文章编号:　1000-5013(2009)05-0520-04

路由攻击对移动 Ad Hoc 网络的影响分析

刘菁华[1], 耿　鹏[2]

(1. 华侨大学 计算机科学与技术学院, 福建 泉州 362021;
2. 南京工程学院 通信工程学院, 江苏 南京 211167)

摘要:　典型的移动 Ad Hoc 网络路由协议,如 AODV 等均没有考虑其安全性,面对恶意节点的攻击时,表现得非常脆弱.以拒绝服务攻击为例,对运用 AODV 路由协议的网络平均端对端时延、丢包率、包到达率、路由负荷等性能指标进行模拟和分析.结果表明,当网络中存在此类攻击行为时,各项性能恶化严重.因此,需要设计一种有效的安全机制,通过模拟试验来检验其对抑制攻击的有效性,并应用于 AODV 以外的其他路由协议之上,以增强其可移植性.

关键词:　路由攻击; Ad Hoc 网络; AODV; 拒绝服务
中图分类号:　TP 393.08　　文献标识码:　A

移动 Ad Hoc 网络是一种无需基础设施或接入点的,具有无中心、多跳路由、动态拓扑等特性的自组织网络[1].网络中的每一个终端都可以自由移动且地位相等,兼有主机和路由器两种功能.一方面,作为主机的终端需要运行各种面向用户的应用程序,比如编辑器、浏览器等;另一方面,作为路由器的终端需要运行相应的路由协议,根据路由策略和路由表完成数据的分组转发和路由维护[2].因此,移动 Ad Hoc 网络特别适合应用于军事战场、紧急救援、车载通信及野外作业等特殊场合.移动 Ad Hoc 网络的独特性,使它能够随时随地地进行通信,在未来的网络技术中具有很强的竞争力.但是,由于它具有多跳性、动态拓扑性和无线信道等特点,决定了其网络安全性比传统网络更为脆弱.所以,在有攻击情况下,对移动 Ad Hoc 网络路由协议的研究是非常有必要的.本文对路由攻击类型进行了分类,对存在攻击情况下的 AODV(Ad Hoc On-Demand Distance Vector)[3]的性能进行了模拟试验和分析.

1　移动 Ad Hoc 网络中的路由攻击类型

针对 Ad Hoc 网络路由协议的攻击,可分为被动攻击和主动攻击两大类[4].被动攻击是指恶意节点通过窃听路由数据而获得有用信息,不会破坏整个路由协议的运作;主动攻击是指恶意节点利用某种手段来篡改网络中的数据或通过认证,其危害较大.主动攻击还可进一步划分为外部攻击和内部攻击.其中,外部攻击由网络的外部节点引起;内部攻击由网络的内部节点受损害或被控制所引起.在内部攻击中,由于恶意节点常常是网络内部已被授权节点,其攻击后果往往比外部攻击要严重的多.因此,对付主动型内部攻击在 Ad Hoc 路由安全问题中非常关键.目前,Ad Hoc 网络路由中的主动型内部攻击主要有黑洞攻击(Black Hole)[5]、邻居攻击(Neighbor)、虫洞攻击(Worm Hole)[6]、拒绝服务(DoS, Denial of Service)、信息泄漏(Information Disclosure)、拜占庭式攻击(Byzantine)6 种类型1

2　基于 AODV 的路由攻击模拟

2.1　模拟环境及性能指标

为了较真实地反映现实环境,采用的模拟工具是 NS-2.2,模型为 Random Way-point 移动模型[7].即

收稿日期:　2008-02-19
通信作者:　刘菁华(1980-),女,助教,主要从事语音信号处理、多媒体信息融合及网络安全的研究. E-mail: babysiyu@hqu.edu.cn.

网络中节点均在规定范围内进行随机地移动, 节点随机选择一个目的位置, 然后在预先设定的速度范围内随机地选择一个值, 匀速移向该目的位置. 到达该目的位置之后做一段时间的停留(也可以不停留), 然后选择另一个目的位置并随机选择一个速度继续运动.

模拟参数设定如表 1 所示. 性能指标主要包括以下 4 个方面1(1) 平均端对端时延1 应用层上数据包从发送到接收所需要的平均时间1(2) 丢包率1 丢失的数据包与源节点产生的数据包之比1(3) 包到达率1 正确到达目的节点的数据包与源节点产生的数据包之比1(4) 路由负荷1 路由分组总数与数据分组总数的比值, 即每个数据分组所承担的路由分组数. 在这里, 路由分组按跳计算, 若一个路由分组传了 4 跳, 则会被计算 4 次.

表 1　模拟参数的设定

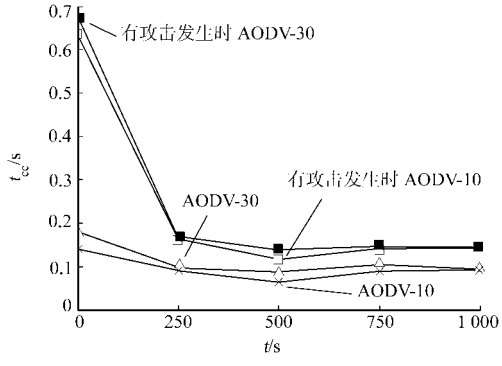
Tab. 1　The parameters of simulation

参数类型	参数值
路由协议	AODV
运动区域	1 000 m@1 000 m
最大运动速度	20 m# s^{-1}
模拟时间	1 000 s
节点数	50
最大连接数	10, 30
最大暂停时间	1 000 s
最大恶意节点数	20
节点间数据传输类型	CBR
发包频率	4 包# s^{-1}
数据包长	512 B
MAC 层协议	IEEE 802.11
物理层带宽	2 MB
攻击类型	DoS 攻击

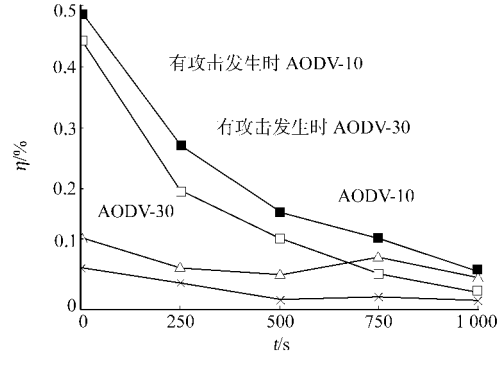
在该环境中, 恶意节点向网络中注入大量的 RREQ 报文(发送RREQ 频率为 10), 致使 Ad Hoc 网络处于饱和状态, 无法进行正常的数据传输. 同时, 恶意节点选择一些不属于本网络的 IP 地址作为目的节点, 然后向这些目的节点发送 RREQ 报文来要求建立链接. 由于目的节点实际并不存在, 中间节点无法获得 RREP, RREQ 报文便会在网络中大面积蔓延开来.

2.2　模拟结果及性能分析

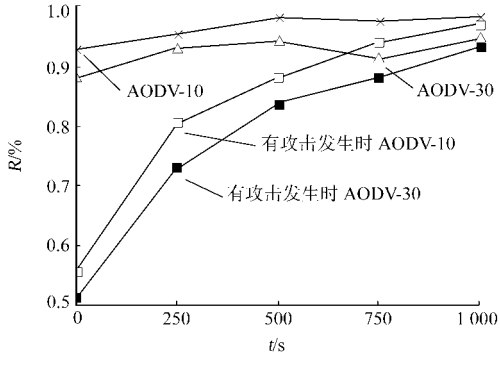
设置恶意节点个数为 10, 暂停时间分别为 0, 250, 500, 750, 1 000 s, 其他参数与表 1 一致, 试验结果如图 1 所示. 其中, 分别用/ AODV2100和/ AODV2300表示在没有攻击发生时最大连接数为 10 和 30 的情况, 而用/ 有攻击发生时 AODV2100和/ 有攻击发生时 AODV2300分别表示在有攻击发生时最大连接数为 10 和 30 的情况.



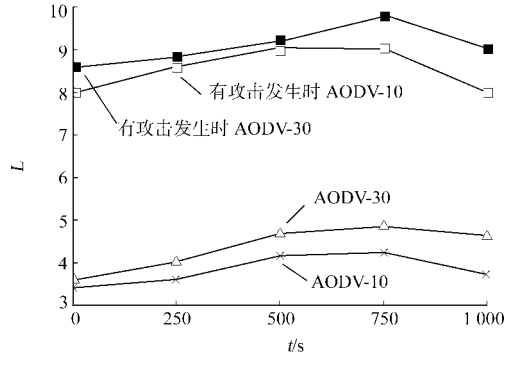
(a) 平均端对端时延



(b) 丢包率



(c) 包到达率



(d) 路由负荷

图 1　路由攻击的模拟结果

Fig. 1　The simulation results of routing attack

由图1的模拟结果可以看出,在没有恶意节点的情况下,网络的平均端对端时延(t_{ee})、丢包率(G)、包到达率(R)及路由负荷(L)等性能都比较平稳1 当网络中存在恶意节点时,各项性能恶化严重.图1(a)表明,DoS攻击使得时延上升,最大约3.4倍;图1(b),(c)表明,DoS攻击使得网络数据包的丢包率上升,包到达率下降,反映出网络吞吐量的降低1 如果以节点正确接收到数据包的平均速率来计算,当网络中存在共计行为时,吞吐量最大下降了40%;图1(d)表明,存在攻击情况下的路由负荷比正常情况下平均上升了1.7倍.

3 结束语

针对目前移动Ad Hoc网络路由信息的各种攻击方法,分析路由攻击对网络性能可能产生的影响.试验结果表明,恶意节点对移动Ad Hoc网络的影响是不可忽略的.因此,作为一个以军事等特殊场合为主要应用的网络技术,对移动Ad Hoc网络安全协议的研究是十分必要的.

参考文献:

[1] CHARLES E, PERKINS. Ad Hoc networking[M]. Boston: Addison2Wesley, 2001.
[2] 郑相全. 无线自组网技术实用教程[M]. 北京: 清华大学出版社, 2004.
[3] PERKINS C E, ROYER E M, DAS S. Ad Hoc on2demand distance vector (AODV)[EB/OL]. [2003207221]1 http: M rfc. net/ rfc3561. html.
[4] PERKINS C E, ROYER E M. Ad2Hoc on2demand distance vector routing[C]M Proc 2nd IEEE Workshop on Mo2bile Comp Sys and Appsl New Orleans: [s. n.], 1999: 902100.
[5] UUSHONA N, PENZHORN W T. Towards the security of routing in Ad Hoc networks[J]. ISIE 2005, IEEE In2ternational Symposium on Industrial Electronicsl Dubrovnik: [s. n.], 2005: 178321788.
[6] HU Yih2chun, ADRIAN P, DAVID B J. Wormhole attacks in wireless networks[J]. IEEE Journal on Selected Are2as in Communications, 2006, 24(2): 3702380l
[7] BROCH J, MALTZ D A, JOHNSON D B, et al. A performance comparison of mult2hop wireless Ad Hoc network routing protocols[C]M Proceedings of the Fourth Annual ACM/ IEEE International Conference on Mobile Compu2ting and Networkingl New York: ACM Press, 1998: 852297.

The Effect of Routing Attacks on Mobile Ad Hoc Network

LIU Jing2hua[1], GENG Peng[2]

(1. College of Computer Science and Techrology, Huaqiao University, Quanzhou 362021, China;
2. College of Communications Engineering, Nanjing Institute of Technology, Nanjing 211167, China)

Abstract: The typical routing protocols of mobile Ad Hoc networks such as Ad Hoc on2demand distance vector (AODV) leave out of consideration about their security. They are very fragile when the malicious nodes attack them. The perform2ance of average end2to2end delay, packet drop ratio, packet delivery ratio and routing load are simulated by adding the de2nial of service (Dos) attack on the AODV. Computer simulation results show that the network performance is deteriorated sharply if there have DoS routing attack in the Ad Hoc network. Therefore, it is need to design an effective security mechanism, through the simulation experiment to test its effectiveness in inhibiting the attack, and applied to AODV rou2ting protocol to enhance its portability.

Keywords: routing attack; mobile Ad Hoc network; Ad Hoc on2demand distance vector; denial of service

(责任编辑: 钱 筠 英文审校: 吴逢铁)