

MANET 节点不相交多路径安全源路由协议

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 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 西安 710071)

³⁾(甘肃联合大学数学与信息科学学院 兰州 730010)

摘 要 多路径路由实现是移动 Ad hoc 网络(MANET)可靠运行的有效保证. 现有 MANET 节点不相交多路径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. 针对节点不相交多路径路由协议 MNDP 协议在主动攻击者安全模型中的安全缺陷,提出了可证明安全的 MANET 节点不相交多路径动态源路由协议——SMNDP 协议. SMNDP 协议路由由请求算法中,建立了中间节点路由由请求消息传播策略的检错机制,SMNDP 协议路由应答算法中建立了消息防篡改机制和身份认证机制. 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由集合概念和节点不相交多路径源路由由协议的安全定义,并应用于 SMNDP 协议的安全分析. 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.

关键词 MANET; MNDP; 可证明安全; 可模糊路由; SMNDP

中图法分类号 TP309 **DOI 号:** 10.3724/SP.J.1016.2009.01126

Multiple Node-Disjoint Paths Secure Source Routing for MANET

FENG Tao^{1),2)} GUO Xian^{1),3)} MA Jian-Feng²⁾ LI Xing-Hua²⁾

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

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

³⁾(School of Computer and Mathematics, Gansu Lianhe University, Lanzhou 730010)

Abstract The implementation of multipath routing provides guarantee for reliable running of mobile Ad hoc network (MANET). Most of existing node-disjoint multipath routing focuses mainly on establishment issues of multiple node-disjoint paths and efficiency issues of identifying multiple node-disjoint paths. Multiple Node-Disjoint Paths (MNDP) has secure faults in the secure model of active adversary. To address this issue, a provably Secure Multiple Node-Disjoint Paths source routing (SMNDP) is proposed in this paper. Error-check scheme is used for the transmission of the route quest in the algorithm of route request for SMNDP. In addition, the schemes such as the message authentication and the digital signature are used in the algorithm of route reply for SMNDP. The concept of plausible route is extended in this paper, and the definition of plausible-route set is given. And then, security definition of multiple node-disjoint paths routing is presented. The security of SMNDP can be reduced to the security of the message authentication code and the digital signature.

Keywords MANET; MNDP; provably secure; plausible route; SMNDP

收稿日期:2008-10-28;最终修改稿收到日期:2008-12-24. 本课题得到国家“八六三”高技术研究发展计划项目基金(2007AA01Z429)、国家自然科学基金(60573036,60633020,60702059)、甘肃省自然科学基金(2007GS04823)、兰州理工大学博士基金(BS14200901)资助.

冯 涛,男,1970 年生,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. E-mail: fengt@lut.cn. 郭 显,男,1971 年生,博士研究生,讲师,主要研究方向为 Ad hoc 网络安全. 马建峰,男,1963 年生,教授,博士生导师,主要研究领域为计算机安全、密码学、移动与无线网络安全. 李兴华,男,1978 年生,博士,副教授,主要研究方向为信息安全、可信计算.

1 引言

多路径路由实现是移动 Ad hoc 网络(MANET)可靠运行的有效保证. 为改进网络的可靠性和吞吐量,多路径路由协议成为近几年 MANET 邻域的研究热点. 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. 节点不相交多路径因其各条路径中除源节点和目的节点之外没有其它任何共用节点,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和负载均衡能力.

基于流网络(flow network)理论, Liu 等^[1]提出了实现 MANET 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)协议. 然而, MNDP 协议主要关注节点不相交多路径的可实现性和效率问题,而没有考虑安全问题,如果存在主动攻击者,该协议不能抵抗 active-n-m 攻击^[2].

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”路由算法试图解决安全问题,如 SecMR^[3]、SRP^[4]等. 然而,都没有用严格的数学方法分析这些协议的安全性而关注的仍是多路径实现问题. 文献[4]虽用形式化方法(BAN 逻辑)分析了 SRP 协议的安全性,但文献[5]对 SRP 协议分析发现,SRP 仍存在安全缺陷,并且已证明,路由协议的安全性不经过严格的数学证明是不可靠的.

针对无线 Ad hoc 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^[5-6],提出了多路径可模糊路由集合概念和节点不相交多路径路由协议的安全定义;基于 MNDP 协议,提出了 MANET 节点不相交多路径动态安全源路由协议——SMNDP 协议. SMNDP 协议计算辅助路径的路由请求算法中,建立了中间节点路由请求消息传播策略检错机制;SMNDP 协议路由应答算法中,建立了消息的防篡改机制和认证机制. 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.

2 节点不相交多路径源路由协议的安全定义

2.1 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完成协议需求的功能. 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 攻击无效;

(2) 节点仅能够接收到通信信号强度范围内的其它节点传输的信息, Wormholes 攻击无效;

(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,攻击者能用任意攻陷身份假冒这些相邻节点.

2.2 基于攻陷的网络拓扑模型

讨论 MANET 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 MANET 的安全自举^[7]. 基于攻击者能力模型, MANET 拓扑模型的无向图 $G(V, E)$ 可以定义为一个构造(configurations)^[5-6], 用 $conf$ 表示,如图 1.

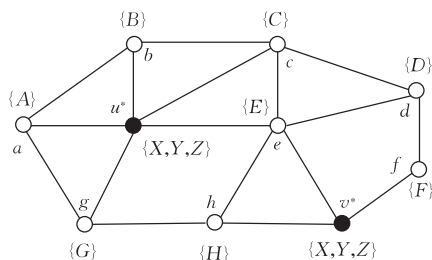


图 1 网络构造

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节点集合 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 $D: V \rightarrow 2^{L^*}$ (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:

$$\forall v \in V, D(v) = \begin{cases} l, & v \in V \setminus V^* \\ L^*, & v \in V^* \end{cases}, l \in L \setminus L^*.$$

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.

2.3 可模糊路由集合

图 1 中的身份序列 $\{A, X, E, D\}$, $\{A, X, Y, E,$

$D\}$, $\{A, X, Y, Z, E, D\}$ 等是顶点 a, d 之间同一条路径路由 $\{a, u^*, e, d\}$, 主动攻击者能够使用 L^* 中的所有身份, 使身份序列路径路由与顶点序列路径路由不一致. 为实现 $conf$ 上的身份序列路径路由与真实存在的路径路由一致, 文献[5-6]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, \dots, l_n 是身份序列, 如果存在 V 中的顶点序列 $v_1, v_2, \dots, v_k (2 \leq k \leq n)$ 和正整数序列 j_1, j_2, \dots, j_k 使得

- (1) $j_1 + j_2 + \dots + j_k = n$;
- (2) $\{l_{j_i+1}, l_{j_i+2}, \dots, l_{j_i+j_i}\} \subseteq D(V_i) (1 \leq i \leq k)$, 如果 $i=1, J_i=0$, 如果 $i>1, J_i=j_1+j_2+\dots+j_{i-1}$;
- (3) $(v_i, v_{i+1}) \in E (1 \leq i \leq k)$.

则称身份序列 l_1, l_2, \dots, 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 $\{C\}$ 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 构成图 G 中一条简单路径, 该例中 $k=4, j_1=1, j_2=3, j_3=1, j_4=1$; 那么 $J_1=0, J_2=j_1=1, J_3=j_1+j_2=4, J_4=j_1+j_2+j_3=5$, 因此该身份序列路由 $\{l_1, \{l_2, l_3, l_4\}, l_5, l_6\}$ 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 $(V_i \cap V_j) \setminus \{u, v\} = \emptyset$, 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.

如图 1 中, $\{\{A, G, H, X, Y, Z, F, D\}, \{A, X, Y, Z, E, D\}, \{A, B, C, D\}\}$ 是顶点 a 和 d 之间的可模糊路由集合, 除源顶点 a 和 d 外, 它们分别与图 1

中顶点不相交路径 $\{a, g, h, v^*, f, d\}, \{a, u^*, e, d\}, \{a, b, c, d\}$ 对应.

2.4 路由协议的安全定义

定义 3. 如果对任意构造 $conf=(G(V, E), V^*, D)$ 和任意攻击者 A , 一个节点不相交多路径源路由协议仅以可以忽略的概率返回非可模糊路由集合, 则称该协议是一个节点不相交的多路径安全源路由协议.

节点不相交多路径源路由协议的安全意味着, 任何攻击者不能使路由发现的发起者以不可忽略的概率接受非可模糊路由集合. 就是说, 节点不相交多路径安全源路由协议仅以可以忽略的概率返回一个非可模糊路由集合, 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、消息认证码)的可能是小概率事件.

3 MNDP 协议概述

假设源节点为 B , 目的节点为 E , MNDP 协议主要步骤是: 首次路由发现中, 使用动态源路由协议 DSR^[8] 计算首条参考路径(reference path); 第二次路由发现中, 基于流网络计算最大流的 Ford-Fulkerson 方法^[9], 中间节点根据首条参考路径和路由请求传播策略计算辅助路径(auxiliary path); 节点 E 生成路由由应答并单播得到的辅助路径给源节点 B ; 节点 B 根据参考路径和新辅助路径, 重组生成两条节点不相交路径. 后续路由发现中, 协议将前次获得的 k 条节点不相交路径作为参考路径, 计算新辅助路径, 直到某次路由发现找不到新的辅助路径为止. 此时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.

再假设中间节点为 t , 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. 传播策略如表 1 所示, 其中 $rp_x (1 \leq x \leq n, n$ 是参考路径集合中的路径条数) 表示参考

表 1 MNDP 协议辅助路径路由请求传播策略

节点 p, t 与 rp_x 关系	节点 p, t 在同一 rp_x 中的位置关系	t 策略		策略序号
		传播	身份	
$P, t \in rp_i$	p 是 t 后续	广播	追加	1
	p 是 t 前驱	不传播	不追加	2
	rp_i 中非邻居	单播给 rp_i 前驱	追加	3
$P \in rp_i, t \in rp_j$	无	单播给 rp_i 前驱	追加	4
$P \in rp_i, t \notin rp_x$	无	广播	追加	5
$p \notin rp_x, t \in rp_i$	无	单播给 rp_i 前驱	追加	6
$P, t \notin rp_x$	无	广播	追加	7

路径集合 rp 中的某条参考路径.

4 SMNDP 协议及其安全分析

4.1 SMNDP 协议

MNDP 协议没有采用任何安全机制和检错机制,主动攻击者可以通过攻陷中间节点违反计算辅助路径的路由请求传播策略、修改路由请求消息中的参考路径信息、修改路由应答消息中的辅助路径信息,使得 MNDP 协议建立节点不相交多路径路由的协议需求难以实现.在此情况下得到的路径本文称为非辅助路径(nonauxiliary path).

本文提出的 SMNDP 协议与 MNDP 协议不同的是:(1)基于第 2 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,计算辅助路径的路由请求算法中引入了检错机制;(2)SMNDP 协议的路由应答算法中引入了身份签

名认证机制和消息认证码(MAC)防篡改机制.

4.1.1 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径路由请求算法.类似 MNDP,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径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 $ap=(l_1,\cdots,l_{m-1},l_m)$ 的辅助路径, 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,传播策略如表 2 所示.表 2 中 rp^* 表示参考路径集合中任意一条路径,传播策略括号中的编号表示 SMNDP 的检错机制检测到 l_m 违背了 MNDP 传播策略的某条规则.

表 2 SMNDP 协议辅助路径路由请求传播策略

节点 l_{m-1}, l_m, l_{m+1} 与 rp^* 的关系		节点与 rp_x 的关系	节点在同一 rp_x 中的位置关系	l_{m+1} 策略		
消息接收者 l_{m+1}	ap 中后两节点 l_{m-1}, l_m			传播	身份	编号
$l_{m+1} \notin rp^*$	$l_{m-1} \notin rp^*, l_m \notin rp^*$	无	无	广播 RREQ	追加	1
	$l_{m-1} \in rp^*, l_m \notin rp^*$	$l_{m-1} \in rp_i$;	无	广播 RREQ	追加	2
	$l_{m-1} \notin rp^*, l_m \in rp^*$	$l_m \in rp_i$;	无	不传播(7)	不追加	3
	$l_{m-1} \in rp^*, l_m \in rp^*$	$l_{m-1} \in rp_i; l_m \in rp_j$	无	不传播(5)	不追加	4
		$l_{m-1}, l_m \in rp_i$	l_{m-1} 是 l_m 后续	广播 RREQ	追加	5
			l_{m-1} 是 l_m 前驱	不传播(3)	不追加	6
			l_{m-1}, l_m 非邻居	不传播(4)	不追加	7
$l_{m+1} \in rp^*$	$l_{m-1} \notin rp^*, l_m \notin rp^*$	$l_{m+1} \in rp_i$;	无	单播给 rp_i 上 l_{m+1} 前驱	追加	8
	$l_{m-1} \in rp^*, l_m \notin rp^*$	$l_{m+1} \in rp_i$	不需考虑	单播给 rp_i 上 l_{m+1} 前驱	追加	9
	$l_{m-1} \notin rp^*, l_m \in rp^*$	$l_m \in rp_i; l_{m+1} \in rp_j$	无	不传播(7)	不追加	10
		$l_m, l_{m+1} \in rp_i$	l_m 是 l_{m+1} 后续	广播 RREQ	追加	11
			l_m 是 l_{m+1} 前驱	不传播(7)	不追加	12
			l_m, l_{m+1} 非邻居	不传播(7)	不追加	13
	$l_{m-1} \in rp^*$	$l_{m-1}, l_m \in rp_i, l_{m+1} \in rp_j$	l_{m-1} 是 l_m 后续	单播给 rp_j 上 l_{m+1} 前驱	追加	14
			l_{m-1} 是 l_m 前驱	不传播(3)	不追加	15
			l_{m-1}, l_m 非邻居	不传播(4)	不追加	16
		$l_{m-1} \in rp_i, l_m, l_{m+1} \in rp_j$	l_m 是 l_{m+1} 后续	广播 RREQ	追加	17
			l_m 是 l_{m+1} 前驱	不传播(5)	不追加	18
			l_m, l_{m+1} 非邻居	不传播(5)	不追加	19
		$l_{m-1}, l_{m+1} \in rp_i, l_m \in rp_j$	不需考虑	不传播(5)	不追加	20
			$l_{m-1}, l_m, l_{m+1} \in rp_i$	l_{m-1} 是 l_m 后续	广播 RREQ	追加
	l_{m-1} 是 l_m 前驱或 l_m 是 l_{m+1} 前驱			不传播(3)	不追加	22
	l_{m-1}, l_m 非邻居或 l_m, l_{m+1} 非邻居			不传播(4)	不追加	23
	$l_{m-1} \in rp_i, l_m \in rp_j, l_{m+1} \in rp_k$	无	不传播(5)	不追加	24	

引理 1. 基于攻陷的网络拓扑模型,如果消息认证机制(MAC)是安全的,那么 SMNDP 协议返回 $conf$ 上一条非辅助路径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径, $ap=(\cdots l_i, l_{i+1}, \cdots, l_{i+q}, l_{i+q+1}, \cdots)$,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}, \dots, 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^* , 为计算该辅助路径 ap 节点 l_{i+q+1} 收到的路由请求消息是

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

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 $rp_x \in rp (1 \leq x \leq n, n$ 是参考路径条数), 节点 l_{i+q+1} 要做如下验证和处理:

(1) $v^* \in rp_x (1 \leq x \leq n)$, 即 v^* 在某条参考路径 rp_x 上, 根据 SMNDP 协议中辅助路径发现协议的传播策略 3~7 以及 10~24, 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 协议中辅助路径路由请求传播策略的要求, 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 ID 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, 如果消息认证机制是安全的, SMNDP 协议返回 $conf$ 上一条非辅助路径的概率是可以忽略的.

(2) $v^* \notin rp_x (1 \leq x \leq n)$, 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, 2, 8, 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 $rp_x (1 \leq x \leq n)$ 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 $rp_x (1 \leq x \leq n)$ 上, 但给 u 转发消息的顶点既不是路径 $rp_x (1 \leq x \leq n)$ 上顶点 u 的前驱, 也不是 u 的后继), 需 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由集合在源节点重组不会出现相交路由. 因此, 出现这种情况得到的路由如果是可模糊路由, 重组仅产生可模糊路由集合的要求仍能满足, 我们把该 ap 仍当作辅助路径.

4.1.2 SMNDP 协议路由应答算法

SMNDP 协议在路由应答算法中引入了节点身份认证机制(签名机制)和消息认证机制(MAC). 身份认证机制是 SMNDP 协议返回可模糊路由的保证, 消息认证机制是 SMNDP 协议返回辅助路径的保证. 假设当前参考路径集合为 rp , SMNDP 协议的路由应答算法如图 2 所示.

引理 2. 基于攻陷的网络拓扑模型, 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 $ap = (l_B, l_1, \dots, l_n, l_E)$ 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为

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

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, 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 $(l_B, l_1, \dots, l_n, l_E)$, 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, \dots, P_k 是路由 $(l_B, l_1, \dots, l_n, l_E)$ 的分割并且是唯一分割, 身份

- (1) 目的节点 E 处理路由请求 RREQ: 目的节点 E 收到路由请求
 $\langle RREQ, l_B, l_E, ID, rp, ap = (l_1, \dots, l_i, \dots, l_n) \rangle$.
 目的节点 E 对源与目标节点的身份 l_B 和 l_E , 与 ap 生成签名 Sig_{l_E} , 并且用与 B 协商的密钥 $K_{B,E}$ 生成对 ID, rp 的消息认证码 $MAC_{K_{B,E}}(ID, rp)$ 以及生成路由应答消息
 $\langle RREP, l_B, l_E, ID, ap, MAC_{K_{B,E}}(ID, rp), Sig_{l_E} \rangle$.
 随后, 目的节点 E 将该 RREP 单播给 ap 中的最后一个节点 l_n , 并删除 RREQ 其它副本.
- (2) 中间节点 i 处理路由应答消息 RREP: 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, 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
 $\langle RREP, l_B, l_E, ID, ap, MAC_{K_{B,E}}(ID, rp), Sig_{l_E}, Sig_{l_n}, \dots, Sig_{l_i} \rangle$.
- (3) 源节点 B 收到如下 RREP 时
 $\langle RREP, l_B, l_E, ID, ap, MAC_{K_{B,E}}(ID, rp), Sig_{l_E}, Sig_{l_n}, \dots, Sig_{l_i} \rangle$.
 (a) $rp = \emptyset$, 验证 ap 中第一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 作为第一条参考路径, 否则删除 RREP;
 (b) 如果 $rp \neq \emptyset$, 除验证 ap 中第一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 $MAC_{K_{B,E}}(ID, rp)$ 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径, 否则删除 RREP 并启动新的路由发现.

图 2 SMNDP 协议路由应答算法

序列 $(l_B, l_1, \dots, l_n, l_E)$ 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 $P_i = \{l_j\}$, $P_{i+1} = \{l_{j+1}, \dots, l_{j+q}\}$ 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}, \dots, 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.

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它前面身份为 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 $Sig_{l_{j+1}}$.

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:

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

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

$$msg'' = \langle ID, RREP, l_B, l_E, ap, MAC_{K_{B,E}}(sid, rp),$$

$$Sig_{l_E}, Sig_{l_n}, \dots, Sig_{l_{j+q+1}} \rangle.$$

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, 这与第二种情况的假设矛盾.

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 SMNDP 协议返回一条非可模糊路由的概率是可以忽略的.

4.2 SMNDP 协议安全性分析

SMNDP 协议的每次路由发现主要由 4 个步骤组成:

1. 为启动一次路由发现过程, 源节点 B 广播路由请求: $\langle RREQ, l_B, l_E, ID, rp, ap \rangle$, 其中 l_B, l_E 是源与目的节点身份, ID 是路由请求标识符, rp 是节点 B 得到的节点不相交路径集合, ap 为空;

2. 中间节点 i 处理路由请求 RREQ: 如果中间节点 i 已处理过该 RREQ, 删除该 RREQ; 否则, 如果 $rp = \emptyset$, 按 DSR 的路由请求算法向目的节点转发 RREQ; 如果 $rp \neq \emptyset$, 如表 2 处理路由请求;

3. 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, 如图 2;

4. 源节点处理路由应答 RREP(图 2)并重组; 重组算法与 MNDP 协议的重组算法类似, 参见文献[1].

定理 1. 如果签名机制和消息认证机制是安全的,那么 SMNDP 协议是可证明安全的 MANET 节点不相交多路径源路由协议。

证明. 仅给出主要的证明思路. 对任意构造 $conf=(G(V,E),V^*,D)$ 和任意攻击者 A ,说明路由发现过程启动者 B 收到非可模糊路由或非辅助路径的概率是可以忽略的即可,即说明:

(1)某次路由发现得到的辅助路径 ap 是 $conf$ 上的一条非可模糊路由的概率是可以忽略的. 见引理 2.

(2)某次路由发现得到的 ap 是 $conf$ 上的一条非辅助路径的概率是可以忽略的;

SMNDP 协议返回非辅助路径的唯一可能是攻击者修改参考路径集合 rp ,见引理 1. SMNDP 协议路由应答算法中对参考路径集合 rp 使用了防篡改机制(消息认证码 MAC),路由发现的启动者 B 根据 MAC 能够发现这种攻击并删除包含非辅助路径的路由应答. 因此,只要消息认证机制是安全的,本次路由发现得到的 ap 是 $conf$ 上的一条非辅助路径的概率是可以忽略的.

由(1)、(2)可见,SMNDP 协议本次路由发现返回非辅助路径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,SMNDP 协议是可证明安全的 MANET 节点不相交多路径源路由协议. 证毕.

5 总 结

建立节点不相交多路径是 MANET 的困难问题,基于 MNDP 协议本文提出了节点不相交多路径安全源路由协议 SMNDP 协议. 与 MNDP 协议不同的是,该协议的路由发现算法中采用了检错机制和密码学机制,并且证明 SMNDP 协议满足提出的安全定义. 本文主要讨论了节点不相交多路径源路由

协议的安全问题,以后将用类似方法讨论其它类型多路径路由协议(如距离适量多路径路由协议)的安全性. 再者,以后将对 SMNDP 协议的效率进行优化,如中间节点使用单一聚合签名(aggregate signature)机制降低网络开销等.

参 考 文 献

- [1] Liu Chang-Wen, Yarvis Mark, Conner W Steven, Guo Xing-Gang. Guaranteed on-demand discovery of node-disjoint paths in Ad hoc networks. Computer Communications, 2007, 30: 2917-2930
- [2] Hu Y-C, Perrig A. A survey of secure wireless Ad hoc routing. IEEE Security and Privacy Magazine, 2004, 2(3): 28-39
- [3] Kotzanikolaou Panayiotis, Mavropodi Rosa, Douligeris Christos. Secure multipath routing for mobile Ad hoc networks. Ad Hoc Networks, 2007, 5(1): 87-99
- [4] Papadimitratos P, Haas Z. Secure routing for mobile Ad hoc networks//Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference. San Antonio, Texas, 2002: 27-31
- [5] Acs G, Buttyan L, Vajda I. Provably secure on-demand source routing in mobile ad hoc networks. International Association for Cryptologic Research, Technical Report 159, 2004
- [6] Acs Gergely, Buttyan Levente, Vajda Istvan. Provably secure on-demand source routing in mobile ad hoc networks. IEEE Transactions on Mobile Computing, 2006, 5(11): 1533-1546
- [7] Feng Tao, Ma Jian-Feng. 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)
(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)
- [8] Johnson David B, Maltz David A. Dynamic source routing in ad hoc wireless networks. Mobile Computing, 1996, 12(6): 10-23
- [9] Cormen T H, Leiserson C E, Rivest R L. Introduction to Algorithms. 2nd Edition. Cambridge, MA: The MIT Press, 1993

His major research interests focus on mobile ad hoc networks security.

MA Jian-Feng, born in 1963, professor, Ph. D. supervisor. His major research interests include computer security, cryptography, mobile and wireless networks security.

LI Xing-Hua, born in 1978, Ph. D., associate professor. His major research interests include information security, trusted computing.



FENG Tao, born in 1970, Ph. D., professor. His major research interests include wireless sensor networks security, universally composable of protocols security.

GUO Xian, born in 1971, Ph. D. candidate, lecturer.

Background

Routing is a basic functionality for multi-hop mobile ad hoc networks (MANETs). These networks are decentralized, with nodes acting both as hosts and routers, forwarding packets for nodes that are not in transmission range of each other. Generally, routing is classified into two main classes: single-path routing and multi-path routing. Compared with single-path routing, multi-path routing has advantages in fault-tolerance and load sharing etc. So, multi-path routing has recently attracted extensive attentions. We are mainly concerned with the security of multiple node-disjoint paths, because security is also one of important problems for MANETs. There is no algorithm till date that claims to identify a maximal set of node-disjoint paths between a given source and a destination in a single route discovery. In fact, Ash *et al.* have proved that computing a maximal set of node-disjoint paths, from a list of paths traversed by different copies of a route request query, either at the source or at the destination, is an NP-complete problem. Based on flow-network theory, Liu et al. proposed a new method that identifies the maximal set of node-disjoint paths and designed a

Multiple Node-Disjoint Paths routing called MNDP. MNDP computes node-disjoint paths in multiple route discoveries and in an incremental fashion. However, if there exists the active adversary, MNDP can't defend against active-n-m attack, it focuses mainly on efficiency problem and implement of multi-path routing. To address the security issue, we propose a provably Security Multiple Node-Disjoint Paths (SMNDP) source routing based on MNDP. In SMNDP, we introduce error-check and cryptographic mechanisms. These two schemes provide guarantees to identify node-disjoint paths even if there exists the active adversary in the network. We analyze the security of SMNDP with a rigorous mathematical method.

This work is supported by the National Natural Science Foundation of China under grant Nos. 60573036, 60633020, 60702059, National High Technology Research and Development Program (863 Program) of China under grant No. 2007AA01Z429 and the Natural Science Grand Foundation of Gansu No. 2007GS0482, the Ph. D. Programs Foundation of Lanzhou University of Technology No. BS14200901.