Ad hoc网络中认证路由协议的改进及其安全性分析

闫丽丽[1,2]，彭代渊[1]，高悦翔[1,3]

(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;
3. 四川师范大学计算机科学学院 成都 610068)

【摘要】提出了Ad hoc网络中的ARAN协议存在合谋和重放两种攻击。为了克服ARAN协议中的上述缺陷，给出了一个改进协议eARAN。改进协议在原有协议的基础上，在路由请求数据包中添加了发送该数据包的所有中间节点的身份，即路由路径，而目的节点要对最终得到的完整的路由路径进行签名，并将其作为路由响应数据包的一部分发回给发起节点，以此保证路由路径的正确性和完整性。最后，使用扩展后的串空间理论分析了改进协议eARAN的安全性，分析结果显示，eARAN协议是安全的。

关 键 词 Ad hoc网络; 形式化分析; 路由协议; 串空间
中图分类号 TP393 **文献标识码** A doi:10.3969/j.issn.1001-0548.2011.03.021

Security Analysis of Extensible Authenticated Routing for Ad hoc Networks

YAN Li-li[1,2], PENG Dai-yuan[1], and GAO Yue-xiang[1,3]

(1. Information Security and National Computing Grid Laboratory, Southwest Jiaotong University Chengdu 610031;
2. The Department of Network Engineering, Chengdu University of Information Technology Chengdu 610225;
3. College of Computer Science, Sichuan Normal University Chengdu 610068)

Abstract First, conspiracy and replay attacks of authenticated routing for Ad hoc networks (ARAN) have been found in the paper. In order to overcome the above defects of ARAN, an improved protocol is proposed, by appending the identity of the intermediate nodes which broadcast the route discovery packet，that is, routing path. The routing path is signed with the destination node's private key and appended to reply packet. Then, the destination node unicasts reply packet back along the reverse path to the source. The correctness and integrity of the routing path are therefore guaranteed. Finally, the security of eARAN is analyzed by the extended strand spaces, and the analysis proves the correctness of the protocol.

Key words Ad hoc networks; formal analysis; routing protocols; strand spaces

Ad hoc网络是一种没有有线基础设施支持的移动网络，网络中所有节点的地位平等，节点不仅具有普通移动终端所需的功能，还具有报文转发功能。由于Ad hoc网络的自身特点，无论在军用、民用，还是商业领域都具有广泛的应用前景，因此与之相关的安全问题也已成为当前Ad hoc网络研究的一个重要方向。

路由协议的安全分析和设计是Ad hoc网络安全所关注的核心问题之一，研究人员先后提出多种安全路由协议，如ARAN[1-2]、Ariadne[3]和SRP[4]等，但这些所谓的安全路由协议先后被发现存在多种安全漏洞。其中，Ariadne是2002年提出的一种安全路由协议，但是在随后的几年间，文献[5-7]先后发现了Ariadne协议中存在的攻击，并对该协议进行了改进；文献[5]中也公布了针对SRP的攻击。ARAN是一个安全路由协议，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。

本文针对ARAN路由协议中存在的合谋和重放两种攻击，提出了一个改进的路由协议eARAN，并使用扩展后的串空间理论形式化地分析了改进协议的安全性，证明过程未发现eARAN路由协议存在安全漏洞。

收稿日期：2010－03－10; 修回日期：2011－02－18
基金项目：四川省教育厅青年基金(08zb025)
作者简介：闫丽丽(1980－)，女，博士生，主要从事信息安全、密码协议分析方面的研究.

1 ARAN

ARAN[1]的原型为：

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

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

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

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

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

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包来源于哪一个发起节点，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的过程相同。当B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，B建立一个新的路由表项，记录目的节点为X，下一跳节点为C。然后B对该数据包签名并添加自己的证书，将其发送给路由表项中记录的下一跳节点。

2 ARAN协议存在的攻击

对ARAN协议进行分析，发现存在以下两种攻击[8-9]，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。

1) 中间节点v_i收到路由响应数据包$\{\{\text{REP, IP}_S, N_S\}K_D^{-1}\}K_{v_{i+1}}^{-1}, \text{cert}_D, \text{cert}_{v_{i+1}}$后，发起重放攻击，将收到的REP包直接转发给路由表项中记录的目的节点为S的下一跳节点v_{i-1}，由于节点v_{i-1}的路由表项中没有记录应从哪个节点接收数据包，所以节点v_{i-1}无法验证该数据包是否由真正的上一跳节点发出，重放攻击成功。

攻击路径如图1所示，中间节点v_i在收到REP包后直接转发给下一跳节点v_{i-1}，这样也能正常完成一轮协议的运行，但由此会产生错误的路由路径，造成发现路由失败。

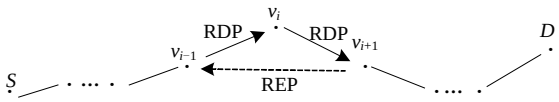

图1 ARAN协议的重放攻击路径

2) 中间节点v_i收到路由响应数据包$\{\{\text{REP, IP}_S, N_S\}K_D^{-1}\}K_{v_{i+1}}^{-1}, \text{cert}_D, \text{cert}_{v_{i+1}}$后，联合节点$P$发起合谋攻击，$v_i$将收到的REP包用$P$的私钥重新签名，并添加上$P$的证书后发给下一跳节点$v_{i-1}$，由于节点$v_{i-1}$的路由表项中没有记录应从哪个节点接收数据包，节点$v_{i-1}$无法验证该数据包是否由真正的上一跳节点发出，所以无法发现该合谋攻击。

攻击路径如图2所示，中间节点发起合谋攻击也能成功完成数据的转发，不影响本轮协议的运行，但由此产生的路由路径是错误的，会造成发现路由失败。

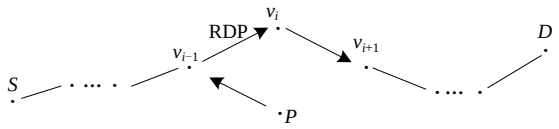

图2 ARAN协议的合谋攻击路径

3 ARAN协议的改进和分析

针对ARAN协议存在的攻击，本文给出了一个改进后的安全路由协议eARAN，其原型为：

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

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

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

$$X \to \text{C: } \{\text{REP, IP}_A, N_A, (B,C)\}K_X^{-1}, \text{cert}_X$$

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

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

eARAN协议在发送RDP数据包的过程中，RDP包经过的所有中间节点，都要添加自己的身份标识到RDP包中，当RDP数据包到达目标节点X后，X将收到的中间节点的身份序列记录到REP包中，并使用X的私钥签名。由此，REP数据包返回的路径必须符合X记录的节点顺序，收到REP包的中间节点都要对此进行检查，如果发现不符合，马上丢弃REP包，

这就保证了发现路由路径的正确性和完整性。

3.1 eARAN协议的安全性分析

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，但中间节点可能有多个，而且有可能是恶意节点。

另外，在eARAN协议的路由发现过程中，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eARAN路由协议分析时，使用串空间的弱一致性概念，并添加了中间节点可信条件，使其能够用于分析Ad hoc网络中路由协议的安全性。

eARAN协议中发起节点和目的节点满足串空间中的一致性条件，即发起节点和目的节点具有相互的认证性，因此本文只分析中间节点的一致性。

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。

3.2 eARAN串空间

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，…，v_n表示主体的标识符。

2) 映射$K: T_{\text{name}} \to \kappa$，该映射将主体与其公开密钥绑定。将$K(S)$写成$K_S$，并假设该映射是单射的，即若$K(S)=K(D)$，则有$S$=$D$。

根据串空间理论，首先对eARAN协议进行形式化处理，如图3所示。

定义 1　设（Σ，ρ）是一个被渗透的串空间，如果Σ由发起节点串、中间节点串、目的节点串和攻击节点串4种串组成，其中间节点串可以表示成下面3种形式。

1) 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}, $v_1, v_2, \cdots, v_n$]，其迹为：

$$\langle -\{\text{RDP}, \text{IP}_D, N_S\}K_S^{-1}, \text{cert}_S, +$$
$$\{\{\text{RDP}, \text{IP}_D, N_S\}K_S^{-1}\}K_{v_1}^{-1}, \text{cert}_S, \text{cert}_{v_1}, v_1, -$$
$$\{\{\text{REP}, \text{IP}_S, N_S, (v_1, v_2, \cdots, v_n)\}K_D^{-1}\}K_{v_2}^{-1}, \text{cert}_D, \text{cert}_{v_2}, +$$
$$\{\{\text{REP}, \text{IP}_S, N_S, (v_1, v_2 \cdots v_n)\}K_D^{-1}\}K_{v_1}^{-1}, \text{cert}_D, \text{cert}_{v_1} \rangle$$

2) 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}, $\text{cert}_{v_{i+1}}$, $v_1, v_2, \cdots, v_n$]，其迹为：

$$\langle -\{\{\text{RDP}, \text{IP}_D, N_S\}K_S^{-1}\}K_{v_{i-1}}^{-1}, \text{cert}_S, \text{cert}_{v_{i-1}}, v_1, v_2, \cdots, v_{i-1} +$$
$$\{\{\text{RDP}, \text{IP}_D, N_S\}K_S^{-1}\}K_{v_i}^{-1}, \text{cert}_S, \text{cert}_{v_i}, v_1, v_2, \cdots, v_i, -$$
$$\{\{\text{REP}, \text{IP}_S, N_S, (v_1, v_2, \cdots, v_n)\}K_D^{-1}\}K_{v_{i+1}}^{-1}, \text{cert}_D, \text{cert}_{v_{i+1}}, +$$
$$\{\{\text{REP}, \text{IP}_S, N_S, (v_1, v_2, \cdots, v_n)\}K_D^{-1}\}K_{v_i}^{-1}, \text{cert}_D, \text{cert}_{v_i} \rangle$$

3) 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}, $v_1, v_2, \cdots, v_n$]，其迹为：

$$\langle -\{\{\text{RDP}, \text{IP}_D, N_S\}K_S^{-1}\}K_{v_{n-1}}^{-1}, \text{cert}_S, \text{cert}_{v_{n-1}}, v_1, v_2, \cdots,$$
$$+\{\{\text{RDP}, \text{IP}_D, N_S\}K_S^{-1}\}K_{v_n}^{-1}, \text{cert}_S, \text{cert}_{v_n}, v_1, v_2, \cdots,$$
$$v_{n-1} v_n, -\{\text{REP}, \text{IP}_S, N_S, (v_1, v_2 \cdots v_n)\}K_D^{-1}, \text{cert}_D, +$$
$$\{\{\text{REP}, \text{IP}_S, N_S, (v_1, v_2 \cdots v_n)\}K_D^{-1}\}K_{v_n}^{-1}, \text{cert}_D, \text{cert}_{v_n} \rangle$$

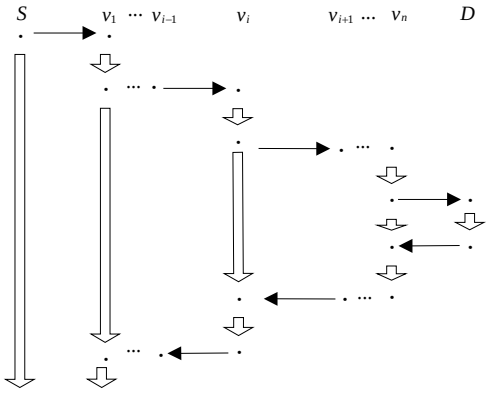

图3　协议的形式化表示

3.3 中间节点一致性证明

首先扩展原有串空间定义的攻击者迹[10]，其定义如下。

定义 2　攻击者迹包含以下内容：M为正文信息$\langle +t \rangle$，其中$t \in T$；F为接收消息$\langle -g \rangle$；T为接收并多次发送消息$\langle -g, +g, +g \rangle$；$C$为连接接收的消息$\langle -g, -h, +gh \rangle$；$S$为分解接收的消息$\langle -gh, +g, +h \rangle$；$K$为发送密钥$\langle +K \rangle$，$K \in K_p$；$E$ / Si为加密消息/签名

$\langle -K,-h,+\{h\}_K\rangle$；De/$V$ 为解密消息/签名认证 $\langle -K^{-1},-\{h\}_K,+h\rangle$。

下面以中间节点2串为例分析eARAN协议的安全性，其他两种中间节点串的安全性证明类似。首先分析中间节点 $s\in$ Intermediate2[ ] 中的 $\langle s,2\rangle$:+{{RDP, IP$_D$, N_S}K_S^{-1}}$K_{v_i}^{-1}$，cert$_S$，cert$_{v_i}$，v_1，v_2，…，v_i 是否有可能源自攻击节点串，依据串空间中对攻击者迹的定义对 $\langle s,2\rangle$ 具体分析如下。

M：由于 $K_S^{-1}\notin K_p$，因此结点 $\langle s,2\rangle$ 不可能源于M串。

F：由于节点 $\langle s,2\rangle$ 符号为正，不可能源于F串。

T：当中间节点v_{i+1}收到 $\langle s,2\rangle$ 后，首先根据cert中的公钥判断签名是否正确，再检查RDP数据包中记录的节点序列中的最后一个节点是不是签名的节点，如果以上都没有问题，v_{i+1}认为该RDP包来源于合法节点。由于RDP包中的节点身份标识是以明文方式发送，所以v_i可以将从节点v_{i-1}收到的RDP包直接转发给v_{i+1}，从而实现重放攻击，这样 $\langle s,2\rangle$ 可能源于T串。但是根据eARAN路由发现协议的特性，如果发生该类攻击，由此生成的路由节点的序列就会变成〈 $v_1,v_2,\cdots,v_{i-1},v_{i+1},\cdots,v_n$ 〉。而这样一条路由路径不存在，即当REP包按照该路径返回时，无法正常到达起始节点S，该路由发现失败。除此之外，在eARAN路由协议中，节点在发送RDP包时采用的是广播方式，$\langle s,2\rangle$ 如果源于T串，说明v_i广播发送了{{RDP, IP$_D$, N_S}K_S^{-1}}$K_{v_{i-1}}^{-1}$，cert$_S$，cert$_{v_{i-1}}$，v_1，v_2，…，v_{i-1}，而该数据包可以被其一跳范围内的v_{i-1}接收到，由此v_{i-1}是可以发现该重放攻击的。综上所述，节点 $\langle s,2\rangle$ 不可能源于T串。

S：节点 $\langle s,2\rangle$ 不可能源于S串。

K：节点 $\langle s,2\rangle$ 不可能源于K串。

D / V：节点 $\langle s,2\rangle$ 不可能源于D / V串。

Si+C：当节点v_i收到{{RDP, IP$_D$, N_S}K_S^{-1}}$K_{v_{i-1}}^{-1}$，cert$_S$，cert$_{v_{i-1}}$，v_1，v_2，…，v_{i-1}后，首先根据 cert$_{v_{i-1}}$ 中存储的v_{i-1}的公钥解密该数据项，得到h={{RDP, IP$_D$, N_S}K_S^{-1}, cert$_S$, v_1, v_2, …, v_{i-1}，接下来节点v_i可以根据合谋者的密钥 $k=K_\rho^{-1}$ 及其证书 $g=$cert$_\rho$ 得到 $\{h\}_k\,g=\{\{\text{RDP, IP}_D,N_S\}\,K_S^{-1}\}\,K_\rho^{-1}$，cert$_S$，cert$_\rho$，$v_1$，$v_2$，…，$v_{i-1}$，$\rho$，随后$v_i$将生成的该RDP包广播出去，而节点$v_{i+1}$收到该RDP包后，认为该RDP包是合法的，因此该节点 $\langle s,2\rangle$ 可能源自Si+C串。但是从eARAN协议运行的整个过程可以发现，由于eARAN协议中RDP包经过的每个节点都要记录当前的节点序列，假设 $\langle s,2\rangle$ 源自Si+C串，那么节点v_{i+1}记录的节点序列为v_1，v_2，…，v_{i-1}，ρ。当REP返回时，所有收到REP包的中间节点都要检查由目的节点签名的节点序列与自身记录的是否一致，不一致该REP包将被丢弃。如果 $\langle s,2\rangle$ 源自Si+C串，当v_{i+1}收到REP包后，它必然会将REP包回送给节点 ρ，但是由于节点 ρ 不存在于路由路径上，该REP包无法正常到达起始节点S，也就是路由发现失败，因此节点 $\langle s,2\rangle$ 不可能源自Si+C串。

通过以上分析，可以发现节点 $\langle s,2\rangle$ 不源于攻击者串，这就说明目的节点收到的节点序列 ($v_1,v_2,\cdots,v_n$) 是正确的。而目的节点收到RDP包后，要对收到的节点序列签名，并将其作为REP包的一部分返回给起始节点，由于 $K_D^{-1}\notin K_p$，所以攻击者节点无法更改节点序列，该REP包必然会按照节点序列记录的节点顺序正确地返回给起始节点，REP包传送的过程中不可能存在攻击，由此说明了节点 $\langle s,4\rangle$ 不源于攻击者节点。综上所述，eARAN协议中的中间节点不源于攻击者串，该协议既满足起始节点、目的节点的一致性条件，又满足中间节点的一致性条件，证明该协议是安全的。

4 结 论

本文指出ARAN协议中存在合谋和重放两种安全攻击，并针对这两种攻击，提出了一种新的改进路由协议eARAN。使用扩展后的串空间理论，形式化地分析了eARAN协议的安全性。由于eARAN协议的攻击主要存在于发现路由过程中的中间节点，而起始节点和目的节点是安全的，所以本文主要对协议的中间节点的一致性进行了证明。分析结果未发现eARAN协议存在安全漏洞。

由于Ad hoc网络的特性，目前很少有安全路由协议可以抵御虫洞[11](wormhole attacks)攻击。如果要抵御虫洞攻击，可以通过添加定位服务器[12]来实现，即每个网络节点必须通过定位服务器更新其邻居节点的位置信息，但如此必然要增加网络的负担。本文在对ARAN协议进行安全性分析时并未考虑该类攻击。

参 考 文 献

[1] SANZGIRI K, DAHILL B, 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, 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] HU Y C, PERRIG A, JOHNSON D. Ariadne: a secure on-demand routing protocol for Ad hoc networks[C]// Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002). Atlanta, GA: ACM, 2002: 12-23.

[4] PAPADIMITRATOS P, HAAS Z. Secure routing for mobile Ad hoc networks[C]//SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS). San Antonio, TX, USA: [s.n.], 2002.

[5] BUTTYAN L, VAJDA I. Towards provable security for Ad hoc routing protocols[C]//Proceedings of 2nd ACM Workshop on Security in Ad hoc and Sensor Networks (SASN 2004). Washington DC, USA: ACM, 2004.

[6] ACS G, BUTTYAN L, VAJDA I. Provably secure on-demand source routing in mobile Ad hoc networks[J]. IEEE Transactions on Mobile Computing, 2006, 5(11): 1533-1546.

[7] LIU Jing, FU Fei, XIAO Jun-mo, et al. Secure routing for mobile Ad hoc networks[C]//Proceedings of Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, and Parallel/Distributed Computing (SNPD 2007). Qingdao: IEEE Computer Society, 2007.

[8] 闫丽丽, 彭代渊. Ad hoc网络中ARAN路由协议的安全性分析[J]. 电子与信息学报, 2010, 32(9): 2241-2244.
YAN Li-li, PENG Dai-yuan. Security analysis of ARAN routing protocol for Ad hoc networks[J]. Journal of Electronics & Information Technology, 2010, 32 (9): 2241-2244.

[9] 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, 2008, 35(6): 1063-1068.
MAO Li-qiang, MA Jian-feng. Analysis of provably secure on-demand distance vector routing in MANET[J]. Journal of Xidian University, 2008, 35(6): 1063-1068.

[10] THAYER F J, HERZOG J C, 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.

[11] HU Y C, PERRIG A, JOHNSON D B. Packet leashes: a defense against wormhole attacks in wireless networks[C] //Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003). San Francisco, CA: IEEE, 2003: 1976-1986.

[12] NICULESCU D, NATH B. Ad hoc positioning system(APS) [C]//Global Telecommunications Conference. San Antonio, TX , USA: IEEE, 2001: 2926-2931.

编 辑 漆 蓉