ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.21, No.7, July 2010, pp.1717−1731
doi: 10.3724/SP.J.1001.2010.03576

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

可证明安全的节点不相交多路径源路由协议*

冯 涛[1,2+], 郭 显[1,3], 马建峰[2], 李兴华[2]

[1](兰州理工大学 计算机与通信学院,甘肃 兰州 730050)

[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](甘肃联合大学 电子信息工程学院,甘肃 兰州 730010)

Provably Secure Approach for Multiple Node-Disjoint Paths Source Routing Protocol

FENG Tao[1,2+], GUO Xian[1,3], MA Jian-Feng[2], LI Xing-Hua[2]

[1](School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China)

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

[3](School of Electronics and Information Engineering, Gansu Lianhe University, Lanzhou 730010, China)

+ Corresponding author: E-mail: fengt@lut.cn, http://www.lut.cn

Feng T, Guo X, Ma JF, Li XH. Provably secure approach for multiple node-disjoint paths source routing protocol. *Journal of Software*, 2010,21(7):1717−1731. http://www.jos.org.cn/1000-9825/3576.htm

Abstract: The multi-path routing scheme provides reliable guarantee for mobile ad hoc networks. This paper proposes a new method used to analyze the security of multi-path routing protocol within the framework of Universally Composable (UC) security. Based on the topological model that exist in adversarial nodes, the concept of plausible route is extended and the definition of plausible-route set is presented. Plausible-Route set is used to describe the multi-path routing for ad hoc networks, and a formal security definition based on UC-RP is given. A provably Security Multiple Node-Disjoint Paths source routing (SMNDP) is proposed and used to address secure fault issue of MNDP (multiple node-disjoint paths) in the active adversary model. The new approach shows that the security of SMNDP can be reduced to the security of the message authentication code and the digital signature. SMNDP implements the correctness of route discovery process, the authentication of nodes identifier and the integrality of route information.

Key words: ad hoc network; MNDP (multiple node-disjoint paths); provably security; plausible route; SMNDP (security multiple node-disjoint paths)

摘 要: 多路径路由实现是移动ad hoc网络可靠运行的有效保证.针对多路径路由协议的安全性分析,建立了基于UC(universally composable)框架的可证明安全路由协议的新方法.基于攻陷的网络拓扑模型,扩展了可模糊路由概念,提出了多路径可模糊路由集合概念,用于描述攻陷网络拓扑结构的移动ad hoc网络多路径路由;基于UC安全模

* Supported by the National Natural Science Foundation of China under Grant Nos.60573036, 60972078, 60702059 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant No.2007AA01Z429 (国家高技术研究发展计划(863)); the Gansu Provincial Natural Science Foundation of China under Grant No.2007GS04823 (甘肃省自然科学基金); the Ph.D. Programs Foundation of Lanzhou University of Technology of China under Grant No.BS14200901 (兰州理工大学博士基金)

Received 2008-07-16; Revised 2008-10-28; Accepted 2009-01-20

型,提出了基于 UC-RP(universally composable security framework for ad hoc networks routing protocol)框架的路由协议形式化安全定义;针对 MNDP(multiple node-disjoint paths)协议存在的安全问题,提出了新的移动 ad hoc 网络节点不相交多路径动态源路由协议(简记为 SMNDP(security multiple node-disjoint paths)协议).将基于 UC-RP 框架的可证明安全路由协议的新方法应用于 SMNDP 协议的安全分析.SMNDP 协议的可证明安全性可以归约为消息认证码和签名机制的安全性.SMNDP 协议实现了路由发现协议的正确性、节点身份的认证性和路由消息的完整性.

关键词: ad hoc 网络;MNDP(multiple node-disjoint paths);可证明安全;可模糊路由;SMNDP(security multiple node-disjoint paths)

中图法分类号: TP393 **文献标识码**: A

移动 ad hoc 网络没有固定的基础设施,网络节点既是主机又是路由器.同时,网络节点的移动性导致网络拓扑是动态变化的.路由问题是移动 ad hoc 网路可靠运行的关键问题.路由协议通常分为单路径路由和多路径路由.传统的单路径路由主要分为两大类:按需路由协议,例如动态源路由协议 DSR[1]、按需距离适量路由协议 AODV[2]等;主动式路由协议,例如目的节点序列号距离矢量路由协议 DSDV[3]等.单路径路由协议算法简单,易于管理和配置.与单路径路由相比,多路径路由在路由容错、路由可靠性、平衡网络负载、提高服务质量(QoS)等方面具有优势而成为近几年移动 ad hoc 网络路由协议的研究热点[4–6].

多路径路由可以分为 3 种:节点不相交(node-disjoint)多路径、链路不相交(link-disjoint)多路径和相交多路径.节点不相交多路径也称为完全不相关多路径,是指各条路径中除源节点和目的节点之外没有其他任何共用节点.链路不相交多路径是指各条路径间没有任何共用的链路,但有可能有共用的节点.相交多路径是指各条路径间既有共用的节点,又有共用的链路.节点不相交多路径因其各条路径中除源节点和目的节点之外没有其他任何共用节点,因此与链路不相交多路径和相交多路径相比具有更强的容错能力.本文主要讨论安全的节点不相交多路径路由协议.

基于流网络(flow network)理论,Liu 等人[7]提出了实现移动 ad hoc 网路节点不相交多路径集合的新方法,利用多次路由发现协议,设计了 k 条节点不相交路径的动态源路由协议 MNDP(multiple node-disjoint paths).最近,Ash 等人[8]改进了 MNDP 协议,提出了多企图多路径路由协议 MAMR(multiple attempt multipath routing).MAMR 协议在不改变 MNDP 协议基本结构的情况下提高了路由协议的执行效率.上述路由协议主要关注节点不相交多路径的可实现性和效率问题,但是,如果存在主动攻击者,本文发现上述路由协议不能抵抗 active-n-m 攻击[9],存在一定的安全性问题.

安全路由是 MANET 重要的安全需求,目前提出的几个多路径“安全”路由算法试图解决路由协议的安全问题,如 SDMSR[10],SecMR[11],SRP[12]等.然而,文献[10,11]没有用严格的数学方法分析 SDMSR 和 SecMR 的安全性.文献[12]虽用 BAN 逻辑形式化方法分析了 SRP 协议的安全性,但文献[13,14]发现 SRP 仍存在安全缺陷.路由协议的安全定义和路由协议可证明安全的相关方法和技术一直是网络安全领域的难点问题.研究人员提出了一些试图分析路由协议安全性的形式化方法,但都具有一定的局限性[15,16].路由协议的安全性能够用严格的数学方法定义和分析是很有必要的.

最近,Acs,Buttyan 和 Vajda[13,14]提出了定义和分析路由协议安全性的形式化安全框架(我们称其为 ABV 框架).ABV 框架借鉴 Pfitzmann 和 Waidner[17]定义的反应式系统(reactive system)描述了路由协议的安全需求;基于攻陷的网络拓扑模型,建立了可模糊路由概念;利用不可区分的复杂性计算理论,提出了路由协议的形式化安全定义.文献[18]讨论了基于 ABV 框架的单路径路由协议 endairA.然而,在任意的和不可预测的 Internet 中,路由协议实例通常是并发执行的,ABV 框架不能描述路由协议在异步并发网络环境情况下的安全,并且 ABV 框架仅仅反映了单路径路由协议的安全问题.

基于交互式图灵机(interactive Turing machines)计算模型,Canetti 提出了通用可复合(universally compassable,简称 UC)[19]的密码协议安全定义框架,UC 安全模型能够描述密码协议在异步并发网络环境情况下的安全[20].本文将 UC 安全模型引入异步并发网络环境情况下路由协议可证明安全的研究,建立了 UC-路由

协议安全框架,简称 UC-RP(universally composable security framework for ad hoc networks routing protocol)框架.UC-RP 框架可以描述和分析并发复合情况下路由协议的安全性.UC-RP 框架的基本思路是,利用“理想函数”描述路由协议的安全需求,“协议仿真”概念定义路由协议的安全性,以及“协议复合操作理论”实现路由协议的通用可复合安全属性.在 UC-RP 框架中满足安全定义的路由协议称为 UC 安全的路由协议.

针对移动 ad hoc 无线网络,基于攻陷的网络拓扑模型,本文扩展了可模糊路由概念,提出了多路径可模糊路由集合概念,用于描述多路径路由协议;基于 UC 安全模型,提出了基于 UC-RP 框架的节点不相交多路径路由协议的形式化安全定义和可证明安全路由协议的新方法;针对 MNDP 协议存在的安全问题,提出了新的安全的移动 ad hoc 网络节点不相交多路径动态源路由协议(简记为 SMNDP 协议).SMNDP 协议辅助路由请求传播策略中,建立了中间节点路由请求传播策略的检错机制.SMNDP 协议路由应答算法中采用了消息的防篡改机制和认证机制.在 UC-RP 框架中,利用可证明安全路由协议的新方法,SMNDP 协议的安全性可以归约为消息认证码和签名机制的安全性.SMNDP 协议实现了路由发现协议的正确性、节点身份的认证性和路由消息的完整性.

1 路由协议安全定义

1.1 攻击者的能力模型

通过控制攻陷节点,攻击者能够阻止路由协议建立节点不相交多路径的功能.当考虑路由协议的安全问题时,本文假设攻击者能力模型为:

(1) 节点之间用身份相互认证,Sybil 攻击[21]无效;

(2) 根据无线通信链路特点,节点仅能够接收到通信信号强度范围内其他节点传输的信息,Wormholes 攻击[22]无效;

(3) 路由发现过程的源节点和目标节点未被攻陷.攻击者不能修改或控制未攻陷节点之间的所有通信消息;

(4) 攻击者通过攻陷节点实施攻击,并可以使用攻陷节点的所有秘密信息;

(5) 当攻陷节点相邻时,攻击者能够用任意攻陷身份假冒这些相邻节点.

1.2 基于攻陷的网络拓扑模型

在讨论 ad hoc 网络路由协议之前,假定网络节点通过邻居发现协议已建立了网络拓扑,实现了 ad hoc 网络的安全自举[23].基于攻击者能力模型,表示移动 ad hoc 网络拓扑模型的无向图 $G(V,E)$可以定义为一个构造(configuration)[13,14],简称构造 conf,如图 1 所示.本文在构造 conf 中讨论路由协议的安全问题.

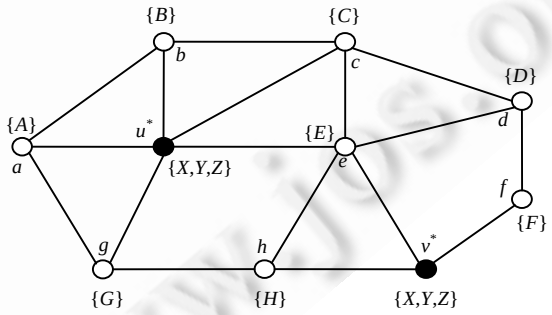

Fig.1 A configuration of network

图 1 网络构造

用Γ表示网络中节点集合 N 的所有子集 $N^{\#}$的集合(即集合 N 的幂集),攻击者可以选择任意集合 $N^{\#}\in\Gamma$并攻陷 $N^{\#}$中的所有节点.$N^{\#}$表示攻陷节点集合,如果 $N^{\#}$中的攻陷节点相邻,则多个相邻的攻陷节点定义为构造 conf

中的一个顶点;如果 $N^{\#}$中的攻陷节点不相邻,则攻陷节点具有独立性,定义为构造 conf 中的一个顶点,所有攻陷顶点集合定义为 V^*.V 中的顶点由未攻陷节点和攻陷顶点集合 V^*组成,V^*是 $N^{\#}$的子集,并且 V^*中的顶点不相邻.

根据无线通信链路特点和邻居发现协议,如果能在两个未攻陷节点之间建立无线链路,那么与这两个未攻陷节点相对应的顶点 u 和 v 之间有一条边;如果能在一个未攻陷节点和攻陷顶点集合 V^*中的某攻陷节点之间建立一条无线链路的话,那么未攻陷节点和攻陷节点相对应的顶点 u 和 v^*之间也有一条边.两个相邻攻陷节点 u^*和 v^*之间没有边,它们被看成了攻陷顶点集合 V^*中的单一顶点.

用 L 表示身份集合,L^*表示攻陷身份集合,用身份分配函数 $D:V\to 2^L$(2^L 是 L 的幂集)给 V 中的每个顶点分配身份标识.身份分配函数 D 定义如下:$\forall v\in V,D(v)=\begin{cases}1, & v\in V\setminus V^*\\ L^*, & v\in V^*\end{cases}$,其中,$l\in L\setminus L^*$.

用三元组$(G(V,E),V^*,D)$表示构造 conf,假设存在攻击者,那么实黑顶点表示 V^*中的攻陷顶点(V^*中的顶点在图 G 中不相邻),每个顶点用函数 D 分配给它的身份集合作标记.实际上,路由协议是该静态网络构造 conf 上的分布式算法,由于相邻攻陷节点看成了单一攻陷节点,构造 conf 上的顶点不相交多路径路由协议实际上是指未攻陷节点和不相邻攻陷节点不相交多路径路由协议.

1.3 可模糊多路径路由

图 1 中的身份序列$\{A,B,C,D\}$是$\{a,d\}$顶点之间一条真实存在的路径路由.当构造 conf 中顶点是由未攻陷节点构成的时候,那么满足下列条件的身份序列 $l_1,l_2,\ldots,ln(n\geqslant 2)$是一条真实存在的路径路由:

(1) 身份序列 $l_1,l_2,\ldots,l_n$ 中的每一个身份是不相同的;

(2) 在顶点集合 V 中存在一个顶点序列 $v_1,v_2,\ldots,v_n$,使得$(v_i,v_{i+1})\in E$ 并且 $D(v_i)=\{l_i\}(1\leqslant i\leqslant n)$.

图 1 中的身份序列$\{A,X,E,D\}$,$\{A,X,Y,E,D\}$,$\{A,X,Y,Z,E,D\}$等是$\{a,d\}$顶点之间同一条路径路由$\{a,u^*,e,d\}$,主动攻击者能够使用集合 L^*中的所有身份,使得身份序列路径路由与顶点序列路径路由并不一致.为了实现构造 conf 上的身份序列路径路由与真实存在的路径路由相一致,ABV 框架建立了可模糊路由概念,本文扩展了可模糊路由概念,提出了多路径可模糊路由集合概念.

定义 1(可模糊路由(plausible route)). 假设构造 $conf=(G(V,E),V^*,D)$,$l_1,l_2,\ldots,l_n$ 是身份序列,如果存在 V 中的顶点序列 $v_1,v_2,\ldots,v_k(2\leqslant k\leqslant n)$和正整数序列 $j_1,j_2,\ldots,j_k$,使得

(1) $j_1+j_2+\ldots+j_k=n$;

(2) $\{l_{J_i+1},l_{J_i+2},\ldots,l_{J_i+j_i}\}\subseteq D(V_i)(1\leqslant i\leqslant k)$,如果 $i=1,J_i=0$;如果 $i>1,J_i=j_1+j_2+\ldots+j_{i-1}$;

(3) $(v_i,v_{i+1})\in E(1\leqslant i\leqslant k)$,

则称身份序列 $l_1,l_2,\ldots,l_n$ 是一条可模糊路由.

图 1 中的身份序列$\{l_1,l_2,l_3,l_4,l_5,l_6\}=\{A,X,Y,Z,E,C\}$是可模糊路由,因为该序列可被划分成$\{A\}$,$\{X,Y,Z\}$,$\{E\}$和$\{C\}$这 4 部分,使得$\{A\}\subseteq D(a)$,$\{X,Y,Z\}\subseteq D(u^*)$,$\{E\}\subseteq D(e)$,$\{C\}\subseteq D(c)$.顶点序列 a,u^*,e 和 c 构成一条路径路由,该例中,$k=4,j_1=1,j_2=3,j_3=1,j_4=1$,那么 $J_1=0,J_2=j_1=1,J_3=j_1+j_2=4,J_4=j_1+j_2+j_3=5$.因此,该路由$\{l_1,\{l_2,l_3,l_4\},l_5,l_6\}$满足可模糊路由的定义.

定义 2(可模糊路由集合(plausible-route set)). 对任意构造 $conf=(G(V,E),V^*,D)$,假设 P 是图 G 中任意一对顶点 u,v 之间多路径路由的集合,如果 P 满足以下条件:

(1) 任意 $p_i\in P,p_i$ 是一条可模糊路由;

(2) 任意 $p_i,p_j\in P(i\neq j)$,与 p_i 和 p_j 对应的顶点集合分别是 V_i 和 V_j,并且$(V_i\cap V_j)\setminus\{u,v\}=\varnothing$,即 p_i 和 p_j 是两条除顶点 u,v 外,顶点不相交的可模糊路由,

则称 P 是顶点 u,v 之间的可模糊路由集合.

可模糊路由集合定义了未攻陷节点和不相邻攻陷节点不相交多路径路由集合.如图 1 所示,$\{\{A,G,H,X,Y,Z,F,D\},\{A,X,Y,Z,E,D\},\{A,B,C,D\}\}$是顶点 a 和 d 之间的可模糊路由集合.除源顶点 a 和 d 以外,它们分别与图 1 中顶点不相交路径$\{a,g,h,v^*,f,d\}$,$\{a,u^*,e,d\}$,$\{a,b,c,d\}$相对应.

1.4 UC-RP路由协议安全框架

完成路由发现功能并建立路径路由,是安全路由协议设计的一个本质任务.为此,需要建立一个恰当的数学模型表示路由协议,然后在该数学模型中描述协议任务需求的形式化安全定义.ABV 框架仅仅反映了单路径路由协议的安全定义,不能描述路由协议在异步并发网络环境情况下的安全状况.UC 安全模型能够描述密码协议在异步并发网络环境情况下的安全状况.本文将 UC 安全模型引入异步并发网络环境情况下路由协议可证明安全的研究,建立了 UC-RP 框架.UC-RP 框架可以描述和分析并发复合情况下路由协议的安全性.

在 UC-RP 框架中,路由协议被看作是一个 n 方计算协议$\pi.n$ 方计算协议π可以描述为一个交互式的图灵机系统,该系统由 n 个交互式图灵机 P_i 组成,其中 $0<i<n$.首先,协议π的安全服务需求被定义为“理想函数 F”,针对理想函数,存在虚拟攻击者 S(通常称为仿真器 S),该模型称为理想模型;其次,在真实的运行环境中,参与方可以实现协议的功能,同时存在真实的攻击者实体 A,该模型称为真实模型.基于“计算不可区分”概念,UC-RP 框架模型定义了一个特殊的攻击者实体“环境机 Z”,它代表着外部环境.路由协议π的安全被定义为:从环境机 z 的角度看,参与方在任何真实环境中的协议交互信息与参与方在具有可信任“理想函数”的理想模型中的协议交互信息是“计算不可区分的”,即 UC-RP 安全协议π安全实现理想函数 F.

1.4.1 真实模型(real-world model)

用 $REAL_{conf,\pi,A,Z}(k,z,r)$表示真实模型,$conf=(G(V,E),V^*,D)$,$A$ 是真实世界的攻击者,π是真实模型中运行的路由协议,k 是安全参数,z 是“环境机 Z”的输入信息,r 是随机信息集合,$r=\{r_Z,r_A,r_1,r_2,\ldots,r_n\}$.$REAL_{conf,\pi,A,Z}(k,z,r)$由一组图灵机$\{M_1,M_2,\ldots,M_n,A,Z\}$组成,$M_i$代表 V 中未攻陷顶点,A_i代表 V^*中的顶点,图灵机都是概率多项式时间图灵机.图灵机通过路由协议及相关算法调度执行,每个图灵机的行为由具体的协议决定,图灵机之间可通过纸带通信.

用 $OUT_{Real,conf,\pi,A,Z}(k,z,r)$表示真实模型的路由信息输出.当 r 均匀分布时,路由信息分布空间: $X=\{out_{Real,conf,\pi,A,Z}(k,z,r)\}_{k\in N,Z\in\{0,1\}^*}$.简记为 $OUT_{Real,conf,\pi,A,Z}$.

1.4.2 理想模型(ideal-world model)

用 $IDEAL_{conf,F,S,Z}(k,z,r)$表示理想模型,$conf=(G(V,E),V^*,D)$,$S$ 是理想世界的攻击者,F 是理想函数,k 是安全参数,z 是“环境机 Z”的输入信息,r 是随机信息集合,$r=\{r_Z,r_A,r_1,r_2,\ldots,r_n\}$.$IDEAL_{conf,F,S,Z}(k,z,r)$也由一组图灵机$\{M_1',M_2',\ldots,M_n',S,Z\}$构成,它们的定义及运行方式与真实模型中的相应图灵机类似,主要差别是理想函数 F 描述了路由协议π仅返回非错误路由的安全需求.

在具体的理想函数 F 中,理想函数 F 能够识别出包含错误路由的路由应答消息(conf 是理想函数 F 的参数),并对该路由应答消息作标记.除路由发现协议的启动者外,其他图灵机 M_i' 处理未作标记的路由应答消息与处理作了标记的路由应答消息方法相同.当路由发现的启动者收到路由应答消息时,它首先执行路由协议要求的对路由应答消息的各种验证.如果这个消息通过了所有的验证,那么它验证这个消息是否被标记为错误路由,如果是,则删除这个消息,否则,继续处理.这样定义的理想函数确保在理想模型中包含错误路由的每个路由应答消息由路由发现的启动者接收并删除,即能捕获协议π仅返回非错误路由的要求.

用 $OUT_{Ideal,conf,F,S,Z}(k,z,r)$表示理想模型的路由信息输出.当 r 均匀分布时,路由信息分布空间: $X=\{out_{Ideal,conf,F,S,Z}(k,z,r)\}_{k\in N,Z\in\{0,1\}^*}$.简记为 $OUT_{Ideal,conf,F,S,Z}$.

1.4.3 路由协议安全定义

多路径路由协议的主要步骤是:在首次路由发现中,协议使用单路径动态源路由协议发现首条参考路径 rp(reference path);在第 2 次路由发现中,中间节点根据首条参考路径和中间节点路由请求传播策略计算一条辅助路由 ap(auxiliary path);然后,当目的节点 E 收到路由请求消息时,通过单播方式发送得到的辅助路由给源节点 B,源节点根据已有的参考路径和得到的新辅助路由,利用重组算法获得两条节点不相交路径.在后续的路由发现过程中,协议将前次获得的 k 条节点不相交路径作为参考路径,并根据该参考路径和中间节点路由请求传播策略发现一条新的辅助路由,直到某次路由发现找不到新的辅助路由为止.源节点通过启动多次路由发现过程,最后得到的节点不相交路径集合就是节点不相交的最大路径集合.

协议参与方的消息格式描述如下:$(sndr,rcvr,(msg,erf))$,其中,$sndr,rcvr$ 是构造 conf 中消息发送者和接收者的

身份,例如,M_{ini},M_{tar} 分别表示路由发现的源节点和目标节点,M_i 表示路由发现的中间节点,*msg* 是协议消息,*erf* 是错误路由标记(error route flag),*erf*∈{true,false,*undef*}.具体的路由协议理想函数 $F_{Routing}$ 如下:

多路径路由协议理想函数 $F_{Routing}$.

(1) 根据从协议启动者 M_{ini} 接收的 *Startup* 消息⟨*RREQ*,l_B,l_E⟩,生成一个唯一的子会话标识 *ssid*,
保存 *Startup*(*ssid*,*RREQ*,l_B,l_E)记录并向攻击者 *S* 发送⟨*ssid*,*RREQ*,l_B,l_E,*rp*,*ap*⟩;

(2) 根据从攻击者 *S* 收到的消息(*ssid*,*RREQ*,l_B,l_E,*rp*,*ap*):
如果 *rp*=∅(首次路由发现过程),协议参与者 M_i 生成路由请求消息 *msg*,并把 *msg* 发送给 M_i 的邻居;
如果 *rp*≠∅(多路径路由发现过程),判定 *ap* 是否是正确的辅助路由.
如果通过检测,协议参与者 M_i 生成路由请求消息 *msg*,并按辅助路由转发策略发送 *msg* 给 M_i 的邻居;

(3) 根据从攻击者 *S* 收到的消息(*ssid*,*RREQ*,l_B,l_E,*rp*,*ap*):
如果 *rp*=∅(首次路由发现过程),协议参与者 M_{tar} 生成路由应答消息 *msg*,并根据 *ap* 把 *msg* 单播给邻居 M_i;
如果 *rp*≠∅(多路径路由发现过程),协议参与者 M_{tar} 生成路由应答消息 *msg*,并根据 *ap* 把 *msg* 单播给邻居 M_i;

(4) 根据从攻击者 *S* 收到的消息(*ssid*,*RREP*,l_B,l_E,*ap*,*msg*),协议启动者 M_{ini} 判定:
a) *rp*=∅(首次路由发现过程),*ap* 是否是可模糊路由.如果通过检测,接受 *ap*,生成 *rp*;
b) *rp*≠∅(多路径路由发现过程),*ap* 是否是可模糊路由和正确的辅助路由.
如果通过检测,接受 *ap*,根据重组算法获得多路径路由.

理想函数把一个消息(*sndr*,*rcvr*,*msg*)复制到协议参与方通信输入纸带之前,理想函数给消息 *msg* 附加 *erf* 标记,规则如下:

(1) 如果 *msg* 是路由请求消息 *RREQ*,那么 *erf*=*undef*;

(2) 如果 *msg* 是路由应答消息 *RREP*,并且 *msg* 所包含的路由是构造 conf 上重组不会出现非可模糊路由集合的路由,那么 *erf*=true;否则,*erf*=false.

当协议参与方 M_i 从其通信输入纸带中读取消息(*sndr*,*rcvr*,(*msg*,*erf*))时:

(1) 若 *sndr* 是它的邻居并且 *rcvr*∈{M_i},则 M_i 是该消息的目标接收者,执行理想函数 $F_{Routing}$ 要求的操作;

(2) 如果 *msg* 是 M_i 的路由应答消息并且 *erf*=false,则 M_i 执行理想函数 $F_{Routing}$ 要求的操作删除 *msg*,且把这些消息放在输出纸带 out_i 中;

(3) 如果 *msg* 不是路由应答消息,或者 M_i 不是发起者,那么 M_i 忽略 *erf* 标记,M_i 生成的路由协议消息没有标记信息,并且把这些消息放在输出纸带 out_i 中.

定义 3(路由协议安全实现理想函数 $F_{Routing}$). 令 $n\in\mathbb{N}$,$F_{Routing}$ 是路由协议理想函数,π是 *n* 方路由协议,若对任意真实模型攻击者 *A* 存在一个理想过程攻击者 *S*,使得外部环境 *Z* 对于分布空间 $OUT_{Ideal,conf,F,S,Z}$ 和 $OUT_{Real,conf,\pi,A,Z}$ 多项式时间计算不可区分,则称π安全实现 $F_{Routing}$,并表示为

$$OUT_{Ideal,conf,F,S,Z}\approx OUT_{Real,conf,\pi,A,Z} \tag{2.1}$$

由于理想函数的控制,理想世界模型中运行的理想协议不可能返回一条错误路由,那么真实世界模型中运行的路由协议也不可能返回一条错误路由,否则不存在理想世界的攻击者能够仿真该真实世界攻击者的行为.换句话说,如果路由协议是安全的,那么在真实世界模型中返回错误路由的概率是可以忽略的.与这个“可以忽略概率”相关的事实是,攻击者伪造密码学原语(如签名机制)的可能事件是小概率事件.

2 MNDP 协议及其安全性分析

2.1 MNDP协议

基于流网络 G^F 中计算最大流的 Ford-Fulkerson 方法[24],Liu 等人提出了节点不相交多路径路由协议 MNDP

协议.中间节点路由请求传播策略是MNDP协议的关键,该传播策略也称为辅助路由路由请求算法.假设源节点为 *B*,目的节点为 *E*,中间节点为 *t*,如果节点 *p* 是路由请求消息的发送者(*p* 有可能是源节点 *B*),*t* 是路由请求消息的接收者(*t* 有可能是目的节点 *E*),当节点 *t* 接收到节点 *p* 的路由请求消息(*RREQ*)时,根据节点 *t* 是否是属于参考路径 rp_i 上的节点,分别执行不同的消息传播策略,传播策略见表1.表1中,rp_x(1≤*x*≤*n*,*n* 是参考路径集合中的路径条数)表示参考路径集合 *rp* 中的某条参考路径.

Table 1 Transmission scheme of the route quest for computing the auxiliary path in MNDP

表 1 MNDP 辅助路由路由请求传播策略

Sender *p*, Receiver *t*		The transmission strategy of *t*		No.
The relation of nodes *p*, *t* and rp_x	The location relation of nodes *p*, *t* on a reference path rp_i	The style of forwarding	Identifier	
$p,t\in rp_i$	*P* is a successor of *t*	Broadcasts	Appends	1
	p is a predecessor of *t*	Discards	No	2
	p and *t* are not neighboring on rp_i	Unicasts to the predecessor of *t* on rp_i	Appends	3
$p\in rp_i$, $t\in rp_j$	No	Unicasts to the predecessor of *t* on rp_i	Appends	4
$p\in rp_i$, $t\notin rp_x$	No	Broadcasts	Appends	5
$p\notin rp_x$, $t\in rp_i$	No	Unicasts to the predecessor of *t* on rp_i	Appends	6
p, $t\notin rp_x$	No	Broadcasts	Appends	7

2.2 MNDP协议安全性分析

图2中,实黑顶点表示攻陷节点,其他节点表示未攻陷节点.图中节点的编号用于识别节点的身份,用身份序列表示一对节点之间的路由.

如果不存在主动攻击者,假设 MNDP 协议通过两次路由发现协议获得从源节点 *B* 到目标节点 *E* 的参考路径集合 *rp*={{1,4},{2,5}}.在第3次辅助路由发现协议中,节点5接收到节点1的路由请求消息中已发现辅助路由 *ap*={3,4,1}的信息时,按照 MNDP 协议传播策略(表1中的规则4)单播路由请求消息给节点2,节点2接收到节点5的路由请求消息中已发现辅助路由 *ap*={3,4,1,5}的信息时,按照传播策略(表1中的规则5)广播路由请求消息.最终,目的节点 *E* 返回的辅助路由 *ap*={3,4,1,5,2,6},源节点 *B* 根据重组算法获得节点不相交多路径{{2,6},{1,5}, {3,4}}.

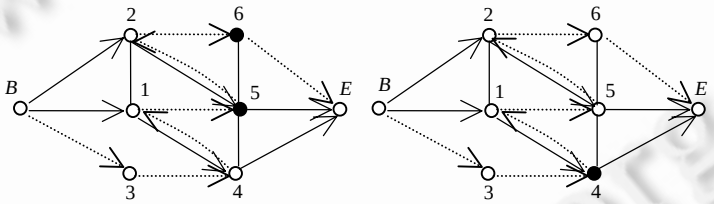

Fig.2 Configurations where attacks against MNDP

图2 MNDP 协议攻击实例

由于 MNDP 协议没有采用任何安全机制和检错机制,因此主动攻击者很容易通过攻陷中间节点破坏 MNDP 协议的辅助路由发现过程.例如,主动攻击者通过违反消息的传播策略、修改路由请求中的参考路径信息、修改路由应答中的辅助路由信息等,最终使得建立节点不相交多路径路由的协议需求无法实现,即某次路由发现得到的路径与参考路径重组无法产生节点不相交的路径集合.本文把在这种情况下得到的路径 *ap* 称为非辅助路由.active-*n*-*m* 攻击模型是指攻陷 *n* 个节点并且使用 *m* 个攻陷身份的主动攻击[9].MNDP 协议不能抵抗 active-*n*-*m* 攻击.下面通过3个实例说明 MNDP 协议存在的安全缺陷.

攻击实例 1.如图2(a)所示,假设 MNDP 协议通过两次路由发现协议获得从源节点 *B* 到目标节点 *E* 的参考路径集合 *rp*={{1,4},{2,5}}.在第3次辅助路由发现协议中,攻陷节点5接收到节点1的路由请求消息中已发现辅助路由 *ap*={3,4,1}的信息时,攻击者不按照 MNDP 协议辅助路由路由请求传播策略(表1中的规则6)单播路由请求消息给节点2,而是单播给节点 *E* 使 *ap*={3,4,1,5}.这样,当源节点 *B* 收到包含该 *ap* 的当前辅助路由的路

由应答消息时,把已发现节点不相交路径集合与本次路由发现得到的辅助路由 *ap* 重组,生成多路径路由集合{{1,5},{2,5},{3,4}},该集合中有两条相交路由通过攻陷节点 5,无法实现节点不相交多路径路由的协议需求.MNDP 协议不能抵抗这种简单的 active-1-1 攻击.

攻击实例 2.如图 2(a)所示,假设已发现从源节点 *B* 到目标节点 *E* 的参考路径集合 *rp*={{1,4},{2,5}},本次路由发现找到的辅助路由 *ap*={3,4,1,5,2,6}.当攻击者控制的节点 5 收到包含该路由的路由应答消息时,攻击者把 *ap* 修改为 *ap*={3,4,1,5},并单播修改后的路由应答消息给节点 1.这样,当源节点 *B* 收到包含该 *ap* 的路由应答消息时,把已发现节点不相交多路径集合与本次路由发现得到的辅助路由 *ap* 重组,得到路由集合{{1,5},{2,5},{3,4}},同样存在两条通过攻陷节点的相交路由,MNDP 协议不能抵抗这种 active-2-2 攻击.

攻击实例 3.如图 2(b)所示,假设已发现从源节点 *B* 到目标节点 *E* 的参考路径集合 *rp*={{1,4},{2,5}}.当攻击者控制的节点 4 收到包含 *rp*={{1,4},{2,5}}和 *ap*={3}的路由请求消息时,把 *rp* 修改为{{1,4},{2,6}}(6 是攻击者假冒的攻陷节点身份),把身份 4 追加到 *ap*={3,4},并单播该路由请求消息给节点 1,当节点 5 收到该请求消息时,把身份 5 追加到 *ap*={3,4,1,5}并广播该请求消息(节点 5 不在参考路径上,传播策略中的规则 5).这样,当目标节点 *E* 收到包含 *ap*={3,4,1,5}的路由请求消息时,生成包含该 *ap* 的路由应答消息,并按 *ap* 逆向 *B* 单播路由应答消息.当源节点 *B* 收到包含该 *ap* 的路由应答消息时,把已发现节点不相交多路径集合与本次路由发现得到的辅助路由 *ap* 重组,得到路由集合{{3,4},{1,5},{2,5}}.MNDP 协议不能抵抗这种 active-2-2 攻击.

在攻击实例 2、攻击实例 3 中,攻击者通过在攻陷节点上修改路由信息中的辅助路由 *ap* 和参考路径 *rp*,实现了攻击 MNDP 辅助路由发现过程的目的.

3 SMNDP 协议方案

针对 MNDP 协议存在的安全缺陷,本文提出了新的移动 ad hoc 网络节点不相交多路径动态源路由协议 SMNDP 协议.SMNDP 协议的路由发现过程由 3 部分组成:路由请求算法、路由应答算法和源重组算法.重组算法与 MNDP 协议类似,本文不作讨论.

SMNDP 协议与 MNDP 协议的主要区别是:

(1) 基于第 1 节提出的网络拓扑模型,SMNDP 协议利用构造 conf 中攻陷顶点不相邻这一事实,辅助路由路由请求算法中引入了检错机制,该机制把 MNDP 协议两节点路由请求传播策略扩展为 3 节点路由请求传播策略.仅通过 3 个相关节点在参考路径上的位置关系,路由请求接收者能够判断出参考路径上的攻陷节点是否遵循协议要求转发 *RREQ*;

(2) SMNDP 协议路由应答算法中引入了消息认证码防篡改机制和签名机制,通过消息认证码防篡改机制,路由发现启动者能够检测出主动攻击者是否修改路由请求中的参考路径信息,为根据当前参考路径集合计算辅助路由提供保证;签名机制为返回的辅助路由是一条可模糊路由提供保证.

3.1 SMNDP协议路由请求算法

SMNDP 协议路由请求算法包括首条参考路径路由请求算法和辅助路由路由请求算法.类似 MNDP 协议,采用 DSR 协议路由请求算法,计算首条参考路径,本文不作详述,重点讨论根据参考路径计算辅助路由的路由请求传播策略.假设源节点为 *B*,目的节点为 *E*,身份为 l_{m+1} 的中间节点收到的路由请求包含 *ap*=(l_1,…,l_{m-1},l_m)的辅助路由,l_m 有可能是源节点 *B*,l_{m+1} 有可能是目的节点 *E*.当节点 l_{m+1} 接收到该路由请求消息 *RREQ* 时,根据节点 l_{m-1},l_m,l_{m+1} 是否属于参考路径 rp^* 上的节点和它们在参考路径上的位置关系,分别执行不同的消息传播策略,传播策略见表 2.表 2 中,rp^*表示参考路径集合中任意一条路径,传播策略以括号中的编号来表示,SMNDP 的检错机制检测到 l_m 违背了 MNDP 传播策略的某条规则.

Table 2 Transmission scheme of the route quest for computing the auxiliary path in SMNDP

表 2 SMNDP 协议辅助路由路由请求传播策略

The relation of nodes l_{m-1}, l_m, l_{m+1} and rp*		The relation of nodes l_{m-1}, l_m, l_{m+1} and rp_x	The relation of nodes l_{m-1}, l_m, l_{m+1} on some path rp_x	The transmission strategy of l_{m+1}		
Receiver l_{m+1}	The last two nodes l_{m-1}, l_m in ap			The style of forwarding	Identifier	No.
$l_{m+1}\notin rp^*$	$l_{m-1}\notin rp^*$, $l_m\notin rp^*$	No	No	Broadcasts	Appends	1
	$l_{m-1}\in rp^*$, $l_m\notin rp^*$	$l_{m-1}\in rp_i$;	No	Broadcasts	Appends	2
	$l_{m-1}\notin rp^*$, $l_m\in rp^*$	$l_m\in rp_i$;	No	Drops (7)	No	3
	$l_{m-1}\in rp^*$, $l_m\in rp^*$	$l_{m-1}\in rp_i$; $l_m\in rp_j$	No	Drops (5)	No	4
		l_{m-1},$l_m\in rp_i$	l_{m-1} is a successor of l_m	Broadcast	Appends	5
			l_{m-1} is a predecessor of l_m	Drops (3)	No	6
			l_{m-1} is not a neighbor of l_m	Drops (4)	No	7
$l_{m+1}\in rp^*$	$l_{m-1}\notin rp^*$, $l_m\notin rp^*$	$l_{m+1}\in rp_i$;	No	Unicasts to the predecessor of l_{m+1} on rp_i	Appernds	8
	$l_{m-1}\in rp^*$, $l_m\notin rp^*$	$l_{m+1}\in rp_i$	Doesn't consider	Unicasts to the predecessor of l_{m+1} on rp_i	Appends	9
	$l_{m-1}\notin rp^*$, $l_m\in rp^*$	$l_m\in rp_i$; $l_{m+1}\in rp_j$	No	Drops (7)	No	10
		l_m,$l_{m+1}\in rp_i$	l_m is a successor of l_{m+1}	Broadcast	Appends	11
			l_m is a predecessor of l_{m+1}	Drops (7)	No	12
			l_m, l_{m+1} are not neighboring	Drops (7)	No	13
	$l_{m-1}\in rp^*$, $l_m\in rp^*$	l_{m-1},$l_m\in rp_i$, $l_{m+1}\in rp_j$	l_{m-1} is a successor of l_m	Unicasts to the predecessor of l_{m+1} on rp_j	Appends	14
			l_{m-1} is a predecessor of l_m	Drops (3)	No	15
			l_{m-1}, l_m are not neighboring	Drops (4)	No	16
		$l_{m-1}\in rp_i$, l_m,$l_{m+1}\in rp_j$	l_m is a successor of l_{m+1}	Broadcast	Appends	17
			l_m is a predecessor of l_{m+1}	Drops (5)	No	18
			l_m, l_{m+1} are not neighboring	Drops (5)	No	19
		l_{m-1},$l_{m+1}\in rp_i$, $l_m\in rp_j$	Doesn't consider	Drops (5)	No	20
		l_{m-1},l_m,$l_{m+1}\in rp_i$	l_{m-1} is a successor of l_m l_m is a successor of l_{m+1}	Broadcast	Appends	21
			l_{m-1} is a predecessor of l_m or l_m is a predecessor of l_{m+1}	Drops (3)	No	22
			l_{m-1}, l_m are not neighboring or l_m, l_{m+1} are not neighboring	Drops (4)	No	23
		$l_{m-1}\in rp_i$, $l_m\in rp_j$, $l_{m+1}\in rp_k$	No	Drops (5)	No	24

3.2 SMNDP协议路由应答算法

假设当前参考路径集合为 rp,SMNDP 协议的路由应答算法如下:

SMNDP 协议路由应答算法.

(a) 目的节点 E 处理路由请求 $RREQ$:目的节点 E 收到路由请求 $RREQ$:$\langle ssid,RREQ,l_B,l_E,rp,ap=(l_1,\ldots,l_i,\ldots,l_n)\rangle$ 目的节点 E 对源与目标节点的身份 l_B,l_E,和 ap 生成签名 Sig_{l_E},并且用与 B 协商的密钥 $K_{B,E}$ 生成对 sid,rp 的消息认证码 $MAC_{K_{B,E}}(ssid,rp)$ 以及生成路由应答消息$\langle ssid,RREP,l_B,l_E,ap,MAC_{K_{B,E}}(ssid,rp),Sig_{l_E}\rangle$.

随后,目的节点 E 把该 $RREP$ 单播给 ap 中的最后一个节点 l_n,并删除 $RREQ$ 其他副本.

(b) 中间节点 i 处理路由应答消息 $RREP$:中间节点 i 收到路由应答消息 $RREP$ 时,验证自己的身份 l_i 是否属于 ap,l_i 的前驱(源节点在 ap 中没有前驱)和后继(目的节点在 ap 中没有后继)是 l_i 的邻居以及验证 ap 中 l_i 后面的节点和目标节点的签名,如果验证失败,则节点 i 删除该 $RREP$,否则节点 i 对 l_B,l_E,ap 生成签名 Sig_{l_i} 以及生成路由应答消息:$\langle ssid,RREP,l_B,l_E,ap,MAC_{K_{B,E}}(ssid,rp),Sig_{l_E},Sig_{l_n},\ldots,Sig_{l_i}\rangle$.

(c) 源节点 B 处理路由应答消息 $RREP$:$\langle ssid,RREP,l_B,l_E,ap,MAC_{K_{B,E}}(ssid,rp),Sig_{l_E},Sig_{l_n},\ldots,Sig_{l_1}\rangle$.

(1) $rp=\varnothing$,验证 ap 中第 1 个节点是否是它的邻居以及 *RREP* 中的所有签名,如果这些验证成功,B 接受 ap 作为第 1 条参考路径,否则删除 *RREP* 并启动新的路由发现;(2) 如果 $rp\neq\varnothing$,除验证 ap 中第 1 个节点是否是它的邻居以及 *RREP* 中的所有签名外,源节点 B 还根据当前参考路径集合 rp 验证消息认证码 $MAC_{K_{B,E}}(ssid,rp)$ 是否正确,如果这些验证成功,B 接受 ap 作为一条新的辅助路由,否则删除 *RREP* 并启动新的路由发现.

3.3 SMNDP协议

SMNDP 协议路由发现过程描述如下:

SMNDP 协议路由发现算法.

(a) 源节点 B 广播路由请求$\langle ssid,RREQ,l_B,l_E,rp,ap\rangle$,其中,$l_B,l_E$ 是源节点与目的节点的身份,$ssid$ 是路由发现标识符,rp 是源节点 B 路由缓存表中已发现的节点不相交多路径集合,ap 为空,用于记录首条参考路径或辅助路由;

(b) 中间节点 i 处理路由请求 $RREQ$:$\langle ssid,RREQ,l_B,l_E,rp,ap=(l_1,\ldots,l_{m-1},l_m)\rangle$.如果中间节点 i 已处理过该 *RREQ*,则删除该 *RREQ*;否则,如果 $rp=\varnothing$,按 DSR 的路由请求算法向目的节点转发 *RREQ*;如果 $rp\neq\varnothing$,按表 2 所述方式处理路由请求;

(c) 目的节点 E 生成路由应答 *RREP* 和中间节点 i 处理路由应答 *RREP*:如 SMNDP 协议路由应答算法所示;

(d) 源节点 B 处理路由应答 *RREP* 并重组:源节点 B 处理 *RREP* 见 SMNDP 协议路由应答算法,重组算法与 MNDP 协议的重组算法类似,参见文献[7];

(e) 重复步骤(a)~步骤(d),直到已发现所需的 k 条节点不相交路径或找不到新的辅助路由为止.

4 SMNDP 协议的安全性分析

引理 1. 基于攻陷的网络拓扑模型,在 UC-RP 框架理想模型中,如果签名机制对选择消息攻击是安全的,那么 SMNDP 协议返回 conf 上一条非可模糊路由的概率是可以忽略的.

证明:假设 SMNDP 协议某次路由发现返回的路由 $ap=(l_B,l_1,\ldots,l_n,l_E)$是构造 conf 中的一条非可模糊路由,并且源节点 B 收到的与路由 ap 相对应的路由应答消息:

$$msg=\langle ssid,RREP,l_B,l_E,ap,MAC_{K_{B,E}}(ssid,rp),Sig_{l_E},Sig_{l_n},\ldots,Sig_{l_1}\rangle.$$

进一步假设在源节点 B 中,msg 通过了由 SMNDP 协议路由应答算法要求的所有验证,这意味着 msg 中的所有签名都是正确的,攻击者没有伪造未攻陷节点的签名,源节点 B 有一个身份为 l_1 的邻居.

由构造 conf 的定义可知,攻陷顶点不可能是邻居,每个未攻陷顶点有一个分配给它的未攻陷的唯一身份,那么包括$(l_B,l_1,\ldots,l_n,l_E)$,每个路由都可以这样分割:每个未攻陷的身份形成一个分割,每个连续的攻陷身份序列形成一个分割.让 $P_1,P_2,\ldots,P_k$ 是路由$(l_B,l_1,\ldots,l_n,l_E)$的分割并且是唯一分割,身份序列$(l_B,l_1,\ldots,l_n,l_E)$是非可模糊路由意味着至少下面两种情况之一成立:

(1) 存在两个相邻分割 $P_i=\{l_j\}$和 $P_{i+1}=\{l_{j+1}\}$,l_j 和 l_{j+1} 是未攻陷的身份,但是与 l_j 和 l_{j+1} 相对应的未攻陷的顶点 u,v 不相邻;

(2) 存在 3 个相邻分割 $P_i=\{l_j\}$,$P_{i+1}=\{l_{j+1},\ldots,l_{j+q}\}$和 $P_{i+2}=\{l_{j+q+1}\}$,其中,l_j 和 l_{j+q+1} 是未攻陷身份,$l_{j+1},\ldots,l_{j+q}$ 是攻陷身份,但是与身份 l_j 和 l_{j+q+1} 相对应的未攻陷顶点 u,w 没有共同的相邻攻陷顶点.

我们来说明在以上两种情况中,攻击者肯定伪造了一个未攻陷节点的签名.

在第 1 种情况中,因为身份为 l_{j+1} 的节点未被攻陷,并且它发现路由表中其前面身份为 l_j 的节点不是它的邻居,因此,身份为 l_{j+1} 的节点不会对路由应答消息签名.这样,攻击者肯定在 msg 中伪造了签名 $Sig_{l_{j+1}}$.

在第 2 种情况中,假设攻击者没有伪造任何未攻陷节点的签名,那么身份为 l_j 的节点肯定在顶点 u 上收到了攻击者 A 在攻陷顶点 v^*(v^*与顶点 u 相邻)上转发给它的消息:

$$msg'=\langle ssid,RREP,l_B,l_E,ap,MAC_{K_{B,E}}(ssid,rp),Sig_{l_E},Sig_{l_n},\ldots,Sig_{l_{j+1}}\rangle.$$

又因为 l_{j+1} 是已攻陷节点身份,这样,未攻陷节点不可能发送具有签名 $Sig_{l_{j+1}}$ 的路由应答消息 msg'.攻击者 A

要在攻陷顶点 v^*上生成消息 msg',它肯定收到了来自与攻陷顶点 v^*相邻的另一顶点 v_x(某攻陷或未攻陷的顶点)转发的消息 $msg''=\langle ssid,RREP,l_B,l_E,ap,MAC_{K_{B,E}}(ssid,rp),Sig_{l_E},Sig_{l_n},...,Sig_{l_{j+q+1}}\rangle$.

由假设,身份为 l_{j+q+1}的节点未攻陷,攻击者 A 不可能伪造身份为 l_{j+q+1}的节点签名,那么只有身份为 l_{j+q+1}的节点在与其对应的未攻陷顶点 w 上生成并转发消息 msg'',即与攻陷顶点 v^*相邻的顶点 v_x就是未攻陷顶点 w.也就是说,攻陷顶点 v^*是与未攻陷顶点 u 和 w 都相邻的攻陷顶点,这与第 2 种情况的假设矛盾.

由以上两种情况说明,“攻击者没有伪造未攻陷节点签名”的假设不可能成立,攻击者 A 肯定伪造了一个未攻陷节点的签名.但是,如果 SMNDP 协议签名机制对选择消息攻击是安全的,攻击者 A 伪造一个未攻陷节点的签名的概率是可以忽略的.即在 UC-RP 框架的理想模型中,SMNDP 协议返回一条非可模糊路由的概率是可以忽略的. □

引理 2. 基于攻陷的网络拓扑模型,在 UC-RP 框架理想模型中,如果消息认证机制(message authentication code,简称 MAC)是安全的,那么 SMNDP 协议返回 conf 上一条非辅助路由的概率是可以忽略的.

证明:假设 ap 是 SMNDP 协议本次路由发现找到的非辅助路由,$ap=(\ldots,l_i,l_{i+1},\ldots,l_{i+q},l_{i+q+1},\ldots)$,其中,$l_i,l_{i+q+1}$是未攻陷节点的身份,分别分配给了 conf 中的顶点 u,w.$l_{i+1},\ldots,l_{i+q}$是攻击者 A 拥有的攻陷身份的任意一个序列,分配给了 conf 中的攻陷顶点 v^*,为计算该辅助路由 ap 节点 l_{i+q+1}收到的路由请求消息是

$$\langle ssid,RREQ,l_B,l_E,rp,ap=(\ldots,l_i,l_{i+1},\ldots,l_{i+q})\rangle.$$

那么在路由发现过程中,当节点 l_{i+q+1}收到该 $RREQ$ 时,对每条参考路径 $rp_x\in rp(1\leqslant x\leqslant n,n$ 是参考路径条数),节点 l_{i+q+1}要作如下验证和处理:

- $v^*\in rp_x(1\leqslant x\leqslant n)$,即 v^*在某条参考路径 rp_x上

根据 SMNDP 协议中辅助路由发现协议的传播策略 3~策略 7 以及策略 10~策略 24,节点 l_{i+q+1}能够检测出攻击者 A 在顶点 v^*上是否遵循 SMNDP 协议中辅助路由发现协议的要求转发或删除路由请求消息 $RREQ$.如果攻击者 A 未按 SMNDP 协议要求转发路由请求,节点 l_{i+q+1}将删除由攻击者 A 在顶点 v^*上转发给它的路由请求 $RREQ$,如表 2 中的传播策略 3.由于 v^*在某条参考路径 rp_x上,u 和 w 都不在参考路径上,则攻击者 A 在顶点 v^*上应把 $RREQ$ 单播给参考路径 rp_x上顶点 v^*的前驱.因此,当节点 l_{i+q+1}在顶点 w 上收到来自顶点 v^*的 $RREQ$ 时,删除该 $RREQ$ 而不转发.

也就是说,如果攻击者控制的攻陷节点在参考路径上,未攻陷节点 l_{i+q+1}根据未攻陷顶点 u,w 与攻陷顶点 v^*在参考路径集合 rp 上的位置关系转发 $RREQ$,而没有直接根据攻击者在 v^*上转发的 $RREQ$ 转发 $RREQ$.这样,由于这种错误检测机制的引入,节点 l_{i+q+1}能够检测出攻击者不按 SMNDP 协议要求转发 $RREQ$ 的错误行为,并取消其转发的 $RREQ$.攻击者要使本次路由发现得到的 ap 是非辅助路由的唯一可能是修改参考路径集合 rp.

然而,源节点 B 收到的来自目的节点 E 的路由应答消息 $RREP$ 中,包含目的节点 E 对收到的路由请求中参考路径集合 rp 和路由发现标识符 $ssid$ 的消息认证码 MAC,源节点 B 根据 MAC 和路由缓存表中已发现节点不相交路径集合,能够检测到攻击者在某攻陷节点上修改参考路径集合的攻击并删除该路由应答消息.因此,在 UC-RP 框架理想模型中,如果消息认证机制是安全的,那么 SMNDP 协议返回 conf 上一条非辅助路由的概率也是可以忽略的.

- $v^*\notin rp_x(1\leqslant x\leqslant n)$,即 v^*不在任何参考路径上

在这种情况下,当 $RREQ$ 到达 w 时,根据未攻陷顶点 u,w 和攻陷顶点 v^*在参考路径上的位置关系(表 2 中的传播策略 1、策略 2、策略 8、策略 9),节点 l_{i+q+1}无法判断攻击者是否按协议要求转发 $RREQ$,因为攻击者收到的 $RREQ$ 可能是 u 的广播消息(u 不在任何参考路径上,或 u 在某条参考路径 $rp_x(1\leqslant x\leqslant n)$上并且给 u 转发消息的顶点是路径 rp_x上顶点 u 的后继),也可能是窃听到的 u 单播给它的直接前驱的单播消息(u 在某条参考路径 $rp_x(1\leqslant x\leqslant n)$上,但给 u 转发消息的顶点既不是路径 $rp_x(1\leqslant x\leqslant n)$上顶点 u 的前驱,也不是 u 的后继),需要 ap 中的节点 l_{i-1}协助才能做出正确判断.不过,如果顶点 v^*不在参考路径上,即使攻击者不按照 SMNDP 协议执行,得到的 ap 与路由表中的可模糊路由集合在源节点重组也不会出现相交路由.因此,出现这种情况得到的路由如果是可模糊路由,并且重组仅产生可模糊路由集合的要求仍能满足,则我们把该 ap 仍当作辅助路由来看待. □

从引理 1、引理 2 我们可以看出,在 UC-RP 框架理想模型中,SMNDP 协议返回错误路由(非可模糊路由和非辅助路由)的概率是可以忽略的.

定理 1. 如果签名机制和消息认证机制是安全的,那么 SMNDP 协议是 UC-RP 框架中可证明安全的节点不相交多路径源路由协议.

证明:证明思路如下:首先,使用可证明安全的仿真器技术建立各种仿真情景;其次,证明本文的定义 3 成立.

令 A 是主动攻击者,构造一个理想过程中针对 $F_{Routing}$ 的攻击者 S(称为仿真器),在理想过程中,S 可以与理想函数 $F_{Routing}$ 和环境机 Z 交互.S 因 A 的副本 $\tilde{A}$ 调用而工作,副本 $\tilde{A}$ 与现实模型中的 A 交互.对于仿真器 S,在理想过程中的交互称为仿真器 S 的外部交互,与 A 的副本 $\tilde{A}$ 之间的交互称为仿真器 S 的内部交互.仿真器 S 的工作情况如下:

(1) 仿真首次路由发现过程

基于攻陷拓扑模型的构造 conf,存在主动攻击者 A,仿真器 S 在内部交互的仿真过程中,通过 $\tilde{A}$ 获得真实参与者 M_i(A 攻陷参与者 M_i)提供的消息($ssid$=1,$RREQ$,l_B,l_E,rp=∅,ap_1).仿真器 S 在外部交互中模仿参与者 M_i 获得从 $F_{Routing}$ 发向虚拟参与者 M_i 的消息$\langle ssid=1,RREP,l_B,l_E,rp=\varnothing,ap_1,Sig_{l_E},Sig_{l_n},...,Sig_{l_{i-1}}\rangle$.

(2) 仿真第 x 次路由发现过程

基于攻陷拓扑模型的构造 conf,存在主动攻击者 A,仿真器 S 在内部交互的仿真过程中,通过 $\tilde{A}$ 获得真实参与者 M_i(A 攻陷参与者 M_i)提供的消息($ssid=x,RREQ,l_B,l_E,rp,ap_x$).仿真器 S 在外部交互中模仿参与者 M_i 获得从 $F_{Routing}$ 发向虚拟参与者 M_i 的消息($ssid=x,RREP,l_B,l_E,ap_x,Sig_{l_E},Sig_{l_n},...,Sig_{l_{i-1}},MAC_{K_{B,E}}(ssid,rp)$).

通过上面的描述,仿真器 S 仿真了路由协议路由发现过程的全部状态.

定义 3 的证明.由于 Z 和 A 及 UC-RP 参与方交互获得的观察序列与理想过程中 Z 和 S 及在内部交互中副本 $\tilde{A}$ 的观察序列等价,Z 的观察序列的不可区分性证明转化为仿真器 S 的内部交互仿真与外部交互仿真的不可区分证明.对任意构造 $conf=(G(V,E),V^*,D)$和任意攻击者 A,在理想模型中,路由发现过程的启动者 B 收到错误路由(非可模糊路由和非辅助路由)的概率是可以忽略的,即可说明仿真器 S 仿真是完美仿真的.本文使用反证法证明不可区分性.假设 Z 可以区分仿真器 S 的行为,那么存在两种情况:

(1) 路由发现得到的路由 ap 是 conf 上的一条非可模糊路由的概率是可以忽略的.由于在目标节点和中间节点返回包含路由 ap 的路由应答消息时,SMNDP 协议中使用了签名机制,因此 ap 是非可模糊路由的唯一可能是攻击者伪造未攻陷节点的签名.那么,如果 SMNDP 协议路由应答消息中所采用的签名机制是安全的,在 UC-RP 理想模型中,路由应答消息 msg 包含的路由 ap 是非可模糊路由的概率是可以忽略的.见引理 1;

(2) 辅助路由发现得到的路由 ap 是 conf 上的一条非辅助路由的概率是可以忽略的.由引理 2 可知,SMNDP 协议的路由发现算法返回非辅助路由的唯一可能是攻击者修改参考路径集合 rp.由于 SMNDP 协议中对参考路径集合 rp 使用了防篡改机制(消息认证码),只要该机制是安全的,那么在 UC-RP 理想模型中,本次路由发现得到的路由 ap 是 conf 上的一条非辅助路由的概率是可以忽略的.

由情况(1)、情况(2)可见,在 UC-RP 理想模型中,SMNDP 协议路由发现返回错误路由(非辅助路由和非可模糊路由)的概率是可以忽略的.因此,源节点 B 重组产生非可模糊路由集合的概率也是可以忽略的.这样,SMNDP 协议是 UC-RP 框架中可证明安全的节点不相交多路径源路由协议.证毕. □

5 相关工作比较

现有移动 ad hoc 网络节点不相交多路径路由协议(如 SDMSR,SecMR 等)都可以解决一些安全问题,但这些协议的设计者仅用非形式化的方法分析协议的安全性.本文在设计 SMNDP 协议和分析其安全时,明确了攻击者的攻击模型(active-n-m 攻击),提出了路由协议 UC-RP 安全框架以及提出基于该框架的节点不相交多路径路由协议安全定义,在 UC-RP 框架中分析 SMNDP 协议的安全性.

网络中的攻陷节点可能不按协议要求转发路由请求,多路径路由协议 SDMSR,SecMR 等没有检错机制,

SMNDP协议辅助路由发现算法中采用了3节点路由请求错误检测机制.在该机制中,收到路由请求的中间节点仅判断3个相关节点在参考路径上的位置关系而不使用任何密码学操作.与MNDP协议的辅助路由发现算法相比,只增加了收到路由请求的中间节点判断3个相关节点在参考路径上位置关系的计算开销.

基于动态源路由方式的多路径路由协议,如在SDMSR等协议中,一般要求路由请求*RREQ*经过的所有中间节点都要对路由请求消息执行密码学操作.由于动态源路由协议采用泛洪技术,这意味着网络中的每个节点对经过它的每个路由请求*RREQ*执行密码学操作,这样就大大增加了网络中节点的计算开销和网络开销.但SMNDP协议仅要求返回辅助路由的路由应答消息*RREP*中采用密码学机制(签名、消息认证机制),而路由应答消息*RREP*仅由辅助路由中的节点处理,其他网络节点不参与路由应答消息*RREP*的处理,这样就能极大地减少计算和网络开销.

假设V是移动ad hoc网络中网络节点的集合,$deg(v)$是节点$v\in V$邻居节点的个数,B与E是源与目的节点,V'是源节点B与目的节点E之间的所有k条节点不相交多路径上的节点集合.通信负载是ad hoc网络路由协议复杂性和性能的主要指标.对于按需路由协议而言,通信负载主要是单播消息和广播消息.在大规模的移动ad hoc网络中,单播负载仅占广播负载的一小部分.因此,在比较这些协议的效率时,我们主要考虑广播负载,即网络节点转发路由请求的次数.SMNDP,SDMSR,SecMR协议均采用了密码学机制,假设这些方案的复杂性是相同的,这样我们仅比较协议中密码操作的次数.

在SMNDP协议中,当目的节点和中间节点返回发现的路径信息时,目的节点和中间节点要对路由应答消息签名,源节点和中间节点要验证签名.因此,签名和验证签名的密码算法操作次数是$|V'|+k\sum_{i=1}^{|V'|/k+1} i+2k$.另外,每次路由发现过程中,目的节点要对本次路由发现的参考路径生成消息认证码MAC,源节点要验证MAC,生成与验证MAC的密码算法操作次数是$2k$.因此,SMNDP协议完成路由发现的密码运算次数是$|V'|+k\sum_{i=1}^{|V'|/k+1} i+4k$.

在SDMSR协议中,与SMNDP协议类似,除目的节点与中间节点要对路由应答消息进行签名和验证签名的$|V'|+k\sum_{i=1}^{|V'|/k+1} i+4k$次密码运算外,目的节点和收到路由请求消息的中间节点都要通过源节点的签名或MAC认证路由请求消息,并且中间节点转发收到的每个路由请求(假设发现的路径长度是从大到小的排列).这样,路由请求中密码运算的次数是$\sum_{v\in V} deg(v)+2$.因此,SDMSR协议完成路由发现的密码运算次数是

$$\sum_{v\in V} deg(v)+|V'|+k\sum_{i=1}^{|V'|/k+1} i+4k+2.$$

SecMR协议的密码运算主要是在邻居认证阶段.为实现网络中节点之间的相互认证,网络中的每个节点周期性地给它的一跳邻居发送一个签名,所有邻居验证收到的签名.这样,每个节点要生成一个签名而它的所有邻居节点要验证该签名,用于邻居认证的密码运算次数是$|V|+\sum_{v\in V} deg(v)$.路由请求消息中包含源节点的一次加密和哈希运算,相对应的目的节点有一次解密和哈希运算.另外,当目的节点返回发现的k条路径时,要对这些路径信息做哈希运算,并且源节点要读取这些哈希值.因此,SecMR协议完成路由发现的密码运算次数是

$$|V|+\sum_{v\in V} deg(v)+2k+4.$$

SMNDP协议和MNDP协议都通过多次路由发现增量方式计算节点不相交多路径路由集合,在SMNDP协议和MNDP协议的每次路由发现过程中,中间节点仅转发第1次收到的路由请求.因此,一次路由发现最多转发的路由请求次数是$|V|-1$.那么,找到k条路径k次路由发现过程最多需转发$k(|V|-1)$次路由请求.

SDMSR协议和SecMR协议通过单次路由发现计算节点不相交多路径路由集合.从一次路由发现找到的多条路径中,在路由发现的源节点B或目标节点E选择节点不相交多路径集合.因此,这两个协议都要求中间节点转发所有收到的路由请求.这样,SDMSR协议和SecMR协议至少需转发的路由请求次数应是$|V|-1$,最多需转发的路由请求次数是$\max_{v\in V-\{B,E\}} deg(v)\times(|V|-2)+1-deg(E)$.

本文对 SMNDP 协议以及相关协议方案的比较结果见表 3.

Table 3 Comparison of multiple node-disjoint paths routing

表 3 节点不相交多路径源路由方案比较

	MNDP	SMNDP	SDMSR	SecMR
Adversarial model	No	Active-*n*-*m* attack	No	No
Security model	No	UC-RP	No	No
Security definition	No	Yes	No	No
Error check	No	Yes	No	No
Cryptographic primitives	No	Signature, MAC	*RSA-TC*(*n*,2), Signature, MAC	Signature, Hash, Public key encryption
Number of cryptographic operations	No	$\|V'\|+k\sum_{i=1}^{\|V'\|/k+1} i+4k(\|V'\|<\|V\|)$	$\sum_{v\in V} deg(v)+\|V'\|+k\sum_{i=1}^{\|V'\|/k+1} i+4k+2$	$\|V\|+\sum_{v\in V} deg(v)+2k+4$
Number of route requests	At most $k(\|V\|-1)$	At most $k(\|V\|-1)$	At least $\|V\|-1$ at most $\max_{v\in V-\{B,E\}} deg(v)\times(\|V\|-2)+1-deg(E)$	At least $\|V\|-1$ at most $\max_{v\in V-\{B,E\}} deg(v)\times(\|V\|-2)+1-deg(E)$

6 结 论

鉴于现有移动 ad hoc 网络多路径路由协议中不明确的攻击者模型、不明确的路由协议安全定义以及非形式化的分析方法不能提供路由协议安全信任等问题,本文提出了基于 UC-RP 框架的可证明安全路由协议这一新方法;针对 MNDP 协议存在的安全问题,提出了新的移动 ad hoc 网络节点不相交多路径动态源路由协议(简记为 SMNDP 协议),并将基于 UC-RP 框架的可证明安全路由协议的新方法应用于 SMNDP 协议的安全分析.将可证明安全路由协议新方法应用于距离矢量多路径路由协议的安全性分析,以及对 SMNDP 协议的效率进行进一步优化,将是未来工作的重点.

References:

[1] Johnson DB, Maltz DA. Dynamic source routing in ad hoc wireless networks. Mobile Computing, 1996,12(6):10−23.

[2] Perkins C, Royer E. Ad hoc on-demand distance vector routing. Mobile Systems and Applications, 1999,24(3):59−81.

[3] Perkins CE, Bhagwat P. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In: Proc. of the Special Interest Group on Data Communications (SIGCOMM'94). New York: ACM Press, 1994. 234−244. http://portal.acm.org/citation.cfm?id=190336

[4] Lee SJ, Gerla M. SMR: Split multipath routing with maximally disjoint paths in ad hoc networks. In: Proc. of the Int'l Conf. on Communications (ICC 2001). Helsinki, 2001. 3021−3025. http://www.citeulike.org/user/tianke/article/748409

[5] Ye Z, Krishnamurthy SV, Tripathi SK. A framework for reliable routing in mobile ad hoc networks. In: Proc. of the IEEE Conf. on Computer and Communication (INFOCOM). San Fransisco: IEEE Press, 2003. 270−280. http://www.citeulike.org/group/100/article/278045

[6] Pham PP, Perreau S. Performance analysis of reactive shortest path and multi-path routing mechanism with load balance. In: Proc. of the IEEE Conf. on Computer and Communication (INFOCOM). San Fransisco: IEEE Press, 2003. 251−259. http://www.citeulike.org/user/mcnerney/article/333424

[7] Liu CW, Yarvis M, Conner WS, Guo XG. Guaranteed on-demand discovery of node-disjoint paths in ad hoc networks. Computer Communications, 2007,30(14-15):2917−2930. [doi: 10.1016/j.comcom.2007.05.028]

[8] Abbas AM, Abbasi TA. An improvement over incremental approach for guaranteed identification of multiple node-disjoint paths in mobile ad hoc networks. In: Proc. of the 2nd Int'l Conf. on Communication Systems Software and Middleware. Bangalore: IEEE Press, 2007. 1−10. http://www.ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4267999

[9] Hu YC, Perrig A. A survey of secure wireless ad hoc routing. IEEE Security and Privacy Magazine, 2004,2(3):28−39. [doi: 10.1109/MSP.2004.1]

[10] Berton S, Yin H, Lin C, Ge YM. Secure, disjoint, multipath source routing protocol (SDMSR) for mobile ad-hoc networks. In: Proc. of the 5th Int'l Conf. on Grid and Cooperative Computing (GCC 2006). Washington: IEEE Computer Society Press, 2006. 387−394. http://portal.acm.org/citation.cfm?id=1170621

[11] Kotzanikolaou P, Mavropodi R, Douligeris C. Secure multipath routing for mobile ad hoc networks. Ad hoc Networks, 2007,5(1):87−99. [doi: 10.1016/j.adhoc.2006.05.020]

[12] Papadimitratos P, Haas Z. Secure routing for mobile ad hoc networks. In: Proc. of the Communication Networks and Distributed Systems Modeling and Simulation Conf. San Antonio, 2002. 27−31. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.12.2420

[13] Acs G, Buttyan L, Vajda I. Provably secure on-demand source routing in mobile ad hoc networks. Technical Report, No.159, Int'l Association for Cryptologic Research, 2004.

[14] Acs G, Buttyan L, Vajda I. Provably secure on-demand source routing in mobile ad hoc networks. IEEE Trans. on Mobile Computing, 2006,5(11):1533−1546. [doi: 10.1109/TMC.2006.170]

[15] Marshall J. An analysis of the secure routing protocol for mobile ad hoc network route discovery: Using intuitive reasoning and formal verification to identify flaws [MS. Thesis]. Department of Computer Science, Florida State University, 2003.

[16] Yang S, Baras J. 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://portal.acm.org/citation.cfm?id=986861

[17] Pfitzmann B, Waidner M. A model for asynchronous reactive systems and its application to secure message transmission. In: Proc. of the IEEE Symp. on Security and Privacy. IEEE Press, 2001. 184−200. http://portal.acm.org/citation.cfm?id=884436

[18] Ji XJ, Tian C, Zhang YS. Security analysis of MANET routing protocol. Journal of Applied Sciences, 2007,25(1):30−34 (in Chinese with English abstract).

[19] Canetti R. Universally composable security: A new paradigm for cryptographic protocols. In: Proc. of the 42nd IEEE Symp. on the FOCS. New York: IEEE Computer Society Press, 2001. 136−145. http://ieeexplore.ieee.org/Xplore/login.jsp?reload=true&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F7601%2F20736%2F00959888.pdf%3Farnumber%3D959888&authDecision=-203

[20] Feng T, Ma JF. Universally composable security concurrent deniable authentication based on witness indistinguishable. Journal of Software, 2007,18(11):2871−2881 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/2871.htm [doi: 10.1360/jos182871]

[21] Newsome J, Shi E, Song D, Perrig A. The Sybil attack in sensor networks: analysis & defenses. In: Proc. of the 3rd Int'l Symp. on Information Processing in Sensor Networks (IPSN 2004). Berkeley: ACM, 2004. 259−168. http://portal.acm.org/citation.cfm?id=984660

[22] Hu YC, Perrig A, Johnson D. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. In: Proc. of the 22nd Annual Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM 2003), Vol.3. San Francisco: IEEE Press, 2003. 1976−1986. http://www.citeulike.org/user/burgod/article/945604

[23] Feng T, Ma JF. A general key seed management and assignment model for wireless sensor networks and application. Journal of Computer Research and Development, 2008,45(1):146−153 (in Chinese with English abstract).

[24] Cormen TH, Leiserson CE, Rivest RL. Introduction to Algorithms. 2nd ed., Cambridge: MIT Press, 1993.

附中文参考文献:

[18] 季晓君,田畅,张毓森.MANET 路由协议安全分析.应用科学学报,2007,25(1):30−34.

[20] 冯涛,马建峰.基于证人不可区分的通用可复合安全并行可否认认证.软件学报,2007,18(11):2871−2881. http://www.jos.org.cn/1000-9825/18/2871.htm [doi: 10.1360/jos182871]

[23] 冯涛,马建峰.无线传感器网络密钥种子管理和分配模型及应用.计算机研究与发展,2008,45(1):146−153.

冯涛(1970－),男,甘肃临洮人,博士,研究员,主要研究领域为安全协议复合理论,无线传感器网络安全.

马建峰(1963－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为计算机安全,密码学,移动和无线网络安全.

郭显(1971－),男,博士生,讲师,主要研究领域为 ad hoc 网络安全.

李兴华(1978－),男,博士,副教授,CCF 会员,主要研究领域为信息安全,可信计算.