◎网络、通信与安全◎

MANET 中“虫洞”攻击的位置检测算法设计与仿真

柳 楠[1],杨 森[2],柴乔林[3],王向辉[1]
LIU Nan[1],YANG Sen[2],CHAI Qiao-lin[3],WANG Xiang-hui[1]

1.山东建筑大学 计算机科学与技术学院,济南 250010
2.济南移动通讯公司,济南 250012
3.山东大学 计算机科学与技术学院,济南 250061
1.School of Computer Science and Technology,Shandong Jianzhu University,Ji'nan 250010,China
2.Ji'nan Mobile Communication Corporation,Ji'nan 250012,China
3.School of Computer Science and Technology,Shandong University,Ji'nan 250061,China
E-mail:belovedmilk@126.com

LIU Nan,YANG Sen,CHAI Qiao-lin,et al.Design and simulation for location detection algorithm preventing wormhole attack in MANET.Computer Engineering and Applications,2007,43(34):119-121.

Abstract: Wormhole attack—a kind of seriously malicious attack is analyzed and a brief location detection algorithm that can effectively detect wormhole is brought forward.Then some simulation experiments in OMNeT++ are designed.Aiming at results of simulations,effects on detection algorithm that are brought by all kinds of factors of MANET are analyzed.The validity of the algorithm is certified.

Key words: mobile Ad hoc network;wormhole attack;location detection algorithm;Objective Modular Network Testbed in C++(OMNeT++)

摘 要: 着重研究了移动 Ad hoc 网络中一种严重的恶意攻击——“虫洞”攻击,针对其提出一种简洁高效的位置检测算法,并采用 OMNeT++仿真器进行仿真实验,根据实验分析移动网络中的各种因素对位置检测算法执行的影响,证明了算法的有效性。

关键词: 移动 Ad hoc 网络;虫洞攻击;位置检测算法;OMNeT++
文章编号: 1002-8331(2007)34-0119-03 **文献标识码:** A **中图分类号:** TP309+.2

1 引言

移动 Ad hoc 网络(Mobile Ad hoc NETwork,MANET)是一种无固定结构和中心控制的网络,网络中各移动节点的地位平等,通过无线接口以任意方式动态地与其他节点进行通讯。MANET 具有安装便捷、使用灵活、易于扩展、受自然环境、地形及灾害影响小等优点,因此越来越受到人们的青睐,广泛应用于军事领域、紧急情况应急处理、临时办公和会议、移动通信、传感器网络等方面[1,2]。但是,Ad hoc 技术不光显示它的潜力,其不成熟性及各方面的漏洞不可避免的带来了新的安全问题。由于 MANET 工作在一个开放、合作和高度任意的环境中,具有节点间链接脆弱、拓扑结构动态改变、身份认证缺乏、没有集中监控或管理点等特性,任何有合适的硬件、网络拓扑和协议的终端都能够接入网络,这使潜在的攻击者能够渗入网络执行窃听或转换信息等多种类型的攻击,如欺骗攻击、拒绝服务攻击等等。其中有一种专门针对 Ad hoc 网络的特殊攻击,即“虫洞”攻击,大部分现存的 Ad hoc 网络路由协议缺乏对这种攻击的有效防御或处理机制。

2 “虫洞”攻击原理

“虫洞”(Wormhole)攻击[3],是一种针对 Ad hoc 路由协议,特别是带防御性的路由协议的严重攻击,如图 1 所示。

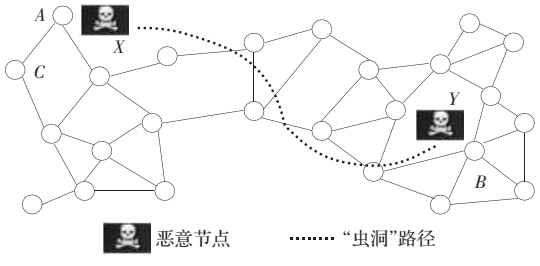

图 1 “虫洞”攻击

它是在两个串谋恶意节点 X、Y 间建立一条高质量高带宽的私有通道,攻击者在网络中的 X 位置上记录数据包或位信息,通过此私有通道将窃取的信息传递到网络的另外一个位置 Y 处。因为私有通道的距离一般大于单跳无线传输范围,所以通过私用通道传递的数据包比通过正常多跳路径传递的数据

作者简介:柳楠,女,硕士研究生,研究方向:网络安全;杨森,男,工程师,硕士研究生,研究方向:网络安全;柴乔林,男,教授,研究方向:计算机网络和人工神经网络应用、远程监控;王向辉,女,硕士研究生,研究方向:网络、数据库技术。

包早到达目标节点,造成比实际路径短的虚假路径,将会扰乱依靠节点间距离信息的路由机制,从而导致路由发现过程的失败。即使网络通讯间存在信任和身份认证,而攻击者并无密钥时仍能够进行攻击;更糟的是,由于虫洞攻击者对于较高层是不可见的,并且虫洞对合法节点的影响会随着节点的移动而改变,虫洞和位于虫洞两端的攻击者在路径中很难被定位。

例如,如果攻击者通过私有通道将由节点 A 发出的 HELLO 数据包传递给节点 B 附近的串谋攻击者,同样攻击者通过私有通道将节点 B 发出的 HELLO 数据包传递给先前的攻击者,那么 A 和 B 将相信它们互为邻节点,这将导致当它们实际不是邻节点时,路由协议将不能找到正确的路径。攻击还会影响虫洞两端点附近的节点。节点 A 广播到达 B 有一跳路径,因此节点 C 将直接通过节点 A 向 B 发送数据包。

3 位置检测算法设计

3.1 算法的模型假设

在此算法的设计过程中,特做如下假设:

(1)通信节点使用当前大多数无线设备采用的无向天线。

(2)通信链路是双向的,即若一个节点可以收到它的邻节点的消息,则它的邻节点同样能收到该节点发出的消息,并且各节点具有相同的传输半径。

(3)节点间能建立安全链接并且所有重要信息都经过加密,现有的有效机制请参考文献[4,5]。

(4)网络可靠性问题并不在算法议考虑之内,消息的丢失和重传将由高层协议来解决。

3.2 网络环境

移动 Ad hoc 网络中的设备主要包括可移动的终端,如笔记本电脑、移动 PC、手机等等。除了这些一般节点,本算法引入一种特殊节点,称之为定位节点(Locating Node)。这些节点除具有一般节点的所有功能外,具有直接定位其传输范围内邻节点位置的功能。定位节点的定位功能可通过 GPS[6]、GLONASS[7] 等技术实现。所有一般节点通过邻接的定位节点来确定各自的相对位置,从而确定各自的邻节点。每个节点都要存储一个邻节点列表和各自的位置坐标及传输半径。为了有效阻止虫洞攻击,算法要求一般节点必须在至少一个定位节点的传输半径内。图 2 中节点 $L1$、$L2$ 为定位节点,定位节点 $L1$ 通过定位技术直接定位得到其邻节点为节点 A、B、C、D、E,同样定位节点 $L2$ 的邻节点为 A、F、G、H、I,一般节点 A 通过其邻接的定位节点得到其邻节点为 $L1$、$L2$、B、F、I。

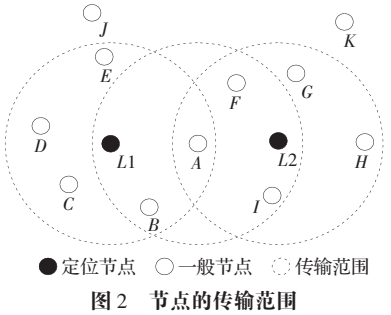

图 2 节点的传输范围

3.3 虫洞检测算法的具体设计

在虫洞检测算法开始前各节点首先需要进行状态初始化:当节点开机后,定位节点广播通知它在网络中的位置。所有在此范围内的节点都会苏醒,回复定位节点。当所有的节点回复后,每个节点将建立一个在它传输范围内的包括定位节点或一般节点的邻节点列表,并存储节点的位置坐标及传输半径。

3.3.1 虫洞检测算法

通过初始化过程,每个节点的内存中都保存了各自的邻节点列表及各个邻节点的位置坐标信息 $Location(x,y)$。无线通讯的特性决定了无线装置的传输是有范围的,只有在彼此传输范围的节点才能够进行通讯。而由虫洞的原理可知,虫洞节点之间使用特殊的装置和高质量的频段,可以进行远距离的直接通讯,这一特点便是检测虫洞的一个有利根据。本算法中检测虫洞的过程包括三次计算,任意一次检测出的异常节点都被视为虫洞节点,将其从网络中丢弃。假设所有节点的传输半径为 R,检测过程为:

(1)对于网络中的任意定位节点 L,计算节点 L 与其邻节点列表 List 中任意一节点 X 的距离 $D(L,X)$,若 $D(L,X)>R$,则认为节点 L 和 X 为虫洞串谋节点。若 $D(L,X)<R$,则进行第 2 步计算;

(2)对于网络中的任意一般节点 A,若邻节点列表中包含至少两个定位节点,则计算其中任意两个定位节点 $L1$,$L2$ 的距离 $D(L1,L2)$,否则转到第 3 步计算。若 $D(L1,L2)>2R$,则节点 A 和距离节点 A 较远的定位节点为虫洞串谋节点,否则转到第 3 步计算;

(3)对于网络中的任意两个一般节点 A、B,假设它们在彼此的传输范围内。计算节点 A 的邻节点列表中的任意一个定位节点 La 与节点 B 邻节点列表中的任意定位节点 Lb 的距离 $D(La,Lb)$。若 $D(La,Lb)>3R$,则认为节点 A、B 为虫洞串谋节点;

(4)抛弃被检测出的节点;

(5)通知路由协议,避免使用该节点建立路径。

3.3.2 虫洞检测算法有效性证明

对于检测过程的第 1 步计算,比较容易理解,因为节点的邻节点必须在此节点的传输范围之内即 $\mathrm{Max}(D(X,Y))<R$,若在传输范围外的节点仍能与此节点通讯,则此节点是虫洞串谋节点。通过此步计算,检测出定位节点中是否有虫洞串谋节点。

对于检测过程的第 2 步计算,其原理示意图如图 3 所示。对于任意一般节点 A,其邻节点与节点 A 的最远距离为其传输半径 R,根据第 1 步检测结果,对于节点 A 的邻节点中任意定位节点 L,都有 $D(L,A)\leqslant R$,那么对于节点 A 邻节点中的任意两个定位节点 $L1$、$L2$,有 $D(L1,A)+D(L2,A)\leqslant 2R$,而根据三角型两边之和大于第三边的定理,就有 $D(L1,L2)\leqslant D(L1,A)+D(L2,A)\leqslant 2R$。因此,如果任意两个定位节点的距离大于 2 倍的传输半径,则节点 A 和距离节点 A 较远的定位节点被认为是虫洞串谋节点。

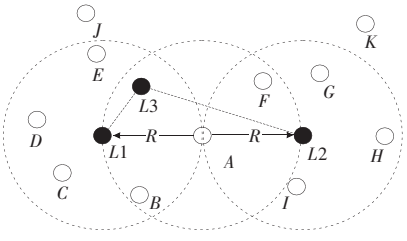

图 3 第 2 步计算原理示意图

对于检测过程的第 3 步计算，其原理示意图如图 4 所示。任意两个一般节点 A、B，它们要想互相通讯，必须在彼此的传输范围内，则 $\mathrm{Max}(D(A,B))=R$。对于节点 A、B 邻节点列表中的定位节点，它们与节点 A、B 之间的最大距离也为其传输半径 R，那么 A 节点的邻节点列表中的任意一个定位节点与 B 节点邻节点列表中的任意定位节点的最大距离 $\mathrm{Max}(D(La,Lb))=3R$。若 $\mathrm{Max}(D(La,Lb))>3R$，则 A、B 节点为虫洞串谋节点。

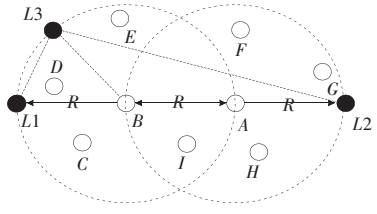

图 4　第 3 步计算原理示意图

4　仿真实验与结果分析

实验采用 OMNeT++(Objective Modular Network Testbed in C++)[6]进行仿真，它是一个跨平台，源码开放、基于独立事件的模拟环境，主要用于网络通讯、协议、多重处理机以及分布式处理系统的模拟和评估复杂软件系统效能。

4.1　仿真模块设计

在实验中，移动节点随机分布在 600 m×800 m 的区域中。节点的无线传输范围为 100 m，信道的数据传输率为 11 Mb/s。节点以 9 m/s 的速度移动，节点的移动方向为 α，且 $\alpha\in(0,2\pi)$，当节点到达仿真边界，将自动沿反边界方向随机移动。

在该仿真网络中，需要建立 3 种类型的节点：一般节点、定位节点和虫洞节点，其中一般节点是基类型节点，定位节点和虫洞节点都具备一般节点的所有功能，此外，定位节点具有直接定位其传输范围内的所有节点的功能，虫洞节点具有能够进行远距离高质量通讯的能力。节点的模块组成如图 5 所示。其中 Mobility 模块的功能是根据预先定义的移动模式改变当前节点的位置，来执行节点的移动，该仿真使用的是随机移动模式；LDP 模块的功能是完成“虫洞”的检测，并与 Route 模块通讯屏蔽“虫洞”节点参与路由选路。仿真运行界面如图 6 所示。

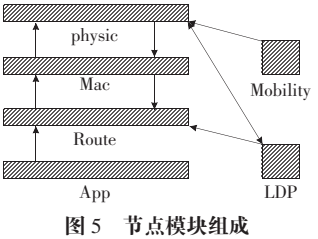

图 5　节点模块组成

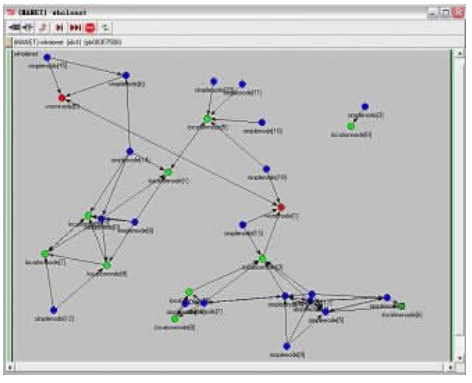

图 6　运行界面

4.2　实验与结果分析

为证明算法的有效性进行了有限数量的定位节点和大规模网络两次仿真实验。

4.2.1　有限数量定位节点的实验

实验分析了算法在不同数量定位节点和一般节点情况下的有效性。在网络中两种节点的比率为 30:20，25:25，20:30，15:35，10:40 和 5:45，虫洞端节点的位置固定在左上角和右下角。在上述条件下执行了 10 次后，结果表明定位节点相对于一般节点的数量越少虫洞被检测到的几率越少，如图 7 所示。

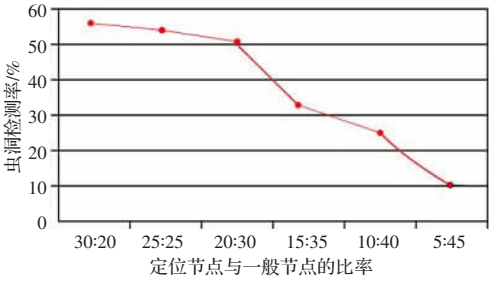

图 7　两类节点的不同比率对检测结果的影响

图 7 中所示的百分率是检测到的虫洞的总数量除以实际虫洞的总数量。从图 7 中可以看出，在定位节点和一般节点比率为 30:20，25:25，20:30 时，算法能够检测出平均 54%~55%的被虫洞影响的节点。但是，当网络中有 35 个一般节点只有 15 个定位节点时，算法的检测率只有 33%。

4.2.2　节点不同密度时的检测实验

实验目的是确定网络在不同的密度下对虫洞检测的影响。通过在同一区域内加入更多的节点来增加网络的密度。在此实验中定位节点和一般节点的比率为 2:3 因为这个比率在前一个实验中已经证明有效。在网络中分别放置 100，75，50，30，20 个节点。按照 2:3 的比率，定位节点和一般节点的数量应为 40:60，30:45，20:30，12:18 和 8:12。虫洞的位置仍然固定在左上角和右下角。实验的结果表明节点密度越低检测出的虫洞的数量就越少如图 8 所示。

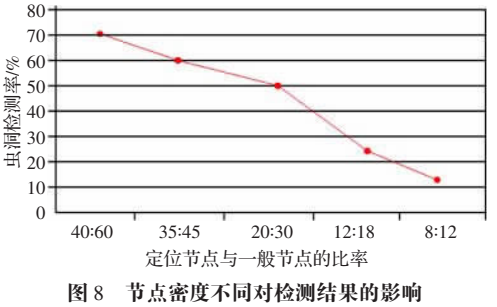

图 8　节点密度不同对检测结果的影响

由上述实验可以看出，虫洞的检测情况依赖于网络的结构、虫洞端节点、定位节点和一般节点的位置。

5　结束语

通过实验验证了位置检测算法对虫洞检测的有效性，但相对于纷繁变化的“虫洞”攻击手段，文章提出的虫洞检测算法还略显简单和稚嫩。限于软硬件环境和技术能力，仿真实现也还存在着诸多不足之处，这些问题都亟待在将来的研究工作中能得到很好地解决。（收稿日期：2007 年 5 月）

（下转 135 页）