一种基于邻居信任评估的虫洞防御机制*)

洪 亮 洪 帆 彭 冰 陈 晶
(华中科技大学计算机科学与技术系 武汉 430074)

摘 要 移动 ad hoc 网是一种新型无线移动网络,具有无中心、自组织、拓扑结构变化频繁以及开放式通讯信道等特性,因此 ad hoc 网络下的路由协议所面临的安全问题比有线网环境中更为严重。虫洞攻击就是其中的一种,能够对 ad hoc 网络产生致命的影响。在这种攻击下,网络的路由机制将会紊乱,特别是那些依赖通过接收对方的广播报文进行邻居探测的路由协议。本文首先从虫洞形成的根源上入手,重新定义了邻居的概念,强调了邻居作为节点信息转发第一站的功能。然后根据邻居定义,引入简化的 Marsh[1] 信任模型,将邻居的以往表现作为信任评估的经验来源,再通过具体公式对邻居关系做出判定。在具体的路由过程中,节点根据信任评估值选取高可信度的邻居作为下一跳的转发节点,从而避免虫洞攻击的危害。为了验证方法的可行性,本文将模型应用于 OLSR 路由协议中并在 NS2 中进行了仿真。

关键词 移动 ad hoc 网络,虫洞攻击,邻居关系,Marsh 信任模型,OLSR,安全路由

Defend against Wormhole Attack Based on Neighbor Trust Evaluation in MANET

HONG Liang HONG Fan PENG Bing CHEN Jing
(Department of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074)

Abstract Mobile Ad hoc Networks(MANET) is a new networking paradigm for wireless hosts. Because of self-organization, dynamic topology and openness of wireless links, the routing security in MANET is more seriously than in wired networks. Wormhole attack is one of the deadly attacks to the MANET, which is executed by two or more attackers by constructing a tunnel to replay the routing protocol. Under this attack, the routing protocol will not work, especially which rely heavily on the reception of broadcast packets as a means for neighbor detection. In this paper we give a new definition of neighbor which stresses the neighbor's function as "the first relay". Then we introduce Marsh model. By gathering data from the neighbor's events the node can evaluate the trustiness of its neighbor. From building the neighbor's trustiness, the false neighbor formed by wormhole attack will be scored lower value because of transmission failures events in MAC layer. When finding the route, the node will choose the higher trust value neighbor to relay the packet. We apply the model in the OLSR protocol and simulate it in NS2.

Keywords Mobile ad hoc network, Worm-hole attack, Neighboring nodes, Marsh model, OLSR, Securing routing

1 引言

移动 ad hoc 网络是一种临时自治的分布式系统,具有无中心、自组织、网络拓扑结构变化频繁等特征。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 ad hoc 网络环境下的路由协议相对于有线网环境下的更易遭受各种攻击。

在"A survey of secure wireless ad hoc routing"[2]一文中,把针对移动 ad hoc 网络路由协议的攻击分为两种:一种是针对路由机制的破坏攻击,一种是针对路由资源(节点的存储资源、计算资源等等)的消耗攻击。比如冒充合法节点,发布虚假路由信息,形成环形路由;或者形成黑洞攻击——攻击者宣称自己是最短路径的入口,导致路由指向自己,但并不转发通讯数据包;或者形成灰洞攻击——类似黑洞,但攻击者可以有选择性地转发一些数据包而丢弃某些数据包。这些都属于针对路由机制的破坏攻击。至于针对路由资源的消耗攻击,最典型的就是拒绝服务攻击,恶意者频繁地发布大量的路由探测包,消耗带宽和节点的计算资源,从而导致正常节点无法占用信道等等。

虫洞攻击是第一种类型的攻击,由两个或两个以上的攻击者联合形成一条隧道,通过隧道将一端监听到的数据包发送到另一端进行重放。这种攻击对路由协议危害最大。一般来说隧道的长度肯定大于普通的一跳距离即节点的信号覆盖半径,但在路由上却体现为一跳距离。因而节点在选择路由时,肯定倾向于虫洞所形成的路径。这样一来,攻击者就可以执行诸如黑洞攻击或者灰洞攻击等等。

虫洞攻击对通过收发广播报文(比如 HELLO 包)来确定邻居关系的路由协议尤为奏效,如图 1 所示。

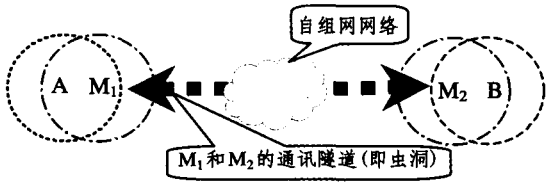

图 1 存在虫洞的网络示意图

*)湖北省自然科学基金(2005ABA243)。洪 亮 博士研究生,主要研究领域为无线网络安全、路由协议的安全评估及仿真;洪 帆 教授,博士生导师,主要研究领域为信息安全;彭 冰 讲师,主要研究领域为网络安全;陈 晶 博士研究生,主要研究领域为网络安全。

其中 A 和 B 是相隔甚远的两个节点，彼此不在信号覆盖范围内，M_1 和 M_2 是虫洞的两端。在这个网络中，邻居探测是通过彼此接收到对方的 HELLO 报文来确定的。当 A 发 HELLO 报文时，M_1 将其通过隧道传给 M_2，由 M_2 将 MAC 帧原封不动地重放。B 由于在 M_2 的信号覆盖范围内，故而接收到重放的 A 的 HELLO 报文，从而判定自己在 A 的信号覆盖范围内，并会在自己的 HELLO 报文中体现；当 B 广播 HELLO 包时，也会被 M_2 通过隧道传给 M_1，然后重放，导致 A 认为自己在 B 的信号覆盖范围内，从而形成 A 和 B 互认为“邻居”，而且此“邻居关系”将会体现在后来的路由机制中。在移动自组网中，常见的路由协议 DSR、AODV、DSDV、TORV、OLSR 等等，都采取这种方式进行邻居探测。

由于虫洞攻击利用了移动 ad hoc 网络的开放式特点，同时攻击者并没有更改协议报文，对节点的路由层而言是不可见的——攻击者并不出现在路由的路径上，所以传统的密码技术并不能检测出这种攻击。

本文基于移动 ad hoc 网络和虫洞攻击的特点，首先从虫洞攻击形成的根源上入手，重新定义了邻居的概念，进而引入了 Marsh 信任模型，通过收集邻居以往信息作为信任评估的经验，然后根据模型对邻居关系进行可信评估。在选择路由时，将选取可信度高的邻居作为下一跳的转发节点，以此来避免虫洞所形成的路径。

本文第 2 节对目前关于虫洞攻击的研究做一个概述性的描述和评价；第 3 节给出邻居的定义以及信任模型的框架；第 4 节是将框架应用于 OLSR 协议并给出仿真结果；最后是全文的总结及下一步展望。

2 相关工作

虫洞攻击最早是由 B. Dahill[3] 发现的。为了抵御这种攻击，曾提出用硬件设计和信号处理方式来解决。一种方法是邻居节点之间通过一种特殊的信号调制方式来传输信息；另一种方法是通过将水印嵌入载波频率中，从而实现物理层级别的认证。但是这两种方式并不能从根本上抵御虫洞攻击，若攻击者复制载波信号，然后在另一段重放这些信号，仍然可以达到攻击的效果。

L Hu 和 D. Evans[4] 采用有向天线来防御虫洞攻击，这种方式是从无线信号的辐射角度来考虑的。每个节点通过检查所接收到信号的来源方向来进行邻居判定，只有双方的方向匹配，才能确定邻居关系。

文[5]提出给每个节点都配备一个硬件装置，这种装置可以对 1bit 的挑战请求进行无延时的响应，通过计算报文的来回时间，然后根据信号传播速度，计算出两个节点之间的距离，以此来判断邻居关系。这种方法主要受到 MAC 层接入延时难以估计的限制，同时排队延时一般比传播时间大一个数量级。因而，通过这种方式进行计算距离，误差比较大。

Y. Hu, A. Perrig, 和 D. Johnson[6,7] 提出用包束缚的方式防御虫洞攻击。包束缚的主要思想是通过在协议报文中添加某些信息来限制数据包的传输范围。文中提出两种包束缚：一种是时间束缚，一种是位置束缚。在实现时间束缚方案时，对网络中节点的时间同步性要求高。当节点发送报文时，将发送时间 t_s 包括到报文中。接收节点收到报文时，记录接收时间 t_r，然后通过传播距离和光速度、传播时间之间的公式，计算出报文的传播距离，然后来判断报文是否超过了传输范围。这种方式仍然有很大的误差性，因为传输时间等于排队时间和传播时间的总和，在时间束缚的方案中简单地把排队时间忽略是不合适的。在通常情况下，排队时间比传播时间大一个数量级。位置束缚是通过为每一个节点配备一个类似 GPS 的位置定位系统，每个节点可以随时获得位置信息。在节点发送报文时，就将自己的位置信息包括到报文中，接收节点通过比较报文中的位置信息和自己的位置信息，来判断报文是否超过了传输范围。这种方式受到地理位置的限制，比如地形影响等等。

3 邻居定义及信任评估模型

3.1 邻居定义

虫洞攻击对路由协议的最大危害就是导致节点之间邻居关系不明、邻居关系不确定，进而影响到路由过程。在移动 ad hoc 网络环境中，节点没有直接手段来判断另一个节点是否是自己的邻居，很多情况下都是靠收发 HELLO 邻居探测报文来实现的。而这些探测报文是可以重放的，故而并不能作为判断邻居关系的确凿证据。虫洞本身并没有攻击性。从某方面来说，虫洞使得两端的通讯距离缩短，本身是一件好事。虫洞两端的节点完全可以作为邻居看待，但虫洞若被攻击者利用，其危害性就大了。故而本文从“邻居作为信息中转第一站”的角度来定义邻居关系。换言之，是否是邻居，要从邻居的表现上来判定，而不是完全按信号覆盖范围来决定。邻居的定义如下：

定义 所谓邻居就是在路由层表现为能够直接通信的节点，并在路由过程中作为信息转发第一站，能够正确无误地完成转发任务。

因而判断某个节点是否是邻居，只要通过收集该节点的以往行为，并通过某种方式根据邻居的定义进行评价，从而对邻居关系做出判定。

3.2 信任评估模型

本文采用了 Marsh 信任模型，这个模型是建立在信任的社会属性上，信任来自于一个实体对另一个实体所有以前行为的评估。通过对行为的重要性和可用性进行量化和分类，然后由信任代理进行信任度的计算。在本模型中，为了简便起见，把行为的重要性和可用性合而为一，统一为权值 W，这个值在信任评估过程中是随时间变化的。

在引入简化的 Marsh 信任模型后，网络中每一个节点都设置一个信任代理。通过收集邻居的行为或者事件，把这些行为进行分类，并根据这些行为对“判断该节点是邻居”的重要性和可用性进行量化，最后由信任代理给出信任度评估。

3.2.1 信任产生

在本模型中，信任产生主要来自于邻节点，因而属于直接信任经验。直接信任经验可从两方面获得。

①在链路层，节点可以收集到的邻居的信息大致包括以下几类：

1)邻节点的数据帧；

2)邻节点的控制帧；

3)邻节点转发的数据帧；

4)邻居点转发的控制帧。

②在网络层：

1)邻节点的数据包；

2)邻节点的控制协议报文(比如路由协议报文)；

3)邻节点转发的数据包；

4)邻节点转发的控制协议报文。

通过对这些事件的收集，并将这些事件分类，就形成产生信任的各种信任类别。

3.2.2 信任量化

在本模型中，用[0，+1]之间的值来代表对“节点是邻居”的信任度评估，+1 代表完全信任，0 代表初始状态。用[0，1]代表某一类事件的重要性，即权值 W。比如，邻节点是否正常转发数据帧这类事件，对于判断邻居关系很重要，那么该类事件就可以赋值为 1，即越重要的信任类别其权值越高。

3.2.3 信任计算

在这一计算过程中，使用了简单贝叶斯模型方法。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。

对于二项分布，$f(y|\theta,m)=\binom{n}{y}\theta(1-\theta)^{n-y}$。当先验概率为 Beta($\alpha$，$\beta$) 分布时，其后验概率分布为：

$$P(\theta)=\frac{\Gamma(\alpha+\beta+n)}{\Gamma(\alpha+y)\Gamma(\beta+n-y)}\theta^{y+\alpha-1}(1-\theta)^{\beta+n-y-1}$$

这是参数为($\alpha+y$，$\beta+n-y$) 的 Beta 分布，可作为估计后验均值 θ，其中 n 表示总实验次数，y 表示成功次数。若 Beta 先验分布为均匀分布，下一次试验成功概率为：

$$P(event=\mathrm{TRUE}|y,n)=\frac{\Gamma(n+2)}{\Gamma(y+1)\Gamma(n-y+1)}\times\frac{\Gamma(y+2)\Gamma(n-y+1)}{\Gamma(n+3)}=\frac{y+1}{n+2}$$

此概率是对实体未来行为的期望值，可用以表示实体的信任程度。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：

$$T^d(s,f)=\frac{s+1}{s+f+2}.$$

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

$$T=\sum_{x=1}^{n}[W_x\times T_x^d(s,f)]$$

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。

4 改进 OLSR 协议及其仿真

4.1 OLSR 协议概述

OLSR[8] 协议包含 4 个重要的过程：邻居探测、中继代理选择、路由控制消息的发布、路由表计算。

OLSR 的邻居探测是通过定期广播邻居探测消息——HELLO 包来实现的，邻居探测消息包含有发布节点 A 的信息以及它的邻居信息。A 的邻居，比如节点 B，接收到 A 的探测包后，先检测其邻居表中是否有 A。若没有，则将 A 添加到邻居表中；若已存在，则刷新 A 的存活时间。当在一个固定的时间间隔内没有接收到来自 A 的探测包时，B 将把 A 从邻居表中删除。

在进行邻居探测过程后，节点将从邻居表根据某种算法选出多点中继代理——MPR。MPR 有两个职责：1)MPR 要负责转发节点的广播报文，节点的其他邻居不能转发，其目的是减小洪泛；2)MPR 要负责在网络中广播它的中继雇主表，其目的是让其他节点知道通过该 MPR 可以到达哪些目的节点。每一个节点选择出 MPR 节点后，会将这一信息反映在下一次的 HELLO 包中。

在邻居表更新，进行中继代理选择之后，中继代理节点将定期广播拓扑控制消息，拓扑控制消息中包含发布节点的邻居信息。其它节点收到消息后，根据消息的序列号来决定是否接收该消息。

在收到拓扑信息报文后，每一个节点都可以得到一个全局的拓扑网络表，然后利用 Dijkstra 算法计算出到其他节点的最短路径，形成路由表。

4.2 引入信任模型的 OLSR 协议

在仿真中，节点只收集表 1 所示的两类事件。

表 1 事件分类

控制帧—Hello 包按时发送(C_h)	Success	s_h
	Fail	f_h
数据帧接收转发(Cd)	Success	s_d
	Fail	f_d

其中 $T_x(C_h)\frac{s_h+1}{s_h+f_h+2}$

$$T_x(C_d)=\frac{s_d+1}{s_d+f_d+2}$$

在信任计算中，利用如下公式计算节点 x 对“节点 y 是邻居”的信任度：

$$T_x(y)=W_x(C_h)\times T_x(C_h)+W_x(C_d)\times T_x(C_d)$$

具体框架图如图 2。

当节点第一次接收到某节点的 HELLO 报文时，在信息收集模块为这个节点建两条记录〈*node_id*，*positive*，*negative*，*even_Hello*〉和〈*node_id*，*positive*，*negative*，*event_dataforward*〉。在后续的时间里，每当按时收到一条 HELLO 报文，第一条记录的 positive 自加 1，反之 negative 自加 1；同理，当被监测节点成功转发数据帧时，第二条记录的 positive 加 1。反之，若是出现链路错误，或者监测到没有转发，negative 加 1。

这两条记录将成为信任计算模块的输入。根据上述公式，将计算出该节点的信任值，并将结果〈node_id，trustvalue〉输入到邻居表中。在进行 MPR 选择时，邻节点的信任值将作为权值。

当节点在广播拓扑控制消息时，所包含的邻居信息都带有权值。进而节点所形成的拓扑结构图将是一个带权值的有向图，其中权值代表着邻节点之间存在链路的可能性。在进行路由表计算过程中，这些权值都将成为 Dijkstra 算法的输入项，计算得到的路径将是可信度最高的路径。从而通过这种自适应的方式来抵御虫洞攻击对路由机制的危害。

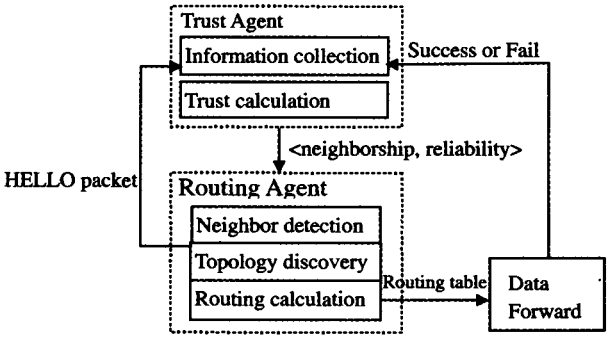

图 2 引入信任模型的 OLSR 路由协议框架图

4.3 仿真

为了验证模型，利用 NS2[9] 仿真环境进行了模拟。在模

拟环境中，构造了两个恶意节点，这两个恶意节点执行虫洞攻击，然后在有攻击的情况下分别模拟了没有信任模型以及有信任模型两种状态下 OLSR 协议的运行情况。具体实验参数如表 2。

表 2　实验参数

正常节点个数	12
攻击者个数	2
仿真时间	90 seconds
正常节点信号覆盖半径	100m
攻击者信号覆盖半径	250m
通信方式	CBR(UDP)
载荷	512 bytes
包发送速率	20kbps
移动模型	静止

12 个正常节点(N_0～N_{11})和 2 个恶意节点(A_1 和 A_2)的坐标如图 3 所示。

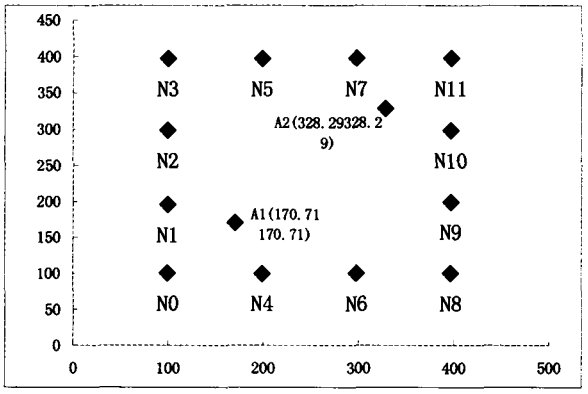

图 3　节点在仿真环境中的坐标分布示意图

在两次仿真中，节点 N_0 将从第 20s 开始发送 UDP 数据包给 N_{11}，包的发送速率是 20kbps，每个包的载荷是 512 字节。然后分别计算两次仿真中 N_0 的实际传输速率，仿真结果如图 4 所示。

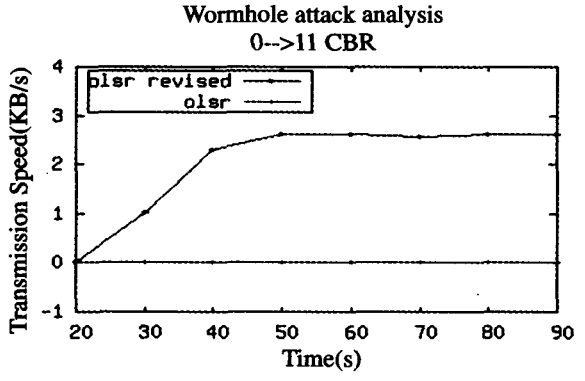

图 4　仿真结果

绿线代表的是没有引入模型的 OLSR 协议运行结果。由图可见，在虫洞攻击的影响下，N_0 的实际传输速率为 0。这就意味着，节点 N_0 根本没有找到一条正确的到达 N_{11} 的路径。由节点的坐标分布图可以知晓，A_1 和 A_2 的虫洞攻击使得 N_0 和 N_{11} 互认邻居，因而导致路由出错。但由于没有相关的反馈机制和监测机制，这一错误无法纠正，致使 N_0 的传输速率为零。

红线是引入信任评估模型后的仿真结果。在仿真中，将控制帧的监测，即 HELLO 包按时收到事件的权值定为 0.3，即 $W_r(C_h)=0.3$；而数据帧正常接收转发事件的权值定为 0.7，即 $W_r(C_d)=0.7$。在初期，由于虫洞的存在，N_0 和 N_{11} 互相以为是邻居，但在 N_0 从第 20s 按邻居关系的一跳路由向 N_{11} 发送数据包的时候，N_{11} 实际并不能接收到数据帧，导致 N_0 链路层出错(MAC Failure)，随着数据帧接收失败的次数增多，N_0 对“N_{11} 作为一个邻居”的信任评估就越来越低，同时通过 N_1、N_2、N_3、N_5、N_7 到 N_{11} 传送成功次数的增加，使得 N_0 对 N_1 的信任评估越来越高，最后在第 50s 时，N_0 的传输速率开始达到稳定，约 2.6kb/s。

总结及下一步工作展望　虫洞攻击是目前影响移动 ad hoc 网络发展的一大威胁。虫洞攻击主要利用了目前路由协议中邻居定义的缺陷——过于注重地理位置而忽视了作为一个邻居应有的表现。本文通过重新定义邻居的概念，强调了邻居作为信息中转第一站的重要性，并以此作为评判邻居关系的标准；同时引入简化的 Marsh 信任模型，对邻居的以往行为进行收集，根据邻居的定义进行实时评估，由评估的结果，来指导具体的路由。通过实验仿真，可以得出采用该信任模型对邻居关系进行评估的方法来抵御虫洞攻击是有效的。

本文所提出的方案相对于以前的工作，有着以下优点：①不需要网络时间同步；②不需要外加辅助设备，比如 GPS 等；③方案实施简单。但该方案也存在缺点，由于评估结果相比虫洞形成在时间上是滞后的，因而具有延迟性。此外，还需要解决诸如如何合理分类经验信息、如何保障经验信息的可靠传递以及如何搜索经验推荐路径等问题，这些都将是我们进一步研究的内容。

参 考 文 献

1　Marsh S P. Formalizing Trust as a Computational Concept:[Ph. D Thesis]. Department of Mathematics and Computer Science, University of Stirling, 1999

2　Hu Yih-Chun, Perrig A. A survey of secure wireless ad hoc routing. Security & Privacy Magazine, IEEE, 2004, 2: 28～39

3　Dahill B, Levine B, Royer E, et al. A secure routing protocol for ad hoc networks:[Tech report]. 02-32, Dept. of Computer Science, University of Massachusetts, Amherst, 2001

4　Hu L, Evans D. Using directional antennas to prevent wormhole attacks. In: Proceedings of Network and Distributed System Security Symposium(NDSS), 2004

5　Capkun S, Buttyan L, Hubaux J. Sector: Secure tracking of node encounters in multi-hop wireless networks. In: Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003

6　Hu Y-C, Perrig A, Johnson D B. Packet leashes: a defense against wormhole attacks in wireless networks. INFOCOM 200. 3, . 2003, 3: 1976～1986

7　Hu Y-C, Perrig A, Johnson D B. Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. In: ACM Workshop on Wireless Security(WiSe 2003), 2003. 30～40

8　Clausen T, Jacquet P, eds. Optimized Link State Routing Protocol (OLSR). RFC 3626, 2003

9　NS-2 Simulation Tool. http://www.isi.edu/nsnam/ns/