软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(7):1641−1651 [doi: 10.3724/SP.J.1001.2011.03866]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于串空间的 Ad Hoc 安全路由协议攻击分析模型*

董学文[1+], 马建峰[1,2], 牛文生[3], 毛立强[1], 谢 辉[1]

[1](西安电子科技大学 计算机学院,陕西 西安 710071)

[2](西安电子科技大学 计算机网络与信息安全教育部重点实验室,陕西 西安 710071)

[3](中国航空计算技术研究所,陕西 西安 710068)

Attack Analysis Model on Ad Hoc Security Routing Protocol Based on Strand Space Model

DONG Xue-Wen[1+], MA Jian-Feng[1,2], NIU Wen-Sheng[3], MAO Li-Qiang[1], XIE Hui[1]

[1](School of Computer Science and Technology, Xidian University, Xi'an 710071, China)

[2](Key Laboratory of Computer Networks and Information Security, Ministry of Education, Xidian University, Xi'an 710071, China)

[3](China Aeronautics Computing Technique Research Institute, Xi'an 710068, China)

+ Corresponding author: E-mail: xddongxuewen@gmail.com

Dong XW, Ma JF, Niu WS, Mao LQ, Xie H. Attack analysis model on ad hoc security routing protocol based on strand space model. *Journal of Software*, 2011,22(7):1641−1651. http://www.jos.org.cn/1000-9825/3866.htm

Abstract: Based on the characteristics of ad hoc security routing protocols (SRPs), the advantages and disadvantages of the strand space theory are analyzed. An analysis model for protocol attacks, which leads to a nonexistent route that is accepted by the protocol, is designed on the basis of the strand space model. Finally, this paper demonstrates the usefulness of this model in the case of a security ad hoc routing protocol: Extended SRP.

Key words: strand space; attack analysis model; nonexistent route; SRP (security routing protocol)

摘 要: 根据 ad hoc 安全路由协议的特点,分析串空间理论的优势和不足,并在串空间分析协议的基础上,设计出一种返回不存在路由的协议攻击分析模型.以扩展 SRP 协议为例,验证了模型的正确性.

关键词: 串空间;攻击分析模型;不存在路由;SRP(security routing protocol)协议

中图法分类号: TP393 **文献标识码**: A

移动 ad hoc 网络(MANET mobile ad hoc networks)是一种不依赖于固定基础设施的无线网络,因其自组织特性,在救灾保障、会务通信、作战指挥、实施远距离或危险环境中的监控等场合具有广阔的应用前景.但同时也导致了更多的安全问题,得到了广泛关注和研究,安全路由协议的设计与分析即是其中之一.

目前,大部分安全路由协议分析都是基于主观分析或者模拟仿真等非形式化方法,其分析过程不够精确和严格,导致很多原来声称"安全"的路由协议后来都被发现存在安全漏洞.近年来,形式化分析方法开始应用于安全路由协议的分析研究上.SRP(security routing protocol)的作者试图用 BAN 逻辑对 SRP 的安全性进行分析[1],但 BAN 逻辑假设参与协议的主体都是可信的,而路由源节点 S 和目标节点 T 依赖中间节点建立安全路

* 基金项目: 国家自然科学基金(60872041, 61072066); 国家科技部重大专项(2011ZX03005-002); 中央高校基本科研业务费项目(JY10000903001, JY10000901034)

收稿时间: 2009-07-24; 修改时间: 2010-02-02; 定稿时间: 2010-05-05

由,MANET 环境下中间节点却可能是敌手节点.所以,BAN 逻辑不适合分析这类路由.文献[2]使用一种基于类型推理的 ad hoc 安全路由协议的形式化验证方法,提出了领域约束的通信演算及其操作语义,并利用子类型、多态、类型依赖在类型系统中对其加以表达,给出了验证方法的正确性证明.然而,文中并未对路由攻击本身作详细研究.文献[3]提出一个基于模拟证明方法的安全按需源路由协议的形式化分析模型(以下称其为 ABV 模型).利用 ABV 模型发现了针对 SAODV 协议[4]的新的攻击,同时证明了 ARAN 协议在扩展 ABV 模型下是安全的.然而文献[5]却发现,ABV 模型中存在合并相邻敌手节点等不合理操作,并且指出 ABV 模型对系统正确状态的定义是不合理的,并给出一种完全遵守 ABV 模型假设的攻击 ARAN 协议的新方法.文献[6]利用扩展的串空间模型分析针对 SAODV 协议的内部攻击,将安全路由目标定义为 liveness 和 safety,前者表示协议能够发现存在的路由,后者表示发现的路由中不能存在敌手节点,但最终没有取得明显意义的结果.文献[7]改进了串空间方法,在协议正确性条件中增加中继者可信条件,使其适用于 ad hoc 移动网络路由协议的分析.但文中将所有的中继节点形式化成一个中继者角色,未对各个中继节点的差异性进行研究.

本文利用串空间模型分析安全路由协议,详细研究中继节点中可能存在的敌手节点的各种攻击方式.在此基础上设计出一种攻击分析模型,能够比较全面地分析导致协议返回不存在路由的攻击.

1 串空间及其分析

Strand 空间模型(strand space model,简称 SSM)[8,9]是 Fàbrega,Herzog 和 Guttman 等人在 1998 年提出来的安全协议分析模型,它借助图论的方法描述协议的执行过程.协议主体的行为序列构成 Strand,而 Strand 空间则是所有 Strand 的集合;不同协议主体的 Strand 之间通过消息数据的收发相互关联,从而形成丛(bundle)或称为线束.在线束的基础上,不同节点之间的偏序关系使得存在极小元,从而又产生了一种类似于归纳法[10]的协议安全性的证明方法.

本文主要研究串空间模型下的路由攻击,为了简化描述,除了串空间理论中的攻击者能力部分,本文将直接引用 Strand 空间模型的其他概念和定理,其基本定义可参阅文献[8,9],认证测试定理参阅文献[11,12].

1.1 攻击者能力

串空间理论建立了攻击者行为模型,对于攻击者的一些基本攻击进行了形式化描述.攻击者的能力主要由两方面因素来描述:一是攻击者所掌握的密钥集,二是攻击者由它所接受的消息产生新消息的能力.其中,攻击者所掌握的密钥集由 kp 表示,攻击者的基本行为由下面攻击者的迹的集合来描述:

M:$\langle +t\rangle$,发送消息;

F:$\langle -t\rangle$,接收消息;

T:$\langle -g+g+g\rangle$,接收到消息后,重复转发该消息;

C:$\langle -g-h+gh\rangle$,分别接收消息 g,h 后,发送消息 gh;

S: $\langle -gh+g+h\rangle$,接收消息 gh 后,分别发送消息 g 和 h;

K:$\langle +k\rangle$,发送密钥 k;

E:$\langle -k-h+\{h\}_k\rangle$,接收消息 h 后,用密钥 k 加密,并发送加密后的消息;

D:$\langle -k^{-1}-\{h\}_k+h\rangle$,接受加密后的消息 $\{h\}_k$,用私钥解密,并发送消息 h.

对于一个协议的攻击,可以看作是这些基本行为的组合.这些攻击者的迹给出了对于攻击者能力的形式化描述,并保证了由攻击者发出的消息对于自由信息空间上的运算是封闭的.后文中直接引用某串攻击(例如 C 串攻击)代表攻击者迹为上述相应攻击串.

1.2 串空间分析

串空间主要用于协议正确性的证明,研究人员无法直接应用它来查找协议中存在的漏洞,并进一步获取为何存在漏洞以及如何进行改进等方面的有用信息.特别是当利用串空间分析安全路由协议时,串空间仅仅对各节点的接收消息、发送消息序列进行形式化分析,而忽略各节点的消息验证过程.比如,各中间节点可以验证该

节点是否在路由之中和该节点相邻节点是否是其邻居节点等等.因此,串空间模型仅仅能够得出协议可能受攻击的类型,比如 *C* 串攻击,但并非所有该类型攻击都能使协议返回一条不存在路由.

协议经过串空间的分析,可知在协议消息传输过程中哪些节点可能受到何种类型攻击.这样可以极大地缩小攻击寻找范围,而不必再分析其他节点以及其他类型攻击的情形.我们设计的攻击分析模型正是基于上述原理.

2 攻击分析模型

为了描述方便,在具体阐述模型之前,首先定义如下几个概念.

- 错误路由节点对:在路由序列中,存在两个相邻节点为非邻居节点,该节点对称为错误路由节点对.
- 无效路由段:*A*,*B* 为返回的路由序列中的两个节点.$A\leftrightarrow B$ 表示路由序列中 *A*,*B* 之间的路由序列.若 $A\leftrightarrow B$ 存在错误路由节点对,则 $A\leftrightarrow B$ 为无效路由段,否则为有效路由段.
- *id* 消息:消息的类型.例如,路由协议运行一般可分为两个阶段:路由请求(request)阶段、路由回复(reply)阶段,因此协议消息可分为 req 消息、rep 消息.下文中对模型的描述,也是以路由协议消息只分为 req 阶段消息、rep 阶段消息为例.
- 后续节点:*id* 消息传输过程中,紧跟着节点 *A* 后面的节点为节点 *A* 的 *id* 后续节点.例如,返回路由路径为 $(L_1,L_2,L_3,L_4,\ldots,L_n)$,其中,$L_1$ 为起始节点、L_n 为目标节点.路由请求阶段,L_3 的 req 消息后续节点为 L_4;路由回复阶段,L_3 的 rep 消息后续节点为 L_2.
- 所有后续节点:*id* 消息传输过程中,跟在节点 *A* 后面的所有节点集合为该节点 *A* 的 *id* 消息的所有后续节点.例如,返回路由路径为 $(L_1,L_2,L_3,L_4,\ldots,L_n)$,其中,$L_1$ 为起始节点、L_n 为目标节点.路由请求阶段,L_3 的 req 消息所有后续节点为集合 $\{L_4,\ldots,L_n\}$;路由回复阶段,L_3 的 rep 消息所有后续节点为集合 $\{L_2,L_1\}$.

同理,可定义前趋节点和所有前趋节点.

- 无效攻击:敌手节点的攻击与协议正常运行的结果完全一致,则该攻击认为是无效攻击;否则,称为有效攻击.

例如,假设路由即 $L_i\leftrightarrow L_j$ 为有效路由段,在协议一轮运行过程中的 req 阶段,L_i 节点接收到 *msg* 消息,按照协议的正常运行,L_j 节点将从 L_{j-1} 节点接收到 *msg*′.假设有敌手节点从 L_i 节点监听到消息 *msg* 并进行转换后,并以 L_{j-1} 节点的身份发送 *msg*″给 L_j.若 *msg*″=*msg*′,则认为敌手节点的该攻击行为为无效攻击.

- 未被攻击消息:在协议一轮运行过程中,req/rep 消息从起始/目标节点出发,到某节点接收到该轮 req/ rep 消息 *msg* 的整个过程中未受到攻击,或者是未收到有效攻击,则称 *msg* 为未被攻击消息;否则,称为已被攻击消息.

模型中,安全路由定义为 plausible routing[3],即不返回不存在的路由.

2.1 模型假设

1. 模型仅分析起始节点、目标节点均为可信节点的路由协议可能存在的攻击.

模型分析的路由协议的节点一般可以进行节点验证,其中最基本的节点验证包括:

① 当任意节点 *v* 第 1 次接收到某路由请求时,*v* 验证积累的路由路径最后一个节点标识必须为 *v* 的邻居节点,如果此时积累的路由路径为空,则验证起始节点为 *v* 的邻居节点.如果验证不通过,则抛弃该路由请求;

② 当任意节点 *v* 收到一个路由回复时,它必须验证 *v* 包含在路由回复消息的路由路径内,并且还要验证路由路径里 *v* 的前趋节点和后续节点为 *v* 的邻居节点.验证不通过的话,则抛弃该路由回复消息.

2. 模型不考虑无效攻击的情况.无特别说明,下文中的攻击均指的是有效攻击.
3. 网络中,任意节点的发送消息、接收消息均可能被敌手节点监听.因为发送消息和接收消息是一一对应的关系,只要存在一个发送消息,必定理论上存在对应的一个接收消息,即使因为网络原因或者其他原因,相应接收节点可能未接收到该消息.为了简化模型的分析,模型中敌手节点仅监听并且能监听到所

有接收消息,包含监听未被接收到的消息.但对于一个具体的攻击实例来说,敌手节点可能只需监听必要的信息即可.

4. 模型将协议中传输的消息分两部分:加密部分和未加密部分.加密部分包含加密、签名、散列等等消息中用密钥处理过的部分,否则为未加密部分.
5. 敌手模型为 *Active-x-y*(x>=1,y>=1)[13].其中,x 表示敌手节点捕获节点的数目,y 表示敌手节点控制节点的数目.因此,模型中敌手初始知识范围包含:I① 所有节点公钥;I② 所有节点标识;I③ x 个捕获节点私钥+敌手节点私钥.

随着协议的运行,敌手节点可以监听所有消息,进行处理后增加的知识范围包含:I④ 消息中未加密部分;I⑤ 消息中加密部分;I⑥ 敌手节点使用其拥有的私钥解密 I④,能解密成功得到的原文数据.

6. 敌手节点消息构造能力包括:在敌手知识范围内加解密、散列和连接等等.下文中的更改某消息为另一消息,执行的就是消息构造.

2.2 敌手节点攻击分析

(1) 在具体的网络中,敌手节点在协议运行过程中并非一直处于攻击状态.实际上,敌手节点可能在某些时刻表现得与可信节点一样,遵循协议的规定,处理消息.模型将所有的恶意行为(非正常协议行为)抽象出来,这个时候,原敌手节点就变成一个可信节点.抽象出一个新的敌手节点专门进行攻击的过程简称敌手节点抽象过程.

具体可以分两种情况:

① 如果敌手节点不在返回路由序列中,则路由序列中所有节点均为可信节点.

② 如果敌手节点在返回路由序列中,如图 1 中左图所示:L_{i+1} 为路由序列中的敌手节点.L_i,L_{i+2} 为可信节点.消息传输经过 3 个节点的顺序是 L_i,L_{i+1},L_{i+2}.由上述分析可知,敌手节点的行为可能在某些时候与可信节点一样.模型将恶意行为从敌手节点中抽象出来,可以将网络转换为等价的图 1 中右图所示情况,其中:L_{i+1} 为可信节点;P 为敌手节点,并拥有 L_{i+1} 的私钥.抽象后如图 1 右中所示的 L_{i+1} 节点属于敌手模型 *Active-x-y*(x>=1,y>=1)中的 x 部分.

Fig.1 Adversarial node abstraction

图 1 敌手节点抽象

敌手节点抽象过程的结论包括:① 敌手节点抽象过程不会改变返回路由序列中各节点的网络结构,仅将返回路由序列中的敌手节点的恶意行为抽象出来,这样返回的路由序列中均是可信节点;② 返回路由序列中的原敌手节点转化为被捕获节点.

(2) 下面详细分析执行敌手节点抽象过程以后,敌手节点所有的攻击方式.N_1,N_2 为返回的不存在路由中的两个可信节点,P 为敌手节点,敌手节点间通过带外信道共享所有信息.因此,多个敌手节点可合并为一个敌手节点 P. *id* 表示路由协议消息类型,一般为 req 和 rep.用函数 *neighbor*(N_i,N_j)=1 表示 N_i,N_j 节点为邻居节点,否则为非邻居节点.具体地,敌手节点攻击方式有如下几种:

P_A:具体表示为 $N_1 \xrightarrow{id:P_A} N_2$. 例如, $N_1 \xrightarrow{rep:P_A} N_2$ 表示存在敌手节点 P,P 监听到 N_1 接收到的 rep 消息 *msg*,不更改 *msg*,并以 N_2 前趋节点身份将 *msg* 转发给 N_2.P_A 的必要条件:*neighbor*(N_1,P)=1;*neighbor*(N_2,P)=1.

P_B:具体表示为 $N_1 \xrightarrow{id:P_B} N_2$. 例如, $N_1 \xrightarrow{rep:P_B} N_2$ 表示存在敌手节点 P,P 监听到 N_1 接收到的 rep 消息 *msg*,更改 *msg* 为 *msg*′,并以 N_2 前趋节点身份将 *msg*′转发给 N_2.P_B 的必要条件:*neighbor*(N_1,P)=1;*neighbor*(N_2,P)=1.

P_C:具体表示为 $N_1 \xrightarrow{id:P_C} N_2$. 例如, $N_1 \xrightarrow{rep:P_C} N_2$ 表示 rep 消息发送到 N_1 节点,节点验证通过.此时存在敌手节点 P,P 构造 rep 消息 msg,并以 N_2 前趋节点身份将 msg 发送给 N_2 节点.其中,敌手节点在构造 msg 消息时,消息外全部由敌手知识范围(详见第 2.1 节中第 5 项,下同)中的 I①~I④构造.这样规定的目的在于区别于 P_A,P_B,因为 P_A,P_B 会使用到敌手知识范围中的 I⑤,I⑥.P_C 的必要条件:$neighbor(N_2,P)=1$;P 可在 I①~I④的基础上构造 msg.

P_D:具体表示为 $N_1 \xrightarrow{id:P_D} N_2$. 例如, $N_1 \xrightarrow{rep:P_D} N_2$ 表示 rep 消息发送到 N_1 节点,节点验证通过.此时存在敌手节点 P,P 从其他轮协议运行中监听到 rep 消息 msg,可能进行修改,并发送 msg'($msg=msg'$或者 $msg\neq msg'$)给 N_2 节点.P_D 的必要条件:$neighbor(N_2,P)=1$;P 可从其他轮协议运行中监听消息 msg.

P_D 攻击是从其他轮协议运行中获取部分消息,然后对本轮协议进行攻击.借用串空间理论中丛的概念(丛本质上表示协议的一轮完整运行的串集合),P_D 攻击即为丛间攻击,而 P_A~P_C 均为丛内攻击.

丛间攻击和丛内攻击之间存在冗余情况.丛内攻击不涉及多轮协议运行,相对简单,因此模型优先分析丛内攻击.

基于不同的冗余情况,具体丛间攻击(P_D 攻击)遵循如下两条原则:

P_D 攻击原则 1. 假设某次 P_D 攻击下,敌手节点从其他某轮协议中监听到 msg(也许再修改 msg 为 msg')对本轮协议进行攻击.而若敌手节点完全能从本轮协议的敌手知识范围中构造相同的 msg 或者 msg',则此次 P_D 攻击与相应的丛内攻击结果相同,没必要重复考虑.

P_D 攻击原则 2. 假设某次 P_D 攻击下,敌手节点从其他某轮协议中监听到 msg(也许再修改 msg 为 msg')对本轮协议进行攻击,导致本轮协议返回了不存在路由 R.而若 msg 所在的该轮协议中,msg 也能被该轮协议下的敌手节点监听(也许再修改 msg 为 msg'),并导致该轮协议返回了不存在路由 R,则认为此次 P_D 攻击与相应的丛内攻击结果相同,没必要重复考虑.

需要注意的是:在 P_A~P_D 攻击中,N_1,N_2 为返回的不存在路由 R 中的两个可信节点,并且 R 中 N_1,N_2 之间部分路由序列中必须存在错误路由节点对.假如 $N_1 \leftrightarrow N_2$ 为有效路由段,则消息按照协议正常运行就可以由 N_1 到达 N_2,而没必要进行攻击.

因此,可以将模型中所有有效攻击方式(P_A~P_D 攻击)简称为跨越路由攻击(cross-route attack).(N_1~N_2)称为跨越节点对.(N_1~N_2)之间跨越路由攻击后可通过 N_2 节点验证的攻击,称为有效的跨越路由攻击;反之,称为无效的跨越路由攻击.(N_1~N_2)之间的跨越攻击表示为 $N_1 \xrightarrow{id:P} N_2$, 例如 $N_1 \xrightarrow{rep:P} N_2$.

由上述分析可知,跨越路由攻击存在如下几条性质:

性质 1. 当返回不存在路由时,在 req 阶段、rep 阶段必定均存在有效的跨越路由攻击.目前,模型仅分析 req 阶段、rep 阶段均存在一个有效的跨越路由攻击的情况,则模型中的 req 阶段、rep 阶段跨越路由段均跨越了路由中的不存在路由部分.

性质 2. 一次跨越路由攻击中,除了监听消息外,有且仅有一个节点的接收消息是已被攻击消息.

性质 3. 模型仅分析 req 阶段、rep 阶段均存在一个有效的跨越路由攻击的情况,因此,在返回的不存在路由中的、并与跨越路由段不重叠的有效路由段上,不存在有效的跨越攻击.而模型中所有有效攻击的攻击方式均为跨越攻击,并且模型不考虑无效攻击,则在有返回的不存在路由中的与跨越路由段不重叠的有效路由段上,不存在有效攻击.

性质 4. 有效的 P_C 攻击一般不存在,因为如果仅根据敌手知识范围中的 I①~I④就能构造有效的 P_C 攻击的话,则说明协议安全性较差.

2.3 模型具体分析步骤

基于上述假设和敌手能力,本文提出一种基于串空间基础上的安全路由协议攻击的分析模型,能够比较全面地分析协议中存在的攻击实例.攻击的结果为路由协议不满足其安全目标,即路由协议返回一条不存在路由.

具体步骤为:

步骤 1. 假设协议在返回一条不存在路由($L_1,L_2,\ldots,L_n$)时,先进行敌手节点抽象过程(见第 2.2 节中第 1 项).

步骤 2. 利用串空间模型对协议进行分析,分析协议的串空间中在哪几个节点可能接受什么类型的攻击.这样就不用考虑其他节点和其他类型攻击行为,大大缩小了攻击的搜索范围.

步骤 3. 路由过程分为 req 和 rep 这两个阶段.将可能遭受攻击的串空间消息节点分别划到这两个阶段中.

步骤 4. 因为在假设协议返回一条不存在路由($L_1,L_2,\ldots,L_n$)时,由跨越路由攻击性质 1 可知,协议 req 阶段、rep 阶段均存在一个有效的跨越路由攻击.逆向分析有效跨越路由攻击的攻击过程,即先分析 rep 阶段遭受的攻击过程,再分析 req 阶段遭受的攻击过程.

例如,假设 rep 阶段节点容易受 *C* 串攻击和 *E* 串攻击,则 rep 阶段的 4 种跨越路由攻击均可能由 *C* 串、*E* 串攻击组成.考虑其中的组合情况,分析可能成功的攻击,然后再分析 req 阶段有效跨越路由攻击的组合情况.

步骤 5. 由步骤 4 可以得到具体攻击实例和该攻击实例所需要的网络拓扑结构 *G*(攻击实例中,*G* 中每条节点相连路径均在消息传输中使用过).

可以通过下述方式简化网络结构:

① 若敌手节点拥有某个中间节点 L_i 的私钥,则认为该中间节点属于敌手模型 *Active-x-y*(x>=1,y>=1)中 x 部分,即被捕获节点;

② 假设 L_i 为被捕获节点,并且 *G* 中 L_i 的邻居节点均为敌手节点的邻居节点,可以认为 L_i 为敌手节点.确认所有相同情况的 L_i 后,从 *G* 中原敌手节点的网络信息中剥离所有 L_i 的网络结构(将原敌手节点的邻居节点中去掉所有 L_i 的邻居节点),剥离后的网络为 *G*′,L_i 为敌手节点.

3 基于扩展 SRP 协议的模型分析

文献[14]指出,经典安全协议是安全协议分析的“实验床”.即每当出现一个新的形式化分析方法,都要先分析经典安全协议,验证新方法的有效性.SRP 协议是 ad hoc 无线移动网络下经典的按需安全路由协议,已被研究人员用多种形式化方法分析过[1,7,15].利用本文提出的基于串空间的安全路由攻击分析模型对 SRP 协议进行分析,对比前人的研究成果,能够充分验证模型的正确性和高效性.

文献[15]对 SRP 协议提出了一种改进方法,在 SRP 协议的基础上增加了 ad hoc 网络中最基本的节点验证过程(见第 2.1 节中的第 1 项).本文称这种改进的 SRP 协议为扩展 SRP 协议.

下面以扩展 SRP 协议为例,使用本文提出的攻击分析模型对其进行分析.

步骤 1. 假设某轮协议运行,返回一条不存在的路由 $R_0=(L_1,L_2,\ldots,L_n)$.经过敌手节点抽象过程后如图 2 所示.$L_1,L_2,\ldots,L_n$ 均为可信节点,L_1 为起始节点,也称为 *S* 节点;L_n 为目标节点,也称为 *T* 节点;*P* 为敌手节点.

由跨越路由攻击性质 1 可知,模型将返回的不存在路由分解为 3 个部分:从起始节点 L_1 开始的最长的有效路由段 $L_1\leftrightarrow L_i$;从目标节点 L_n 逆向回溯的最长的有效路由段 $L_k\leftrightarrow L_n$;$L_i\leftrightarrow L_k$ 之间路由部分就是无效路由段.图中用⊥区分 3 个路由段.无效路由段 $L_i\leftrightarrow L_k$,节点 L_i 和 L_k 之间有 m 个节点 $L_{i+1},\ldots,L_{i+m}$,其中,$m\geqslant 0$,$k=i+m+1$.

当 $m>0$ 时,$neighbor(L_i,L_{i+1})=0$,$neighbor(L_{i+m},L_k)=0$;$0\leqslant i<k\leqslant n$;

当 $m=0$ 时,$neighbor(L_i,L_k)=0$.

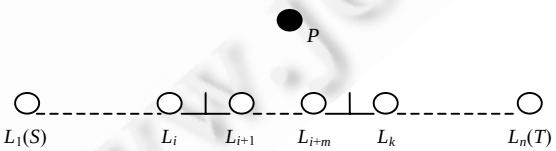


Fig.2 Network topology

图 2 网络拓扑图

P 为敌手节点,模型定义 *P* 可以监听任何消息,则 *P* 默认为可与 $L_1,L_2,\ldots,L_n$ 相连.图 2 中隐藏了 *P* 与其他所有节点的连接.因为对于某次具体攻击来说,*P* 可能只需监听部分信息,也就是说,*P* 只需与部分节点相连即可.在

后面的分析中,与攻击有关的必要的节点相连信息才会标记出来.

步骤 2. 文献[7]使用串空间模型对 SRP 协议进行了分析.串空间仅能对消息序列进行形式化分析,而不能对节点验证过程进行分析.因此,使用串空间对扩展 SRP 协议的分析过程等于对 SRP 协议的分析过程.

那么,扩展 SRP 协议的串空间表示如下:

- 发起者串 $init[N_s,N_t,K_{st},K_h,S,T,R]$,其迹为$+S,N_s,\{N_s,K_{st}\}K_h;-S,R,T,N_t,\{S,R,T,N_t,K_{st}\}K_h$
- 响应者串 $resp[N_s,N_t,K_{st},K_h,S,T,R]$,其迹为$-S,R,N_s,\{N_s,K_{st}\}K_h;+S,R,T,N_t,\{S,R,T,N_t,K_{st}\}K_h$
- 中继者串 $intermediate[N_s,N_t,K_h,S,T,R]$,其迹为$-S,N_s,\{N_s,K_{st}\}K_h;+S,R,N_s,\{N_s,K_{st}\}K_h;$
  $-S,R,T,N_t,\{S,R,T,N_t,K_{st}\}K_h;+S,R,T,N_t,\{S,R,T,N_t,K_{st}\}K_h$

其中,S 为起始节点,T 为目标节点,N_s,N_t 为随机数,K_{st} 表示两个节点的共享密钥.其中,下标表示产生该项的节点.特别地,单向散列函数用 K_h 表示(这里的 h 不表示节点),它只有加密密钥,没有相应的解密密钥,并且散列密钥只能在 S,T 中.

文献[7]得出结论:发起者串和响应者串中的节点均不会源自于攻击者串,而中继者串 $intermediate[]$的$\langle r,2\rangle$节点有可能源自攻击者串中的 C 串,而不会源自于其他攻击者串,即仅容易受到 C 串攻击.同理,中继者串 $intermediate[]$的$\langle r,3\rangle$,$\langle r,4\rangle$节点也容易受 C 串攻击.而 $uns\_term(\langle r,3\rangle)=uns\_term(\langle r,4\rangle)$.仅以$\langle r,3\rangle$为例,进行说明:

C 串:则 $g=S,T,N_t,\{S,R,T,N_t,K_{st}\}K_h,h=R,gh=S,R,T,N_t,\{S,R,T,N_t,K_{st}\}K_h$,由此可以看出该节点可能源自 C 串.具体 C 串攻击时,理论上 g,h 存在其他几种可能性,但因为散列函数是单向的,敌手节点没有散列密钥;而 S,T 均为可信节点标识,N_t 为随机数,对它们进行修改,没有意义或者很容易被验证不通过.因此,$\langle r,3\rangle$遭受的 C 串攻击均是敌手节点可能对 R 部分进行处理.$\langle r,2\rangle$,$\langle r,4\rangle$节点亦同理.

扩展 SRP 协议消息结构中未涉及到各中间节点公钥和私钥,因此,敌手节点知识范围内的被捕获节点私钥对攻击没有作用.

需要注意的是:第 1.2 节指出,协议经过串空间的分析,可知在协议消息传输过程中哪些节点可能受到何种类型攻击.这样可以大大缩小攻击寻找范围,而不必再分析其他节点以及其他类型攻击的情形.扩展 SRP 协议经过串空间分析后,指出仅中继者串 $intermediate[]$的$\langle r,2\rangle$,$\langle r,3\rangle$,$\langle r,4\rangle$节点容易受到 C 串攻击,而其他串和其他节点不会受到攻击.并且,协议本身存在的安全机制和节点验证机制保证:并非任意 C 串攻击都能使得扩展 SRP 协议返回一条不存在路由.因此,需要进一步将 C 串攻击和跨越路由攻击结合起来加以分析.

步骤 3. 扩展 SRP 协议运行可分成两个阶段:req 阶段和 rep 阶段.其中,可能遭受攻击的中继者串 $intermediate[]$的$\langle r,2\rangle$属于 req 阶段,$\langle r,3\rangle$,$\langle r,4\rangle$属于 rep 阶段.因 $uns\_term(\langle r,3\rangle)=uns\_term(\langle r,4\rangle)$,结合跨越路由性质 2 和串空间理论,则跨越路由攻击,不需要分析$\langle r,4\rangle$.

步骤 4. 在串空间分析的基础上,根据模型分析扩展 SRP 协议的返回为不存在路由的攻击过程.

假设在某轮协议中,协议返回了一条不存在的路由 $R_0=(L_1,L_2,\ldots,L_n)$,使得用到的随机数、共享密钥分别为 $N_{s0},N_{t0},\ K_{st0}$.具体过程为:req 阶段,L_1 发出消息 $msg\_req\_L_1$ 为$+S,N_{s0},\{N_{s0},K_{st0}\}K_h$;而 rep 阶段攻击结果为:$L_1$ 接收到返回消息 $msg\_rep\_L_1$ 为$-S,R_0',T,N_{t0},\{S,R_0',T,N_{t0},K_{st0}\}K_h$ 并验证通过,接受返回路径 R_0,其中,$R_0'=(L_2,\ldots,L_{n-1})$.

首先分析路由回复阶段,即 rep 阶段:$L_i\leftrightarrow L_k$ 为无效路由段,则 rep 阶段存在一个有效的跨越路由攻击,该攻击成功跨越了 $L_i\leftrightarrow L_k$ 这个路由段.假设该攻击是在$(L_{k'}\sim L_{i'})$这个跨越节点对上进行的,即 $L_{k'}\xrightarrow{rep:P}L_{i'}$,如图 3 所示.其中,$1\leqslant i'\leqslant i;k\leqslant k'\leqslant n$.

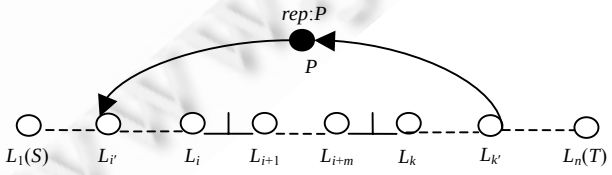


Fig.3 Cross-Route attack in the rep stage

图 3 rep 阶段跨越路由攻击

因为 $L_1 \leftrightarrow L_{i'}$为有效路由段,则根据跨越攻击性质 3 和协议规则,rep 阶段 $L_{i'}$接收到的消息应为

$$msg\_rep\_L_{i'}{:}{-}S, R'_0, T, N_{t0}, \{S, R'_0, T, N_{t0}, K_{st0}\}K_h.$$

模型仅考虑 req 阶段、rep 阶段均只有一个跨越攻击的情况,并且由跨越攻击性质 2 和步骤 3 结论可以得出结论:对于中间节点 $L_{i'}$来说,其消息串 *intermediate*[]中的$\langle r,3\rangle$,即 $L_{i'}$收到的消息 $msg_rep_L_{i'}{:}{-}S, R'_0, T, N_{t0}, \{S, R'_0, T, N_{t0}, K_{st0}\}K_h$遭受了 *C* 串攻击.

下面详细分析 rep 阶段 *C* 串攻击结合跨越攻击的具体过程及其合理性.

C 串+P_B:具体过程为:敌手节点监听 $L_{k'}$的 rep 消息 *msg*,并由步骤 2 分析可知,敌手节点只能修改 *msg* 中 *R* 这一部分,变成 *msg*′,然后以 $L_{i'+1}$的身份发送 *msg*′给 $L_{i'}.L_{k'} \leftrightarrow L_n$为有效路由段,可知 rep 阶段的 *msg* 是未被攻击过的消息,且 $R' \neq R$,而 rep 阶段 $L_{i'}$的所有后续节点未遭遇跨越攻击,均按照协议正常运行处理消息,则 L_1 接收到的消息为 *msg*′.根据散列函数性质,L_1 将检测出 *msg*′有误,不接受路由 *R*′,这与假设中协议运行接受一条路由相矛盾.因此, rep 阶段排除 *C* 串+P_B 攻击的可能性,该情况不成立.

C 串+P_C:文献[16]对“入检测定理”进行扩展,同理可以得到扩展的“主动检测定理”.因单向散列函数 K_h 只有加密密钥,没有相应的解密密钥,并且散列密钥只能在可信节点 *S*,*T* 中,可知 $msg_rep_L_{i'}$中的$\{S, R'_0, T, N_{t0}, K_{st0}\}K_h$部分必定来自可信节点 *S* 或 *T*,敌手节点 *P* 不能在其敌手知识范围中 *I*①~*I*④的基础上构造 *msg*.因此,rep 阶段排除 *C* 串+P_C 攻击的可能性,该情况不成立.

C 串+P_D:具体过程为:假设敌手节点从其他轮扩展 SRP 协议监听到 rep 消息 *msg* 为 $S, R_1, T, N_{t0}, \{S, R_2, T, N_{t0}, K_{st0}\}K_h$,分两种情况:

① 假设 $R2 = R'_0$,则在得到 *msg* 的该轮协议中,修改 R_1 为 R'_0,该轮协议即可返回一条不存在路由 R_0,不满足 P_D 攻击原则 2;

② 假设 $R2 \neq R'_0$,因为散列函数是单向的,并且敌手节点没有散列密钥,因此敌手节点不能由 *msg* 构造 $msg\_rep\_L_{i'}$.

因此,rep 阶段排除 *C* 串+P_D 的可能性,该情况不成立.

C 串+P_A:敌手节点监听 $L_{k'}$接收到的 rep 消息 *msg*,然后以 $L_{i'+1}$ 的身份发送 *msg* 给 $L_{i'}$.这种攻击是可能存在的.仅需满足 $neighbor(L_{i'+1}, L_i)=1$ 和 $msg=msg\_rep\_L_{i'}{=}{-}S, R'_0, T, N_{t0}, \{S, R'_0, T, N_{t0}, K_{st0}\}K_h$,*msg* 在 $L_{i'}$及其所有后续节点都能满足节点验证.因为$(L_{k'} \leftrightarrow L_n)$为有效路由段,根据扩展 SRP 协议规则可知,在该 *C* 串+P_A 之前,L_n 发出的消息亦为 *msg*.

综上所述,得出 rep 阶段结论为:假设某轮协议中,协议返回了一条不存在的路由 $R_0=(L_1, L_2, \ldots, L_n)$,使用到的随机数、共享密钥分别为 N_{s0}, N_{t0}, K_{st0}.仅需满足:rep 阶段,L_n 发送消息 $msg\_rep\_L_n$ 为$+S, R'_0, T, N_{t0}, \{S, R'_0, T, N_{t0}, K_{st0}\}K_h$,然后在$(L_{k'} \sim L_{i'})$这个跨越节点对处遭受了 *C* 串+$P_A$ 攻击.

再分析路由请求阶段,即 req 阶段:$(L_i \leftrightarrow L_k)$为无效路由段,则存在一个有效的跨越路由攻击,该攻击成功跨越了$(L_i \leftrightarrow L_k)$这个路由段.假设该攻击是在$(L_{i''} \sim L_{k''})$这个跨越节点对上进行的,即 $L_{i''} \xrightarrow{req:P} L_{k''}$,如图 4 所示.其中, $1<=i''<=i; k<=k''<=n$.

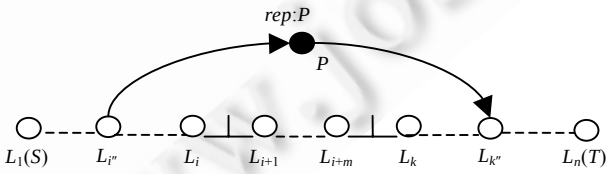


Fig.4 Cross-Route attack in the req stage

图 4 req 阶段跨越路由攻击

L_n 节点为可信节点,为了满足 rep 阶段的结论,因此 req 阶段的攻击结果应为:L_1 发出消息 $msg\_req\_L_1$ 为$+S, N_{s0}, \{N_{s0}, K_{st0}\}K_h$,$L_n$ 节点接收到的 req 消息为 $msg\_req\_L_n{=}{-}S, R'_0, N_{s0}, \{N_{s0}, K_{st0}\}K_h$,其中, $R'_0=(L_2, \ldots, L_{n-1}).L_{k''} \leftrightarrow L_n$

为有效路由段.根据跨越攻击性质 3 和协议运行规则,req 阶段 $L_{k''}$ 接收的消息 $msg\_req\_L_{k''}=-S,R_3,N_{s0},\{N_{s0},K_{st0}\}K_h$,其中,$R_3=(L_2,\ldots,L_i,\ldots,L_k,\ldots,L_{k''-1})$.

下面详细分析 req 阶段 C 串攻击结合跨越攻击的具体过程及其合理性.

C 串+P_A:$L_1\leftrightarrow L_{i''}$为有效路由,且各节点均为可信节点.根据跨越攻击性质 3,$L_{i''}$积累的路由 R 为$(L_2,\ldots,L_{i''-1})$,被敌手节点转发到 $L_{k''}$.这与 req 阶段 $L_{k''}$接收到的消息 $msg\_req\_L_{k''}=-S,R_3,N_{s0},\{N_{s0},K_{st0}\}K_h$ 的路由部分 R_3 不同,因此 req 阶段不可能遭受 C 串+P_A 攻击,该情况不成立.

C 串+P_C:与 rep 阶段的 C 串+P_C 相同,根据扩展的"主动检测定理",因单向散列函数 K_h 只有加密密钥,没有相应的解密密钥,并且散列密钥只能在可信节点 S,T 中,可知 req 阶段 $L_{k''}$接收到的消息 $msg\_req\_L_{k''}=-S,R_3,N_{s0},\{N_{s0},K_{st0}\}K_h$ 中的$\{N_{s0},K_{st0}\}K_h$部分必定来自可信节点 S 或 T,P 不能在其敌手知识范围 I①~I④的基础上构造 msg.因此,该情况不成立.

C 串+P_D:具体过程为:敌手节点从其他轮扩展 SRP 协议监听到 rep 消息 msg,更改后为 $msg\_req\_L_{k''}=-S,R_3,N_{s0},\{N_{s0},K_{st0}\}K_h$ 发送给 $L_{k''}$;很明显,$msg_req_L_{k''}$可以完全由本轮协议中敌手节点知识范围构造出来.其中,$S\in I$①,R_3 可由 I①构造,$N_{s0}\in I$④,$\{N_{s0},K_{st0}\}K_h\in I$⑤.因此,不满足 P_D 攻击原则 1,该情况不成立.

C 串+P_B:即 req 阶段,L_1 发出消息 $msg\_req\_L_1=+S,N_{s0},\{N_{s0},K_{st0}\}K_h$,根据跨越攻击性质 3,$L_{i''}$接收到的消息 $msg_req_L_{i''}$为$-S,R_4,N_{s0},\{N_{s0},K_{st0}\}K_h$,其中,$R_4=(L_2,\ldots,L_{i''-1})$.跨越攻击后,$L_{k''}$应接收的消息 $msg\_req\_L_{k''}=-S,R_3,N_{s0},\{N_{s0},K_{st0}\}K_h,R_3=(L_2,\ldots,L_i,\ldots,L_k,\ldots,L_{k''-1})$.显然,$C$ 串+P_B 攻击能得到 req 阶段的攻击结果,仅需敌手节点监听 $L_{i''}$接收到的消息 $msg\_req\_L_{i''}$,修改其中的路由部分为 R_3,转发给 $L_{k''}$.

步骤 5. 由步骤 4 可得出扩展 SRP 的攻击实例:

初始网络条件:如图 2 所示,L_1 为起始节点,也称为 S;L_n 为目标节点,也称为 T.从起始节点 L_1 开始的最长的有效路由段 $L_1\leftrightarrow L_i$,从目标节点 L_n 逆向回溯的最长的有效路由段 $L_k\leftrightarrow L_n$.$L_i\leftrightarrow L_k$ 之间的路由部分就是无效路由段,图中用⊥来区分 3 个路由段.无效路由段 $L_i\leftrightarrow L_k$,节点 L_i 和 L_k 之间有 m 个节点 $L_{i+1},\ldots,L_{i+m}$,其中,$m>=0,k=i+m+1$.

当 $m>0$ 时,$neighbor(L_i,L_{i+1})=0,neighbor(L_{i+m},L_k)=0;0<=i<k<=n$;

当 $m=0$ 时,$neighbor(L_i,L_k)=0$.

具体攻击步骤如下:

① L_1 发出消息 $msg\_req\_L_1$ 为$+S,N_{s0},\{N_{s0},K_{st0}\}K_h$;

② 敌手节点监听 $L_{i''}$接收到的消息 $msg_req_L_{i''}$为$-S,R_4,N_{s0},\{N_{s0},K_{st0}\}K_h$,其中,$R_4=(L_2,\ldots,L_{i''-1})$.构造消息 $msg\_req\_L_{k''}=S,R_3,N_{s0},\{N_{s0},K_{st0}\}K_h$,其中,$R_3=(L_2,\ldots,L_i,\ldots,L_k,\ldots,L_{k''-1})$,并以 $L_{k''-1}$ 的身份发送消息 $msg_req_L_{k''}$给 $L_{k''}$.其中,$1<=i''<=i,k<k''<=n$;

③ 协议继续运行,直至 L_n 接收到 req 消息,并发送 rep 消息 $msg\_rep\_L_n$ 为$+S,R_0',T,N_{t0},\{S,R_0',T,N_{t0},K_{st0}\}K_h$,$R_0'=(L_2,\ldots,L_{n-1})$;

④ $L_{k'}$接收到 rep 消息 $msg\_rep\_L_{k'}=S,R_0',T,N_{t0},\{S,R_0',T,N_{t0},K_{st0}\}K_h$,敌手节点监听到该消息,并以 $L_{i'+1}$ 身份发送消息 $msg\_rep\_L_{i'}=S,R_0',T,N_{t0},\{S,R_0',T,N_{t0},K_{st0}\}K_h$ 给 $L_{i'}$.其中,$1<=i'<I,k<=k'<=n$;

⑤ 协议继续运行,L_1 接收到 rep 消息,并验证通过.

这样,协议就返回一条不存在路由 $R_0=(L_1,L_2,\ldots,L_n)$.

攻击条件:

① 敌手能力如本文第 2.1 节所示;

② 网络条件:除初始网络条件以外,还需有如下网络条件:

- 敌手节点 P 与 $L_{i'},L_{k'},L_{i''},L_{k''}$相连,即 $neighbor(P,L_{i'})=neighbor(P,L_{k'})=neighbor(P,L_{i''})=neighbor(P,L_{k''})=1$;
- $L_{k''-1}$ 与 $L_{k''}$相连,即 $neighbor(L_{k''-1},L_{k''})=1$.因 $neighbor(L_{k-1},L_k)=0$,可得出 $k''>k$;
- $L_{i'+1}$ 与 $L_{i'}$相连,即 $neighbor(L_{i'+1},L_{i'})=1$.因 $neighbor(L_i,L_{i+1})=0$,可得出 $i'<i$.

特殊情况下,当 $i'=i''=i-1,k'=k''=k+1$ 时,即 $L_{i'}$与 $L_{i''}$为同一节点 L_{i-1},并且 $L_{k'}$与 $L_{k''}$为同一节点 L_{k+1} 时,攻击过程与文献[15]中的结论相一致.

4 结束语

我们提出了一种基于串空间分析结论上的 ad hoc 安全路由协议的攻击分析模型,攻击目标为返回一条不存在的路由,并以扩展 SRP 协议分析为例,分析出该协议下的攻击实例.模型的提出,使得串空间的结论能够有效地运用在 ad hoc 安全路由协议这类比较复杂的协议中,极大地扩展了串空间的应用范围.

模型理论上能够分析 *active-x-y*(x>=1,y>=1)敌手模型情况下的所有攻击.但模型仍然存在一些不足之处:

① 具体分析时,需要考虑敌手节点具有哪 x 个中间节点的私钥.而扩展 SRP 协议中的消息结构没有用到中间节点的私钥、公钥,使得分析时不用考虑这个问题;

② 模型分析的攻击中,目前仍局限于 req 阶段、rep 阶段均仅存在一个有效跨越攻击的情况.

后续工作的重点在于增加模型分析范围,设计并实现基于串空间理论的路由攻击自动化分析工具.

References:

[1] Papadimitratos P, Haas ZJ. Secure routing for mobile ad hoc networks. In: Proc. of the CNDS 2002. San Antonio: Sage Science Press, 2002. 1−13. http://www.ee.kth.se/~papadim/publications/fulltext/secure-routing-cnds02.pdf

[2] Li Q, Zeng QK. Verifying mobile ad-hoc security routing protocols with type inference. Journal of Software, 2009,20(10): 2822−2833 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3504.htm [doi: 10.3724/SP.J.1001.2009.03504]

[3] Ács G, Buttyán L, Vajda I. Provable security of on-demand distance vector routing in ad hoc networks. In: Molva R, Tsudik G, Westhoff D, eds. Proc. of the ESAS 2005. LCNS 3813, Berlin: Springer-Verlag, 2005. 113−127.

[4] Zapata MG, Asokan N. Securing ad hoc routing protocols. In: Proc. of the WiSE 2002. Atlanta: ACM Press, 2002. 1−10. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.1667&rep=rep1&type=pdf [doi: 10.1145/570681.570682]

[5] Mao LQ, Ma JF. Analysis of provably secure on-demand distance vector routing in MANET. Journal of Xidian University (Natural Science), 2008,35(6):1063−1068 (in Chinese with English abstract).

[6] Yang SH, Baras JS. Modeling vulnerabilities of ad hoc routing protocols. In: Proc. of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks. Fairfax: ACM Press, 2003. 12−20. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.97.3998&rep=rep1&type=pdf [doi: 10.1145/986858.986861]

[7] Wang JZ, Wang YL. Security analysis for ad hoc routing protocols based on improved strand space. Journal of Software, 2006, 17:256−261 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17s/256.htm

[8] Fábrega FJT, Herzog JC, Guttman JD. Strand spaces: Why is a security protocol correct? In: Proc. of the 1998 IEEE Symp. on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1998. 160−171. http://ieeexplore.ieee.org/iel4/5528/14832/00674832.pdf?tp=&arnumber=674832&isnumber=14832

[9] Fábrega FJT, Herzog JC, Guttman JD. Strand spaces: Proving security protocols correct. Journal of Computer Security, 1999,7(2-3): 191−230.

[10] Paulson LC. The inductive approach to verifying cryptographic protocols. Journal of Computer Security, 1998,6(1):85−128.

[11] Guttman JD, Fábrega FJT. Authentication tests. In: Proc. of the 2000 IEEE Symp. on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 2000. 96−109. http://ieeexplore.ieee.org/iel5/6864/18435/00848448.pdf?tp=&arnumber=848448&isnumber= 18435 [doi: 10.1109/SECPRI.2000.848448]

[12] Guttman JD, Fábrega FJT. Authentication tests and the structure of bundles. Theoretical Computer Science, 2002,283(2):333−380. [doi: 10.1016/S0304-3975(01)00139-6]

[13] Hu YC, Perrig A, Johnson DB. Ariadne: A secure on-demand routing protocol for ad hoc networks. In: Proc. of the MobiCom 2002. Atlanta: ACM Press, 2002. 12−23. http://www.ece.cmu.edu/~adrian/projects/secure-routing/ariadne.pdf [doi: 10.1145/570645.570648]

[14] Qing SH. Twenty years development of security protocols research. Journal of Software, 2003,14(10):1740−1752 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1740.htm

[15] Buttyán L, Vajda I. Towards provable security for ad hoc routing protocols. In: Proc. of the SASN 2004. Washington: ACM, 2004. 94−105. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.75.8495&rep=rep1&type=pdf [doi: 10.1145/1029102.1029119]

[16] Ji XJ, Tian C, Zhang YS. Secure DSR routing protocol analysis and design. Journal on Communications, 2006,27(3):136−140 (in Chinese with English abstract).

附中文参考文献:

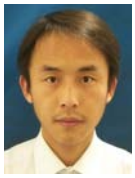
[2] 李沁,曾庆凯.利用类型推理验证 Ad Hoc 安全路由协议.软件学报,2009,20(10):2822−2833. http://www.jos.org.cn/1000-9825/3504.htm [doi: 10.3724/SP.J.1001.2009.03504]

[5] 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.西安电子科技大学学报(自然科学版),2008,35(6):1063−1068.

[7] 王继志,王英龙.基于改进的串空间分析 Ad Hoc 路由协议安全性.软件学报,2006,17:256−261. http://www.jos.org.cn/1000-9825/17s/256.htm

[14] 卿斯汉.安全协议 20 年研究进展.软件学报,2003,14(10):1740−1752. http://www.jos.org.cn/1000-9825/14/1740.htm

[16] 季晓君,田畅,张毓森.安全 DSR 路由协议分析与设计.通信学报,2006,27(3):136−140.



董学文(1981－),男,湖北黄冈人,博士生,讲师,CCF 会员,主要研究领域为无线网络安全,安全协议分析.

毛立强(1978－),男,博士生,讲师,主要研究领域为无线网络安全,安全协议设计与分析.

马建峰(1963－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为密码学,信息安全.

谢辉(1978－),男,博士生,CCF 学生会员,主要研究领域为无线网络路由算法及安全.

牛文生(1967－),男,博士,研究员,博士生导师,CCF 高级会员,主要研究领域为航空电子系统安全.