Ad hoc网络中ARAN路由协议的安全性分析

闫丽丽[①②]　彭代渊[①]
[①](西南交通大学信息安全与国家计算网格实验室　成都　610031)
[②](成都信息工程学院网络工程学院　成都　610225)

摘　要：由于 Ad hoc 网络的特性，传统的串空间理论无法分析其路由协议的安全性，该文首先对串空间理论进行了扩展，添加了证明中间节点可信的条件。随后，使用扩展后的串空间理论分析了 ARAN 路由协议的安全性，提出了使用该理论分析 Ad hoc 网络中安全路由协议的新方法。分析和证明结果表明，ARAN 路由协议中存在重放和合谋两种攻击，说明采用文中提出的分析方法对 Ad hoc 网络中的按需距离矢量路由协议的安全性进行分析是有效的。

关键词：Ad hoc网络；路由协议；串空间；形式化分析；一致性
中图分类号：TP393.08　　**文献标识码**：A　　**文章编号**：1009-5896(2010)09-2241-04
DOI: 10.3724/SP.J.1146.2009.01265

Security Analysis of ARAN Routing Protocol for Ad hoc Networks

Yan Li-li[①②]　Peng Dai-yuan[①]
[①](*Information Security and National Computing Grid Laboratory*, *Southwest Jiaotong University*, *Chengdu* 610031, *China*)
[②](*The Department of Network Engineering*, *Chengdu University of Information Technology*, *Chengdu* 610225, *China*)

Abstract: Because of the characteristics of Ad hoc networks, the theory of strand spaces can not analyzes the security of routing protocol. In this paper, the theory of strand spaces is first extended and the credibility of intermediate node is added. Subsequently, this extended theory is applied to analyzing the security of ARAN routing protocol and a new formal analysis method is proposed for Ad hoc networks routing protocol. The results show that it has replay attacks and conspiracy attacks in ARAN routing protocol. The method is proved to be valid.

Key words: Ad hoc network; Routing protocol; Strand spaces; Formal analysis; Agreement property

1　引言

安全路由协议的设计和分析，是 Ad hoc 网络安全中的核心问题。安全路由协议的目标是获取正确的路由信息，研究人员已经先后提出了多种安全路由协议，如：ARAN[1,2]，Ariadne，SPR 和 SEAD 等。但由于路由协议的复杂性，对其安全性分析一直缺乏有效的方法。目前大部分的安全路由协议的分析，仍然采用非形式化的方法，即基于主观分析或者模拟仿真，这只能对已知攻击进行分析，而对于未被发现的攻击却无能为力。近年来，采用形式化的方法来分析路由协议的安全性越来越受到研究者的重视，其中的串空间理论[3−5]是结合定理证明和协议迹的混合方法，也是现有的形式化方法中最为直观、有效的方法。

ARAN(Authenticated Routing for Ad hoc Networks)是由 Sanzgiri 提出的一个安全路由协议，它为 Ad hoc 网络提供了身份鉴别、信息完整性和不可抵赖性等安全保证。在文献[1]中 Sanzgiri 使用非形式化的分析方法，根据已经发现的攻击方式对该协议的安全性进行了分析。文献[6]对 ARAN 协议的分析使用了形式化的分析方法，通过对 ABV 模型进行扩展，证明了 ARAN 协议在扩展 ABV 模型下是安全的。而文献[7]的作者指出文献[6]使用扩展 ABV 模型对 ARAN 协议的安全性证明过程存在错误，并给出 ARAN 协议的一个安全漏洞。本文将使用串空间理论形式化地分析 ARAN 路由协议的安全性。由于 Ad hoc 路由协议的特性，文中修改了串空间理论中的一致性属性，合并了串空间中入侵者迹所具有的原子行为，通过建立协议的串空间模型，对协议中所有节点的一致性进行了分析，成功地发现了协议中潜在的缺陷和漏洞。由此也说明了文中提出的基于串空间理论分析 Ad hoc 网络中安全路由协议的新方法是有效的。

2009-09-25 收到，2010-03-15 改回
国家自然科学基金(60872015)资助课题
通信作者：闫丽丽　yanlili@vip.163.com

2 串空间理论扩展

由于Ad hoc网络的特殊性，在本节中将对串空间理论中的“正确性”概念进行修改，扩展串空间理论使其能够描述Ad hoc网络中安全路由协议的正确性。关于构造串空间所需的基本定义和攻击者迹的描述，这里就不再赘述，详细的内容见文献[3–5]。

在Ad hoc网络中，当两个移动主机在彼此的通信覆盖范围内时，它们可以直接通信，但是由于移动主机的通信覆盖范围有限，如果两个相距较远的主机要进行通信，则需要通过中间节点的中继来实现。所以，在Ad hoc网络中发起节点和目的节点是唯一的，但中间节点可能多个，而且有可能是恶意节点。

另外，在Ad hoc网络的路由发现过程中，通常的方法都是发起节点采用泛洪的方式进行广播，ARAN协议就是一个例子。由于发起节点和目的节点之间可能存在多条路径，当发起节点广播一条路由请求时，目的节点可能会收到多条路由请求，这就不满足串空间中的强一致性。因此，在对ARAN路由协议分析时，我们使用串空间的弱一致性概念，并添加了中间节点可信的条件，使其能满足Ad hoc网络的特性。

响应者一致性：每一次主体B作为响应者使用数据项x完成了一个回合的协议执行时，对于B来说他是在与A通信；于是确实存在一轮协议执行，A作为发起者也使用了数据项x，并且与其通信的为B。

发起者一致性：每一次主体A作为发起者使用数据项x完成了一个回合的协议执行时，对于A来说他是在与B通信；于是确实存在一轮协议执行，B作为响应者也使用了数据项x，并且与其通信的为A。

中间节点一致性：每一次主体A作为发起者，主体B作为响应者，使用数据项x完成了一个回合的协议执行时，存在中间节点v转发了数据项x；于是确实存在一轮协议执行，中间节点v转发了数据项x，数据项x的发起者为A、响应者为B，并且发起者A和响应者B之间经由中间节点v存在着一条有效的路由路径。

发起者和响应者的一致性条件保证了发起节点和响应节点的合法性，中间节点的一致性保证了中间节点的可信性，所以，通过证明协议中节点满足一致性属性就可以保证协议运行过程中节点的合法性，即正确性。

3 ARAN协议原型

ARAN(Authenticated Routing for Ad hoc Networks)[1,2]是由Sanzgiri提出的一个安全路由协议，它为Ad hoc网络提供了身份鉴别、信息完整性和不可抵赖性等安全保证。ARAN协议如下：

$A \rightarrow$ brdcast: $\{\text{RDP}, \text{IP}_X, N_A\}K_A^{-1}, \text{cert}_A$

$B \rightarrow$ brdcast: $\{\{\text{RDP}, \text{IP}_X, N_A\}K_A^{-1}\}K_B^{-1}, \text{cert}_A, \text{cert}_B$

$C \rightarrow$ brdcast: $\{\{\text{RDP}, \text{IP}_X, N_A\}K_A^{-1}\}K_C^{-1}, \text{cert}_A, \text{cert}_C$

$X \rightarrow C$: $\{\text{REP}, \text{IP}_A, N_A\}K_X^{-1}, \text{cert}_X$

$C \rightarrow B$: $\{\{\text{REP}, \text{IP}_A, N_A\}K_X^{-1}\}K_C^{-1}, \text{cert}_X, \text{cert}_C$

$B \rightarrow A$: $\{\{\text{REP}, \text{IP}_A, N_A\}K_X^{-1}\}K_B^{-1}, \text{cert}_X, \text{cert}_B$

消息项中的RDP(Route Discovery Packet)标志数据包是路由发现数据包，REP(Reply Packet)标志数据包是响应数据包，IP_X表示X节点的IP地址，K_A表示A的公钥，K_A^{-1}表示A的私钥。cert_A表示由可信的认证中心T发给A的证书，$\text{cert}_A = \{\text{IP}_A, K_A, t, e\}K_T^{-1}$，其中$t$表示证书的创建时间，$e$表示证书的过期时间。$N_A$是由$A$产生的随机数，目的是用来唯一地确定RDP包来自哪一个发起节点，每一次A发起路由发现请求时，会产生一个单调递增的N_A，在网络的整个生命周期中N_A的值是递增的。

ARAN协议的目标不是发现最短的，即跳数最少的路由，而是延迟最小的路由。路由源节点A广播目的节点为X的RDP包，当中间节点C收到该数据包后，首先验证包中的签名和临时值，如果验证成功，C建立一个路由表项，记录目的节点为A，下一跳节点为B。然后C对该数据包签名并添加自己的证书，继续广播路由请求数据包。当目标节点X收到该路由请求后，以相同的方式更新自己的路由表，并构建路由响应REP数据包，回复给路由表项中记录的下一跳节点。当中间节点接收到路由响应数据包后，与路由请求数据包处理过程相同。

4 ARAN协议的形式化分析

本节将根据前面定义的“正确性”概念，通过分析发起节点、响应节点和中间节点的合法性来说明ARAN协议的安全性。在应用串空间理论进行分析之前，先将项代数进一步具体化：

(1)标识符集合$T_{\text{name}} \in T$，文中用S，D，v_1，v_2，…，表示主体的标识符。

(2)映射 K：$T_{\text{name}} \rightarrow \kappa$。这个映射将主体与它的公开密钥绑定。将$K(S)$写成$K_S$，并假设这个映射是单射的，即若$K(S) = K(D)$，则有$S$=$D$。

4.1 ARAN串空间

根据串空间理论，首先对ARAN协议进行形式

化的处理，如图1所示。

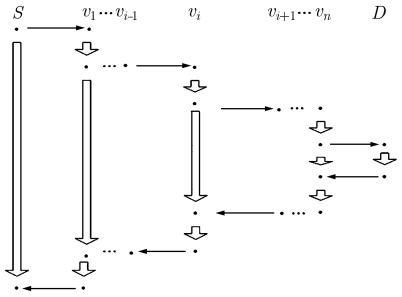

图1 协议的形式化表示

假设发起节点S向目的节点D应用ARAN协议发现路由，其中$v_1, v_2, \cdots, v_n$为路由发现的中间节点。其串空间模型如下：

定义1 设(Σ, ρ)是一个被渗透的串空间，如果Σ由以下6种串组成，就称它为一个ARAN串空间：(1)攻击节点串$s \in \rho$。(2)发起节点串$s \in \text{source}$[RDP, REP, IP_D, IP_S, N_S, K_S^{-1}, K_D^{-1}, $K_{v_1}^{-1}$, cert_S, cert_D, cert_{v_1}]，其迹为：$\langle +\{\text{RDP}, \text{IP}_D, N_S\}K_S^{-1}, \text{cert}_S, -\{\{\text{REP}, \text{IP}_S, N_S\}K_D^{-1}\}K_{v_1}^{-1}, \text{cert}_D, \text{cert}_{v_1} \rangle$。(3)目的节点串$s \in \text{dest}$[RDP, REP, IP_D, IP_S, N_S, K_S^{-1}, K_D^{-1}, $K_{v_n}^{-1}$, cert_S, cert_D, cert_{v_n}]，其迹为：$\langle -\{\{\text{RDP}, \text{IP}_D, N_S\}K_S^{-1}\}K_{v_n}^{-1}, \text{cert}_S, \text{cert}_{v_n}, +\{\text{REP}, \text{IP}_S, N_S\}K_D^{-1}, \text{cert}_D \rangle$。(4)中间节点1串$s \in$ Intermediate1[RDP, REP, IP_D, IP_S, N_S, K_S^{-1}, K_D^{-1}, $K_{v_1}^{-1}$, $K_{v_2}^{-1}$, cert_S, cert_D, cert_{v_1}, cert_{v_2}]，其迹为：$\langle -\{\text{RDP}, \text{IP}_D, N_S\}K_S^{-1}, \text{cert}_S, +\{\{\text{RDP}, \text{IP}_D, N_S\}K_S^{-1}\}K_{v_1}^{-1}, \text{cert}_S, \text{cert}_{v_1}, -\{\{\text{REP}, \text{IP}_S, N_S\}K_D^{-1}\}K_{v_2}^{-1}, \text{cert}_D, \text{cert}_{v_2}, +\{\{\text{REP}, \text{IP}_S, N_S\}K_D^{-1}\}K_{v_1}^{-1}, \text{cert}_D, \text{cert}_{v_1} \rangle$。(5)中间节点2串$s \in$ Intermediate2 [RDP, REP, IP_D, IP_S, N_S, K_S^{-1}, K_D^{-1}, $K_{v_{i-1}}^{-1}$, $K_{v_i}^{-1}$, $K_{v_{i+1}}^{-1}$, cert_S, cert_D, $\text{cert}_{v_{i-1}}$, cert_{v_i}, $\text{cert}_{v_{i+1}}$]，其迹为：$\langle -\{\{\text{RDP}, \text{IP}_D, N_S\}K_S^{-1}\}K_{v_{i-1}}^{-1}, \text{cert}_S, \text{cert}_{v_{i-1}}, +\{\{\text{RDP}, \text{IP}_D, N_S\}K_S^{-1}\}K_{v_i}^{-1}, \text{cert}_S, \text{cert}_{v_i}, -\{\{\text{REP}, \text{IP}_S, N_S\}K_D^{-1}\}K_{v_{i+1}}^{-1}, \text{cert}_D, \text{cert}_{v_{i+1}}, +\{\{\text{REP}, \text{IP}_S, N_S\}K_D^{-1}\}K_{v_i}^{-1}, \text{cert}_D, \text{cert}_{v_i} \rangle$。(6)中间节点3串$s \in$ Intermediate3[RDP, REP, IP_D, IP_S, N_S, K_S^{-1}, K_D^{-1}, $K_{v_{n-1}}^{-1}$, $K_{v_n}^{-1}$, cert_S, cert_D, $\text{cert}_{v_{n-1}}$, cert_{v_n}]，其迹为：$\langle -\{\{\text{RDP}, \text{IP}_D, N_S\}K_S^{-1}\}K_{v_{n-1}}^{-1}, \text{cert}_S, \text{cert}_{v_{n-1}}, +\{\{\text{RDP}, \text{IP}_D, N_S\}K_S^{-1}\}K_{v_n}^{-1}, \text{cert}_S, \text{cert}_{v_n}, -\{\text{REP}, \text{IP}_S, N_S\}K_D^{-1}, \text{cert}_D, +\{\{\text{REP}, \text{IP}_S, N_S\}K_D^{-1}\}K_{v_n}^{-1}, \text{cert}_D, \text{cert}_{v_n} \rangle$。

4.2 发起节点和响应节点一致性证明

命题 1 设C是Σ中的一个丛，$X \in T_{\text{name}}$，且$K_X^{-1} \notin K_p$。于是，不存在形如$\{g\}_{K_X^{-1}}$的项起源于C中的一个攻击者节点。

证明 见文献[5]。

命题2 若$\{H\}_{K_X^{-1}}$，起源于一个正则串s，则有以下结论

(1)若$s \in \text{source}$，则$H = \text{RDP}, \text{IP}_D, N_S$

(2)若$s \in \text{dest}$，则 $H = \text{REP}, \text{IP}_S, N_S$

证明 根据串空间定义，如果项$\{H\}_{K_X^{-1}}$起源于m， m的符号为正。若$s \in \text{source}$，则$m = \langle s, 1 \rangle$。于是$\text{term}(m)$形如$\{\text{RDP}, \text{IP}_D, N_S\}K_S^{-1}, \text{cert}_S$，它唯一的加密子项为$\{\text{RDP}, \text{IP}_D, N_S\}K_S^{-1}$，具有命题结论(1)的形式。同理，若$s \in \text{dest}$，则$m = \langle s, 2 \rangle$。于是$\text{term}(m)$形如$\{\text{REP}, \text{IP}_S, N_S\}K_D^{-1}, \text{cert}_D$，它唯一的加密子项为$\{\text{REP}, \text{IP}_S, N_S\}K_D^{-1}$，具有命题结论(2)的形式。

推论1 设s是Σ中的一个正则串：(1)若$\{\text{RDP}, \text{IP}_D, N_S\}K_S^{-1}$起源于$s$，则$s \in \text{source}$，此消息起源于结点$\langle s, 1 \rangle$。(2)若$\{\text{REP}, \text{IP}_S, N_S\}K_D^{-1}$起源于$s$，则$s \in \text{dest}$，此消息起源于结点$\langle s, 2 \rangle$。

证明 由于s是正则串，$s \in \text{source} \cup \text{dest}$，应用命题3即得。

定理1 设C是Σ中的一个丛，N_S在C中是唯一起源的，且$K_S^{-1}, K_D^{-1} \notin K_p$。如果$s \in \text{source}[\,]$的$C$-高度为2，则存在$C$-高度为2的正则串$s_{\text{dest}} \in \text{dest}[\,]$。

证明 串s的迹为$< +\{\text{RDP}, \text{IP}_D, N_S\}K_S^{-1}, \text{cert}_S, -\{\{\text{REP}, \text{IP}_S, N_S\}K_D^{-1}\}K_{v_1}^{-1}, \text{cert}_D, \text{cert}_{v_1} >$。因为$K_D^{-1} \notin K_p$，由命题2可知，$\{\text{REP}, \text{IP}_S, N_S\}K_D^{-1}$是起源于一个正则结点$m$。由推论4可知，该结点位于目的节点串dest上，因此$\langle s_{\text{dest}}, 2 \rangle \in C$，可以确定$s_{\text{dest}}$的$C$-高度为2。

定理2 设C是Σ中的一个丛，N_S在C中是唯一起源的，且$K_S^{-1}, K_D^{-1} \notin K_p$。如果$s \in \text{dest}[\,]$的$C$-高度为2，则存在$C$-高度至少为1的正则串$s_{\text{source}} \in \text{source}[\,]$。

证明过程同定理5。

通过以上证明，可以得到发起节点和目的节点满足一致性条件的结论。

4.3 中间节点一致性证明

分析ARAN协议的操作过程，可以发现发起节点发送的RDP包如果被攻击，目的节点的REP包将无法正常返回给发起节点，该路由路径不会被采用，所以可以确定协议中的RDP包不会被攻击节点攻击，安全问题主要存在于REP包的传送过程。

因此这里只分析中间节点$s \in \text{Intermediate}[\,]$中的$\langle s, 3 \rangle$，$\langle s, 4 \rangle$是否有可能源自攻击节点串，下面以$s \in \text{Intermediate2}[\,]$的结点$\langle s, 4 \rangle$为例，对其进行具体分析：

M：由于 $K_D^{-1} \notin K_p$，因此结点 $\langle s,4\rangle$ 不可能源于 M串。

F：由于结点 $\langle s,4\rangle$ 符号为正，不可能源于 F串。

T：由于对于节点 v_{i-1}，它的路由表项中只记录了目的节点为 S，REP包发送的下一跳节点为 v_{i-2}，但没有记录将从哪个上一跳节点接收该REP包，所以节点 v_i 可以将收到的 $g=\{\{\text{REP}, \text{IP}_S, N_S\}K_D^{-1}\}K_{v_{i+1}}^{-1}, \text{cert}_D, \text{cert}_{v_{i+1}}$ 直接转发给节点 v_{i-1}，而节点 v_{i-1} 无法发现此类攻击，因此该结点 $\langle s,4\rangle$ 可能源自 T串。节点的攻击方式如图2所示。

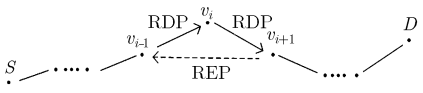

图2 ARAN协议的重放攻击路径

S：显然结点 $\langle s,4\rangle$ 不可能源于 S串。

K：显然结点 $\langle s,4\rangle$ 不可能源于 K串。

D：显然结点 $\langle s,4\rangle$ 不可能源于 D串。

$E+C$：当节点 v_i 收到 $\{\{\text{REP}, \text{IP}_S, N_S\}K_D^{-1}\}K_{v_{i+1}}^{-1}, \text{cert}_D, \text{cert}_{v_{i+1}}$ 后，首先可以根据 $\text{cert}_{v_{i+1}}$ 中存储的 v_{i+1} 的公钥解密该数据项，得到 $h=\{\text{REP},\text{IP}_S, N_S\}K_D^{-1}$, cert_D，接下来根据合谋者的密钥 $k=K_\rho^{-1}$ 及其证书 $g=\text{cert}_\rho$ 可以得到 $\{h\}_k g=\{\{\text{REP}, \text{IP}_S, N_S\}K_D^{-1}\}K_\rho^{-1}, \text{cert}_D, \text{cert}_\rho$，与 T串相同，由于节点 v_{i-1} 无法确认其上一跳节点，因此该结点 $\langle s,4\rangle$ 可能源自 $E+C$ 串。节点的攻击方式如图3所示。

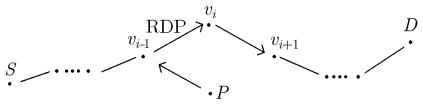

图3 ARAN协议的合谋攻击路径

通过以上分析得到了图2和图3所示的两种攻击方式，说明中间节点不满足一致性条件，即中间节点不具备可信条件，可能为攻击者节点。

5 结论

对Ad hoc网络中路由协议的安全性分析是一个复杂的问题，为了能够使用串空间理论分析ARAN协议，文中对串空间理论中“正确性”概念进行了修改，对攻击者迹的原子行为进行了合并，并提出了基于串空间理论分析Ad hoc网络安全路由协议的形式化分析方法。文中通过该方法分析了ARAN协议中所有节点的合法性，即ARAN协议的正确性，结果发现协议中存在如图2和图3所示的两种攻击，其中图3所示的攻击与文献[7]发现的攻击相同，由此也说明了文中所提出的分析方法的有效性。因此，可以得出本文中提出的基于串空间理论的形式化分析方法，适用于分析Ad hoc网络中此类路由协议的安全性。

参 考 文 献

[1] Sanzgiri K, Dahill B, and LaFlamme D. Routing for Ad hoc Networks[J]. *IEEE Journal on Selected Areas in Communications* (*Special issue on Wireless Ad hoc Networks*), 2005 23(3): 598–610.

[2] Sanzgiri K, Dahill B, and Levine B. A secure routing protocol for Ad hoc networks[C]. Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP). Paris: IEEE Press, 2002: 78–87.

[3] Thayer F J, Herzog J C, and Guttman J D. Strand spaces: Why is a Security Protocol Correct[C]. Proceedings of the 1998 IEEE Symposium on Security and Privacy. Los Alamitos: IEEE Computer Society, 1998: 160–171.

[4] Thayer F J, Herzog J C, and Guttman J D. Strand Spaces: proving security protocols correct[J]. *Journal of Computer Security*, 1999, 7(2,3): 191–230.

[5] Thayer F J, Herzog J C, and Guttman J D. Strand spaces: honest ideals on strand spaces[C]. Proceedings of the 1998 IEEE Computer Security Foundations Workshop. Los Alamitos: IEEE Computer Society, 1998: 66–77.

[6] Acs G, Buttyan L, and Vajda I. Provable security of on-demand distance vector routing in Ad hoc networks[C]. Proc of ESA2005. Berlin：Springer，2005, LCNS 3813: 113–127.

[7] 毛立强, 马建峰. 可证明安全的 MANET 按需距离矢量路由协议分析[J]. 西安电子科技大学学报(自然科学版), 2008, 35(6): 1063–1068.
Mao Li-qiang and Ma Jian-feng. Analysis of provably secure on-demand distance vector routing in MANET[J]. *Journal of Xidian University*, 2008, 35(6): 1063–1068.

闫丽丽： 女，1980 年生，讲师，博士生，研究方向为信息安全.
彭代渊： 男，1955 年生，教授，博士生导师，研究方向为密码学、网络信息安全.