件及其时序关系的谓词、公理和推理规则。定义了安全属性匿名路由，并且利用 ECL 给出了形式化规范，此例阐释了 ECL 作为验证 Ad Hoc 匿名路由协议的能力。

参考文献：

[1] KONG J, HONG P. ANODR: Anonymous on demand routing with untraceable routes for mobile Ad-Hoc networks [C]// Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing. Maryland: ACM Press, 2003: 291－302.

[2] ZHANG Y, LIU W, LOU W. MASK: Anonnymous on-demand routing in mobile Ad Hoc networks [J]. IEEE Transactions on Wireless Communications, 2006, 5(9): 2376－2385.

[3] BOUKERCHE A, EL-KHATIB K, XU L, KORBA L. SDAR: A secure distributed anonymous routing protocol for wireless and mobile Ad Hoc networks [C]// Proceedings of the 29th Annual International Conference on Local Computer Networks. Washington, DC: IEEE Computer Society, 2004: 618－624.

[4] DATTA A, DEREK A, MITCHELL J, *et al.* Abstraction and refinement in protocol derivation [C]// Proceedings of the 17th Computer Security Foundations Workshop. Washington, DC: IEEE Computer Society, 2004: 30－45.

[5] DURGIN N, MITCHELL J, PAVLOVIC D. A compositional logic for proving security properties of protocols [J]. Journal of Computer Security, 2003, 11(4): 677－721.

[6] GARCIA F D, HASUO I, PIETERS W, *et al.* Provable anonymity: Workshop on formal methods in security engineering [C]// Proceedings of the 2005 ACM Workshop on Formal Methods in Security Engineering. New York: ACM Press, 2005: 63－71.

[7] SCHNEIDER S, SIDIROPOULOS A. CSP and anonymity [C]// Proceedings of the 4th European Symposium on Research in Computer Security. London: Springer-Verlag. 1996: 198－218.

[8] HUGHES D, SHMATIKOV V. Information hiding, anonymity and privacy: A modular approach [J]. Journal of Computer Security, 2004, 12(1): 3－36.

[9] HALPERN J, O'NEIL K. Anonymity and information hiding in multiagent systems [J]. Journal of Computer Security, 2005, 13(3): 483－514.

[10] SYVERSON P, STUBBLEBINE S. Group principals and the formalization of anonymity [C]// Proceedings of the World Congress on Formal Methods in the Development of Computing Systems. London: Springer-Verlag, 1999: 814－833.

[11] CHAUM D. Untraceable electronic main, return address, and digital pseudonyms [J]. Communications of ACM, 1981, 24(2): 84－90.

[12] CHATZIKOKOLAKIS K, PALAMIDESSI C, PANANGADEN P. Anonymity protocols as noisy channels [J]. Information and Computation, 2008, 206(2/4): 378－401.

[13] SERJANTOV A, DANEZIZ G. Towards an information theoretic metric for anonymity [C]// Proceedings of Privacy Enhancing Technologies. London: Springer-Verlag, 2003: 259－263.

[14] DIAZ C, SEYS S, CLAESSENS J, *et al.* Towards measuring anonymity [C]// Proceedings of 2002 International Workshop on Private Enhancing Technologies. London: Springer-Verlag, 2002: 54－68.