基于 RTT 的统计分析方法检测与防御虫洞攻击①

杨 姣[1]，王 东[2]

[1](湖南大学 软件学院，长沙 410082)
[2](湖南大学 计算机与通信学院，长沙 410082)

摘 要：移动 Ad hoc 网是一种新型的无线移动网络，具有无中心、自组织、拓扑结构动态变化以及开放式通信等特性，使得 Ad hoc 网络易遭受攻击。虫洞攻击是针对 Ad hoc 路由协议的攻击，对 Ad hoc 网络造成的威胁最大。提出一种基于 RTT(往返时间)的统计分析检测方法，在路由发现过程中，目的节点在返回路由应答(RREP)之前统计并分析获得的路由信息，得到各条链路在所有路由中出现的频率，再结合两两节点间的 RTT 时间来选择路由。由于在路由过程中就检测出虫洞，因此可以很好地抵御虫洞的攻击。同时，RTT 的计算由各个节点自己完成，计算量不大且维持较少的开销。仿真实验表明，该方法能有效地检测出虫洞攻击并提高虫洞的检测率。

关键词：移动 Ad hoc 网络；虫洞攻击；统计分析；分裂路由协议

Detecting and Avoiding Wormhole Attacks by Statistical Analysis Based on RTT

YANG Jiao[1], WANG Dong[2]

[1](College of Software, Hunan University, Changsha 410082, China)
[2](School of Computer and Communication, Hunan University, Changsha 410082, China)

Abstract: Mobile Ad hoc Networks (MANET) is a new networking for wireless hosts. Because of self-organization, dynamic topology and openness of wireless communication, it makes them very attractive to attackers. Wormhole attack is one of the most severe threats to ad hoc networks. They create a higher level virtual tunnel between two malicious colluding nodes in the network. In this paper, we proposed a novel statistical analysis mechanism based on RTT (Round Trip Time) to detect and avoid wormhole attacks. It detected wormhole attacks during route setup procedure by statistically analyzing the route information and the transmission time between every two successive nodes along the established path before sending RREP to the source node. The wormhole will be recognize before it can do harm to the network in the route setup. And each node compute the RTT, it only introduces very limited overhead. Simulation results showed that the method can efficiently detect wormhole attacks and have better detection rate.

Keywords: mobile Ad hoc networks; wormhole attack; statistical analysis; split multi-path routing

移动 Ad hoc 网络(MANET)不依赖于固定基础设施，这种网络以无中心方式通过每个节点自身作为路由器实现分布式路由并与其他节点通讯。但是 MANET 工作在一个任意、开放的环境中，其网络拓扑的高动态性和自组织等特性使其面临更多的安全威胁。

虫洞(wormhole)攻击是一种针对移动 Ad hoc 路由协议的严重攻击，因为现有的路由协议没有对这种攻击的有效的防御机制。相隔甚远的两个恶意节点间通过一条高质量高带宽的私有链路直接通信。恶意节点在隧道的一端记录数据包或位信息，通过隧道将窃取的信息传送到隧道的另一端，然后再重放。由于私有链路的长度一般大于单跳无线传输范围，故通过私有链路传送的数据包要比通过正常多跳路径传递的数据包早到达目的节点。从而，对选择最短路径的路由协议来说，虫洞将吸引较大的网络流量。虫洞攻击如果

① 基金项目:湖南省自然科学基金(10JJ5069)
收稿时间:2010-09-13;收到修改稿时间:2010-10-11

成功，攻击者就能够以此进行更多的攻击，如主动丢包或者改变数据包内容。

虫洞攻击又有两类：隐式虫洞攻击和显示虫洞攻击。显示虫洞攻击恶意节点像正常节点行为一样，将自己的信息放入到数据包中，而在隐式虫洞攻击中恶意节点隐藏自己的信息，正常节点不知道它们的存在。

1　相关工作

目前针对 Ad hoc 网络中的虫洞攻击，许多研究者已经提出了一些检测与防御的方法。文献[1]提出一种端到端的虫洞攻击检测方法。先估算好源节点到目的节点的最短跳数，如果收到的路由的跳数值比估计值还小的话就认为受到攻击。该方法在源节点到目的节点间隔不是很远的情况下是有效的。DelPHI[2]方法尽量找到发送节点和接收节点间所有可能的不相交路径，然后计算每条路径的时延和长度，就可以得到每条路径中每跳的平均时延。因为存在虫洞攻击的路径上的平均每跳时延必定远远大于正常路径上的值。这种方法能发现虫洞攻击，但是不能定位恶意节点。

文献[3]提出了基于邻居信任评估的方法。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时延。

文献[4]提出统计分析每条链路在所有路径中出现的频率的方法。在受到攻击的情况下，统计数据会发生较大的变动。该方法不能检测出隐式虫洞攻击，因为隐式虫洞攻击节点并不显示在路由中。文献[5]和文献[6]都提出基于时间的理念来检测虫洞攻击，但是方法有所不同。文献[5]计算的是已建立路由中两两节点的时间。而文献[6]中要求每一个节点计算其与所有邻居节点的通信时间。计算量大无异于增加了网络开销。

文献[7]通过比较正常邻居和伪邻居的产生是否导致非法拓扑结构来判断是否存在虫洞攻击。另外，一些方法大多依赖于时钟的严格同步或特殊的硬件设备，很难应用到实际的网络中。

综上所述，以上解决方法有一定的局限性。有些要求严格的时钟同步或消耗大量的系统资源。因此在不依赖特殊条件保证较低网络开销同时，能有效地检测出虫洞的存在，进而提升网络安全是我们的主要工作。

2　基于RTT的统计分析检测方法

2.1 统计分析多径路由中链路信息

本文以分裂路由协议（SMR）为基础，对其进行了改进。改进后的协议在一次路由过程中能够获得更多的到达目的节点的路由信息，在目的节点可以进行提取、统计。在遭受虫洞攻击的情况下，统计得到的数据会发生较大的变动[4]。因为恶意节点所在的链路在路由表中出现的比例要高于正常链路。下面是本文统计分析使用到的参数：

R：一次路由过程中得到的路由信息的集合；

L：R 中包含的链路（不重复）组成的集合；

N：R 中所有链路（重复）的总和；

l_j：L 中第 j 条链路；

n_j：l_j 在 R 中出现的次数；

P_j：l_j 链路在 R 中出现的频率

统计分析方法能够有效地检测路由中的显示虫洞攻击，但是对于隐式虫洞攻击，该方法不能检测出来。因为在隐式虫洞攻击中，恶意节点不将自己的身份信息暴露到网络中，不会显示地存在路由中。

为了解决这一问题，本文在统计分析检测方法中引入时间机制，在发送路由应答过程中计算路由中两两节点间的 RTT 时间。因为在隐式虫洞的影响下，不在彼此通信范围内的两个节点会互相认为对方是自己的邻居节点，故伪邻居节点间的 RTT 要远大于正常节点间的[2]。通过比较两两节点的 RTT 来检测出路由中是否存在虫洞攻击，从而检测和抵御隐式虫洞攻击。

2.2 RTT（Round Trip Time）

RTT 是路由过程中节点从发送 RREQ 到接收 RREP 所用时间。在路由建立过程中，每一节点计算其到目的节点的 RTT 并把该值送回源节点。源节点收集所有的 RTT 值后，由此计算出路由中两两节点间的 RTT 值[5]。下面是一条路由：$\overline{\quad}\ \overline{\quad}\ \overline{\quad}$ S 是源节点，D 是目的节点。S 与 A 的时间记为 RTTSA，它等于 S 发送 RREQ 到接收 RREP 的时间减去 A 转发 RREQ 到接收 RREP 的时间。其他节点间计算方法也如此。在网络正常情况下，计算出的各节点间的时间相差无几。但假若 A 与 B 之间存在隐式虫洞，RTT_{AB}

一定明显大于其他各个节点间的时间值。

2.3 基于 RTT 的统计分析方法检测算法

网络中的通信链路是双向的，即如果一个节点可以收到它的邻居点的消息，则它的邻节点同样能收到该节点发出的消息。本文中虫洞攻击检测流程如图 1 所示，具体如下：

(1) 对目的节点收集到的路由进行统计分析，得到各条链路在所有路由中出现的频率。

(2) 对于出现频率高的链路，视为异常，执行步骤 3。否则，执行步骤 5。

(3) 对于异常的链路，发送测试包等待响应(ACK),执行步骤 4。

(4) 确定该链路遭到虫洞攻击（显示），则告知源节点和邻居节点并将该链路剔除出网络。如果没有受到攻击，则执行步骤 5。

(5) 目的节点选择路由发送 RREP,源节点收集 RTT 计算出路由中各个节点间的时间值并进行比较。如果受到虫洞攻击（隐式），则发出警报通知网络中的其他节点，从而将攻击者排除出网络。若未受到攻击，则选择路由发送数据进行网络通信。

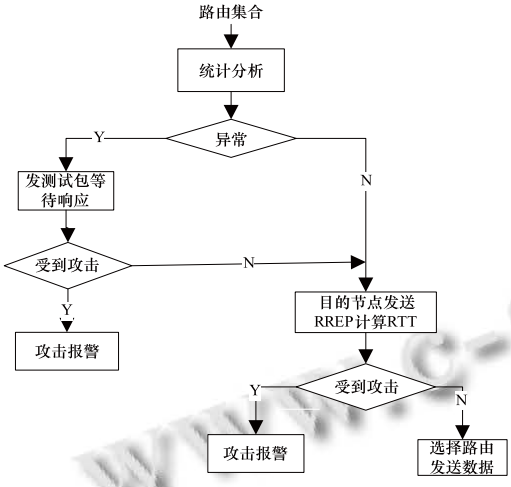

图 1 虫洞检测流程

3 仿真分析

本文利用 NS2 仿真平台进行仿真实验。仿真时，网络环境参数设置为 50 个节点随机分布在 1000m×1000m 平面区域内，每个节点的通信范围是 100m。在 50 个节点中选择两个节点作为恶意节点形成显示虫洞攻击，并在网络中随机放置两个恶意节点作隐式虫洞攻击。为减少误差，实验结果是经 100 次的模拟后取平均值计算得到的。

仿真结果如下图所示。为便于说明把统计分析方法、基于时间的统计分析方法分别简记为 SA、SAT。

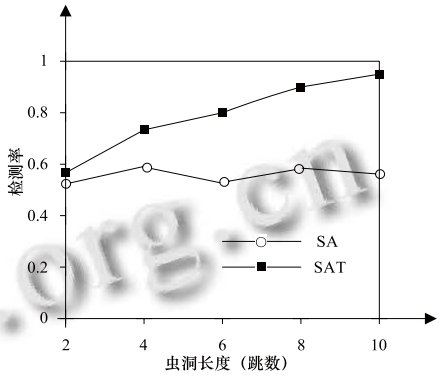

图 2 检测率（SA/SAT）

图 2 说明 SAT 方法攻击检测率要明显高于 SA 方法。并且检测率是与隐式虫洞长度成正比的。随着虫洞长度的增加，检测率显著提高。虫洞长度越长则伪节点间的通信时间越长，从而更易于检测出攻击。当虫洞长度为 10 跳以上，检测率将达到 100%。图 3、图 4 分别是两种方法下攻击的误判率、漏判率。

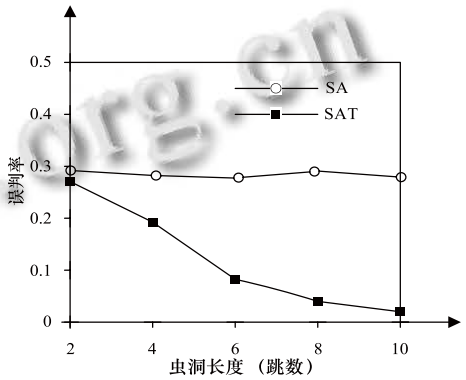

图 3 误判率 (SA/SAT)

图 5 是 SMR 协议和安全算法 SAT 在网络正常和受到虫洞攻击两种情形下，分组传输率的比较。从图中可以看出，在网络正常情况下它们的分组传输率相差不大。而当网络受到攻击时，SMR 协议下的分组传输率大幅度下降，而 SAT 仍有较高的传输率。在检测出虫洞攻击的同时，协议仍有较好的性能。

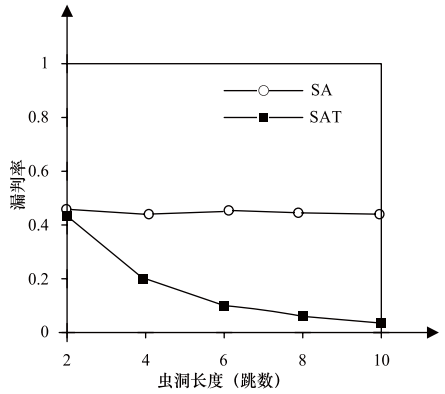

图 4　漏判率 (SA/SAT)

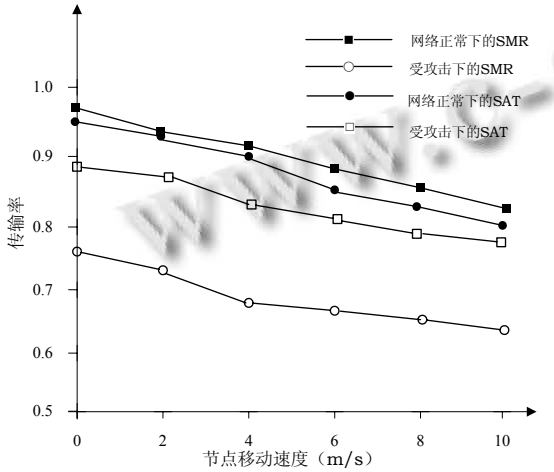

图 5　分组传输率

4　仿真分析

本文在改进的 SMR 协议基础上，针对统计分析方法无法检测出隐式虫洞攻击的问题，将统计分析方法与时间机制相结合，提出一种简单有效的基于 RTT 的统计分析方法来检测和防御虫洞攻击。这种方法先统计分析路由信息，再结合路由中两两节点的 RTT 时间值来解决无法检测出隐式虫洞攻击的问题。该方法具有以下优点：在节点进行数据通信之前就将攻击排除出网络，不需要节点的位置信息和严格的时钟同步（RTT 的计算是由各个节点根据自己的时钟来完成，不要求网络中所有的时钟保持精准的一致），不依赖特殊的硬件设备，计算简单。仿真实验表明该方法能有效地检测并防御虫洞攻击。

参考文献

1 Wang X, Wong J. An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks. 31st Annual International Computer Software and Applications Conference-Vol. 1- (COMPSAC 2007), 2007: 39–46.

2 Chiu HS, Lui KS. DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks. International Symposium on Wireless Pervasive Computing ISWPC, 2006: 6–11.

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

4 Qian LJ, Song N, Li XF. Detecting and locating wormhole attacks in Wireless Ad Hoc Networks through statistical analysis of multi-path. IEEE Wireless Communications and Networking Conference, 2005: 2106–2111.

5 Tran PV, Hun LX, Lee YK, et al. TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks. Wireless Sensor Network Track at IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, USA, 2007: 593−598.

6 Zhen J, Srinivas S. Preventing replay attacks for secure routing in ad hoc networks. Proc. of 2nd Ad Hoc Networks & Wireless (ADHOCNOW'03), 2003:140−150.

7 姚胜,冷甦鹏等.基于 OLSR 路由协议的 HIDA 算法.计算机工程,2010,36(9):147−149.