软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(5):1009−1019 [doi: 10.3724/SP.J.1001.2011.03801]

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

拓扑隐藏的 MANET 安全多路径路由协议*

胡 琪[1,2], 张 娇[1,2], 张玉军[1+], 李忠诚[1]

[1](中国科学院 计算技术研究所 网络技术研究中心,北京 100190)

[2](中国科学院 研究生院 信息科学与工程学院,北京 100049)

Topology-Hiding Secure Multipath Routing Protocol for MANET

HU Qi[1,2], ZHANG Jiao[1,2], ZHANG Yu-Jun[1+], LI Zhong-Cheng[1]

[1](Network Technology Research Center, Institute of Computing Technology, The Chinese Academy of Sciences, Beijing 100190, China)

[2](School of Information Science and Engineering, Graduate University, The Chinese Academy of Sciences, Beijing 100049, China)

+ Corresponding author: E-mail: zhmj@ict.ac.cn, http:// www.ict.ac.cn

Hu Q, Zhang J, Zhang YJ, Li ZC. Topology-Hiding secure multipath routing protocol for MANET. *Journal of Software*, 2011,22(5):1009−1019. http://www.jos.org.cn/1000-9825/3801.htm

Abstract: This paper provides a detailed analysis on the threats of topology-exposure in Mobile Ad Hoc Network (MANET) and proposes a secure topology-hiding multipath routing protocol based on the analysis. In Route Discovery, the new protocol exposes no routing information in packets to hide the network topology and adopts a node-excluded mechanism to find multiple paths. During this process, this protocol implements on-demand Neighbor Discovery to verify node identities. In Route Maintenance, a fault detection mechanism is designed to provide assurance that the selected paths are available and secure. Considering the factors of both reaction time and the path length, the scheme aims to find the shortest secure path. The security analysis shows that this scheme can resist the black hole attack, the wormhole attack, the rushing attack, the sybil attack, and other types of common attacks. Through extensive simulations, results demonstrate that this approach can find many more active paths than SRP without bringing negative influences into the normal scenario. Furthermore, this solution largely improves the packet delivery ratio in the black hole attack scenario at an acceptable cost.

Key words: topology-hiding; mobile ad hoc network; routing security; multipath routing; shortest path

摘 要: 分析了移动自组网(mobile ad hoc network,简称 MANET)暴露拓扑带来的安全问题,提出了一种拓扑隐藏的安全多路径路由协议.在路由发现过程中,不在路由包中携带任何路径信息,从而有效隐藏网络拓扑.通过按需的邻居发现进行身份认证并建立路由表项,最终采用排除节点的方法实现多路径的选取;在路由维护过程中,设计了专门的错误发现机制以检验所选路径的有效性和安全性.该协议综合考虑时间因素和路径长度因素,实现了安全的最短路径确定.安全分析表明,该方案可以抵御黑洞攻击、虫洞攻击、rushing 攻击和 sybil 等典型攻击,同时对一般类型的攻击也具有抵御能力.仿真结果表明,与 SRP(secure routing protocol)这种典型的安全多路径方案相比,该方案能够找到更多节点不相交的多路径;在普通场景中,该方案没有对协议性能带来额外影响;在黑洞攻击场景中,该方案只需付出一定的信令开销即可大幅度提高数据包转发率,可有效抵御黑洞攻击.

* 基金项目: 国家自然科学基金(60803139); 国家科技支撑计划(2008BAH37B07)
收稿时间: 2008-12-24; 修改时间: 2009-06-09; 定稿时间: 2009-11-26

关键词: 拓扑隐藏;无线自组网;安全路由;多路径路由;最短路径
中图法分类号: TP393 文献标识码: A

MANET(mobile ad hoc network)是由带有无线通信收发装置的移动终端节点构成的多跳、无中心的网络.MANET 网络的主要目标是确立节点间的有效路由以实现信息的及时无误传送,因此,选路被误导将严重影响网络的正常运行.获取网络拓扑信息是很多现有攻击实施的基础,而携带在路由包中路径信息的机密性无法得到有效保证,存在暴露拓扑的安全隐患.本文分析暴露拓扑的安全隐患,提出一种拓扑隐藏的安全多路径路由协议,在隐藏拓扑的前提下仍能找到数量足够多的路径,并实现按需邻居认证和安全最短路径确定.

本文第 1 节进行问题分析.第 2 节介绍相关工作基础.第 3 节详细说明提出的方案.第 4 节进行安全分析.第 5 节进行性能分析,分析方案的建路能力、在普通场景和攻击场景的网络性能.第 6 节总结全文.

1 问题分析

网络的拓扑信息是通过携带在数据包中的路径信息进行传播的,而 MANET 网络开放介质的特点使得数据包中路径信息的机密性无法得到有效保证.携带在数据包中的路径信息可能暴露给两类节点:一类是合法的授权节点,一类是非授权的恶意节点.对于合法的授权节点,一方面收集其所在路径的路由信息,另一方面通过监听邻居节点获得路径信息和节点信息,授权节点可能利用这些信息采取自私行为或成为攻击节点的信息收集工具;对于非授权的恶意节点,一方面通过暴力方式破解数据包中的信息,另一方面利用一些投降节点来获取网络中的信息.在获得这些网络的拓扑信息后,恶意节点就会相应地实施各种攻击.

对已有的攻击类型进行分析后发现,MANET 网络现有的很多攻击手段都需要获取相应的网络拓扑信息才能得以实施.表 1 列举了网络层的几种典型攻击对网络拓扑信息的依赖关系.除了其中列举的几种攻击手段,还有很多攻击需要网络拓扑信息作为攻击的辅助工具.例如数据包监听,一般都是有针对性的对核心位置节点进行监听,因此获取网络中的拓扑信息是实现监听攻击的必要条件.

Table 1 Attacks dependence on the network topology

表 1 攻击对网络拓扑的依赖

Attack	Description	Dependence
Black hole[1]	Advertise having paths to the node it want to intercept and discard all the packets	Need routing messages
Wormhole[2]	Place the attacker in a powerful position, tunnel the data to disrupt routing	Choose the location
Sybil[3]	Present multiple identities to disrupt routing	Acquire node identities
Man-in-the-Middle[4]	Stay in the middle of nodes to monitor the communication	Get communication paths
Routing loops	Redirect the routing messages to format loop routing	Need routing messages

从上面的分析不难看出,在 MANET 网络中,携带在数据包中的路径信息无法得到有效的机密性保证,而现有的很多攻击手段都是在获取网络拓扑的基础上实施的.因此,隐藏拓扑信息将从源头上避免攻击的有效实施,这对于保障 MANET 网络的安全起着十分重要的作用.

2 相关工作

在 MANET 网络安全路由领域,近两年的研究工作集中在利用多路径提高路由协议的安全性.文献[5]综合考虑常规因素和安全因素,基于模糊逻辑来选取多条路径以增加网络的生存性.文献[6]使用门限方法基于多路径进行数据传输,可容忍一定的分片丢失.文献[7]提出“失效安全”的思想使用多路径来保证最短路径的安全性.但这些安全方案为找到多条路径往往携带大量路径信息,忽略暴露拓扑带来的安全隐患.在安全路由领域,只有 ARAN(authenticated routing for ad hoc networks)[8]提到隐藏拓扑的安全需求.在安全需求分析中,ARAN 给出了开放环境、管理环境和敌手环境 3 种环境下相应的安全需求,并在敌手环境中特别提到了隐藏拓扑的安全需求.ARAN 的实现方案本身具备拓扑隐藏的特性,但它是一种单路径的安全路由协议.

典型的 MANET 网络安全多路径路由协议包括 SRP(secure routing protocol)[9],SecMR(secure multipath

routing protocol)[10],SMORT(scalable multipath on-demand routing protocol)[7]等.SRP 辨别和丢弃虚假路由信息,确保获取正确的拓扑信息,但其不能避免恶意节点被包含在建立的路径中;同时,拓扑信息将通过路由信息暴露给敌手和未授权节点.SecMR 针对拒绝服务攻击,引入邻居发现机制保证链路到链路的安全,但需周期性地维护邻居信息,带来不可忽视的负担.此外,SecMR 可以在给定的最大跳数内找到足够多的节点不相交路径,但其路由包携带大量路径信息会带来很大的安全隐患.SMORT 使用“失效安全(fail-safe)”的思想来进行多路径的选取,其核心是保障最短路径的安全,但仅将最先到达的路径作为最短路径不能确保路径的安全性.另外,SMORT 要求路由应答消息携带完整的路径信息,同样存在暴露网络拓扑的安全隐患.

综上,现有 MANET 网络安全多路径路由协议往往在路由包中携带大量路由信息,均存在暴露网络拓扑的安全隐患.有些方案为实现链路级认证引入邻居发现机制,提高了安全性但引入大量信令开销.在确定最短路径方面,现有方案仅将路径长度或者时间作为选取最短路径的依据,难以找到安全而有效的最短路径.

3 拓扑隐藏的安全多路径路由协议

本文基于 AODV[11]提出拓扑隐藏的安全多路径路由协议(topology-hiding secure multipath routing,简称 THSMR).AODV 是一种距离向量按需路由协议,其特点是快速适应动态链路环境,内存开销小,节点不保存路径信息也不交换路由表信息.基于 AODV 的特点,本文方案通过在路由发现过程中不在路由包中携带任何路径信息实现网络拓扑信息的隐藏.THSMR 协议分为路由发现过程和路由维护过程.路由发现过程通过路由请求和路由应答两个阶段来实现;路由维护过程设计了专门的错误发现机制以保证所选路径的有效性和安全性.下面将详细阐述本协议的路由发现和路由维护过程,并说明通过这两个过程最终确定安全最短路径的方法.

3.1 路由发现过程

路由发现过程分为路由请求和路由应答两个阶段:路由请求阶段主要实现按需的邻居发现,并在中间节点建立相应的路径信息为选路做准备;路由应答阶段采用排除节点的方法实现最终的选路.此过程不会造成节点信息膨胀.中间节点仅在路由请求阶段维护所有邻居信息,选路完成后只维护其所在路径的下行邻居信息.即使某个节点处在多对源目的节点的通信路径上,也仅需为每对源目的节点分别维护一条邻居信息.而且,路由请求阶段维护所有邻居信息的时间是很短暂的,不会引起每个节点都需保存大量信息的情况发生.

路由发现过程不会出现循环路由:路由请求阶段,使用(源节点标识、广播包标识)唯一标识路由请求消息,节点不重复处理来自源节点的广播包;路由应答阶段,下一跳节点不会选用排除节点列表中的节点,而之前被选中的节点会加入排除节点列表中,同一节点不会被选中两次,因此也不会出现循环路由.

3.1.1 路由请求阶段

任意节点 A 在加入网络前都可以采取文献[12]中提出的方法获得由认证中心 T 签名的认证证书 $cert_A$:

$$T \Rightarrow A: cert_A=[ID_A,PK_A,T,Te]SK_T.$$

证书的内容包括节点的唯一标识 ID_A、节点的公钥 PK_A、签发时间 T 和有效期 Te.每个节点需要维护自己的公私钥对信息(PK_A,SK_A),并在转发路由请求消息时携带邻居认证信息 $Nmsg_A$:

$$Nmsg_A=[t,ID_A,SK_A(t,ID_A),cert_A].$$

每个节点维护一张可信邻居表,用来按需记录邻居信息,见表 2.记录的内容包括邻居节点标识、公钥信息、证书颁发时间、证书过期时间和表项的过期时间.

Table 2 Node A's trusted neighbor table

表 2 节点 A 的可信邻居表

Neighbor_ID	*Public_Key*	*T_cert*	*Te_cert*	*Te_entry*
ID_B	PK_B	T_B	Te_B	Te

源节点首先检查路由表中是否存在到目的节点的有效路径,若没有,则广播路由请求消息.方案在消息中添加了邻居认证消息,数据包格式定义如图 1 所示.其功能如下:一方面,通过携带源目的标识在中间节点建立相应

的路由表项,用于路由应答阶段选路;另一方面,通过携带邻居认证消息实现按需的邻居认证.

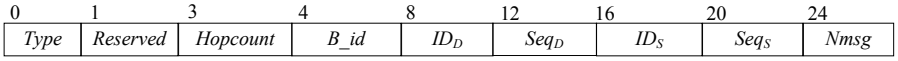


Fig.1 Structure of route request message

图 1 路由请求消息的结构

THSMR 路由请求阶段动作时序如下(*表示广播,*S* 为源节点,*D* 为目的节点,*A* 和 *B* 为任意中间节点):

Step 1. $S \xrightarrow{*} A: RREQ = [[ID_S, Seq_S, broadcast\_id, ID_D, Seq_D, hopcount]SK_S, Nmsg_S]$.

源节点 *S* 广播路由请求消息,携带源节点标识 ID_S、源节点序列号 Seq_S、广播包标识 *broadcast_id*、目的节点标识 ID_D、目的序列号 Seq_D、跳数 *hopcount* 并用源节点私钥签名,同时携带邻居认证消息 $Nmsg_S$.

Step 2. $A \xrightarrow{*} B: RREQ = [[ID_S, Seq_S, broadcast\_id, ID_D, Seq_D, hopcount]SK_A, Nmsg_A]$.

当中间节点收到路由请求消息时,依照算法 1 进行处理.源节点对于收到的路由请求消息也进行邻居认证消息验证,并将合法邻居保存到自身的可信邻居表中,最后丢弃消息.

Step 3. $B \xrightarrow{*} D: RREQ = [[ID_S, Seq_S, broadcast\_id, ID_D, Seq_D, hopcount]SK_B, Nmsg_B]$.

当目的节点收到路由请求消息时,同样依照算法 1 进行处理,只是在接受到第 1 个路由请求消息时开启等待定时器,而不是继续转发消息.

算法 1. 路由请求处理算法.

(1) 初始化:数据包 *p* 映射为路由请求消息 *rq*,获得当前节点标识 *i* 和可信邻居表 TNT_i;

(2) **if** 存在(*rq*→*broadcast_id*,*rq*→*src*) **then** 丢弃分组;

(3) **else** 记录(*rq*→*broadcast_id*,*rq*→*src*);

(4) **if** 转发节点 *rq*→*forward* 未通过认证 **then** 丢弃分组;

(5) **if** *not first one from rq*→*forward* **then** 丢弃分组;

(6) **else** 将 *rq*→*forward* 存入 TNT_i,建立路由表项 $Entry_{i\to s}$;

(7) **if** *first one from rq*→*src* **then** 转发分组;

(8) **else** 丢弃分组.

路由请求阶段实现按需的邻居发现.通过将邻居认证信息携带在路由请求消息中,邻居发现过程伴随路由发现过程一同完成.不同于文献[10]中独立的邻居发现过程需要周期性的签名和身份验证,本方案没有引入额外消息,也不需要周期性的广播.另外,路由请求阶段在中间节点建立有效路径,为选路做好准备.

3.1.2 路由应答阶段

当目的节点等待定时器超时后,进入路由应答阶段.路由应答阶段通过广播路由应答消息来实现,其数据包格式定义如图 2 所示.路由应答消息的功能就是实现选路.利用路由请求阶段在中间节点建立的路由表项,通过排除节点列表选择合适的下一跳节点,在中间节点实现节点不相交多路径的选取.

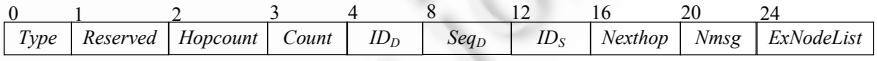


Fig.2 Structure of route reply message

图 2 路由应答消息的结构

路由应答消息添加排除节点列表和下一跳节点字段实现选路.下一跳节点字段给出当前节点选中的需要处理该路由应答消息的下一跳节点信息,排除节点列表字段记录不能作为转发路由应答消息的下一跳节点.

THSMR 路由应答阶段动作时序如下(*表示广播,*S* 为源节点,*D* 为目的节点,*A* 和 *B* 为任意中间节点):

Step 1. $D \xrightarrow{*} B: RREP = [[ID_S, ID_D, Seq_D, nexthop, ExNodeList]SK_D, Nmsg_D]$.

目的节点 *D* 检查邻居表,将路由请求阶段的所有邻居节点添加到排除节点列表,并广播路由应答消息.消息

中携带源节点标识 ID_S、目的节点标识 ID_D、目的序列号 Seq_D、下一跳节点信息 *nexthop* 和排除节点列表 *ExNodeList* 并用目的节点私钥签名,同时携带目的节点的邻居认证消息 $Nmsg_D$.

Step 2. $B \xrightarrow{*} A: RREP = [[ID_S, ID_D, Seq_D, nexthop, ExNodeList]SK_B, Nmsg_D]$.

中间节点收到路由请求消息时,依据算法 2 进行处理:若为目的节点一跳邻居,则通过检查自身标识是否在排除节点列表字段中来判断是否处理消息;若不为目的节点一跳邻居,则通过检查自身是否为下一跳字段中标识的被选中节点来判断是否进行消息转发.

Step 3. $A \xrightarrow{*} S: RREP = [[ID_S, ID_D, Seq_D, nexthop, ExNodeList]SK_A, Nmsg_D]$.

源节点收到路由应答消息,同样依据算法 2 进行处理:在路由表中建立一条到目的节点的表项,保存消息中携带的目的节点身份信息,并在接受到第 1 个路由应答消息时开始收集路径信息.

算法 2. 路由应答处理算法.

(1) 初始化:数据包 *p* 映射为路由应答消息 *rp*,获得当前节点标识 *i* 和可信邻居表 TNT_i;

(2) **if** *i* 为 *rp*→*src* 的邻居 **then**

(3) **if** *rp*→*src*∈ TNT_i **then** 丢弃分组;

(4) **else** 将 *rp*→*src* 存入 TNT_i,建立路由表项 $Entry_{i\to d}$;

(5) **if** *i*∉*rp*→*ExNodeList* **then** 丢弃分组;

(6) 标记 $Entry_{i\to s}$ 为不可选,满足 $Entry_{i\to s}$→*nexthop*∈*rp*→*ExNodeList*;

(7) 依 $l_{\min}$ 取 $Entry_{i\to s}$→*nexthop* 为 *rp*→*nexthop*;

(8) **if** 无可用 *rp*→*nexthop* **then** 丢弃分组;

(9) **else** 将 *rp*→*nexthop* 加入 *rp*→*ExNodeList*,转发 *rp*;

(10) **else if** *rp*→*forward*∉ TNT_i **then** 丢弃分组;

(11) **if** *has forwarded* 路由应答 *rp* **then** 丢弃分组;

(12) 标记 $Entry_{i\to s}$ 为不可选,满足 $Entry_{i\to s}$→*nexthop*∈*rp*→*ExNodeList*;

(13) **if** *i*≠*rp*→*nexthop* **then** 丢弃分组;

(14) 依 $l_{\min}$ 取 $Entry_{i\to s}$→*nexthop* 为新的 *rp*→*nexthop*;

(15) **if** 无可用 *rp*→*nexthop* **then** 丢弃分组;

(16) **else** 将 *rp*→*nexthop* 加入 *rp*→*ExNodeList*,创建 $Entry_{i\to d}$,转发 *rp*.

以图 3(a)中 9 个节点网络为例(原始拓扑图),分析本方案建路过程.选取仅转发第 1 个路由请求消息的多路径方案[9,13,14]作为对比方案,简称 OFC(only first copy).图 3(b)和 3(c)显示(路由请求阶段),在路由请求阶段,本文方案没有对网络的连通性造成任何影响,每个节点为其合法邻居建立一条路由缓存消息.而 OFC 方案由于只转发并保存第 1 次收到的路由请求消息,因此对网络连通性造成很大的影响.图 3(d)和 3(e)显示(路由应答阶段),在路由应答阶段,本文方案最终返回 3 条节点不相交多路径 0-1-5-8,0-2-4-6-8 和 0-3-7-8.而 OFC 方案由于受到路由请求阶段保存路径信息的限制,且采用只处理第 1 个 RREP 消息的转发机制,只得到两条节点不相交路径 0-1-5-8 和 0-2-4-7-8.

本方案使用排除节点列表和下一跳字段在中间节点有效完成选路过程.通过广播排除节点信息,极大地减小了选路时后续节点选择同一节点的概率.下一跳字段保证路由应答消息的有效传播,也降低网络中的信令开销.选路过程在中间节点实现,降低了源目的节点的处理开销.因此,选路过程所需的开销很小.

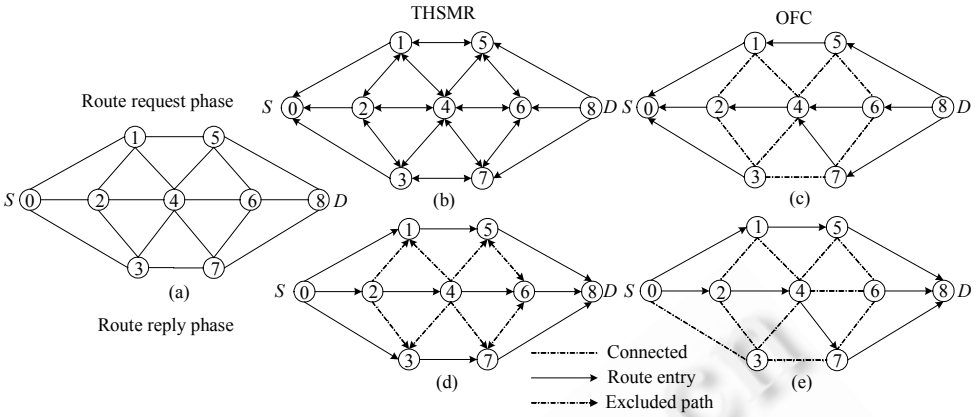
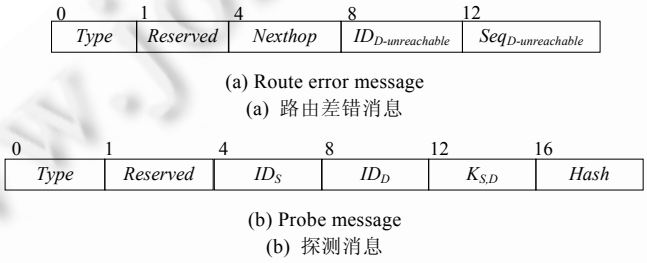


Fig.3 How to build multiple paths during route discovery

图 3 如何在路由发现过程中建立多条路径

3.2 路由维护过程

由于路由发现过程隐藏网络拓扑,多路径的选取是在中间节点完成的.为了确保所选路径的有效性和安全性,本方案设计了专门的错误发现机制来实现路由维护.错误发现机制包含两种路由消息:路由差错消息和探测消息.报文格式定义如图 4 所示.路由差错消息和 AODV 类似,探测消息为本方案新引入的消息.



(a) Route error message

(a) 路由差错消息

(b) Probe message

(b) 探测消息

Fig.4 Structure of route maintenance message

图 4 路由维护消息的结构

探测消息用数据包头进行封装,类型字段 *flag*=0 表示源到目的,*flag*=1 表示目的到源.对称密钥字段填充目的节点公钥加密的对称密钥 $PK_D(K_{S,D})$,$K_{S,D}$ 为源和目的节点通信共享密钥,目的节点使用 $K_{S,D}$ 对探测消息中携带的哈希值进行验证.哈希值由下列方式计算:

$$Value_{hash}=hash_{K_{S,D}}(ID_S,ID_D,Seq,hopcount).$$

路由差错消息的功能是在路由维护阶段进行可达性维护.当出现链路断开或者节点不可达的情况时,发现节点将发送路由差错消息,把目的不可达消息沿反向路径单播至源节点并对消息签名.

探测消息实现以下 3 个方面的验证:

第一,配合路由差错消息检测所选路径的可达性.如果路径不可达,源节点无法收到目的节点的探测应答消息,则不选择此路径转发数据,可在一定程度上减少丢包.

第二,探测是否有恶意节点丢包.探测消息被伪装成数据包,黑洞节点会将其作为普通数据包进行丢弃.源节点无法收到探测应答包,不会使用该路径从而绕开黑洞节点减少数据包损失.

第三,实现端到端的认证.探测消息携带被目的节点公钥加密的共享密钥 $K_{S,D}$,哈希值确保目的节点可以验证共享密钥的有效性,实现完整的端到端认证.

3.3 安全最短路径确定

现有 MANET 网络路由协议使用时间或者路径长度作为最短路径的判断依据,会分别遭受 rushing 和虫洞攻击,无法保证最短路径的安全性.本文提出的方案综合考虑时间和路径长度的影响,设计了一种安全的最短路径确定方法:考虑路径长度因素,在路由请求阶段缓存所有邻居路由请求消息,并在路由应答阶段采用路径长度最短的原则进行选路;考虑时间因素,在路由维护过程使用时间作为最短路径的最终判决标准.

该方法的合理性在于:路由发现过程发送的路由包是广播包,容易遭受 rushing 攻击,使用路径长度选路可以有效抵御 rushing 攻击;路由维护过程使用的探测消息是单播转发不会遭受 rushing 攻击,使用时间作为判断标准,消除了所选路径受虫洞攻击的影响.此外,探测消息排除黑洞节点所在的路径.所以,最后确定的最短路径可以抵御黑洞、虫洞和 rushing 攻击,是一条安全而准确的最短路径.

4 安全性分析

本节对方案抵御各种攻击的能力进行分析.着重分析方案在抵御几种典型攻击方面的表现,并简要分析对于一般类型的攻击,方案所采取的应对措施.

黑洞攻击:节点通过谎称拥有到目的节点的路径,将所有流经数据包都丢弃的攻击行为.典型攻击过程为:源节点 S 广播路由请求消息 $S\rightarrow *:RREQ$,攻击节点 A 回复路由应答并携带到达目的的路径 $R_{AD}:A\rightarrow S:R_{AD}\in RREP$,$S$ 发送数据包 $P_a:S\rightarrow A:P_a$,A 则丢弃所有 P_a.本文方案不允许中间节点 A 应答路由请求消息,且路径 R_{AD} 无法携带在数据包中.被丢弃数据包 P 满足 $P_a\in P$ and $P_r\notin P$,将 $PROBE$ 伪装成 P_a,则 A 将丢弃 $PROBE.S$ 无法收到探测应答则不在此路径转发数据,绕开黑洞节点,避免了不必要的数据损失.

虫洞攻击:合谋节点通过建立私有隧道实施攻击,能造成比实际路径短的虚假路由.典型攻击过程为:合谋节点依据网络拓扑 t 选取核心区域插入位置 p_1 和 p_2,满足 $p_1,p_2\in key(t)$.本文方案隐藏网络拓扑,合谋节点很难获取拓扑 t,从而无法有效选取 p_1 和 p_2.实施攻击时,攻击节点将实际路径长度 l 修改为 l',满足 $l'<l_{\min}$($l_{\min}$ 为最短路径长度),依路径长度选路的路由机制将受到影响.而传输时间 t 是客观值,不受路径长度影响.本文方案采用时间作为最终判决,将有效抵御虫洞攻击改变路径长度的影响.

Rushing 攻击:一种高效的拒绝服务攻击,对任意一种以固定方式转发路由请求消息的路由协议都能有效地实施攻击.典型攻击过程是:为减小冲突,无线网络广播包转发时会随机延迟 t_d 满足 $0<t_d\leqslant\Delta t_d$,攻击节点则不作延迟震荡 $t_d=\Delta t_d=0$,使其转发的数据包更快到达,导致合法路由请求消息被丢弃.本方案使用邻居认证信息 $Nmsg_A$ 保证路由请求消息的合法性,并保存所有合法路由请求消息;选路时,采用路径长度 l 作为依据,不受路由请求消息到达先后时间 t 的影响,可以有效抵御 Rushing 攻击.

Sybil 攻击:恶意节点通过扮演不同的身份来扰乱路由发现的攻击方式.典型攻击过程为:攻击节点 A 设法获得网络中合法节点身份信息 $\{I_1,I_2,I_3,\ldots,I_n\}$,然后伪装成合法节点 $\{I_p,I_q,\ldots\}\subseteq\{I_1,I_2,I_3,\ldots,I_n\}$,同时参与多条路径的通信.本文方案不携带路径信息和节点列表,攻击节点 A 很难获取其他节点身份信息;此外,方案采用身份认证的方式保证节点只有唯一的合法身份.因此,方案可以有效抵御 Sybil 攻击.

一般类型攻击:一般路由协议容易遭受的攻击有篡改、假冒、虚构.对于篡改路由消息的攻击,本文方案要求每个数据包都必须由转发节点进行签名,因此任何恶意的修改都会被发现.对于假冒节点身份的攻击,方案采用集中授权的方式保证只有授权节点才可以参与网络;同时,邻居认证实现了链路级的身份认证.对于虚构消息的攻击,方案不能完全消除这种攻击,授权节点可能发送虚假消息,但是不可抵赖.

5 性能分析

为了对方案进行性能评价,使用 NS-2(network simulator-2)进行系统仿真.仿真中,节点依据随机游走模型进行移动,传输范围为 250 米;使用 802.11 作为链路层协议,CBR(constant bytes rate)作为会话数据流,信道能力为 2 兆位/秒.SRP 是一种典型的安全多路径协议,很多安全多路径方案[10,15,16]都将 SRP 作为比较方案来分析自身的性能.本方案与其他安全多路径方案的关注点不同,不具备可比性,因此选用公认的 SRP 作为性能分析的比较

方案.

5.1 建路能力

选取 1000m×1000m,100 个节点的静态场景对建路能力进行评估.在不同源目的节点最短距离下,对比本方案和 SRP 的平均建路能力.图 5 显示,随着源目的节点对间最短距离的增大,平均建路数呈下降趋势;本方案的平均建路数比 SRP 多 1.5 条左右;最短距离高达 4 跳时,本方案仍能找到 3 条以上的路径.

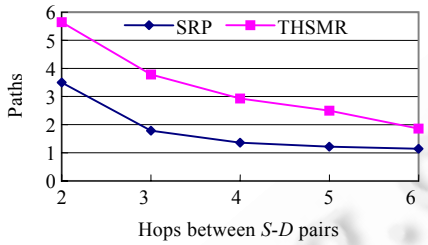


Fig.5 Capability of path finding

图 5 建路能力

5.2 场景分析

典型地,选取 670m×670m,50 个节点的场景[10],对 THSMR 和 SRP 在普通场景和黑洞场景下的性能进行分析比较.仿真时间 800 秒,前 160 秒内产生 CBR 连接,最大连接数为 10.数据包为 512 字节,发包速率为 1 包/秒.节点以 0~12 米/秒速度运动,停留时间为 30 秒[7,8].

本文方案的路由收敛时间受目的节点等待定时器配置参数影响.本实验场景中的等待时间经验值为 0.3 秒,此参数下的平均路由收敛时间,THSMR 约为 0.4 秒,SRP 约为 0.2 秒.造成差异的原因为:第一,为找到更多节点不相交多路径,THSMR 选取相对更长的路径来绕开其他节点;第二,THSMR 等待最后一个路由请求消息到达后才发送路由应答消息.THSMR 付出一定路由收敛时间的代价,但找到更多节点不相交多路径,减少了路由发现的次数.

方案选用的评价参数如下:

- 数据包转发率(packet delivery ratio,简称 PDR):

$$\overline{PDR}=\frac{\sum packet\ received\ by\ desitination\ node}{\sum packets\ sent\ by\ source\ node}\times 100\%.$$

- 数据包端到端延时(end-to-end delay for data packet,简称 EDP):

$$\overline{EDP}=\frac{\sum time\ from\ sending\ to\ receiving\ for\ received\ packets}{\sum num\ of\ packets\ correctly\ received}.$$

- 每个成功发送的数据包的平均信令开销(route-level messages per correct delivery,简称 RMD):

$$\overline{RMD}(pkt)=\frac{\sum message\ packets\ on\ route\ layer}{\sum packets\ correctly\ received},$$

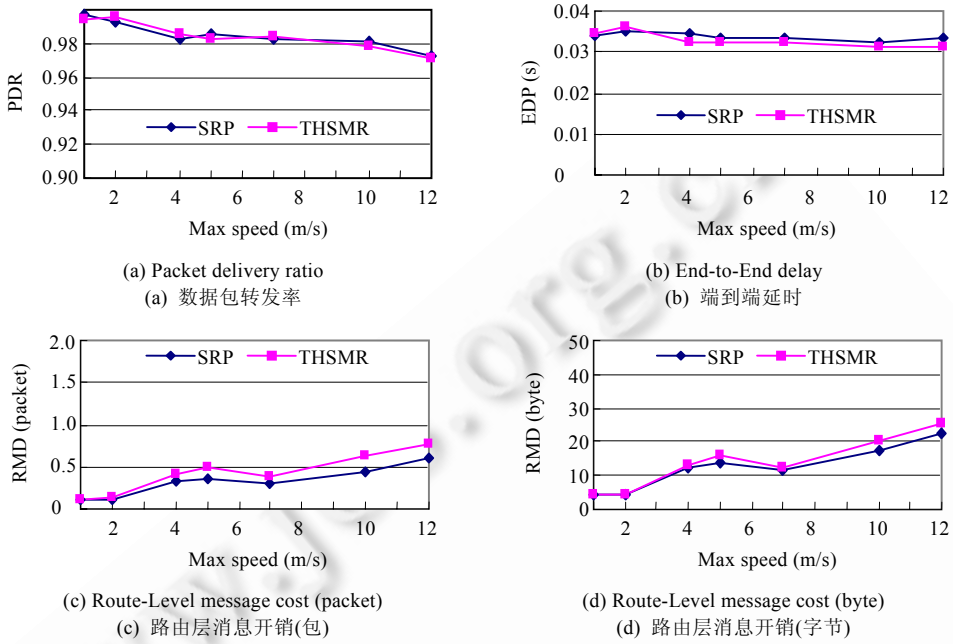
$$\overline{RMD}(bytes)=\frac{\sum message\ size\ on\ route\ layer}{\sum packets\ correctly\ received}.$$

5.2.1 普通场景

首先分析在普通场景下本文方案对协议性能的影响.选取节点运动的最大速率为横坐标,分析数据包转发率,端到端延时和平均信令开销随速率的变化情况.图 6(a)显示,两种方案的数据包转发率随速度的提高呈下降趋势,但均高达 97%以上.图 6(b)显示,在端到端延时方面,THSMR 与 SRP 相当,保持在 0.03 秒~0.035 秒之间.图 6(c)和图 6(d)显示,随着速度的提高,信令开销呈上升趋势.其中,THSMR 和 SRP 在信令开销方面表现相

当,THSMR 略高于 SRP.这是由于 THSMR 引入了探测消息,携带邻居发现信息和排除节点列表信息,而 SRP 本身携带路径信息,因此两者信令开销相当.

从上述性能效果图中可以看出,在普通场景下,THSMR 各个性能参数均和 SRP 协议相当,对性能几乎没有影响.而 THSMR 具有拓扑隐藏的特性,实现了按需的邻居发现,并可以安全确定最短路径,这些对于安全性能的提升几乎没有付出额外的代价.



(a) Packet delivery ratio
(a) 数据包转发率

(b) End-to-End delay
(b) 端到端延时

(c) Route-Level message cost (packet)
(c) 路由层消息开销(包)

(d) Route-Level message cost (byte)
(d) 路由层消息开销(字节)

Fig.6 Performance in the normal scenario

图 6 普通场景下的性能

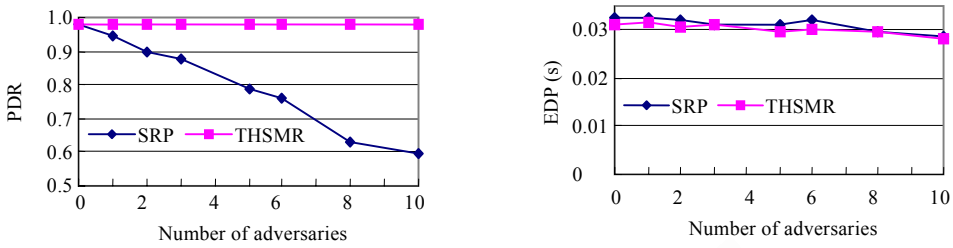
5.2.2 黑洞场景

黑洞攻击在 MANET 网络中极易发生,很多安全方案[17]也将黑洞攻击作为典型场景来进行仿真评价.采用与文献[17]相同的方法,恶意节点通过丢弃所有数据包来仿真此攻击.选取恶意节点数为 1~10 的攻击场景,节点以 0~10m/s 的速度进行移动.仍然采用上述性能参数,对两种方案进行性能比较.

图 7 为两种方案在黑洞场景下的数据包转发率,端到端延时和平均信令开销的效果图.图 7(a)显示,SRP 随着恶意节点数的增加,数据包转发率呈明显的下降趋势,而 THSMR 则一直保持在 97%以上.图 7(b)显示,在端到端延时方面,两种方案的效果和恶意节点数为 0 的普通场景相当.图 7(c)和图 7(d)显示,THSMR 的信令开销高于 SRP,且呈缓慢上升趋势.这是由于 THSMR 通过发送探测消息避开黑洞节点所在路径,可用路径数量减少,重新发起路由发现的次数增多.同时,随着恶意节点数的增加,收到的数据包数量会有所减小,因此,SRP 的信令开销也所有增大并加剧了 THSMR 的信令开销.

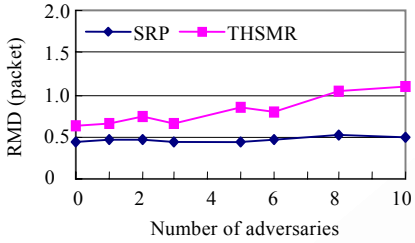
从上述分析可以看出,在黑洞攻击场景下,THSMR 只需付出一定的信令开销的代价就可以显著提高数据包转发率,而数据包转发率是衡量方案抵御攻击能力最重要的指标[17].从图 7(a)中可以看出,在恶意节点数高达 10 时,THSMR 的数据包转发率依然保持在 97%以上,说明方案具备很强的抵御黑洞攻击的能力.

性能分析说明,THSMR 具备良好的建路能力,在普通场景下对协议性能没有带来影响.而 THSMR 具备拓扑隐藏的特性,实现了按需的邻居发现,可安全确定最短路径,有效提升了网络的安全性能.在黑洞场景下,THSMR 只需付出一定信令开销的代价就能大幅度提高数据包转发率,可以有效地抵御黑洞攻击.

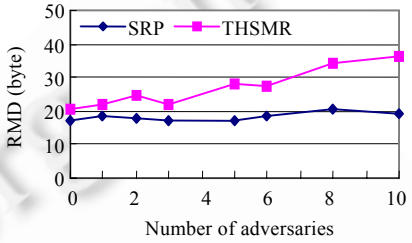


(a) Packet delivery ratio
(a) 数据包转发率

(b) End-to-End delay
(b) 端到端延时



(c) Route-Level message cost (packet)
(c) 路由层消息开销(包)



(d) Route-Level message cost (byte)
(d) 路由层消息开销(字节)

Fig.7 Performance in the black hole scenario
图 7 黑洞场景下的性能

6 结 论

MANET 网络现有安全多路径路由协议均在数据包中携带大量路径信息,忽视暴露拓扑带来的安全隐患.通过对 MANET 网络特性和现有攻击的分析,指出隐藏拓扑对于提高网络安全的重要作用,并提出一种拓扑隐藏的安全多路径路由协议 THSMR.目前,本文的方案不涉及数据包转发策略,下一步将结合数据包转发机制和完善的错误发现机制,提出一个完整的解决方案.

References:

[1] Deng HM, Li W, Agrawal DP. Routing security in wireless ad hoc networks. IEEE Communications Magazine, 2002,40(10):70−75. [doi: 10.1109/MCOM.2002.1039859]

[2] Hu YC, Perrig A, Johnson DB. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. In: Proc. of the IEEE INFOCOM 2003. 2003. 59−63. [doi: 10.1109/INFCOM.2003.1209219]

[3] Douceur JR. The Sybil attack. In: Proc. of the 1st Int'l Workshop on Peer-to-Peer Systems (IPTPS 2002). 2002. 251−260.

[4] Bengio S, Brassard G, Desmedt Y, Goutier C, Quisquater JJ. Secure implementation of identification systems. Journal of Cryptology, 1991,4(3):175−184. [doi: 10.1007/BF00196726]

[5] Lima MN, da Silva HW, dos Santos AL, Pujolle G. Survival multipath routing for MANETs. In: Proc. of the IEEE NOMS 2008. 2008. 425−432. [doi: 10.1109/NOMS.2008.4575164]

[6] Lou WJ, Liu W, Zhang YC, Fang YG. SPREAD: Improving network security by multipath routing in mobile ad hoc networks. Journal on Wireless Networks, 2009,15(3):279−294. [doi: 10.1007/s11276-007-0039-4]

[7] Reddy LR, Raghavan SV. SMORT: Scalable multipath on-demand routing for mobile ad hoc networks. Elsevier Ad hoc Networks Journal, 2007,5(2):162−188. [doi: 10.1016/j.adhoc.2005.10.002]

[8] Sanzgiri K, Dahill B, Levine BN, Shields C, Belding-Royer EM. A secure routing protocol for ad hoc networks. In: Proc. of the 2002 IEEE Int'l Conf. on Network Protocols. 2002. 78−84. [doi: 10.1109/ICNP.2002.1181388]

[9] Papadimitratos P, Haas Z. Secure routing for mobile ad hoc networks. In: Proc. of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conf. (CNDS). 2002. 27−31.

[10] Kotzanikolaou P, Mavropodi R, Douligeris C. Secure multipath routing for mobile ad hoc networks. In: Proc. of the 2nd Annual Conf. on Wireless On-Demand Network Systems and Services (WONSS). 2005. 89−96. [doi: 10.1109/WONS.2005. 31]

[11] Perkins CE, Belding-Royer EM, Das SR. Ad hoc on-demand distance vector routing. IETF RFC 3561, 2003. http://www.ietf.org/rfc/rfc3561.txt [doi: 10.1145/581291.581305]

[12] Sanzgiri K, Dahill B, LaFlamme D, Levine B, Shields C, Belding-Royer EM. Authenticated routing for ad hoc networks. IEEE Journal on Selected Areas in Communications, 2005,23(3):598−610. [doi: 10.1109/JSAC.2004.842547]

[13] Marina MK, Das SR. Ad hoc on-demand multipath distance vector routing. ACM SIGMOBILE Mobile Computing and Communications Review, 2002,6(3):14−23.

[14] Nasipuri A, Das SR. On-Demand multipath routing for mobile ad hoc networks. In: Proc. of the IEEE INFOCOM'99. 1999. 64−70. [doi: 10.1109/ICCCN.1999.805497]

[15] Vaidya B, Pyun JY, Park JA, Han SJ. Secure multipath routing scheme for mobile ad hoc network. In: Proc. of the 3rd IEEE International Symp. (DASC 2007). 2007. 163−171. [doi: 10.1109/DASC.2007.29]

[16] Mavropodi R, Kotzanikolaou P, Douligeris C. Performance analysis of secure multipath routing protocols for mobile ad hoc networks. Wired/Wireless Internet Communications, 2005,3510:269−278. [doi: 10.1007/11424505_26]

[17] Awerbuch B, Curtmola R, Holmer D, Nita-Rotaru C, Rubens H. ODSBR: An on-demand secure Byzantine resilient routing protocol for wireless ad hoc networks. ACM Trans. on Information and System Security (TISSEC), 2008,10(4):1−35. [doi: 10.1145/1284680.1341892]

胡琪(1984－),女,湖北武汉人,硕士,主要研究领域为网络安全,安全路由.

张玉军(1976－),男,博士,副研究员,主要研究领域为下一代网络,移动计算.

张娇(1983－),女,硕士,主要研究领域为移动网络安全.

李忠诚(1962－),男,博士,研究员,博士生导师,主要研究领域为计算机网络.