

基于信任保留的移动 Ad Hoc 网络安全路由协议 TPSRP

付 才¹⁾ 洪 帆¹⁾ 洪 亮²⁾ 彭 冰¹⁾ 崔永泉¹⁾

¹⁾(华中科技大学计算机科学与技术学院 武汉 430074)

²⁾(西北工业大学自动化学院 西安 710072)

摘 要 Ad Hoc 网络的移动特性是安全路由中不能忽略的一个重要因素. 在一个频繁变化甚至高速移动的网络中, 目前大部分安全路由协议难以完成可信通信方的认证, 从而无法建立起安全的路由通道. 这是由于认证过程是一个连续的消息交互过程, 移动特性使得这个连续交互无法保证. 文中在链路状态路由协议 OLSR 的基础上提出了基于信任保留的安全路由协议 TPSRP, 该协议采用信任保留的方式对节点进行认证, 解决高速移动网络中节点认证问题. TPSRP 还针对目前信任评估方法缺少有效的自适应性提出了一种新的信任评估手段, 使得节点可以通过综合的信任信息, 自我辨别并限制内部背叛节点的恶意行为, 同时有效地检测与抵抗 Ad Hoc 网络中的协作攻击, 如虫洞攻击等. 最后的仿真显示, 在网络移动特性增强的情况下, TPSRP 的认证性能要优于传统认证协议, 并能够有效孤立攻击节点.

关键词 Ad Hoc 网络; 安全路由; 信任评估; 身份认证; 移动特性

中图法分类号 TP309

Mobile Ad Hoc Secure Routing Protocol Based on Trust Preserving

FU Cai¹⁾ HONG Fan¹⁾ HONG Liang²⁾ PENG Bing¹⁾ CUI Yong-Quan¹⁾

¹⁾(College of Computer Science & Technology, Huazhong University of Science & Technology, Wuhan 430074)

²⁾(College of Automation, Northwestern Polytechnical University, Xi'an 710072)

Abstract Moving characteristic is a important factor in secure routing for Ad Hoc networks. Most secure routing protocols are difficult to finish the authenticating processing and can't set up the secure routing in a mutative and high speed moving network because authenticating is a continuous processing for messages exchanging and the moving characteristic can't ensure the continuity. This paper proposes the trust preserving based secure routing protocol based on OLSR, the trust preserving method is adopted to accomplish the authenticating and resolve the high speed moving authenticating problem, which is proved with the formal language. Aiming at the low flexibility of most trust evaluating system, a novelty evaluating system is proposed, by which the nodes get the trust information, identify and limit the vicious nodes, at the same time, it can resist the associated attacks, such as worm-hole attack. The simulations shows that in a high speed moving network, The TPSRP's authenticating performance is more better than that of the traditional and can isolate the attacking nodes effectively.

Keywords Ad Hoc networks; secure routing; trust evaluation; identity authenticating; moving characteristic

收稿日期: 2007-05-08; 修改稿收到日期: 2007-07-22. 本课题得到国家自然科学基金(60403027)资助. 付 才, 男, 1976 年生, 博士, 讲师, 主要研究方向为无线网络安全、路由协议安全与软件脆弱性. E-mail: stand_fucai@126.com. 洪 帆, 女, 1942 年生, 教授, 博士生导师, 主要研究领域为信息安全、网络安全和密码学. 洪 亮, 男, 1979 年生, 博士, 讲师, 主要研究方向为 Ad Hoc 网络技术、安全及密码学. 彭 冰, 男, 1972 年生, 博士, 讲师, 主要研究方向为无线网络安全、密码学. 崔永泉, 男, 1977 年生, 博士, 讲师, 主要研究方向为密码学与访问控制.

1 引 言

移动自组网中安全路由的研究已经成为无线网络中的一个研究热点,由于没有固定的网络基础设施、网络拓扑结构频繁动态变化、无线信道完全开放、网络缺乏自稳定性等原因,移动自组网环境下的路由协议相对于有线网环境更易遭受各种攻击,比如路由报文的篡改、假冒节点进行路由欺骗、黑洞攻击、拒绝服务以及虫洞攻击(Wormhole attack)等等,因此设计安全的路由协议非常重要。

关于移动自组网中安全路由协议的设计,国外很多研究机构已经提出自己的方案,如 Papadimitratos 和 Haas 提出的 SRP^[1]安全协议框架,可以应用于现存的几种协议(主要适用于 DSR);Sanzgiri 等提出的 ARAN^[2]路由协议,在协议中需要身份认证以及一个可信赖的认证服务器 CA;文献[3]中提出了一种基于 DSR 和 TESLA 的安全按需路由协议;SEAD^[4]是 Hu,Johnson 和 Perrig 提出的一种基于距离矢量路由协议 DSDV 的安全路由协议;我们在文献[5]中提出了基于 OLSR 的安全路由协议 SOLSR 等.这些安全路由协议都有一个特点,那就是需要对节点或是报文进行认证,身份认证是大部分安全路由协议的基础。

认证过程是一个从未知身份到可信身份的渐进过程.无论哪个身份协议,都需要首先为对方提交一些待确认信息.通过对这些信息的检验、计算才可能完成身份认证,因此,消息的交互必须是有序的;另外,传统的身份认证消息交互必须是一个连续的过程,如果身份认证过程出现中断,这个中断超出处理时限,则认为认证失败.在 Ad Hoc 网络中,对于传统的身份认证协议,由于节点移动的随机性以及路由拓扑变化的随机性,导致上述要求没有办法满足.首先,Ad Hoc 网络中如果节点移动频繁导致路由变化频繁,很容易导致报文丢失,其次,Ad Hoc 网络中的报文传输顺序比较难以保障.因此,对于传统的认证协议在一个移动性较强的自组织网络中往往认证效率非常低下,并且认证步骤越多,效果越差.图 1 是针对 SOLSR 认证协议进行模拟仿真的结果.该仿真参数为:节点数 50,节点随机移动,移动速度从 50m/s~500m/s,整个节点活动范围为 1km×1km,每个消息从接收处理再发送回复消息时间为 500ms,这个时间包括报文计算验证时间、在协议栈与网卡里面的缓冲时间以及路由查找时间。

可以看出,随着认证步骤的增加以及节点移动性能加剧,认证成功率在急剧下降,认证成功率下降的结果是整个事务处理的效率降低.因此,有必要研究新的适合 Ad Hoc 网络的认证方式。

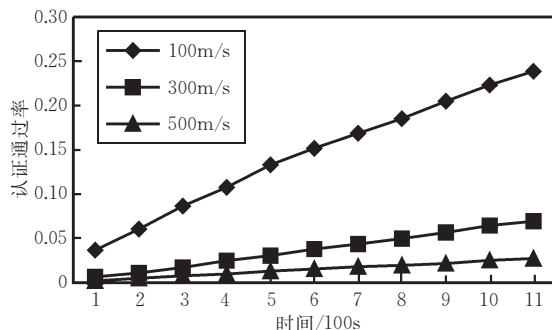


图 1 SOLSR 移动认证协议性能示意图

本文在 OLSR 的基础上提出了基于信任保留的安全路由协议 TPSRP,该协议采用信任保留的方式对节点进行认证,解决高速移动网络中节点认证问题,同时针对目前信任评估缺乏可扩展性以及自适应性的问题,提出了一种采用关联规则的信任评估手段,使得节点可以通过综合的信任信息,能够自我识别并限制内部背叛节点的恶意行为,同时有效地检测与抵抗 Ad Hoc 网络中的协作攻击,如虫洞攻击等。

本文第 2 节对 OLSR 的安全需求进行分析;第 3 节描述 TPSRP 协议;第 4 节阐述信任评估系统;第 5 节进行安全性分析,并通过仿真分析 TPSRP 的工作性能;第 6 节为小结。

2 OLSR 安全需求分析

OLSR 协议没有充分考虑移动自组网环境的安全问题,仅提到引入 IPSec 来解决其安全问题,这并不合适,因为 IPSec 提供的是一个端到端的安全信道,可以为用户数据传输提供一定安全保障,而 OLSR 的路由信息传输是一对多的,因而对于路由安全无能为力.所以设计一个 OLSR 的安全方案必须考虑到这一特点.针对 OLSR 的特点,恶意节点可以通过以下途径来发动攻击:缺乏报文的源鉴别机制,恶意节点可随意发布大量虚假路由报文,导致 OLSR 路由失效,或是达到某种恶意目的,如路由黑洞;缺乏报文的完整性保护,恶意节点可随意更改路由报文,而接收节点作为正确报文接收,进而导致 OLSR 路由机制失效;缺乏 OLSR 路由机制的相关防护配套措施.由于无线网的特点,很多网络功能的

具体实现都需要节点之间的协同工作,若某些节点存在自私行为,比如有目的地转发路由报文,但不转发数据报文,可能导致 OLSR 形成的路由表中某些相关项失效;此外,虫洞攻击对采用转发 HELLO 报文来进行邻居探测的路由协议具有致命的效果,OLSR 和 AODV 等路由协议都不能幸免。

这里描述一下第 3 种攻击情景. 为了叙述方便,约定以下符号: $A \rightarrow *: \text{content}$, 表示 A 广播内容为 content 的报文; $A \rightarrow B: \text{content}$, 表示 A 向 B 发内容为 content 的数据包。

在图 2 中, A 和 B 是两个合法节点,但彼此不在对方信号覆盖范围内, M 为恶意节点,同时在 A 和 B 的信号覆盖范围内,如图 2 所示. 其中圆圈代表节点的信号覆盖范围。

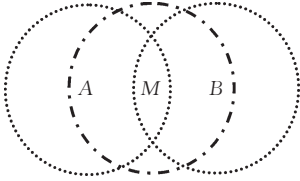


图 2 节点分布示意图

攻击过程如下:

$A \rightarrow *: A, NS, Neighbor(A)$, 其中 $NS(Neighbor\ Sensing)$ 表示报文类型是邻居探测类型, $Neighbor(A)$ 表示节点 A 的邻居集合; $M \rightarrow *: A, NS, Neighbor(A)$; B 将把 A 添加到邻居集合 $Neighbor(B)$ 中去;

$B \rightarrow *: B, NS, Neighbor(B)$, 其中 $Neighbor(B)$ 表示节点 B 的邻居集合; $M \rightarrow *: B, NS, Neighbor(B)$; A 将把 B 添加到邻居集合 $Neighbor(A)$ 中去。

这样,恶意节点 M 便导致 A 和 B 互相认为对方是自己的邻居,然后两节点将把这一错误信息通过拓扑信息报文散播到全网络中去,导致节点在形成路由表时出现错误。

解决这一问题时,文献[6]提出了“看门狗”机制,节点广播邻居探测包之后,同时将这个包拷贝到一个缓冲区里,然后监听网络,若在一个探测周期内,发现监听到同样的报文,就知道某个恶意节点潜伏在自己信号覆盖范围内转发了邻居探测包. 基于这个思想,当 M 在转发 A 的邻居探测包时,由于线路是开放的,所以 A 同样能收到该报文, A 将此报文与缓冲区内缓存的对象进行比对,发现一致,便可探测到这种攻击行为. 不过这一机制当遇到有两个以上的恶意节点联合发动“虫洞攻击”时,就无效了. 如图 3 所示。

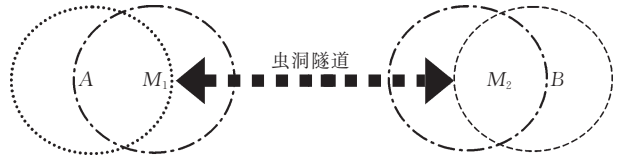


图 3 虫洞攻击示意图

其中, $M1$ 和 $M2$ 是两个恶意节点,它们可以通信,通信的内容将用会话密钥加密. 攻击如下:

$A \rightarrow *: A, NS, Neighbor(A)$;

$M1 \rightarrow M2: \{A, NS, Neighbor(A)\}_K$, 其中报文用 $M1$ 和 $M2$ 的密钥 K 加密,因而中间节点无法得知报文内容;

$M2 \rightarrow *: A, NS, Neighbor(A)$;

B 将把 A 添加到邻居集合 $Neighbor(B)$ 中去;

$B \rightarrow *: B, NS, Neighbor(B)$;

$M2 \rightarrow M1: \{B, NS, Neighbor(B)\}_K$;

$M1 \rightarrow *: B, NS, Neighbor(B)$;

A 将把 B 添加到邻居集合 $Neighbor(A)$ 中去。

因为 $M1$ 和 $M2$ 接收到探测包后,并没有广播,而是以加密后的普通数据包形式发给虫洞的另一端,由另一端解密后再广播,从而 A (或者 B)无法探测到这种攻击,进而导致双方互相认为对方是自己的邻居. 虫洞攻击中,攻击者无须知道合法节点的机密信息,只是简单地接收和转发报文,便可导致节点在形成自己的邻居集合时出错,当节点向全网其它节点广播自己的链路状态(即拓扑消息)后,错误将扩大至全网,使每个节点形成有错误的网络拓扑图,形成的路由表将是不可用的。

3 基于信任保留的安全路由协议(TPSRP)

基于信任保留的安全路由协议 TPSRP(Trust Preserving based Secure Routing Protocol)采用 OLSR 路由协议作为基础,增加邻居节点安全身份认证以及路由报文安全措施,同时引入信任评估机制,以解决移动 Ad Hoc 网络中的 OLSR 路由安全问题。

3.1 信任保留定义

在 Ad Hoc 网络安全路由中,每个节点如果要加入自组织网络,必须跟邻居节点进行身份认证,通过后才能够进行正常的路由信息处理. 在一般的身份认证协议中,只有等认证消息全部通过后,才可能建立安全路由,一旦报文丢失或是超出时限,则认为认证失败,如果遇到合适节点,则需要重新启动认

证. 针对自组织网络的移动特性, 可以采取信任保留的方法, 该方法的基本思路为: 对每个报文接收的状态进行记录, 保留认证步骤中收到的最后一个报文的验证结果. 在信任保留方案中, 对每个认证过程消息验证结果都保留下来, 一旦重新检测到对方节点邻居广播报文, 则直接发送下一个认证消息, 而不需要重新启动认证过程, 这种保留上次认证结果的方式, 称之为信任保留.

基于信任保留的认证方式对于高速移动的自组织网络身份认证有着较好的应用效果, 有利于提高认证成功, 从而使得安全路由建立更加高效.

3.2 身份认证协议

为了建立安全路由, 需要对新邻居节点进行身份认证, 从而决定是否允许新节点能被加入到其他各个节点的通信路由表中. 认证方案的前提是各个节点获得了自己的公钥证书, 并能够验证其它节点的证书, 在 Ad Hoc 网络中, 这可以通过分布式 CA^[7-8]或是自组织公钥管理机制^[9]实现, 该方案跟我们在文献[5]提出的 SOLSR 认证类似, 并在此基础上增加了 DH 单跳密钥协商机制, 由于引入认证双方随机数因子, 因而能够有效抵抗重放攻击, 另外利用 DH 协商单跳密钥, 对用户数据报文进行加密与摘要处理, 一方面防止窃取以及进行完整性检测, 另外一方面相对公钥签名较好地提高了验证效率. 具体身份认证与协商过程如下:

(1) A 产生一个大的随机数 R_A (其位数和安全级别有关), 随机选取一个 $x (x < m)$, 计算 $g^x \bmod m$ (这里 m 是事先选取的一个大素数, g 是一个模 m 的原根), 然后将公钥证书和节点标识填充到报文中, 报文最后附加上 A 对报文的散列值的签名, 发送给 B . 公式中的 H 为单向散列函数:

$$M_1(A \rightarrow B): A, B, g^x, Cert_A, R_A, \text{sign}(H(A, B, g^x, Cert_A, R_A)).$$

(2) B 收到 A 的报文后, 先验证 A 的公钥证书. 然后用公钥证书中所包含的 A 的公钥验证签名, 有效之后, 产生一个大的随机数 R_B , 随机选取 $y (y < m)$, 计算 $g^y \bmod m$, 将其和自己的公钥证书以及节点标识填充到报文, 然后附加上 B 对上述项进行单向散列运算之后的签名, 发送给 A :

$$M_2(B \rightarrow A): B, A, g^y, Cert_B, R_B, \text{sign}(H(B, A, g^y, Cert_B, R_A, R_B)).$$

(3) A 先验证 B 的证书, 若证书有效, 然后验证签名, 签名也有效的话, A 便可确定 B 是自己的邻居, 并得到一个共享单跳密钥 $g^{xy} \bmod m$, 同时 A 将

产生对 B 的回应报文:

$$M_3(A \rightarrow B): A, B, \text{sign}(H(A, B, R_A, R_B, g^{xy})).$$

(4) B 收到 A 的报文, 验证签名有效后, 就可以确定 A 的合法身份, 同样得到共享单跳密钥 $g^{xy} \bmod m$.

3.3 安全路由计算

(1) 安全路由形成

安全路由的形成一般是从两个节点作为种子节点开始的, 首先这两个节点进行身份认证, 通过后形成可信节点, 然后第三个节点再与这两个其中之一进行身份认证后加入进来, 同理, 后面加入的节点任取一个 Ad Hoc 网络节点进行身份认证后加入, 这种身份认证过程如图 4(a) 所示.

在自组织网络的形成过程中, 还有另外一种形式, 那就是各个节点前阶段形成了多个小网络, 这些小网络之间通过某两个节点认证最后形成一个整体网络. 该认证过程如图 4(b) 所示.

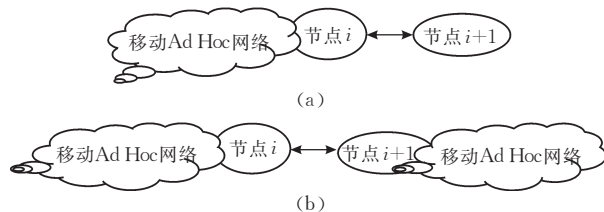


图 4 安全路由形成示意图

对认证节点来讲, 有两种认证模式: 主动模式与被动模式. 主动模式是指发送第一个认证报文的模式, 而被动模式则是指另外一个节点模式. 主动模式工作流程如图 5 所示, 被动模式则如图 6 所示.

在主动模式中, 节点只要接收到报文, 先检查源节点是否通过可信评估, 如果未通过, 则直接丢弃该报文; 否则, 继续下一步处理. 如果收到某个节点发送的广播报文, 则判断该节点是否存在于安全路由表中, 如果存在, 则说明已经通过认证, 如果不存在, 就检查该节点认证保留状态, 检查是否收到过 M_2 . 如果收到过 M_2 , 则说明认证已经完成; 否则就需要发送认证消息 M_1 , 以发起新的认证请求. 在接收报文中, 如果发现是消息 M_2 , 则直接发送消息 M_3 , 以完成认证过程.

在被动模式中, 同样首先进行信任评价, 如果通过, 则判断如果是广播报文, 则检查该节点是否存在于安全路由表中, 如果不存在, 则判断是否接收过 M_1 , 接收过则检查是否收到过 M_3 , 收到说明认证已经完成; 否则发送 M_2 认证报文. 在接收报文的过程中, 如果收到 M_2 认证消息, 则说明自己已经发送过 M_1 , 此时向对方发送 M_2 , 以完成认证过程.

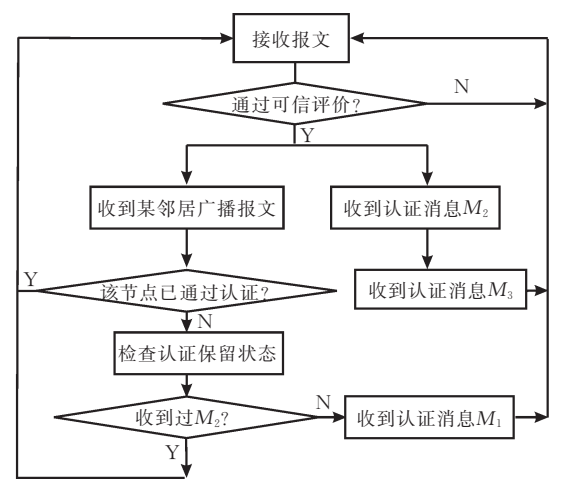


图 5 认证主动模式流程图

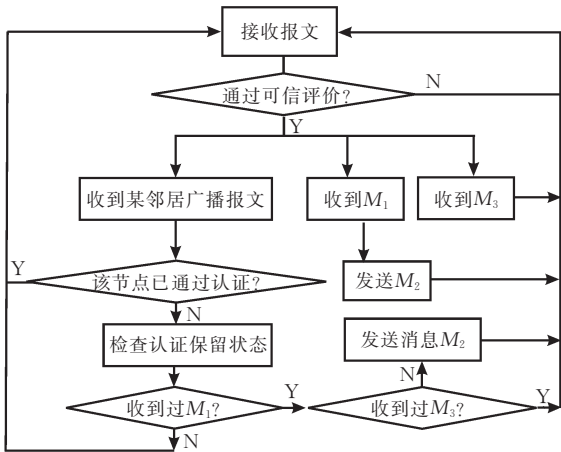


图 6 认证被动模式流程图

基于信任保留的认证流程跟一般认证流程有两点区别：首先是认证中不需要一次连续的将所有认证报文处理完，而是认证状态保留，认证过程中不存在因为超时认证失败的状态；另外就是认证过程采用基于关联规则的可信评价，用来增强整个系统的认证安全性能。

(2) 协议报文的安全附加项

在 OLSR 协议中，所有的消息都是广播形式的，为了抵抗恶意节点广播虚假消息、篡改正常节点的报文等等，TPSRP 提供了一个报文的完整性校验以及接收者验证发布者的机制。

OLSR 的消息格式如图 7 所示。

Message Type	Vtime	Message Size
Originator ID		
Time To Live	Hop Count	Message Sequence Number
MESSAGE		

图 7 OLSR 的消息格式

由图 7 可知，OLSR 的消息项分为两类，一种

是在传输过程中不变的，另一种是在传输过程中要改变的，例如 Time To Live 和 Hop Count 项。针对内容不变的，可以利用数字签名来保证其完整性。对于内容可变项——Time To Live 和 Hop Count，其二者是为了限制报文可传递的范围，可以利用单向散列链表来保证被正确地递减。当发布者要发布消息时，先产生一个随机数 Seed，然后对 Seed 进行 Time To Live 次单向散列运算，其值 $Hash_Hop = H^{Time\ To\ Live}(Seed)$ 。安全附加项的格式如图 8 所示。

Type	Reserved
Hash_Hop	
Seed	
HASH	

图 8 SOLSR 安全报文扩展项

当节点接收到其他节点发布的消息时，决定是否继续转发时，将执行以下步骤：

- ① 先计算 $h^{Time\ To\ Live - Hop\ Count}(Seed)$ 是否和 Hash_Hop 的值相等，若不相等，则表明 Hop Count 被改动过，退出；反之，进行下一步；
- ② 对 Time To Live 自减 1，若大于 0，表明要继续广播该报文，对 Hop Count 自加 1，同时 $Seed = h(seed)$ ，然后转发报文；

图 8 中的 HASH 是发布者对消息中所有不变项进行散列运算后使用单跳密钥加密的密文，基于单跳密钥加密的方式对比公钥加密签名，其效率要高得多，尽量降低了对传输速度的影响。

至此，TPSRP 的报文由于有了安全附加项，保证了报文的完整性，也保证了报文接收者可以验证发布者是否为合法节点。

(3) 路由表的计算

由于 OLSR 协议是基于链路状态的路由协议，因而每个节点是根据全局拓扑结构来选择路由的。在节点定期广播的拓扑控制信息 (TC message) 中，包含有节点对其邻居的信任评价。因而路由计算实际上是在一个边的权值为可信度的有向图中，寻找到达目的节点的一条高可信度的路径。

4 信任评估系统

4.1 信任评估研究现状以及主要问题

目前，信任评估的研究比较多，并提出了相应的支撑理论与方法，如 Guha 等人^[10]提出了基于权重

的信任传递方法; Beth 等人^[11]首先将信任分为直接信任和推荐信任, 利用概率统计的方法计算信任值, 并提出了信任的合成方法. Wang 等人^[12]用贝叶斯网络来解决信誉问题, 通过计算二元评分(正或负)的条件概率值来评估信誉; Yu^[13]等人提出用证据理论解决信任合成问题; Josong 等人^[14]提出了描述和度量信任关系的主观逻辑, 用观点(opinion)来表示主观信任(subjective belief).

上述五种方法是目前信任研究中一般采用的信任计算基础, 这些方法都有一个行为或证据收集阶段, 既可以自己直接获得, 也可以通过其它节点推荐获得, 同时把这些行为或是证据分为恶意的或是合法的, 通过这些收集的信息来计算节点的信任数值. 这些方法不同之处在于信任计算过程、处理过程不同, 其证据或行为如果没有经过事先分类, 则没有办法进行评估. 而在 Ad Hoc 网络中, 新出现的事件、行为是不可完全预知的, 这些方法缺少有效的自适应性和可扩展性, 从而降低了其信任评估的效果. TPSRP 采用基于关联规则的信任评估方案重点是解决信任评估的自适应性问题与可扩展性问题. 关联规则源于数据挖掘, 将数据挖掘引入到信任评估中, 利用它在处理海量数据方面的优势, 可以从大量的网络事件、节点行为中挖掘出正常和恶意行为模式, 自动生成信任评估的规则, 省去了人工区分合法与非法证据的过程.

4.2 基于关联规则的信任评估

数据挖掘是通过仔细分析大量数据来发掘出潜在的、未知的和有用的信息. 在信任评估系统中可以使用数据挖掘技术, 提取用户的行为特征, 总结恶意行为的规律, 从而建立起比较完备的信任规则库来进行恶意行为辨别, 该过程主要分为数据收集、数据的预处理、数据挖掘以及信任值计算 4 个步骤:

(1) 数据采集

为了对 Ad Hoc 网络中各个节点恶意行为进行检测, 需要采集较为全面的原始数据, 每条记录包括的属性: 报文目的 IP(DstIP)、目的物理地址(DstMAC)、目的物理地址对应的主机 IP(DstHostIP)、源 IP(SrcIP)、源物理地址(SrcMAC)、源物理地址对应的主机 IP(SrcHostIP)以及报文收集时间, 则数据项集为 $I = \{Time, SrcMAC, SrcHostIP, SrcIP, DstMAC, DstHostIP, DstIP\}$. 可以在自组织网络中设置多个监听节点, 使得能够监听所有节点的报文, 或是每个节点自身启动监听模式, 也可以完成报文收集过程.

(2) 数据预处理

原始数据项集并不能直接反映 Ad Hoc 网络中的攻击行为, Ad Hoc 网络中很多攻击是针对路由进行攻击, 如黑洞攻击、虫洞攻击等. 因此, 需要将原始数据进行预处理, 以更加直接反映出路由特点; 另外就是需要反映时间相关性, 如果单纯对上述数据进行挖掘, 则只能找出在某个时间点上的规则, 不能反映一定时间内报文的相关性.

根据上述分析, 预处理分为两步:

首先, 对数据进行时间段划分, 设置一个属性, 如最近两秒内的报文有多少. 根据原始数据, 就可以区分出最近两秒内的报文种类属性, 针对某个节点 i 包括 4 类: ① 目的 IP 地址与 MAC 地址都为节点 i 的报文数量, 设为 N_1 , 这表示节点 i 自己需要处理的报文; ② 目的 IP 地址不是节点 i , 但 MAC 地址为节点 i 的报文数量, 设为 N_2 , 这表示节点 i 接收的是需要转发的报文; ③ 源 IP 地址不是节点 i , 但源 MAC 地址为节点 i 的报文数量, 设为 N_3 , 这表示节点 i 发送的为转发的报文; ④ 源 IP 地址是节点 i 且源 MAC 地址为节点 i 的报文数量, 设为 N_4 , 这表示节点 i 自己发送的报文.

对于数据挖掘来讲, 由于报文数量是一个整数类型, 如果直接用来数据挖掘, 将会导致挖掘效率低下甚至挖掘失败, 整数类型的属性值并不适合进行数据挖掘, 预处理的第二步是将数值属性划分为几个区间, 从而将数值属性转换为分类型后, 再采用成熟的布尔型关联规则挖掘算法进行挖掘. 为了避免产生太多的规则, 可以将报文数量划分为高、中、低三个区间, 然后采用 k -means 方法分别对数量进行聚类划分^[15].

k -means 方法是数据挖掘中聚类分析算法的一种. 该算法以 k 作为参数, 把 n 个对象分为 k 个簇, 使簇内具有较高的相似度, 而簇间的相似度较低. 通常采用的聚类准则函数是聚类集中的每个样本点(数据或对象)到该类中心的距离平方之和, 并使它最小化, 算法的流程如下:

1. 选 k 个初始聚类中心: $z_1(l), z_2(l), \dots, z_k(l)$ 括号内的序号为寻找聚类中心的迭代运算的次序号. 聚类中心的向量值可以任意设定, 一般可用开始 k 样本点作为初始聚类中心.

2. 逐个将需分类的样本 $\{x\}$ 按最小距离原则分配给聚类中心的某一个 $z_j(l)$. 假如 $i=j$ 时, $D_j(l) = \min\{\|x - z_i(l)\|, i=1, 2, \dots, k\}$, 则 $x \in S_j(l)$, 其中 l 为迭代运算次序号, 第一次迭代则 $l=1$, S_j 表示第 j 个聚类, 其聚类中心为 z_j .

3. 计算各个聚类中心新的向量值, 即求各聚类域中包

含样本的均值向量 $z_j(l+1) = \frac{1}{N_j} \sum_{x \in S_j(l)} x, j=1,2,\dots,k$, 其中 N_j 是第 j 个聚类域 S_j 中所包含的样本数. 以均值向量为新的聚类中心, 可以使聚类准则函数 $J_j = \sum_{x \in S_j(l)} \|x - z_j(l+1)\|$ 最小, 其中 $j=1,2,\dots,k$.

4. 如果 $z_j(l+1) \neq z_j(l), j=1,2,\dots,k$, 则 $l=l+1$, 回到步 2, 将样本逐个重新分类, 重复迭代计算. 如果 $z_j(l+1) = z_j(l), j=1,2,\dots,k$, 则算法收敛, 计算完毕.

通过使用 k -means 方法, 将原始数据中的数值分类转化为使用 L, M, H 来代替, 并且还得到了这三个类的中心点, 对各个报文统计数值字段进行相同的处理, 这样就将原有的包含数值属性的字段全部替换为布尔型, 而后就可以采用经典的关联规则挖掘方法来进行知识发现.

(3) 关联规则挖掘

在数据预处理完成后, 即可采取数据挖掘算法进行关联规则挖掘. 我们采用 Apriori 算法^[16], Apriori 算法于 1993 年由 Agrawal 提出, 其核心是基于两阶段频集思想的递推算法. 基本思想是:

首先, 由较小的频繁项目集 L_k 产生较大的候选频繁集 L_{k+1} , 如此反复, 找出所有的频集. 这些项集出现的频繁性至少和预定义的最小支持度一样, 然后由频集产生关联规则, 这些规则必须满足最小的支持度和最小的可信度.

(4) 信任计算

经过上述几个步骤, 可形成初始化的信任评估准则, 主机定时进行流量分析与关联规则匹配, 对不符合关联规则的网络流量, 即可认为是恶意行为, 作为一次恶意行为处理, 其信任度计算按照直接信任、推荐信任进行综合计算.

直接信任使用经验贝叶斯估计公式. 根据社会学个人信任行为, 在相同环境条件下, 实体采取的行为近似于概率 P 的二项事件, 因此可利用二项事件后验概率分布服从 Beta 分布的特性推导信任关系. 若用 s, f 分别表示成功次数和失败次数, 直接信任值可表示为

$$D(s, f) = \frac{s+1}{s+f+2}.$$

由于直接信任的经验来自于不同种类, 因而计算直接信任值时, 对不同种类经验赋予不同的权重:

$$D_{i,j} = \sum_{x=1}^n [W_x \times D_x(s, f)],$$

其中 x 代表第 x 种直接经验, W_x 代表第 x 种直接经验的权重.

推荐信任是直接信任和推荐可靠度的函数. 评

估主体 i 对评估客体 j 进行信任评估时, 推荐者 k 的推荐可靠度为 $R_{i,k}$, 那么 i 所采取的间接信任值为 $I_{i,j} = R_{i,k} \times T_{k,j}$, 其中 $T_{k,j}$ 代表 k 对 j 的综合信任, $R_{i,k}$ 代表 k 的可靠度.

为简单起见, 在本模型中 $R_{i,k}$ 就等价于 i 对 k 的综合信任评价 $T_{i,k}$.

因此, 上式就等价于:

$$I_{i,j} = T_{i,k} \times T_{k,j}.$$

若间接信任是来自一条路径 $l: k_1, k_2, \dots, k_n$, 那么此时的间接信任计算公式如下:

$$I_{i,j} = T_{i,k_1} \times T_{k_1,k_2} \times \dots \times T_{k_{n-1},k_n} \times T_{k_n,j},$$

简记为

$$I_{i,j} = T_{i,l} \times T_{l,j},$$

其中 $T_{i,l}$ 为路径 l 的可靠度, $T_{i,l} = T_{i,k_1} \times T_{k_1,k_2} \times \dots \times T_{k_{n-1},k_n}$. 若存在多条推荐路径, 可采用权重最大化算法解决, 将每条推荐路径的可靠度作为信任权重, 得到多条推荐路径信任合成方法:

$$I_{i,j} = \frac{\sum (T_{i,l} \times T_{l,j})}{\sum T_{i,l}},$$

其中 l 代表不同路径.

(5) 综合信任值计算

根据得到的直接信任值和间接信任值, 可得到对目标实体的总体信任值:

$$T_{i,j} = \alpha D_{i,j} + (1-\alpha) I_{i,j},$$

其中 $\alpha \in [0, 1]$, 代表节点对直接信任值和间接信任值的采信程度, 一般由节点自己的策略决定.

5 性能分析与评价

5.1 身份认证协议安全性分析

由于身份认证协议是 TPSRP 协议的关键过程, 这里利用 BAN 逻辑, 对 TPSRP 协议中的身份认证过程进行形式化分析, 论证其正确性.

身份认证过程中的三条消息可以形式化表示为以下三条语句, 其中 A 和 B 是认证的两个实体, K_s^{-1} 是认证机构 S 的私钥:

$$(1) A \rightarrow B: \{ \xrightarrow{k_a} A \}_{K_s^{-1}}, R_a, g^x, \{ H(\xrightarrow{k_a} A, R_a, g^x) \}_{K_a^{-1}};$$

$$(2) B \rightarrow A: \{ \xrightarrow{k_b} B \}_{K_s^{-1}}, R_b, g^y, \{ H(\xrightarrow{k_b} B, R_a, R_b, g^y) \}_{K_b^{-1}};$$

$$(3) A \rightarrow B: \{ R_a, R_b, g^{xy} \}_{K_a^{-1}}.$$

身份认证的目的是要 A 相信消息 2 中的签名确实来自于 B , B 相信消息 1 和 3 的签名确实来自

于 A , 换言之, 要证明 A 相信 B 拥有私钥 k_b^{-1} , B 相信 A 拥有私钥 k_a^{-1} , 即 $A \models B \ni k_b^{-1}$ 和 $B \models A \ni k_a^{-1}$;

初始假设为如下:

$$(i) A \models \xrightarrow{k_a} A, A \models \xrightarrow{k_s} S, A \ni k_s, A \models S \Rightarrow \xrightarrow{k_b} B,$$

$$A \models \#(R_a), A \models \#(\{\xrightarrow{k_b} B\}_{k_s^{-1}}), A \models \phi(\{\xrightarrow{k_b} B\}_{k_s^{-1}});$$

$$B \models \xrightarrow{k_b} B, B \models \xrightarrow{k_s} S, B \ni k_s, B \models S \Rightarrow \xrightarrow{k_a} A, B \models \#(R_b), B \models \#(\{\xrightarrow{k_a} A\}_{k_s^{-1}}), B \models \phi(\{\xrightarrow{k_a} A\}_{k_s^{-1}}).$$

显然, A 确信 k_a 是自己的公钥, k_s 是认证机构 S 的公钥, 同时相信 S 对 k_b 是否是 B 的公钥的判断; A 可以产生有效的随机数 R_a , A 相信 B 的公钥证书的时间有效性; 由于公钥证书的格式是公认的, 自然 B 的公钥证书是可以认知的. 类似的, 关于 B 的假设条件如上;

$$(ii) \text{ 由认知规则可得 } \frac{B \models \phi(\{\xrightarrow{k_a} A\}_{k_s^{-1}}), B \ni k_s}{B \models \phi(\xrightarrow{k_a} A)};$$

$$\text{由消息 1 有 } \frac{B \ni \{\xrightarrow{k_a} A\}_{k_s^{-1}}, B \ni k_s, B \models \phi(\xrightarrow{k_a} A)}{B \models S \sim \{\xrightarrow{k_a} A\}};$$

B 见过 A 的公钥证书, B 拥有 S 的公钥, 而且公钥证书是可以认知的, 自然就可以推出 B 确信 S 曾发布过 A 的证书;

$$\text{由时间有效法则可知 } \frac{B \models \#(\{\xrightarrow{k_a} A\}_{k_s^{-1}}), B \ni k_s}{B \models \#(\xrightarrow{k_a} A)};$$

由前两式, B 可推出 S 相信 k_a 是 A 的公钥这一

$$\text{事实, } \frac{B \models S \sim \{\xrightarrow{k_a} A\}, B \models \#(\xrightarrow{k_a} A)}{B \models S \models \xrightarrow{k_a} A};$$

$$\text{由权限法则得到 } \frac{B \models S \Rightarrow \xrightarrow{k_a} A, B \models S \models \xrightarrow{k_a} A}{B \models \xrightarrow{k_a} A},$$

即 B 相信 k_a 是 A 的公钥;

(iii) 由消息 2, 类似 (ii) 可先得到

$$\frac{A \models \phi(\{\xrightarrow{k_b} B\}_{k_s^{-1}}), A \ni k_s}{A \models \phi(\xrightarrow{k_b} B)},$$

$$\frac{A \ni \{\xrightarrow{k_b} B\}_{k_s^{-1}}, A \ni k_s, A \models \phi(\xrightarrow{k_b} B)}{A \models S \sim \{\xrightarrow{k_b} B\}},$$

$$\frac{A \models \#(\{\xrightarrow{k_b} B\}_{k_s^{-1}}), A \ni k_s}{A \models \#(\xrightarrow{k_b} B)},$$

$$\frac{A \models S \sim \{\xrightarrow{k_b} B\}, A \models \#(\xrightarrow{k_b} B)}{A \models S \models \xrightarrow{k_a} B},$$

$$\frac{A \models S \Rightarrow \xrightarrow{k_b} B, A \models S \models \xrightarrow{k_b} B}{A \models \xrightarrow{k_b} B},$$

即 A 相信 k_b 是 B 的公钥;

又因为

$$\frac{A \models \#(R_a)}{A \models \#(\xrightarrow{k_b} B, R_a, R_b)}, \frac{A \models \#(\xrightarrow{k_b} B, R_a, R_b)}{A \models \#(H(\xrightarrow{k_b} B, R_a, R_b))},$$

由以上结论便可以得到下面式子:

$$\frac{A \ni \{H(\xrightarrow{k_b} B, R_a, R_b)\}_{k_b^{-1}}, A \ni k_b, A \models \xrightarrow{k_b} B, A \models \phi(H(\xrightarrow{k_b} B, R_a, R_b)), A \models \#(H(\xrightarrow{k_b} B, R_a, R_b))}{A \models B \ni k_b^{-1}},$$

即 A 相信 B 拥有 k_b^{-1} , 则 B 的身份得到证明;

(iv) 由消息 3 以及 (ii) 中的结论, 可得到下列结论,

$$\frac{B \ni \{H(R_a, R_b)\}_{k_a^{-1}}, B \ni k_a, B \models \xrightarrow{k_a} A, B \models \phi(H(R_a, R_b)), B \models \#(H(R_a, R_b))}{B \models A \ni k_a^{-1}},$$

即 B 相信 A 拥有 k_a^{-1} , A 的身份得到证明.

经过对三条消息的形式化分析和证明, 可知身份认证的目的达到, 即 $A \models B \ni k_b^{-1}$ 和 $B \models A \ni k_a^{-1}$.

5.2 TPSRP 能够抵御的攻击类型分析

由于采用了安全身份认证协议, 通过前面的分析与证明可知只有合法的用户才可能建立安全路由, 结合路由报文采取的安全机制, 可得知 TPSRP 可以有效地防止来自于外部节点的下列攻击:

(1) 伪造或者篡改攻击. 非法用户由于无法通过身份认证, 无法得到单跳密钥, 从而无法生成一个路由报文所需的摘要.

(2) 重放攻击. OLSR 中每个节点会保存报文的序列号, 而该序列号又包含在单跳密钥生成的 HASH 值中, 重放报文将会被丢弃.

(3) 外部节点合谋攻击. 由于每个路由都是通过认证的节点构成, 外部节点无法进入网络, 因而无法合谋攻击.

(4) 内部节点的虫洞攻击以及中断攻击. 外部由于不能通过身份认证无法实施虫洞攻击, TPSRP 对内部节点的虫洞攻击也能够起到很好的防御作用. 虫洞攻击或是直接的中断攻击最后都会导致丢弃控制报文和数据报文. 当发生攻击时, TPSRP 的信任评估系统将会及时发现这些具备恶意行为的节点, 从而孤立这些节点, 在一定程度上遏制了这种攻击, 仿真中, 将对这些攻击进行分析与说明.

5.3 仿真性能分析

对于移动认证协议,根据 Ad Hoc 网络的特征对其进行了仿真分析,该仿真参数为:节点数为 50,节点随机移动,移动速度从 50m/s 到 500m/s,整个节点活动范围为 1km×1km,每个消息从接收处理再发送回复消息的时间为 500ms,跟运行传统认证协议的仿真参数一样,由于在 SOLSR 安全路由协议中,需要对路由信息进行加密,邻居节点两两之间需要进行身份认证,因此,整个仿真以认证通过率作为性能指标来衡量. 认证通过率 $R = A_{\text{passed}}/C_n^2$,其中, A_{passed} 表示通过的认证过程数量, n 表示总的结点数,认证通过率越高,显然整个网络的连通性能越好.

认证通过率仿真结果如图 9、图 10 所示. 在图 9 中,分别采取 100m/s、300m/s 以及 500m/s 的速度进行计算,从仿真计算结果可以知道,对于传统的 SOLSR 认证过程,其认证通过率随着节点移动速度提高,认证效率下降比较明显,随着时间的推移,其认证通过率的提高非常缓慢,不利于整个网络的畅通.

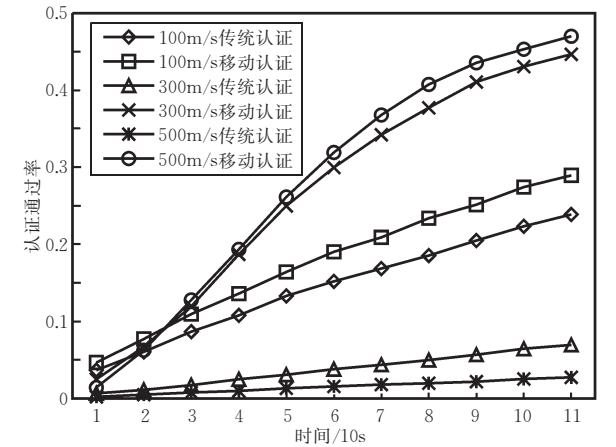


图 9 随时间变化的认证性能对比图

为了更加清晰地了解两种认证方式的差异,根据多次仿真结果,得到如图 10 所示的随速度变化的性能示意图,仿真时间统一为 110s,以不同的速度运行 110s 后,再统计认证通过率. 在图中,对于传统认证协议,随着速度的提高,其总体认证通过率呈下降趋势,尤其是到了 300m/s 以后,整个认证通过率几乎降到了不可用的程度. 对于移动认证协议,在速度较低的情况下,其认证效果跟传统认证协议基本相同,但是随着速度的提高,可以较为明显地看出,其认证效率呈现逐步提高的趋势,这跟传统认证恰好相反. 分析其原因,主要是由于采取信任保留措

施,如果前面认证步骤已经完成,如果节点速度移动较快,则下一次再次相遇的可能性提高,因此,认证效率反而随着速度的提高逐步提高.

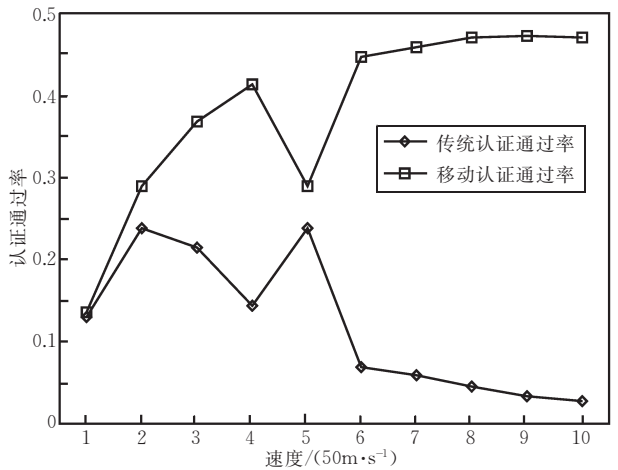


图 10 随速度变化的认证性能对比图

对于抗攻击性能,主要比较在有恶意节点的情况下 TPSRP 与 OLSR 的性能. 采用 NS2 进行仿真,节点个数为 50,仿真时间为 900s,仿真场景为 1000m×1000m,通信连接数为 20 对,节点覆盖半径为 250m,使用 CBR(UDP)通信,节点随机分布. 其中,恶意节点执行的攻击只有如下两种行为:

- (1) 参与路由协议,但不参与其它节点的数据包转发,即自私行为;
- (2) 虫洞攻击,即由两个攻击者联合形成一条隧道,通过隧道将一端监听到的 HELLO 包发送到另一端进行重放,使得本不是邻居的节点,由于互相监听到对方的 HELLO 包而彼此误认为是邻居.

仿真中采取如下性能参数来进行比较.

- (1) 包传输率(packet delivery ration):网络中所有目的节点收到的包与源节点发出包的比率;
- (2) 包丢失率(drop ratio):恶意节点主动丢弃的包与网络中所有节点总共发出包的比率.

模拟的结果如图 11、图 12 所示. 图 11、图 12 所显示的是 TPSRP 和 OLSR 在存在攻击者的情况下,二者的网络性能比较. 为了突出攻击者对网络的破坏效果,我们将节点设置为静止状态(不发生位置变化),从而排除由于节点移动所带来的网络性能影响.

由图 11 可知,随着恶意节点所占比例的变化,两个协议的网络丢包率的变化情况. 当攻击者占有所有节点的 10%~30% 时,TPSRP 的丢包率要比 OLSR 的丢包率平均下降大约 20 个百分点. 但当攻

击者的比例持续上涨时,TPSRP 和 OLSR 的丢包率渐趋一致.如图 12 所示,反应的是 TPSRP 和 OLSR 的包传输率随恶意节点所占比例的变化.当攻击者占有所有节点的 10%~30% 时,TPSRP 的包传输率要好于 OLSR 大约 10 个百分点,随着攻击者的比例上涨,TPSRP 和 OLSR 的网络性能都很糟糕,在攻击者占一半的时候,二者的包传输率都不到 50%.

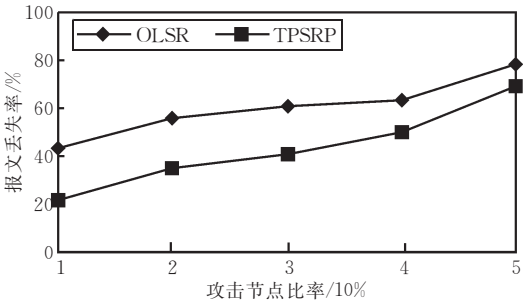


图 11 TPSRP 和 OLSR 的包丢失率比较

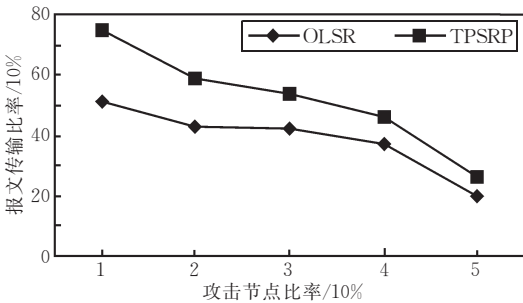


图 12 TPSRP 和 OLSR 的包传输率比较

由图 11、图 12 可知,当网络中攻击者的数目不过半的时候,TPSRP 的性能优于 OLSR.

为进一步说明基于关联规则的信任评估效果,我们单独进行了仿真实验,以虫洞攻击为例,采取如图 13 所示的攻击场景,图中 $N_0 \sim N_{11}$ 为正常节点, A_1 与 A_2 为攻击节点,仿真时间为 200s,正常节点覆盖范围为 100m,攻击节点覆盖范围为 250m,通信方式采取 UDP,包发送速度为 20 个/s,各个节点采取静止的方式.

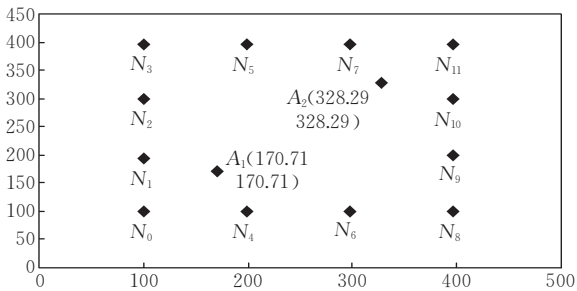


图 13 典型虫洞攻击节点分布示意图

在路由形成过程中,由于 A_1 与 A_2 的相互配合,导致 N_0 认为 N_{11} 是其邻居节点, N_0 发给 N_{11} 的报文全部转发给了 A_1 ,导致通信出现中断.而 N_0 在一般情况下会认为是普通网络故障.在 N_0 上安装了基于关联规则的恶意节点数据挖掘模块以后, N_0 检测所有邻居节点的通信流量,数据存储格式为 $I = \{Time, SrcMAC, SrcHostIP, SrcIP, DstMAC, DstHostIP, DstIP\}$.

在经过 200s 后,得到一定数量的检测数据,按照前面的方案对这些数据进行预处理,预处理后的格式为 $I' = \{Time, OwnRecvNum(N_1), OwnRecvForwardNum(N_2), OwnSendForwardNum(N_3), OwnSendNum(N_4)\}$ 对所有数量按照高、中以及低对其进行聚类分析后,除了时间 Time,其它各个字段只有三种可能的字段值,然后再利用 Apriori 算法对其进行规则挖掘.

在选取支持度的时候,根据 Ad Hoc 网络节点不固定、拓扑结构容易变化的特点,可以选取较低的支持度,以扩大规则的检测面.本仿真中,支持度选取为 10%,可信度设置为 60%,在节点通信中, N_0 使用 UDP 协议随机与其它各个节点通信,将监听到的所有数据保存下来,通过统计计算后得到的规则如表 1 所示.为了减少没有意义的规则,所有规则中接收的属性值在前,发送的属性值在后.

表 1 数据挖掘规则表			
项目集	支持度/%	可信度/%	备注
N_1 (低) N_4 (低)	14.5	89.6	各个节点接收与发送的全局路由报文数量比值
N_3 (低) N_4 (低)	10.2	72.7	正常转发报文应该满足的条件
N_3 (高) N_4 (高)	20.5	78.7	正常转发报文应该满足的条件

从上面挖掘的结果可以知道,第一条规则反映的是路由报文的正常发送与接收统计规律,因为路由控制报文是以比较低的频率发送,第二条与第三条反映的是路由节点在正常情况下,转发报文的统计规律.通过这三条一般规则,就可以针对每个邻居节点进行行为分析,不符合统计规律的节点可以认为是具有恶意嫌疑的行为节点,通过计算其信任值即可判断出是否具备恶意行为.

接下来对 A_1 节点进行统计,采集 20s 的数据,按照上述各个规则对数据进行统计与分析,很快发现,第一条规则基本符合,第二条与第三条支持度以

及可信度几乎为 0, 很快判断出 A_1 为恶意节点, 从而将 A_1 从路由表中去掉, A_1 与 A_2 联合实施的虫洞攻击失效. 通过上述仿真计算表明, 基于关联规则的信任评估机制能够较好地发现路由节点中的恶意行为, 这种恶意行为并不需要事先人为定义, 采取数据挖掘方法就可以完成路由异常的判断工作, 从而提高了整个 Ad Hoc 网络的安全性能.

6 小 结

Ad Hoc 网络的移动特性是安全路由中不能忽略的一个重要因素. 本文的分析与仿真表明, 在一个频繁变化甚至高速移动的网络中, 传统的安全身份认证方式效率极为低下, 这是因为认证过程是一个连续有序的消息交互过程, 移动特性使得这个连续交互无法保证. 为此, 本文一方面提出了基于信任保留的移动身份认证协议, 该协议对每个步骤的认证结果进行保留, 下一次节点相遇的时候继续认证过程, 通过这种认证结果保留的方式, 提高认证的可靠性. 仿真表明, 在节点移动性能较强的情况下, 有效地提高了认证效率. 另外一方面, 采用数据挖掘中基于关联规则的行为检测方法对认证过程中或是认证通过后的节点进行信任评估, 自我识别恶意行为, 以此提高信任评估的可扩展性. 本文设计了针对 Ad Hoc 网络中路由攻击的检测规则, 通过一个典型的虫洞攻击仿真表明, 该方法能够有效检测 Ad Hoc 网络中的异常或是恶意行为.

参 考 文 献

- [1] Papadimitratos P, Haas Z J. Secure routing for mobile Ad Hoc networks//Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDs 2002). 2002: 1-13
- [2] Sanzgiri K, Dahill B, Levine B N et al. A secure routing protocol for ad hoc networks//Proceedings of the 10th IEEE International Conference on Network Protocols. Paris, France, 2002: 78-87
- [3] Hu Y C, Perrig A, Johnson D B. Ariadne: A secure on-demand routing protocol for Ad Hoc networks//Proceedings of the 8th Annual International Conference Mobile Computing and Networking (MobiCom2002). Atlanta, GA, United States, 2002: 12-23
- [4] Hu Y-C, Johnson D B, Perrig A. SEAD: Secure efficient distance vector routing in mobile wireless Ad Hoc networks//Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 02). Callicoon, NY, 2002: 3-13
- [5] Hong Fan, Hong Liang, Fu Cai. Secure OLSR//Shih T K, Shibata Y eds. Proceedings of the 19th International Conference on Advanced Information Networking and Applications. Taipei, China, 2005, 2(1): 713-718
- [6] Marti S et al. Mitigating routing misbehavior in mobile Ad Hoc networks//Proceedings of the 6th Annual International Conference Mobile Computing and Networking (MobiCom 2000). Boston, MA, USA, 2000: 255-265
- [7] Kong Jiejun, Zerfos Petros, Luo Haiyun et al. Providing robust and ubiquitous security support for mobile Ad-Hoc networks//Proceedings of the 2001 International Conference on Network Protocols ICNP. Riverside, CA, 2001: 251-260
- [8] Zhou L, Hass Z J. Securing Ad Hoc networks. IEEE Network, 1999, 13(6): 24-30
- [9] Srdjan Capkun, Levente Buttyan. Self-organized public-key management for mobile ad hoc networks. IEEE Transactions on Mobile Computing, 2003, 2(1): 52-64
- [10] Guha R, Kumar R, Raghavan P. Propagation of trust and distrust//Proceedings of the 13th International World Wide Web Conference Proceedings, WWW2004. New York, 2004: 403-412
- [11] Beth T, Borchherding, MKleinB. Valuation of trust in open networks//Proceedings of Computer Security — ESORICS 94. 3rd European Symposium on Research in Computer Security. Brighton, UK, 1999: 3-18
- [12] Wang Y, Vassileva J. Bayesian network trust model in Peer-to-Peer networks//Proceedings of Agents and Peer-to-Peer Computing. 2nd International Workshop, AP2PC 2003. Melbourne, Vic., Australia, 2004: 23-34
- [13] Yu B, Munindar P. An evidential of distributed reputation management//Proceedings of the 1st International Joint Conference on: Autonomous Agents and Multiagent Systems, AAMAS02. Bologna, Italy, 2002: 294-301
- [14] Josong A. Trust-Based decision making for electronic transactions//Yngstrom L, Svensson T eds. Proceedings of the 4th Nordic Workshop on Secure Computer Systems. Kista: Stockholm University Press, 1999: 1-21
- [15] Yu Feng, Wang Min, Gao Xiang. The research of mining quantitative association rules for intrusion detection system. Computer Applications and Software, 2006, 23(11): 52-53 (in Chinese)
(于枫, 王敏, 高翔. 数值型关联规则挖掘在网络入侵检测系统中的应用研究. 计算机应用与软件, 2006, 23(11): 52-53)
- [16] Agrawal R. Mining association rules between sets of items in large databases//Proceedings of the 1993 ACM SIGMOD International Conference on Management of Data. Washington, DC, USA, 1993: 207-216



FU Cai, born in 1976, Ph.D., lecturer. His main research interests include wireless networking security, routing algorithms and software vulnerability.

HONG Fan, born in 1942, professor, Ph.D. supervisor. Her main research interests include information security

and security model.

HONG Liang, born in 1979, Ph.D., lecturer. His main research interests include networking, routing algorithms and security in Ad-Hoc networks.

PENG Bing, born in 1972, Ph.D., lecturer. His main research interests include wireless networking security and cryptology.

CUI Yong-Quan, born in 1977, Ph.D., lecturer. His main research interests include access control and cryptology.

Background

Due to "infrastructureless", dynamic topology, and openness of wireless links, Ad Hoc network routing protocols face more security problems than that of traditional networks. Recently, a number of protocols have been proposed to secure wireless Ad Hoc routing. Papadimitratos and Haas proposed the Secure Routing Protocol (SRP). Ariadne is a secure on-demand routing protocol based on DSR and TESLA, ARAN is based on AODV and proposed by Dahill, the authors proposed the SOLSR secure routing scheme, designed the wormhole detecting scheme, identity authentication and packet's security extensions to defend against the attacks existing in Ad Hoc networks.

However, All above research didn't pay attention to the moving characteristic in Ad Hoc networks, which is a important factor in secure routing for Ad Hoc networks. Most secure routing protocols are difficult to finish the authenticating processing and can't set up the secure routing in a mutative and high speed moving network because authenticating is a continuous processing for messages exchanging and the moving characteristic can't ensure the continuity.

This paper proposes the trust preserving based secure routing protocol based on OLSR, the trust preserving method is adopted to accomplish the authenticating and resolve the high speed moving authenticating problem, which is proved with the formal language. The authors focus on the following two aspects:

(1) The routing performance of TPSRP. In a moving Ad Hoc networks, because the trust preserving mechanism is adopt, the TPSRP's authenticating performance is more better than that of the traditional, especially when the moving speed is high.

(2) The security of TPSRP. Aiming at the low flexibility of most trust evaluating system, a novel evaluating system based on data mining is proposed, by which the nodes get the trust information, identify and limit the vicious nodes, at the same time, it can resist the associated attacks, such as worm-hole attack.

This paper is supported by the National Natural Science Foundation of China under grant No. 60403027.