MANET虚假路由形式化验证

张毓森[1] 桂荆京[1] 王金双[1] 锁 琰[1] 杨 莉[1] 金 鑫[2]
(解放军理工大学指挥自动化学院 南京 210007)[1] (总参谋部某研究所 北京 100141)[2]

摘 要 提出了Ad-hoc网络虚假路由攻击的形式化验证和分析方法,主要是在参数化Ad-hoc路由协议串空间模型的基础上采用改进的Athena状态表示法来描述问题域,并采用相应的证明搜索过程来完成目标验证。最后设计实现了虚假路由自动验证系统FRpoofor,用它验证和分析了Ariadne安全路由协议运行环境下某些虚假路由的建立过程,以此说明方法的有效性。

关键词 Ad-hoc路由攻击,形式化分析,串空间,证明搜索
中图法分类号 TN918 **文献标识码** A

Formal Verification Approach for False Route in MANET

ZHANG Yu-sen[1] GUI Jing-jing[1] WANG Jin-shuang[1] SUO Yan[1] YANG Li[1] JIN Xin[2]
(Institute of Command Automation, PLA University of Science and Technology, Nanjing 210007, China)[1]
(Research Institute of General Staff Headquarter, Beijing 100141, China)[2]

Abstract It is a general threaten for MANET routing protocol to create the false routes, so analysis of this threaten is an important goal of routing security research. We proposed an approach to formal verification for the false route in MANET. It allows us to represent the basic objective to be proven with the state representation based on our parameterized strand space model of the Ad-hoc routing protocol, and to apply the adapted proof search procedure to automatically verify the basic objective. At last we completed the automatic verification program, called FRpoofor. As a example, we executed FRpoofor to verify and analyze some false route in secure routing protocol Ariadne.

Keywords Ad-hoc routing attack, Formal analysis, Strand space, Proof search

1 引言

移动Ad-hoc网络(MANET)的路由功能需要依赖多个网络节点的相互协作、自组织地实现。然而不可信的网络环境将给Ad-hoc路由协议的有效运行带来诸多威胁,其中产生虚假路由便是一种十分严重的路由威胁。恶意节点可以篡改路由控制信息而伪造不真实的路由,例如"黑洞"攻击[1],也可以通过"虫洞"[2]产生非连通的多跳路由等,最终导致网络层数据交付率大大降低。因此,对虚假路由攻击的分析和防御是Ad-hoc路由协议安全性研究的重要目标。

当前大部分Ad-hoc路由攻击分析研究[3-5]都通过路由协议仿真来评估各种路由攻击的危害,对路由攻击的分析都是通过非形式化的说明。近几年也出现一些Ad-hoc路由安全形式化分析方法[6,7],它们虽然能对路由安全属性提供严格的数学证明,但对具体攻击过程的分析还是需要人工参与。另外,我们在前期工作[8]中提出了一种MANET路由协议安全性分析方法,考虑运用图论原理来计算网络中的虚假路由,并根据串空间理论[9]的相关定理进行安全性证明,然而在较大规模的网络环境下进行手动推理证明将会十分困难。由此本文提出了一种机器自动验证方法来高效地完成虚假路由生成过程合理性证明,并直观地模拟攻击形成过程。最后设计实现了自动验证系统FRpoofor,并应用该系统在Ariadne安全路由协议[12]运行环境下进行了虚假路由攻击验证和模拟。

2 协议串空间模型参数化扩展

虚假路由形式化验证将以Ad-hoc路由协议串空间模型为基础。在协议模型中,对于协议消息的多样化选择就表现为参数变量的各种赋值变换,因此对MANET路由协议的形式化描述需要扩展为参数化串空间模型。

2.1 协议串空间

串空间是一种有效的安全协议形式化分析模型,其基本表示法可以参考文献[9]。Ad-hoc路由协议可抽象的主体有源节点、目的节点、路由节点、网络节点和攻击者。则对于某一个路由发现过程,"源节点串"描述路由请求时源节点主体需要执行的协议行为序列,"目的节点串"描述路由回复时的协议行为序列;同理,可为路径上每一个合法中间节点主体构建"路由节点串",为每一个非路径上合法网络节点主体构建"网络节点串";同时,以网络中恶意节点为主体的"攻击者串"包含M,T,C,S,K,E,D-7类迹(详见文献[9]中定义1),用于描述攻击者所有可能的攻击行为。

到稿日期:2011-03-01 返修日期:2011-07-12
张毓森(1949—),男,教授,博士生导师,主要研究领域为网络信息安全;桂荆京(1981—),男,博士生,主要研究领域为Ad-hoc网络安全、安全协议形式化分析,E-mail:gjj2005whty@163.com(通信作者);王金双(1978—),男,博士,讲师,主要研究领域为机器辅助定理证明。

例如，Ariadne 的安全路由协议[12]串空间模型可以如下方式构建(协议选择采用数字签名认证方案)。

定义 1 产生虚假路径 $S-l_1\cdots l_i-D$ 所对应的 Ariadne 协议串空间由下列 5 类串组成。

(1) 源节点串，其主体标识为 S，且具有迹：

$\langle +\{RREQ, S, D, id, \mathrm{sig}_S\}, (\{RREP, S, D, (l_1\cdots l_i), \mathrm{sig}_D\}\rangle$

(2) 目的节点串，其主体标识为 D，且具有迹：

$\langle -\{RREQ,S,D,id,H(l_1\cdots l_i),(l_1\cdots l_i),SIG(l_1\cdots l_i)\}, +\{RREP,S,D,(l_1\cdots l_i),\mathrm{sig}_D\}\rangle$

(3) 路由节点串，相应主体为 $l_j\in\{l_1\cdots l_i\}$，且 l_j 为正常节点，则具有迹：

$\langle -\{RREQ,S,D,id,H(l_1\cdots l_{j-1}),(l_1\cdots l_{j-1}),SIG(l_1\cdots l_{j-1})\}, +\{RREQ,S,D,id,H(l_1\cdots l_j),(l_1\cdots l_j),SIG(l_1\cdots l_j)\}, -\{RREP,S,D,(l_1\cdots l_i),\mathrm{sig}_D\}, +\{RREP,S,D,(l_1\cdots l_i),\mathrm{sig}_D\}\rangle$

(4) 网络节点串，相应主体为 $l_x\notin\{l_1\cdots l_i\}$，且 l_x 为网络中正常节点，则具有迹：

$\langle -\{RREQ,S,D,id,H(list_1),(list_1),SIG(list_1)\}, +\{RREQ,S,D,id,H(list_1,l_x),(list_1,l_x),SIG(list_1,l_x), -\{RREP,S,D,(list_1,l_x,list_2),sig_D\}, +\{RREP,S,D,(list_1,l_x,list_2),sig_D\}\rangle$

(5) 攻击者串，主体包括所有攻击节点，且具有 7 类攻击者迹：

- $M.\langle +a\rangle$(a 表示原子消息项)；
- $T.\langle -t,+t\rangle$；(t 表示任意消息项)
- $C.\langle -t_1,-t_2,+(t_1t_2)\rangle$($t_1,t_2$ 为不同的两个消息项)；
- $S.\langle -(t_1t_2),+t_1,+t_2\rangle$；
- $K.\langle +k\rangle$(k 为攻击者所获得的密钥)；
- $E.\langle -k,-t,+\{t\}_k\rangle$；
- $D.\langle -k^{-1},-\{t\}_k,+t\rangle$。

以上协议模型包含的消息项符号有：

- RREQ,RREP 分别代表路由请求消息和路由回复消息类型；
- id 为由协议主体产生的唯一标识符；
- sig_{l_i} 为主体 l_i 对要发送的消息项的数字签名；
- $list$ 表示任意的路由列表，$list_1$ 与 $list_2$ 中不包含相同的主体节点；
- $H(list)$表示路由表 $list$ 认证所采用的散列链；
- $SIG(list)$表示与路由表 $list$ 相对应的数字签名序列。

对于 Ad-hoc 路由协议串空间，其串节点的因果连接关系还将包含网络节点的连通性。因此，其因果连接关系“$n1\xrightarrow{a}n2$”不仅说明 $\mathrm{term}(n_1)=+a$，$\mathrm{term}(n_2)=-a$(a 表示任意消息项)，而且表示 n_1 的主体与 n_2 的主体是网络拓扑中的相邻节点。

Ad-hoc 路由协议串空间模型还定义了“被渗透丛”来描述一次成功的虚假路由发现过程。

定义 2 一个被渗透丛 A 是协议串空间 Σ 中边的集合 $E_A\subseteq(\rightarrow\cup\Rightarrow)$，如果 $P\in\Sigma$ 为各种迹的入侵节点串的集合，$s\in\Sigma$为源节点串，N_A 是与 E_A 中各边相对应的节点集合，并且满足：

1)A 是非空、有限、无环图；

2)$A\cap P\neq\emptyset$ 且 $s\in A$；

3)如果 $n_1\in N_A$，且 $term(n_1)$为负，那么存在一个唯一的节点 n_2 使得 $n_1\rightarrow n_2\in A$；

4)如果 $n_1\in N_A$，且 $n_2\Rightarrow n_1$，那么 $n_1\Rightarrow n_2\in A$。

“被渗透丛”包括两个主要特征：1)它必须是个丛结构(文献[9]中定义 2.3)，在串空间模型中用“丛”结构来描述一次合理的协议过程；2)它必须包含源节点串，因为只要协议发起者完成了正确的消息项的发送和接收，就认为相应的路由已建立。因此，如果能在协议串空间中发现一个“被渗透丛”，就说明该虚假路由攻击存在。

2.2 参数化串及相关运算

在串空间中采用参数化变量表示消息项，可以描述广义的协议行为，也为在串空间模型中实现机器验证提供了基础。在虚假路由发现过程中，攻击节点的攻击行为是可以自由选择的，因此攻击者串的 M,F,T,C,S,K,E,D-8 类迹的所有项均可用参数化变量表示；另外，网络节点的部分协议消息项由于会受到攻击者的哄骗，也具有不确定性，故将 Ad-hoc 路由协议串空间中的网络节点串也扩展为参数化串，例如 Ariadne 协议串空间(定义 1)中的网络节点串中的 $list$ 可以看作路径变量。

消息项变量的替换和合一已在文献[10]中定义。对参数化串的相关运算可定义为：

定义 3 用替换 $\sigma=[x/t]$表示变量 x 向消息项 t 的映射，则对参数化串 s 应用替换 $\sigma=[x/t]$就是将串 s 中所有消息项包含的所有变量 x 均替换成项 t。

定义 4 串 s_1 和 s_2 的合一就是存在一个替换 σ，使得 $\sigma(s_1)\subseteq\sigma(s_2)$或者 $\sigma(s_2)\subseteq\sigma(s_1)$。

在 Ariadne 的串空间中，形如 $\mathrm{sig}_{()}$ 和 $H()$的协议消息项需要进行项变换，以适应加密项变量 $\{h\}_K$ 向协议消息项 $\mathrm{sig}_{(*)}$ 和 $H(*)$的替换运算。例如，根据加密原理，sig_{l_i} 就是用主体 l_i 的私钥 $K_{l_i}^{-1}$ 对发送的消息项 t 加密，需要变换为 $\{t\}_{K_{l_i}^{-1}}$，则存在$\{h\}_K$与(sig_{l_i})的合一替换$[(h/t),(K/K_{l_i}^{-1})]$；同理，$H(l_1\cdots l_i)=\mathrm{HASH}[l_i,\mathrm{HASH}[l_{i-1},\mathrm{HASH}[\cdots,\mathrm{HASH}[l_1,\mathrm{sig}_S]\cdots]]]$，其中单向散列算法 HASH 可变换为$\{\ \}_{KE}$($K_E$ 表示空密钥，且 K_E^{-1} 不存在)，则存在$\{h\}_K$与 $\mathrm{HASH}[l_1,\mathrm{sig}_S]$的合一替换$[(h/\langle l_1,\mathrm{sig}_S\rangle),(K/K_E)]$。

3 虚假路由验证分析

对 MANET 虚假路由攻击的形式化验证主要采用一种基于改进的 Athena 状态表示法[10]的证明搜索系统。Athena 方法成功地结合了定理证明和模型检测技术，可以对密码协议的某些安全属性进行自动验证，其核心部分是利用一定的推理规则对特定的状态表达式进行证明搜索。

3.1 目标状态表达式

Athena 状态表示法将搜索状态定义为一个三元组$\langle S,G,B\rangle$，其中 S 是串空间中的一个“半丛”，G 是 S 中未被绑定的目标集合，B 是绑定关系集合。然而，在密码协议串空间模型中，目标绑定关系只考虑消息项关系，不会涉及协议主体的连通性。而在 Ad-hoc 路由协议串空间模型中，主体的连通性将影响串节点间的因果连接关系，则状态中的目标及其绑定关系将被重新定义为：

定义 5 目标 g 就是协议串空间中的一个节点 n，且 $\mathrm{sign}(n)=-$。

定义 6 如果目标 g 对应的串节点与串节点 n 存在因果

连接关系，则称目标 g 绑定到节点 n，并表示为“$g \leftarrow n$”。

在改进的状态表示法中的相关状态表达式的定义仍然成立，如对于串 s 和状态 l，$s \in l$ 表示串 s 中节点和节点关系全部包含于状态 l 的半丛 S 中；如果状态 l 的丛集合[10]为 $\psi(l)$，C 为串空间中的一个丛，则 $C \in \psi(l)$ 表示状态 l 的半丛 S 是 C 的子图。

定义状态表达式 $\psi(l)=\emptyset$ 为证明目标的基本状态表达式(简称“目标式”)。根据 Athena 逻辑[10]，在协议串空间模型 Σ_p 中 $\psi(l)=\emptyset$ 的语义为：

$$[\Sigma_p \mid \psi(l)=\phi] \equiv \forall C \in D_p, C \notin \psi(l)$$

式中，D_p 是 Σ_p 中所有丛的集合。

定义 7 初始状态 $l_0=\langle S_0, G_0, \emptyset \rangle$，其中 S_0 为包含源节点串的最小半丛，G_0 为源节点串中所有负节点的集合。

产生虚假路由反映在协议串空间中的特征属性为串空间模型中至少存在一个“被渗透丛”。根据被渗透丛的定义 2，可知状态 l_0 描述的是被渗透丛的必要特征，则集合 $\psi(l_0)$ 必然包含所有的被渗透丛。由此可得，在协议串空间模型 Σ_p 中“$\psi(l_0)=\emptyset$”表示不存在一个“被渗透丛”，即需要证明的主要目标状态表达式。

3.2 推理规则

当证明搜索过程需要继续时，将应用一定的推理规则把当前目标式转换为多个子目标。这里只需要一个推理规则，表示为：

$$\frac{\psi(l_1)=\phi, \cdots, \psi(l_n)=\phi, \text{其中} \{l_1, \cdots, l_n\}=F(l)}{\psi(l)=\phi} \quad (1)$$

式中，$\psi(l)=\emptyset$ 是当前的目标式，在应用规则后将分离成 n 个子目标式，即 $\psi(l_1)=\emptyset, \cdots, \psi(l_n)=\emptyset$，由核心函数 F 完成状态的转换功能。函数 F 是对 Athena 系统的 split 规则中后续状态函数[7]的改进。假设协议串空间为 Σ_p，对于输入状态 $l=\langle S, G, B \rangle$，则 $F(l)$ 的算法步骤是：

(1) 首先，从状态 l 的目标集 G 中任意选择一个目标 g^*，并在 Σ_p 中查找关于目标 g^* 的绑定者集合 $U(g^*)=\{(\sigma, n) \mid \sigma(g^*) \leftarrow \sigma(n)$，其中 $n \in \Sigma_p$，σ 是 $term(g^*)$ 和 $term(n)$ 的最普遍合一替换$\}$，如果 $U(g^*)$ 为空，则 $F(l)=\emptyset$，否则进入第二步。

(2) 对于 $U(g^*)$ 中的每个元素 $u=(\sigma, n)$，计算后续状态集合 L_u：首先，构建串 s_u，s_u 以节点 $\sigma(n)$ 为结束节点，并且为因果前驱关系(表示为“$\Rightarrow$”)上的回溯闭包，因此它包括节点 $\sigma(n)$ 和对应串上的所有前驱节点；然后，检验状态 l 的半丛 S 中是否存在一个串 s'，使得 s' 与 s_u 能够合一(定义 4)，并根据判定结果计算后续状态 $l'=\langle S', G', B' \rangle$ 后，将 l' 放入集合 L_u：

a) 如果 s' 不存在，则有：

- $S'=\sigma(S) \cup \{s_u\}$；
- $B'=B \cup (\sigma(g^*) \leftarrow \sigma(n))$；
- G' 根据 S' 和 B' 进行更新。

b) 如果 s' 存在且 s' 与 s_u 的合一替换为 σ'，则有：

- $S'=\sigma'(\sigma(S)) \cup \sigma'(s_u)$；
- $B'=B \cup \sigma'(\sigma(g^*) \leftarrow \sigma(n))$；
- G' 根据 S' 和 B' 进行更新。

(3) 根据下面条件检查每个状态 $l^* \in L_u$ 的有效性，删除 L_u 中的无效状态后，则 $F(l)=L_u$。

a) 状态 l^* 的半丛 S^* 中不存在关于关系“$\rightarrow$”和“$\Rightarrow$”的传递闭包；

b) 唯一产生(Unique origination)属性[4]必须满足，如请求 id 必须只能在源节点串中最初生成，如果 S^* 中存在其它主体的串最初生成 id，则状态 l' 将判定为无效；

c) 状态中的消息项格式满足预设限定条件。

如果 $F(l)=\emptyset$，则说明 $\psi(l)=\emptyset$ 成立。根据函数 $F(l)$ 的计算过程易得 $\bigcup_{l' \in F(l)} \psi(l')=\psi(l)$，即 $\psi(l)=\emptyset$ 成立，当且仅当 $\bigcup_{l' \in F(l)} \psi(l')=\emptyset$，因此规则(1)是合理的；同时，规则(1)还是可逆的，因为如果存在一个状态 $l' \in F(l)$，使得 $\psi(l') \neq \emptyset$，也就是串空间中存在一个丛 $C \in \psi(l')$，而 $\psi(l') \subseteq \psi(l)$，因此必然有 $C \in \psi(l)$，即 $\psi(l) \neq \emptyset$。

3.3 证明搜索过程

初始化后的验证目标集合中只有一个目标式 $O_{sa}=\{\psi(l_0)=\emptyset\}$，也是需要证明的主目标式。在证明搜索过程中，通过应用规则(1)更新目标式集合 O_{sa}，如果当前目标式 $\psi(l)=\emptyset$ 没有子目标式(即 $F(l)=\emptyset$)，则从 O_{sa} 中删除该目标，否则将 O_{sa} 中 $\psi(l)=\emptyset$ 替换为其所有子目标式。证明搜索流程图如图 1 所示。

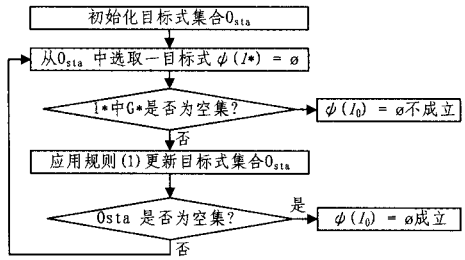


图 1 证明搜索流程图

证明搜索终止的两个条件是：1) 目标式集合 O_{sa} 中发现了一个目标式，其对应状态 l^* 的 $G^*=\emptyset$。根据文献[10]的命题 4.2，可知子目标式 $\psi(l^*)=\emptyset$ 不成立，又由于推理规则的可逆性，因此证明结论为“主目标式 $\psi(l_0)=\emptyset$ 不成立”。2) 目标式集合 O_{sa} 为空集，即所有子目标式都被证明成立，因此证明结论为“主目标式 $\psi(l_0)=\emptyset$ 成立”。为避免证明搜索过程无限制地运行，可以对消息项的最大长度和最大加密深度进行限定。

4 FRproofer 系统执行与应用

我们用 Standard ML of New Jersey 编译器[13]实现了 MANET 虚假路径自动验证系统 FRproofer。系统的输入为一个协议串空间模型和一个网络模型以及一些预定义的前提条件：

- 协议的串空间模型是一个关联表，其键值是序偶(串主体标识、串节点序号)，关联内容为带符号消息项；
- 网络模型为一个三元组 (V, V^*, NEI)，其中 V 和 V^* 表示所有网络节点集合和所有攻击节点集合，定义为字符串表结构，NEI 为所有相邻节点对集合，定义为字符串序偶的表结构；
- 预定义条件包括入侵节点的初始知识集、具有唯一产生属性的消息项和主体标识对、消息项的最大长度和最大加密深度限定值。

FRproofer 或者以证明成功而终止，即证明了主目标式 $\psi(l_0)=\emptyset$ 成立，说明虚假路由无法建立；或者以证明失败告终，即结论为主目标式 $\psi(l_0)=\emptyset$ 不成立，同时将给出一个产生虚假路由的具体示例。

下面以 Ariadne 安全路由协议在图 2(a)网络拓扑下的运行环境为例，应用 FRproofer 系统验证虚假路由 *S-A-D* 能否产生。输入的协议串空间模型以定义 1 为依据，其中攻击节点标识为 X，‖路由表 $S-l_1\cdots l_i-D$ 为 *S-A-D*，网络节点 l_x 为 B；网络模型中 $V=\{S,A,B,X,D\}$、$V^*=\{X\}$、$NEI=\{(S,A),(A,B),(B,D),(B,X),(A,B),(S,X),(D,X)\}$；设定的前提条件有：1)攻击者初始密钥集合$\{K_S,K_D,K_A,K_B,K_E,K_X,K_X^{-1}\}$($K_E$ 为空密钥，用于 HASH 散列运算)、初始原子项集{"*RREQ*","*RREP*","*S*","*D*","*A*","*B*","*X*"}；2)具有唯一产生属性的消息项和主体对为$(S,\{id\})$；3)有最大加密项长度 $Sign_{max}=4$，最大控制包长度 $Pack_{max}=6$，最大加密深度 $Encr\text{-}dep_{max}=4$。运行虚假路由验证系统，最终结果为主目标式证明失败，也就说明虚假路由 *S-A-D* 能够在 Ariadne 协议运行中产生，并且虚假路由产生过程体现为系统停止搜索的最后状态，该状态如图 3 所示。

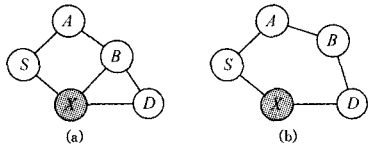
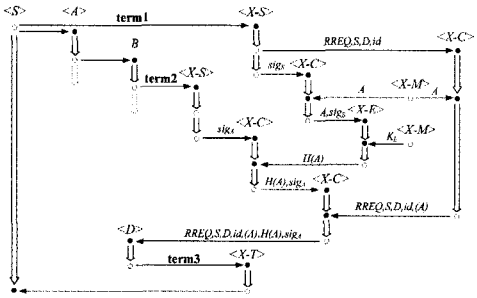


图 2　Ad-hoc 网络拓扑图(其中 X 为恶意节点)



注：〈X－x〉表示主体为 X 的攻击者串的某类迹；
·表示证明搜索过程中出现的目标节点。

图 3　虚假路由攻击过程(被渗透丛结构图)

图 3 是一个描述虚假路由攻击过程的"被渗透丛"结构，它由源节点串〈S〉、目的节点串〈D〉、路由节点串〈A〉、网络节点串〈B〉以及各种攻击者串〈$X-x$〉构成。如图 3 所示，攻击节点 X 需要从源节点 S 中接收消息项 term1＝{*RREQ*,S,D,id,sig_S}、网络节点 B 中接收 term2＝{*RREQ*,S,D,id,$H(A)$,(A),sig_A}和目的节点 D 中接收 term3＝{*RREP*,S,D,(A),sig_D}才可以完成虚假路由攻击。文献[14]也提出了相似的攻击。

同样，还验证了在图 2(b)的网络拓扑中 Ariadne 协议能否产生虚假路由 *S-A-D*。验证结论为主目标式证明成立，也就说明虚假路由 *S-A-D* 不可能在 Ariadne 协议运行中产生。这主要是由于在图 2(b)拓扑中节点 B 和节点 X 不相邻，以至于攻击节点 X 不能接收到消息项 term2，也就不可能构建项{*RREQ*,S,D,id,$H(A)$,(A),sig_A})，从而使得描述虚假路由 S-A-D 发现过程的"被渗透丛"不存在。

在 FRproofer 系统的两次运行过程中，系统终止时分别经过了 58 个状态和 37 个状态搜索，这与应用 Athena 方法验证各认证协议时的搜索状态数[10,11]相当，从而继承了 Athena 方法的优点：能够有效克服状态爆炸。虽然随着网络节点的增多，搜索状态数会增多，但通过预设更低的消息项限定值可以避免系统无穷搜索。另外，可以通过应用相应的状态搜索策略来进一步优化系统运行效率。

结束语　提出了一种 MANET 虚假路由威胁形式化分析方法，它可以看作是基于串空间的 Athena 方法在 MANET 路由协议安全性分析中的扩展。通过对 Athena 状态表示法和证明搜索过程的相应改进，可以有效地描述新的串空间特征属性"被渗透丛存在性"，并且能够实现该属性的自动验证。由此设计的自动验证系统 FRproofer 不仅能够自动完成虚假路由攻击存在性证明，还能最终模拟具体攻击过程。最后以 Ariadne 协议运行环境为例，应用该系统验证虚假路由 *S-A-D* 产生，在不同的网络拓扑环境中得到了不同结论，由此说明除了路由协议，网络拓扑也是形成路由威胁的重要因素。

文献[8]的方法框架在 FRproofer 系统的辅助下，最终能够自动完成 MANET 路由协议的安全性分析，以此可以高效地检验更多、更大规模 Ad-hoc 网络拓扑下路由协议的安全漏洞。下一步将用此方法分析更多 Ad-hoc 路由攻击，并进一步研究 Ad-hoc 路由协议更多安全属性和相应证明。

参 考 文 献

[1] Sergio M, Giuli T J, Kevin L, et al. Mitigating Routing Misbehavior in Mobile Ad-hoc Network[C]// MobiCom 2000. Boston: ACM, 2000: 255-265

[2] Hu Y C, Perrig A, Johnson D B. Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad-hoc Network Routing Protocols[C]// INFOCOM'03. San Francisco, USA, 2003

[3] Wang W C, Lu Y, Bharat B. On Security Study of Two Distance Vector Routing Protocols for Ad-hoc Networks[C]// PerCom'03. IEEE, 2003

[4] Sergio M, Giuli T J, Kevin L. On the Survivability of Routing Protocols in Ad-hoc Wireless Networks[C]// SecureComm'05. Athens, Greece, September 2005

[5] Babakhouya A. A Simulation Analysis of Routing Misbehaviour in Mobile Ad hoc Networks[C]// the 2nd International Conference on NGMAST'08. Cardiff, Wale, UK, 2008

[6] Ács G, Buttyán L, Vajda I. Modelling adversaries and security objectives for routing protocols in wirless sensor networks[C]// SASN, 2006. 2006: 49-58

[7] Nanz S, Hankin C. A Framework for Security Analysis of Mobile Wireless Networks[J]. Computer Science, 2006, 367: 203-227

[8] 桂荆京，张毓森. 基于串空间的 MANET 路由协议安全性分析的新方法[J]. 通信学报，2010，31(9A)：217-222

[9] Javier F, Herzog J C, Guttman J D. Strand Spaces: Why is a Security Protocol Correct[C]// Proc of IEEE Symposium on Security and Privacy. California: IEEE, 1998: 1-13

[10] Song D, Berezin S, Perrig A. Athena: a novel approach to efficient automatic security protocols analysis[J]. Journal of Computer Security, 2010, 9(1): 47-74

[11] 吴光伟，董荣胜. 基于串空间的 Athena 分析技术研究[J]. 计算机科学，2006，33(8)：9-13

[12] Hu Y C, Perrig A, Johnson D B. Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks[C]// MobiCom'02. Atlanta, Georgia, USA, 2002

[13] Pucella R. Notes on Programming Standard ML of New Jersey [DB/OL]. http//: www. smlnj. org/doc/literature. html

[14] Andel T R, Yasinsac A. Adaptive threat modeling for secure ad hoc routing protocols[J]. Electronic Notes in Theoretical Computer Science, 2008, 197: 3-14