计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
44(8):1371~1377, 2007

一种新颖的移动自组网灰洞攻击检测方案

陈 炜 龙 翔 高小鹏 白跃彬
(北京航空航天大学计算机学院 北京 100083)
(buaa_chen@yahoo.com.cn)

A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks

Chen Wei, Long Xiang, Gao Xiaopeng, and Bai Yuebin
(*School of Computer Science, Beihang University, Beijing* 100083)

Abstract Mobile ad hoc networks (MANETs) are typical distribution networks, which have unique characteristics and constraints such as none centralized control, dynamically changed network topology, and limited bandwidth. For the absence of fixed network infrastructure, MANETs are vulnerable to various types of denial of service (DoS) attacks. The gray hole attack is a kind of DoS attacks. In this attack, an adversary silently drops some or all of the data packets sent to it for further forwarding even when no congestion occurs. Firstly, related works, DSR protocol, aggregate signature algorithm and network model are introduced. Secondly, a scheme based on aggregate signature is proposed to trace packet dropping nodes. The proposal consists of three related algorithms: the creating proof algorithm, the checkup algorithm and the diagnosis algorithm. The first is for creating proof, the second is for checking up source route nodes, and the last is for locating the malicious nodes. Finally, the efficiency of the proposal is analyzed. The simulation results using ns-2 show that in a moderately changing network, most of the malicious nodes could be detected, the routing packet overhead is low, and the packet delivery rate is improved after abandoning routes containing bad nodes.

Key words MANET; DSR; aggregate signature; DoS; ns-2

摘 要 移动自组网(mobile ad hoc networks, MANETs)是典型的分布式网络,没有集中式的管理节点,网络拓扑动态变化,而且网络带宽有限.移动自组网无网络基础设施的特点,使其易于受到各种拒绝服务攻击(denial of service, DoS).灰洞攻击是一种类型的拒绝服务攻击,攻击者在网络状态良好的情况下,首先以诚实的方式参与路由发现过程,然后以不被察觉的方式丢弃部分或全部转发数据包.首先介绍了相关工作、DSR算法、聚合签名算法和网络模型.然后基于聚合签名算法,给出了用于检测丢包节点的3个相关算法:证据产生算法、审查算法和诊断算法.证据产生算法用于节点产生转发证据;审查算法用于审查源路由节点;诊断算法用于确定丢包节点.最后分析了算法的效率.ns-2仿真结果表明,在移动速度中等的网络中,提出的算法可以检测出多数丢包节点,且路由包开销较低.舍弃含丢包节点的路由后,数据发送率有相应的改善.

关键词 移动自组网;动态源路由;聚合签名;DoS;ns-2

中图法分类号 TP393;TP393.08

在没有网络基础设施的移动自组网(mobile ad hoc networks, MANETs)[1]中,节点之间互相中继数据包,以实现网络的互联互通.早期的MANET路由算法研究[2-3],只考虑路由建立的可能性以及路由算法的效率,而没有考虑各种网络攻击.近年来,安全路由逐渐成为移动自组网研究的热点[4-5].

收稿日期:2006-09-21;修回日期:2007-05-14
基金项目:国家自然科学基金项目(90612004)

灰洞攻击[6]是针对数据包的 DoS 攻击. 攻击者在网络状态良好的情况下,首先以诚实的方式参与路由发现过程,然后以不被察觉的方式丢弃部分或全部转发数据包. 丢包节点的存在会降低系统的性能,扰乱路由的建立过程,从而造成安全隐患. 一些研究人员提出使用邻居节点监测、响应、探测[7-11]等方法检测丢包节点,但这些方法都不令人满意.

本文使用聚合签名算法产生转发证据,通过要求节点出示转发证据检测丢包节点. 算法有较高的可信度,不要求链路满足双向特性(链路双向是指如果节点 A 在节点 B 的传输范围内,则节点 B 也在节点 A 的传输范围内),丢包节点难以逃避检测等特点.

1 相关工作

Marti 等人[7]提出基于 watchdog/pathrater 检测丢包节点,该方案由 watchdog 算法和 pathrater 算法两个相关的算法组成. 方案有以下特点:①源节点对被检查节点的评估,要参考其他节点的意见. 在有大量不诚实节点的网络环境中,不能保证评估的正确性.②要求链路满足双向性.

Awerbuch 等人[8]提出基于目标节点发送 acknowledgement,发现具有 Byzantine 行为的丢包节点. 方案由路径发现算法,Byzantine 错误检测算法和链路权重管理算法(link weight management)3 个相关的算法组成. 方案有以下特点:①目标节点对所有收到的数据包都要发送 acknowledgement,网络带宽开销大.②所有被检查节点分别与源节点有一个共享密钥,这对密钥的分发是一个挑战.③检测包含有被探测节点链表(probe list),容易与一般数据包区分.

Just 等人[9]对现有的丢包节点检测算法进行分析后,提出基于 probing 方法检测丢包节点. 方案以节点的当前状态,推断节点的历史行为,因此不具有实时性. probing 算法由路径选择算法、探测算法和诊断算法 3 个相关的算法组成. 方案有以下特点:①源节点发现丢包现象后,发起探测过程. 移动自组网动态的拓扑特性和丢包节点行为的不确定性,使得该算法不具有令人满意的可信度.②算法要求链路满足双向特性,不适用于链路不对称的网络.③探测包必须加密,确保丢包节点不能区分探测包和普通数据包.

Huang 等人[10]提出基于单向 Hash 链(one-way hash chain)和一次性 Hash 标识承诺(one-time hash tag commitment)检测丢包节点. 方案有以下特点:①所有参与路由的节点都要产生/转发 acknowledgements,网络带宽开销大.②节点之间必须存在共享密钥,共享密钥的分发对移动自组网是一个挑战.③源节点必须预知下一个要发送的数据包,并在发送当前数据包时包含对下一个数据包的承诺.

Papadimitratos 等人[11]使用路径冗余和门限秘密共享技术,实现数据的安全传输. 方案使用端到端的认证方法,丢包路径的发现过程不需要中间节点参与,但不能检测丢包节点.

2 预备知识

2.1 动态源路由算法

DSR(dynamic source routing)协议[12-13]是按需驱动源路由协议. 路由发现过程在源节点需要路由时启动,每个被发送的数据报都含有完整的路由. 路由发现过程原理如下:源节点广播 RREQ(route request)报文. 中间节点收到 RREQ 后,先将自己的地址添加到 RREQ,然后重新广播 RREQ. 当 RREQ 到达目标节点后,目标节点将所得的源路由添加到 RREP(route reply)报文,并反向将所得的源路由发送到源节点. 源节点收到 RREP 后,将源路由存入缓存,并置入每个数据报的报头. 中间节点根据数据报头中的路由信息中转数据报文.

2.2 聚合签名算法

聚合签名[14-16]是 n 个不同的用户对 n 个不同的消息分别进行签名,所有这些签名能够合成一个签名. 验证方只需对合成后的签名进行验证,便可以确信签名来自指定的 n 个用户. 下面介绍 Boneh 等人[14]提出的基于 Co-Gap Diffie-Hellman 问题的一般聚合签名算法.

系统参数:有限群 G_1 和 G_2,生成元分别是 g_1 和 g_2,ψ 是 G_2 到 G_1 的可计算同构,双线性映射 e:$G_1\times G_2\rightarrow G_T$,Hash 函数 $H:\{0,1\}^*\rightarrow G_1$. 签名算法由以下 5 个算法组成:①KeyGen. 每个用户随机挑选 $x\in Z_p$,计算 $v=g_2^x$. 用户公钥是 $v\in G_2$,相应的私钥是 $x\in Z_p$. 2Sign. 给定消息 $M\in\{0,1\}^*$,用户私钥 x,计算 $h=H(M)$,$h\in G_1$,计算签名 $\sigma=h^x$. ③Verify. 给定公钥 v,消息 M,签名 σ,计算 $h=H(M)$,如果 $e(\sigma,g_2)=e(h,v)$,则签名为合法签名.④Aggregate. 给定用户集合 $u_i\in\cup$,以及用户 u_i 对消息 $M_i\in\{0,1\}^*$ 的签名 $\sigma_i\in G_1$,$M_i\neq M_j$,$i\neq j$,聚合签名是 $\sigma=\prod_{i=1}^{k}\sigma_i$,$\sigma\in G_1$. ⑤Aggregate

$Verify$. 给定聚合签名 σ,消息集合 $M_i \in \{0,1\}^*$,用户 $u_i \in \cup$ 的公钥 v_i,首先验证 $M_i \neq M_j, i \neq j$,然后验证 $e(\sigma, g_2) = \prod_{i=1}^{k} e(h_i, v_i)$,如果等式成立,则聚合签名为合法签名.

3　网络模型

每个节点可以获知其他节点的公钥,用于验证其他节点的聚合签名. 路由协议采用源路由协议,如 DSR 路由算法. 节点有较强的计算能力,但不具有无限的计算能力,如节点可以进行模指数运算、双线性映射(bilinear maps)等计算量较大的公钥密码学运算,但不能有效破解计算困难问题. 中间节点愿意或必须保存转发证据.

4　灰洞攻击检测方案

本文提出的灰洞攻击检测方案由 3 个相关算法组成:①证据产生算法. 所有参与路由的节点都要调用该算法,以产生数据包转发证据. 转发证据基于 Boneh 等人[14]的聚合签名算法产生,用于证明节点接收了数据包. ②审查算法. 源节点发现非正常丢包现象时,如目标节点报告收到的数据包明显少于正常情况,调用该算法检测丢包节点. ③诊断算法. 源节点根据审查算法返回的转发证据,确定丢包节点.

4.1　符号和表结构

本文使用的符号如表 1 所示:

Table 1　Notations

表 1　符号

Notation	Meaning
$\|$	Payload concatenation
S	Source node
N_i	The ith node
ROUTE	Source route
H	Hash function, such as SHA-1
I_{seq}	Index created by H
G_1	Finite field
I_1	The identity of G_1
H_1	Hash function, maps a string to an element in G_1
h_i	An element in G_1 created by H_1
h_{seq}	An element in G_1
M_i	The ith message
TYPE	Message type
N_{seq}	Session number
x_i	Private key
v_i	Public key
σ_{seq}	Aggregate signature

为定位丢包节点,本文采用表 2 所示的索引表结构存储相关的参数. 表中第 1 列是索引值,第 2 列是用于产生聚合签名的 Hash 值.

Table 2　Index Table Structure

表 2　索引表结构

Index	Aggregate Hash Value
I_{seq}	$h_{seq} \in G_1$

4.2　证据产生算法

为检测丢包节点,源节点和中间节点需要保存发送的消息的相关信息. 证据产生算法由以下 6 步组成. 这一小节中的节点泛指源节点和中间节点. ①节点收到消息 ROUTE ‖ TYPE ‖ N_{seq} ‖ M_i. 其中 ROUTE 是源路由,TYPE 是消息类型(这里是 $data$),N_{seq}是会话序列号,M_i 是消息数据部分. ②节点产生索引值 $I_{seq} = H(\text{ROUTE} \| N_{seq})$. 节点根据源路由、会话序列号,调用 Hash 函数 H 产生索引值,所有索引值相同的消息将产生一个聚合签名. ③节点根据索引值 I_{seq},查询索引表,如果没有找到相应的条目,则创建该索引值对应的条目,并将 h_{seq}初始化为群 G_1 的单位元,$h_{seq} = I_1$. ④节点调用 Hash 函数 H_1,将消息 M_i 映射到群 G_1 的一个元素,$h_i = H_1(M_i)$. ⑤节点更新索引值为 I_{seq}的聚合 Hash 值,$h_{seq} = h_i \times h_{seq}$. ⑥节点向源路由的下一个节点转发消息,ROUTE ‖ TYPE ‖ N_{seq} ‖ M_i.

4.3　审查算法

当源节点发现非正常丢包现象后,调用该算法检测丢包节点. 审查算法由以下 5 步组成:①源节点计算索引值 I_{seq},$I_{seq} = H(\text{ROUTE} \| N_{seq})$. ②源节点将 ROUTE ‖ TYPE ‖ I_{seq}发送给其他节点,其中 TYPE 是消息类型,这里是 CREQ (checkup request),I_{seq}是要检查的聚合签名的索引值. ③节点 N_i 收到 CREQ 消息后,根据 I_{seq}在索引表中提取聚合 Hash 值 h_{seq},然后用私钥 x_i 产生聚合签名 $\sigma_{seq} = h_{seq}^{x_i}$. ④节点 N_i 向源节点发送消息 ROUTE ‖ TYPE ‖ I_{seq} ‖ N_i ‖ σ_{seq}. 其中 TYPE 是消息类型,这里是 CREP(checkup reply),N_i 是节点的身份,σ_{seq}是聚合签名. ⑤源节点根据节点身份 N_i,首先获取相应的公钥 v_i,然后根据 I_{seq}查找源节点产生的 h_{seq},最后验证 $e(\sigma_{Seq}, g_2) = e(h_{Seq}, v_i)$. 如果成立,则验证通过.

4.4　诊断算法

根据签名验证结果,有以下 3 种情况:①所有的签名都通过了验证,没有丢包节点. ②如果节点 N_i 拒绝提供签名,则认为该节点是丢包节点. ③如果源路由中最后通过验证的节点是 N_i,且 N_i 不是目标

节点,则有3种可能:①N_i没有转发所有的数据包.②N_i转发了所有的数据包,但由于链路问题,N_{i+1}没有收到所有的数据包.③N_{i+1}收到了所有的数据包,但发送无效证据.综合考虑上述情况,N_i和N_{i+1}都被怀疑是丢包节点.若某节点被怀疑次数超过阈值,则被认为是丢包节点.

4.5 效率分析

时间复杂性:①在证据产生算法中,源节点和所有的中间节点都要进行两次Hash运算,一次模乘法运算.其中一次Hash运算产生索引值I_{seq},一次Hash运算将消息映射到群G_1的一个元素,模乘法运算用于在群G_1中产生聚合Hash值.②在审查算法中,源节点需要执行一次Hash运算,以产生索引值I_{seq},每个中间节点只需执行一次模指数运算,以产生聚合签名.③在诊断算法中,源节点需要对每一个中间节点执行一次双线性映射,以验证聚合签名.

空间复杂性:对每一个会话的每一种源路由,源节点和中间节点都只需要一个索引条目.如果算法采用Boneh等人[17]提出的短签名,则聚合Hash值只有170b左右.

4.6 小 结

本文算法有以下特点:①可信度高.使用数字签名技术,转发证据具有不可否认性.②使用范围广泛.不要求链路满足双向特性,适用于链路非对称环境.③安全性好.源节点在检测过程中,随机要求中间节点返回聚合签名,检测持续时间随机,使丢包节点很难预测检测过程发起时间,难以逃避检测.④检测过程不需要中间节点监控其他节点,极大地减少了带宽占用.

各种相关算法比较如表3所示:

Table 3 Algorithm Comparison

表3 算法比较

Algorithm	Need Cryptography Mechanism	Encrypted Probing Packet	Hop-by-Hop Ack	Bi-Direction Link
Watchdog/pathrater[7]	No		No	Yes
acknowledgement/probing[8]	Yes	Yes	Yes	Yes
DSR_Probe[9]	Yes	Yes	No	Yes
Acknowledgements[10]	Yes		Yes	Yes
Our solution	Yes	No	No	No

5 仿真结果

5.1 仿真环境

本文使用ns-2[18]仿真软件测量了检测率、误检率、路由包开销和数据包发送率4个指标.ns-2参数如表4所示:

Table 4 ns-2 Parameters

表4 ns-2参数设置

Parameter	Value
Number of nodes	50
Simulation area(m^2)	670×670
Simulation time(s)	100
Routing protocols	DSR
MAC type	Mac/802_11
Propagation model	Two-ray Ground Reflection
Movement model	Random waypoint
Transmission range(m)	250
Maximum speed(m/s)	20
Pause time(s)	50
Traffic type	CBR(UDP)
Packet size(B)	512
Packet rate(pps)	4
Types of attacks	Gray Hole attack

5.2 移动模型和攻击模型

仿真使用random waypoint[19]运动模型.节点首先停止暂停时间(pause time),然后以小于最大速度的移动速度运动到随机选择的位置,停留暂停时间后,再次移动到随机选择的位置.实验中将丢包节点建模为路由发现阶段承诺转发数据包,而在数据包转发阶段丢弃数据包.丢包节点不会在收到所有数据包后,故意发送无效证据.

5.3 实验过程

通信模型使用10个CBR连接,包括6个源节点和9个目标节点,其中4个源节点分别对应两个目标节点,两个源节点对应一个目标节点[7].随机选择0,3,5,8,10,13,15[9]个丢包节点,进行100种不同场景实验,最后用这100次实验的平均值作为实验结果,不同丢包节点数实验使用相同的场景.丢包节点数少的实验所对应的丢包节点集合是丢包节点数多的实验对应的丢包节点集合的子集,以确保同一丢包节点在不同实验中都存在.

5.4 积分规则

考虑到节点移动和网络拥塞也会导致丢包,本文通过积分的方法检测丢包节点:源节点根据源路

由要求中间节点提供转发数据包的证据,若源路由中最后通过验证的节点不是源节点,也不是目标节点,则该节点被怀疑是丢包节点,积分加 1. 检测阶段结束后,若某节点积分远大于正常情况积分,源节点在以后的路由中舍弃含该节点的源路由.

5.5　指　标

实验测试了下列指标:①检测率(detection rate). 检测出的丢包节点数和真实丢包节点数的比值. ②误检率(false positive rate). 被误认为是丢包节点的诚实节点数和所有诚实节点数的比值. ③路由包开销(routing packet overhead). 所有路由包与所有传输包的比值,其中路由包指 DSR 路由包和本文使用的检测包,传输包指路由包和数据包. 传输包的每一跳都计为一个单独的包. ④数据包发送率(packet delivery rate). 目标节点收到的 CBR 数据包和源节点发送的 CBR 数据包的比值.

5.6　实验结果

实验中使用的索引值是 160b,聚合签名是 177b[17],节点身份是 32b. 实验将没有丢包节点时,所有节点积分的平均值作为基准,该基准的 5 倍作为阈值,超过该阈值的节点被认为是丢包节点. 每次实验有 50 个节点,有 7 种实验,共 350 个节点,其中 54 个丢包节点,296 个诚实节点. 节点积分如图 1、图 2 所示.

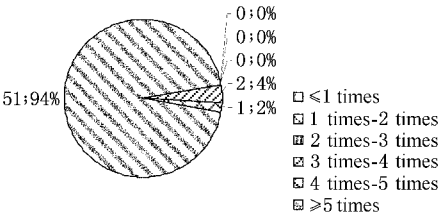

Fig. 1　Values of bad nodes.

图 1　丢包节点积分分布

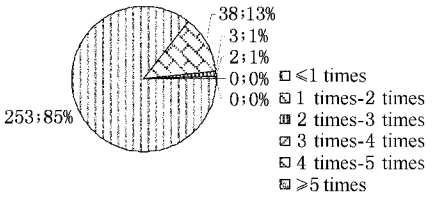

Fig. 2　Values of honest nodes.

图 2　诚实节点积分分布

从图 1 可以看出,有 51 个丢包节点积分为基准的 5 倍以上,占所有丢包节点的 94%;3 个丢包节点的积分在 3 倍基准到 5 倍基准之间,占 6%;从图 2 可以看出,有 253 个诚实节点的积分小于等于基准,占所有诚实节点的 85%;38 个诚实节点的积分在基准到 2 倍基准之间,占 13%;5 个诚实节点的积分在 2 倍基准到 4 倍基准之间,占 2%.

检测率、误检率如图 3、图 4 所示,发送率如图 5 所示,路由包开销如图 6 所示. 我们将这些指标与同是基于源节点检测的 DSR_Probe 算法[9] 进行了比较.

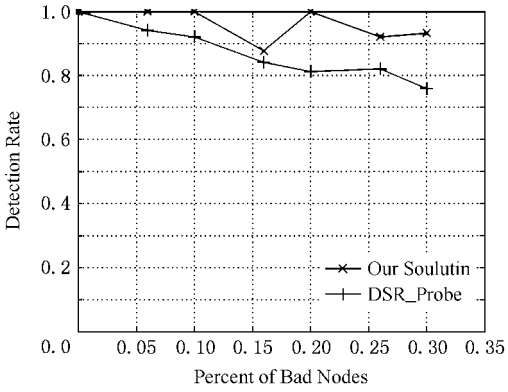

Fig. 3　Detection rate.

图 3　检测率

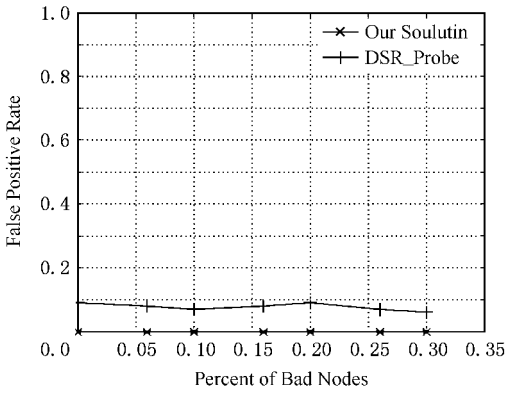

Fig. 4　False positive rate.

图 4　误检率

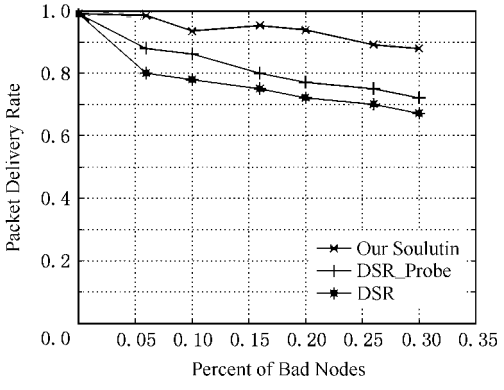

Fig. 5　Packet delivery rate.

图 5　发送率

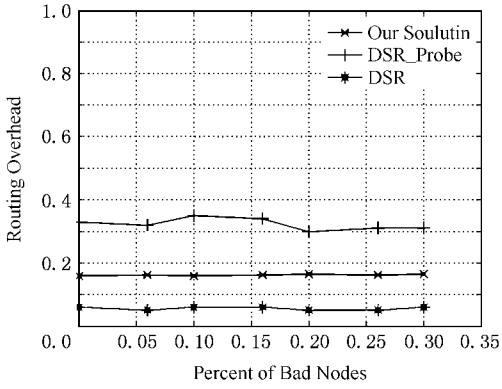

Fig. 6 Routing overhead.

图6 路由包开销

检测率、误检率:从图3和图4可以看出,本文方法的检测率高于87.5%,而误检率很低.上述分析表明,本文方法有效实现了丢包节点和诚实节点的分离,且检测效果优于DSR_Probe算法.

发送率:由于源节点舍弃了含丢包节点的路由,丢包节点不能丢弃数据包,从而使系统发送率有所提高.由于检测效果优于DSR_Probe算法,发送率也优于DSR_Probe算法.

路由包开销:由于有检测包的存在,检查阶段路由包开销基本上是正常情况的2倍,但与DSR_Probe算法比较,路由包开销仅是DSR_Probe算法的一半.

6 结束语

丢包节点在路由发现阶段承诺转发数据包,而在数据包转发阶段恶意丢弃数据包.丢包节点的存在会降低系统性能,扰乱路由建立过程,从而造成安全隐患.本文使用聚合签名算法产生转发证据,通过要求节点出示转发证据检测丢包节点.仿真结果表明,本文算法可以检测出多数丢包节点,误检率较低,路由包开销较小.舍弃含丢包节点的路由后,数据发送率有相应的改善.

本文算法使用数字签名技术检测丢包节点,可信度高;不要求链路满足双向特性,适用于链路不对称的网络环境;丢包节点不能预测检测发起时间,难以逃避检测;中间节点不监控其他节点,效率较高.综上所述,算法有较好的实用价值.

参 考 文 献

[1] IETF MANET Work Group [OL]. http://www.ietf.org/html.charters/manet-charter.html, 2006

[2] Elizabeth M Royer, Chai-Keong Toh. A review of current routing protocols for ad hoc mobile wireless networks [J]. IEEE Personal Communications, 1999, 6(2): 46-55

[3] I Chlamtac, M Conti, *et al*. Mobile ad hoc networking: Imperatives and challenges [J]. Ad Hoc Networks, 2003, 1(1): 13-64

[4] Y C Hu, A Perrig. A survey of secure wireless ad hoc routing [J]. IEEE Security and Privacy, 2004, 2(3): 28-39

[5] Hu Huaping, Hu Guangming, Dong Pan, *et al*. Survey of security technology for large scale MANET [J]. Journal of Computer Research and Development, 2007, 44(4): 545-552 (in Chinese)
(胡华平,胡光明,董攀,等.大规模移动自组网络安全技术综述[J].计算机研究与发展,2007,44(4):545-552)

[6] Y C Hu, A Perrig, D B Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks [C]. In: Proc of the 8th Annual Int'l Conf on Mobile Computing and Networking. New York: ACM Press, 2002. 12-23

[7] S Marti, T J Giuli, K Lai, *et al*. Mitigating routing misbehavior in mobile ad hoc networks [C]. The 6th Annual ACM/IEEE Int'l Conf on Mobile Computing and Networking (MOBICOM 2000), Boston, Massachusetts, 2000

[8] B Awerbuch, D Holmer, C Nita-Rotaru, *et al*. An on-demand secure routing protocol resilient to Byzantine failures [C]. ACM Workshop on Wireless Security (WiSe), Atlanta, Georgia, 2002

[9] M Just, E Kranakis, T Wan. Resisting malicious packet dropping in wireless ad hoc networks [C]. Ad Hoc-NOW, Montreal, Canada, 2003

[10] Q Huang, I C Avramopoulos, H Kobayashi, *et al*. Secure data forwarding in wireless ad hoc networks [C]. IEEE Int'l Conf on Communications, Seoul, Korea, 2005

[11] P Papadimitratos, Z Haas. Secure message transmission in mobile ad hoc networks [J]. Elsevier Ad Hoc Networks Journal, 2003, 1(1): 193-209

[12] D B Johnson, D A Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks [M]. New York: Kluwer Academic Publishers, 1996. 153-181

[13] D B Johnson, D A Maltz, J Broch. DSR: The dynamic source routing protocol for multiple wireless ad hoc networks [G]. In: Perkins C, ed, Ad Hoc Networking. Reading, MA: Addison-Wesley, 2001. 139-172

[14] D Boneh, C Gentry, B Lynn, *et al*. Aggregate and verifiably encrypted signatures from bilinear maps [G]. In: Advances in Cryptology—EUROCRYPT '03, LNCS 2656. Berlin: Springer-Verlag, 2003. 416-432

[15] H Shacham. Sequential aggregate signatures from trapdoor homomorphic permutations [OL]. http://citeseer.ist.psu.edu/shacham03sequential.html, 2003

[16] D Boneh, C Gentry, B Lynn, *et al*. A survey of two signature aggregation techniques [J]. RSA CryptoBytes, 2003, 6(2): 1-10

[17] D Boneh, B Lynn, H Shacham. Short signatures from the Weil pairing [C]. In: Boyd C, ed. Advances in Cryptology—Asiacrypt 2001. Berlin: Springer-Verlag, 2001. 514-532

[18] Ns-2 network simulation [OL]. http://www.isi.edu/nsnam/ns, 2006

[19] J Broch, D A Maltz, D B Johnson, *et al*. A performance comparison of multi-hop wireless ad hoc network routing protocols [C]. The 4th Annual ACM/IEEE Int'l Conf on Mobile Computing and Networking, Dallas, Texas, 1998

Chen Wei, born in 1977. Ph. D. candidate. His main research interests is network security.

陈　炜,1977 年生,博士研究生,主要研究方向为网络安全.

Long Xiang, born in 1963. Ph. D., professor and Ph. D. supervisor. His main research interests include: computer architecture and network security.

龙　翔,1963 年生,博士,教授,博士生导师,主要研究方向为计算机体系结构和网络安全.

Gao Xiaopeng, born in 1970. Ph. D. and associate professor. His main research interests includes: computer architecture and network security.

高小鹏,1970 年生,博士,副教授,主要研究方向为计算机体系结构和网络安全.

Bai Yuebin, born in 1962. Ph. D. and associate professor. His main research interests includes: computer architecture and network security.

白跃彬,1962 年生,博士,副教授,主要研究方向为计算机体系结构和网络安全.

Research Background

Since DARPA's PRNET, the area of routing in ad hoc networks has been an open research topic. However, the availability and efficiency of routing protocol strongly depend on the availability of security provisions, among other factors. In the open, collaborative MANETs environment, practically any node can maliciously or selfishly disrupt and deny communication of other nodes. In this paper, we focus on one type of DoS (denial of service) attacks, namely gray hole attack. In this attack, an adversary silently drops some or all of the data packets sent to it for further forwarding even when no congestion occurs. Some researchers have proposed to trace bad nodes by using watchdog/pathrater, acknowledgements and probing, but the effects are not satisfying. In order to trace packet dropping nodes by using evidence, we propose to use aggregate signature to locate malicious packet dropping nodes, and the simulation results using ns-2 show that this method is more effective than other related works.