移动 Ad Hoc 网络中“虫洞”攻击检测方法*

景 劼

(军械工程学院 计算机工程系,石家庄 050003)

摘要:介绍了 Ad hoc 网络的体系结构和特点,分析了其存在的安全威胁,并指出“虫洞”攻击是一种破坏网络路由机制的攻击,进而提出了几种比较实用的防护方法.

关键词:Ad Hoc 网络;“虫洞”攻击;防护;路由安全

中图分类号:TN86 **文献标识码**:A **文章编号**:1006 - 0707(2009)08 - 0126 - 03

Ad Hoc 一词来源于拉丁语,意思是“for this”,引申为“for this purpose only”,也就是“为某种目的设置的,特别的”,即 Ad Hoc 网络是一种有特殊用途的网络. Ad hoc 网络作为一种特殊网络,起源于军事应用的需要. 它由一组带有无线收发装置的移动终端组成一个多跳临时性自治系统. 网络中,节点间的路由通常由多个网段跳组成,由于终端的无线传输范围有限,两个无法直接通信的终端节点往往要通过多个中间节点的转发来实现通信,所以 Ad hoc 网络是一个多跳的系统. 在移动过程中,节点可以加入或脱离网络,因此网络具有灵活的动态拓扑结构.

1 Ad hoc 网络的安全威胁

由于 Ad Hoc 网络中信息以无线方式传输,信息偷听、欺骗和篡改更容易. 其次,由于 Ad Hoc 网络无固定通信设施、无中心、节点间的关系对等且动态变化,这使得传统的基于身份认证和在线服务器的安全方案难以实现. Ad Hoc 网络的安全性比较脆弱,其路由机制也面临多种威胁,大致可以归纳为以下几类[1-4]:

1) 路由伪造. 路由伪造是指攻击者通过篡改路由消息、伪造路由消息、伪造断链信息、假冒多个节点身份等方式制造虚假的路由信息.

2) 路由隐藏. 路由隐藏是指攻击者通过特殊的方式隐藏可靠路由(仅由内部合法节点构成的路由),使路由协议只能得到受攻击者控制的路由,从而使网络通信流向攻击者控制的节点.

3) 泛洪发送路由更新信息. 通过频繁地发送路由更新信息,攻击者可以阻塞网络.

4) 黑洞攻击. 在这种攻击中,一个恶意节点利用路由协议告诉其它节点自己有到目的节点的最短路径. 在基于扩散的协议中,攻击者窃听路由请求消息. 当攻击者收到源节点到目的节点的路由请求消息后,它发送一个由最短路由组成的路由回复消息. 假如恶意节点的回复消息在诚实节点发出的回复消息之前到达请求节点,那么就会生成一个假的路由. 一旦恶意节点能够把自己加入到通信节点之间,它就可以任意处理通过自己的数据包. 它可以丢弃数据报进行拒绝服务攻击,也可以利用自己在路由中的位置作为中间人攻击的第一步.

5) 虫洞攻击. 一种两个通过私有网络连接的攻击者产生的联合攻击. 恶意节点通过它们之间的直接链路传递接收到的路由控制分组,并在虫洞的另外一端再次广播. 攻击者通过缩短路由分组正常传播的路径来控制一部分通信量.

6) 隐式报文丢弃. 攻击节点通过对路由报文正常转发,但对数据报文实施丢弃或者选择性丢弃,使得一方面路由协议认为路由正常,另一方面数据报文却无法发送.

7) 拒绝服务攻击. 拒绝服务攻击又分为 RREQ flooding 攻击和 DATA flooding 攻击. RREQ flooding 攻击,攻击者不顾路由协议对发送 RREQ 包的限制,发送大量 RREQ 包,尽力消耗网络资源,导致其它节点的路由请求表溢出不能接收合法节点的路由请求,而且消耗了其它节点的电池量. DATA flooding 攻击,攻击节点在网络中泛洪发送大量无用数据报文给一些节点,导致网络中充满了它发送的路由请求包和数据包,其它节点忙于处理这些包而造成其它路由包和数据包的延迟甚至丢失,也消耗了其它节点的电量,阻塞了节点的正常通信. 这种攻击主要针对按需路由协议.

2 “虫洞”攻击原理

Ad Hoc 网络中“虫洞”(Wormhole)攻击是最难以检测与预防的. 它是一种针对 Ad hoc 路由协议,特别是带防御性的路由协议的严重攻击,同时因为虫洞能够造成比实际路

* **收稿日期**:2009 - 05 - 21

作者简介:景劼(1981—),男,石家庄人,硕士研究生,主要从事计算机软件与理论研究.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

径短的虚假路径,将会扰乱依靠结点间距离信息的路由机制,从而导致路由发现过程失败,如图 1 所示.

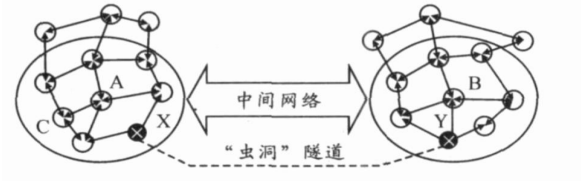

图 1 “虫洞”攻击

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播的距离,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包早到达目标节点. 如果攻击者忠实可靠的通过此通道操作,将不会产生任何不良影响,实际上提供了一个有效的网络连接服务,因为它能够降低数据包到达目标节点的时间. 但是,如果“虫洞”攻击者并不忠实的传递所有数据包,而是故意传递部分数据包,如只传递控制信息数据包,或篡改数据包的内容,将造成数据包的丢失或破坏. 若虫洞将攻击者置于网络中对其他节点非常重要的位置,攻击者能够通过各种方法利用这个位置. 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,不像路由协议中的恶意节点,它们能够轻易地被定位,虫洞攻击者对于较高层是不可见的,虫洞和位于虫洞两端的攻击者在路径中是不可见的. 虫洞对合法节点的影响会随着节点的移动而改变;两个先前通过虫洞有路径连接的合法节点可能不再能够通讯.

因为虫洞能够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. 例如,对于使用 HELLO 数据包来检测相邻节点的周期性路由协议 OLSR(Optimized Link State Routing Protocol),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 都相信它们互为相邻节点,这将导致当它们实际不是相邻节点时,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 有一条路径,因此节点 C 将直接通过节点 A 向 B 发送数据包. 虫洞非常难于检测,因为它用于传递信息的路径通常不是实际网络的一部分,同时它还特别危险,因为它们能够在不知道使用的协议或网络提供的服务的情况下进行破坏. 许多研究者对此提出了各自的方案,其中一些比较实用的检测“虫洞”攻击的方法有如下几种.

1) 基于监听与信赖的方法

这种方法[5]首先设定网络节点天线都是全方向的,并支持混杂模式,这样源节点在发出数据包之后可以对邻居节点进行监听,也就是可以监听邻居节点转发数据包的时间,根据转发时间可以对邻居节点进行信任评估,在源节点发送数据包之前,根据邻居节点的信任值进行选择,如果邻居节点是“虫洞”攻击的恶意节点,那它转发数据包不可能被源节点监听到,也就是说恶意节点的信任值是最低的,从而不会被选择到,这样自然就孤立了恶意节点,也避免了“虫洞”攻击的危害.

2) RTT 的方法

Jane Zhen 和 Sampalli Srinivas[6]使用了一种称之为循环旅行时间(RTT)的方法来检测虫洞. A 节点计算与节点 B 之间的 RTT,通过发送一个信息给 B,要求立刻回复. A, B 间的 RTT 就是从 A 发送请求到接收到 B 的回复所经历的时间. 每个节点都计算与邻居节点间的 RTT,因为 2 个假冒邻居间的 RTT 必然大于真正邻居间的 RTT. 因此通过比较 A 和 A 的邻居间的 RTT,A 节点可以确定哪个邻居是假冒邻居. 这种方法不需要额外的硬件并容易实现,但是对于显式虫洞攻击的检测是无效的.

3) 基于统计分析的方法

SAM 协议[7]是由分裂路由协议(SMR)改进而来,使用统计分析的方法进行虫洞检测,这种方法在多路路由协议的环境下使用,每次检测前,当前节点发起路由发现过程,将所得到的所有路由经过的链接进行统计,因为在虫洞攻击下,恶意节点所在的链接将在路由表中出现的比例很高. 所以此方法统计处出现比例最高的链接,并使用探测包对它进行检测,由此确定恶意节点.

另外还有一种基于统计分析检测方法,称之为邻居数量检测方法[8],这种方法是基于恶意节点周围的邻居数量将增加这个简单的假设之上的,基站将得到所有节点的邻居信息,计算邻居数量分布的估计值,并且使用统计测试来决定是否存在虫洞.

4) 基于邻居信任评估的方法[9]

该方法通过引入信任模型,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,选取高可信度的邻居作为下一跳. 由于评估结果相比“虫洞”形成在时间上是滞后的,因此该方法对“虫洞”的检测存在较大的延时.

文献[10]中提出了一种基于节点间距离进行判断的协议模型,能在一定程度上检测出“虫洞”攻击节点,但这种方法依据了定位节点这个前提,具有一定的局限性.

3 “虫洞”攻击检测方法

“虫洞”攻击非常难于检测,因为它用于传递信息的路径通常不是实际网络的一部分,同时它还特别危险,因为它们能够在不知道使用的协议或网络提供的服务的情况

4 结束语

上述几种检测方法中,基于监听与信赖的方法对硬件有一定的要求(需要网络节点支持混杂模式),而且对节点的电源要求比较高,RTT 的方法最大缺陷在于不能检测显

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

示“虫洞”攻击;基于统计分析的方法对节点能源、计算能力、存储空间均有较高的要求;基于邻居信任评估的算法又有一定的延迟;距离判断法具有一定的局限性.可以看出没有十全十美的算法,笔者认为要根据网络的协议、节点数目、业务类型等实际情况来选择合适的检测方法,或者在现有方法的基础上结合数据加密等技术研究、发现新方法.这样才能更加迅速、高效的检测“虫洞”攻击,为后续有效地解决它提供前提.

参考文献:

[1] 季晓军,田畅. Ad Hoc 网络路由安全.解放军理工大学学报[J],2006,7(4):341 - 345.

[2] Karpijoki V. Security in Ad Hoc Networks. In Proceedings of the Helsinki University of Technology, Seminars on Network Security,2000.

[3] YHu, A. Perringand D. Johnson. Ariadne: A secure on-demand routing Protocol for Ad Hoc networks. In 8th ACM International Conference on Mobile Computing and Networking, September 2002.

[4] 陈天池,王培康. MANET 路由与路由安全问题[J].无线电工程.2006,36(6):2 - 3.

[5] A. Pirzada G. McDonald, Circumventing sinkholes and wormholes in wireless sensor networks in International Conference on Wireless Ad Hoc Networks(W WAN), 2005.

[6] J. Zhen and S. Srinivas Prventing replay attacks for secure routing in ad hoc network Proc of 2nd Ad Hoc Networks & Wireless AD-HOCNOW,2003.

[7] Lijun Qian, Ning Song Xiangfang L Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks through Statistical Analysis of Multi-path IEEE Communications Society WCNC, 2005.

[8] Levente Buttyan La sza. Do ra Istyan Vajda Statistical Wormhole Detection in Sensor Networks Second European Workshop on Security and Privacy in Ad Hoc and Sensor Networks ESAS 2005 Visegad, Hungary July 13 - 14, 2005 128 - 141.

[9] 洪亮,洪帆,彭冰,等.一种基于邻居信任评估的虫洞防御机制[J].计算机科学,2006,33(8):130 - 133.

[10] 柳楠,杨森,柴乔林,等. MANET 中“虫洞”攻击的位置检测算法设计与仿真[J].计算机工程与应用,2007,43(34):119 - 121.

(上接第 88 页)

参考文献:

[1] 刘凤强,孙志强,谢红卫,等.航空维修人为差错影响因素分析中的模糊层次分析法[J].中国安全科学学报,2008,18(7):44 - 48.

[2] 焦猛.基于模糊综合评判的航空维修差错控制能力定量评估[J].空军工程大学学报:自然科学版,2007,8(1):24 - 26.

[3] 张亮,田松,张凤鸣,等.集成神经网络的飞机作战效能评估[J].火力与指挥控制,2007,32(12):89 - 91.

[4] 陈文宇,刘井波,孙世新.层次分析的神经网络集成方法[J].电子科技大学学报,2008,37(3):432 - 434.

[5] 黄书峰,端木京顺.航空维修保障能力的神经网络评估方法与应用[J].航空维修与工程,2008(2):42 - 43.

[6] 李克武,郭建胜,周长飞.航空维修人为因素事故分析系统研究[J].航空维修与工程,2005(6):42 - 43.

[7] 冯国涛,刘沃野,张雪胭,等.基于 BP 网络的装备维修质量评估设计[J].科学技术与工程,2006,9(6):1296 - 1299.

[8] 何明,李彬.基于 Elman 神经网络的装甲装备维修保障系统效能评估[J].指挥控制与仿真,2008,30(4):77 - 79.

[9] 王文成.神经网络及其在汽车工程中的应用[M].北京:北京理工大学出版社,1998.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net