文章编号:1001 - 9081(2008)01 - 0074 - 03

移动 IPv6 网络中的 DoS 攻击

杨新宇[1],杨东旭[1],侯光霞[1],张国栋[2]
(1. 西安交通大学 计算机科学与技术系, 西安 710049; 2. 上海浦东发展银行 总行产品开发部,上海 200233)
(yxyphd@mail.xjtu.edu.cn)

摘 要:介绍了移动 IPv6 协议的工作原理,分析总结了移动 IPv6 网络中三种主要的 DoS 攻击。针对 NS-2 环境提出了一套模拟移动 IPv6 中 DoS 攻击的具体实现方案。经过对仿真实验结果分析表明,DoS 攻击对移动 IPv6 网络性能造成很大的影响。

关键词:移动 IPv6;拒绝服务攻击;NS-2
中图分类号: TP393.08 **文献标志码**:A

DoS attack in mobile IPv6 network

YANG Xin-yu[1], YANG Dong-xu[1], HOU Guang-xia[1], ZHANG Guo-dong[2]
(1. *Department of Computer Science & Technology, Xi'an Jiaotong University, Xi'an Shaanxi* 710049, *China*;
2. *Department Innovation & Promotion, Shanghai Pudong Development Bank, Shanghai* 200233, *China*)

Abstract: The principle of Mobile IPv6 (MIPv6) protocol was researched, and a summary of three main DoS attacks in MIPv6 network were given. A new solution to simulate DoS attacks in MIPv6 for the environment of NS-2 was presented. The simulation result shows that the DoS attacks cause great threats to MIPv6 network.

Key words: MIPv6; Denial of Service (DoS) attack; NS-2

0 引言

移动 IPv6 协议通过定义移动节点和其家乡代理之间的绑定更新注册,保证移动节点在移动的过程中网络连接不中断;定义移动节点和其通信对端之间的绑定更新注册,实现路由优化[1]39-41。但在实现路由优化的同时随之也带来了很多安全问题,如果攻击者在移动节点、家乡代理和通信节点之间的通信链路上截获并篡改相关的信令报文,那么它就能够轻易地发起攻击[2]。目前,移动 IPv6 可能遭受的攻击主要包括拒绝服务攻击、重放攻击,以及信息窃取攻击,其中拒绝服务攻击是移动 IPv6 面临的最严重的一种威胁。移动 IPv6 如不能提供安全可靠的服务,将大大影响其推广应用。

1 移动 IPv6

1.1 移动 IPv6 的基本概念

因特网工程任务组(IETF)在 RFC 3775[1]10-12中定义了移动 IPv6 协议。IETF 提出的移动 IPv6 标准包括以下功能实体:

家乡地址(Home of Address,HoA):移动节点在家乡子网获得的 IPv6 地址。

转交地址(Care-of Address,CoA):移动节点在外地子网自动获得的 IPv6 地址。

家乡代理(Home Agent,HA):本地子网内的一台维持注册移动节点列表的路由器。

绑定(BINDING):移动节点的家乡地址与转交地址的对应关系,外带其生存时间。

隧道:一条从 HA 到 CoA 传送数据包的路径,它是通过封装数据包的形式来实现的。

1.2 移动 IPv6 的通信原理

如图 1 所示,移动节点(Mobile Node, MN)连接到其家乡链路上时,将遵循传统的路由通信方式,不增加任何开销。

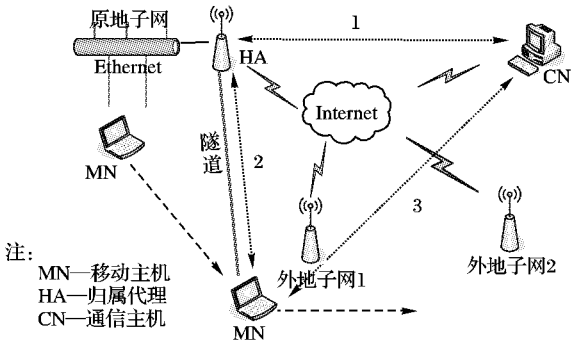

图 1 移动 IPv6 工作原理

MN 通过邻居发现机制检测自己是否已漫游至外地链路,即当 MN 收到来自外地子网 1 上路由器的路由器通告时,利用无状态地址自动配置功能获得外地链路上的转交地址(CoA)[3],向家乡代理发送绑定更新报文,通知其自己的转交地址,并注册。CN 同 MN 通信时,按照 MN 的 HoA 将信息包发送到移动节点的家乡网络上,HA 通过发送代理邻居宣告消息截获发送到 HoA 的数据包(线路 1),利用隧道机制将这些信息包转发给 MN。为了通过隧道(线路 2)发送截获的数据包, HA 对数据包进行 IPv6 封装, 外部 IPv6 报头地址置为移动节点的主 CoA。MN 收到信息包并发现它是由 HA 转发的,就会向 CN 发送绑定更新报文,并将其加入到由 MN 维护

收稿日期:2007 - 07 - 24;**修订日期**:2007 - 09 - 19。
基金项目:国家自然科学基金资助项目(60403028);陕西省自然科学基金资助项目(2004F43)。
作者简介:杨新宇(1973 -),男,教授,博士,主要研究方向:计算机网络安全; 杨东旭(1983 -),男,硕士研究生,主要研究方向:计算机网络安全; 侯光霞(1985 -),女,硕士研究生,主要研究方向:计算机网络安全; 张国栋(1971 -),男,工程师,主要研究方向:计算机网络安全。

的绑定更新列表中。此后,CN 就可以直接与 MN 的 CoA 进行通信(线路 3),从而解决了三角路由的问题。

当 MN 移至外地子网 2 时,将自动获得一个新 CoA,并重新进行登记。此时不仅要向 HA 登记绑定更新信息,而且还要向绑定更新成员表中的每一位成员发送绑定更新信息,以使他们能够随时跟踪 MN。当 MN 回到家乡子网时,取消一切地址绑定。在整个过程中,移动节点的转交地址对于通信主机的用户而言始终是透明的。

2　移动 IPv6 中的 DoS 攻击

从上面可以看出,移动 IPv6 解决路由优化的策略是在家乡代理已有绑定关系的前提下,在通信对端注册家乡地址和转交地址的绑定关系,以实现通信对端和移动节点之间的直接通信。注册通信对端的绑定关系过程本身存在着潜在的安全隐患[4,5]。

拒绝服务攻击是指攻击者为阻止合法用户获得正常服务而采用的攻击手段。这种攻击主要包括两种方式[6]:一种是通过网络向服务器或主机发送大量数据包,使得服务器忙于处理这些无用的数据包而无法响应有用的信息;另一种是直接干扰服务器与主机之间的正常通信。在移动 IPv6 中,攻击者能够通过如下手段达到上述目的:

1)攻击者发送大量地址绑定更新消息来消耗通信节点的资源,从而导致绑定缓存表溢出或者是无法及时处理合法用户的绑定更新报文;

2)恶意主机把因特网上服务器的 IPv6 地址作为大量移动节点的转交地址,发送伪装的绑定更新消息给对端通信节点,引发大量流量发往受害服务器,导致分布式拒绝服务攻击;

3)攻击者可以冒充移动节点,使用移动节点的家乡地址发送绑定更新消息,把自己的地址作为移动节点的新的转交地址,伪装移动节点的移动状况,最终截获发往移动节点的数据包,阻断合法用户的正常通信。

3　仿真实验与性能分析

采用 NS-2 网络模拟平台进行实验,在 NS-2 创建的网络场景中来模拟移动 IPv6 下的 DoS 攻击,通过考查分组丢失、端到端延时等网络性能参数,研究 DoS 攻击对网络性能的影响。

NS-2 是用于网络研究的离散事件模拟系统[7], NS-2 本身没有移动 IPv6 协议支持,笔者选用 MOTOROLA 巴黎研究中心 Thierry Ernst 编写的 NS-2 移动 IPv6 扩展——MobiWan[8]来为 NS-2 增添移动 IPv6 协议。

3.1　模拟实验环境的搭建

3.1.1　网络拓扑

构建如图 2 所示的有线加无线的网络拓扑结构。

以上拓扑结构中包含 6 个通信节点(CN0 ~ CN5),1 个路由器 RT(1.0.0),3 个无线接入路由器 AR0(1.1.0)、AR1(1.2.0)、AR2(1.3.0),一台服务器 SERVER(1.2.1)、一台恶意主机 AK(1.3.1)和 5 个移动节点(MN0 ~ MN4)。

有线部分采用点对点连接,所有 CN 到路由器 RT 采用全双工 100 Mbps 连接,3 个接入路由器与 RT 的连接带宽为 100 Mbps。MN 与 AR 之间采用标准 IEEE 802. 11 连接,带宽为 2 Mbps,在实验中 3 个 AR 分属不同的网段。

3.1.2　数据流的选择

每一个 CN 与其对应的 MN 进行单向通信。其中,CN 作为发送端,对应的 MN 作为接收端,以模拟数据流向。实验选择恒定比特率的 UDP 作为上层数据流,发送端以恒定的周期发送固定大小的 IP 分组。

3.2　实验结果及分析

3.2.1　消耗通信节点资源的 DoS 攻击实验

采用图 2 所示的网络拓扑。MN0 为正常的移动节点,MN0 和 CN0 之间从第 20 s 开始有一个 CBR 数据流。CN0 的绑定缓存大小设置为 5 000。AK 为一个恶意节点,从第 40 s 开始,恶意节点 AK 不断地向 CN0 发送绑定更新消息。从图 3中可以清楚地看到,当 CN0 收到的绑定更新包序号达到 5 000时,绑定缓存溢出,不能再继续注册新的绑定更新包,导致后面发往 CN0 的绑定更新包被丢弃。

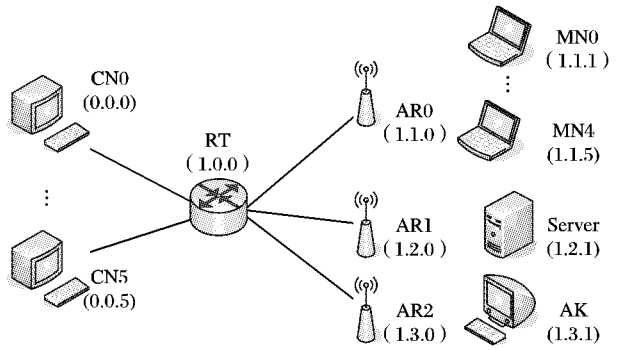

图 2　模拟实验网络拓扑

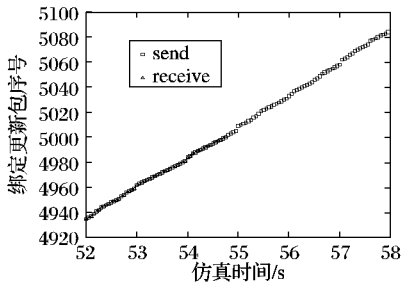

图 3　CN0(第 52 s ~ 第 58 s)接收绑定更新包示意图

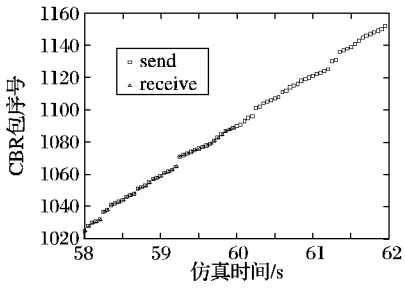

图 4　MN0(第 58 s ~ 第 62 s)接收数据包示意图

对这个结果更充分的证明是第 60 s 的时候,移动节点 MN0 的位置发生移动,转交地址由 1.1.1 变为 1.2.1, MN0 给 CN0 发送绑定更新消息来告诉它的新转交地址。由于 CN0 的绑定缓存满,没办法处理 MN0 发来的绑定更新消息。CN0 仍然将 CBR 数据流发往 1.1.1,导致 CN0 与 MN0 之间的 CBR 数据流的中断。如图 4 所示,在第 60 s 以后 MN0 再没有接收到 CN0 发来的 CBR 包,造成这种现象的原因就是 CN0 的绑定缓存溢出后,无法及时处理有用的绑定更新包。第 60 s时 MN0 发生移动后,CN0 仍然将数据包发往 MN0 旧的转

交地址,导致发送的数据包丢失。

3.2.2 伪造转交地址的 DoS 攻击实验

实验开始 20 s 后,通信节点(CN0 ~ CN4)分别与对应的移动节点(MN0 ~ MN4)进行单向通信,通信节点 CN5 与服务器 SERVER 进行单向通信。AK 为一个恶意节点,从第 40 s 开始,恶意节点 AK 分别向通信节点(CN0 ~ CN4)发送伪装的绑定更新消息,将绑定更新消息中的转交地址设为服务器 SERVER 的地址,从而引发大量的流量发往服务器,导致分布式拒绝服务攻击。

我们截取其一段时间的接收数据包过程进行分析。由图 5 中可以清楚地看到,仿真进行到第 40 s 时,服务器(SERVER)接收到的数据包突然增加。这是由于在第 40 s 时,恶意节点(AK)发送了伪装的绑定更新消息到通信节点(CN0 ~ CN4),从而将通信节点(CN0 ~ CN4)发往(MN0 ~ MN4)的大量数据流量引向了服务器,导致分布式拒绝服务攻击。

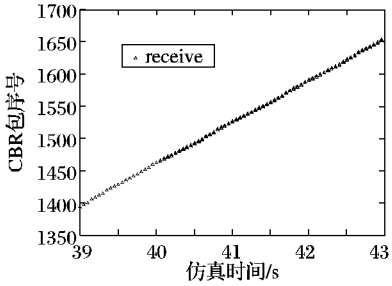

图 5 服务器(第 39 s ~ 第 43 s)接收数据包示意图

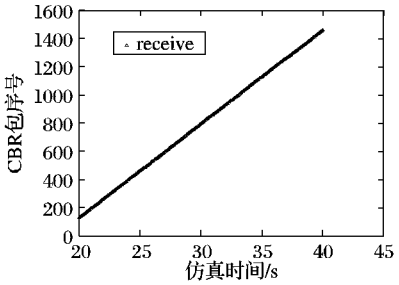

图 6 MN0 接收数据包示意图

由图 6 中可以看出,MN0 从第 20 s 开始接收到 CN0 发来的数据包,但是在第 40 s 以后,MN0 就再也没有收到 CN0 发出的 CBR 包。这是由于从第 40 s 开始,恶意主机 AK 给 CN0 发送了伪造的绑定更新包,将 CN0 发出的数据流引向了服务器(SERVER),阻断了 CN0 和 MN0 的正常通信,同时实现了对服务器(SERVER)的分布式拒绝服务攻击。

3.2.3 伪装节点移动的 DoS 攻击实验

实验中让 MN0 停留在 AR0 信号覆盖范围之内。实验开始 20 s 后,CN0 发送数据包到 MN0 进行正常的单向通信。实验进行到第 80 s 时,恶意主机 AK 使用移动节点 MN0 的家乡地址(1.1.1)发送绑定更新包,把自己的地址(1.3.1)作为移动节点 MN0 的转交地址,伪装移动节点 MN0 的移动状况。对端节点 CN0 收到绑定更新包后,将其添加到绑定缓存中。此后,CN0 发送数据包给 MN0 时,直接将数据包发送到 MN0 在绑定缓存中对应的转交地址即恶意主机的地址(1.3.1)。恶意主机 AK 截获了发往移动节点 MN0 的数据包,阻断了通信节点 CN0 与移动节点 MN0 之间的正常通信。

如图 7 所示,从第 80 s 以后,MN0 就再也没有收到过 CBR 包。这是由于从第 80 s 开始,恶意主机 AK 向 CN0 发送伪造的绑定更新包,伪装移动节点的移动。由图 8 可以看出,恶意主机 AK 在第 80 s 后开始接收 CN0 发来的 CBR 数据包。恶意主机 AK 截获了发往移动节点 MN0 的数据包,阻断了 CN0 和 MN0 的正常通信,发生了拒绝服务攻击。

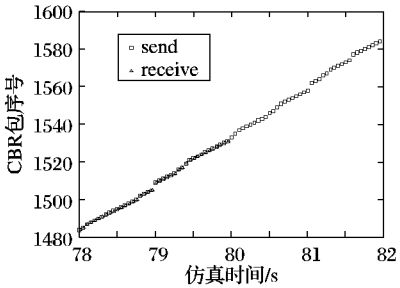

图 7 MN0(第 78 s ~ 第 82 s)接收数据包示意图

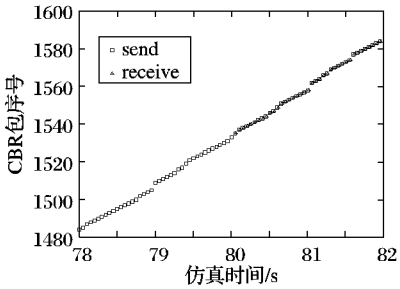

图 8 恶意节点(第 78 s ~ 第 82 s)接收数据包示意图

4 结语

本文在深入研究移动 IPv6 草案的基础上,对移动 IPv6 网络中面临的 DoS 攻击进行了介绍和分类。在 NS-2 网络模拟软件创建的较为复杂的移动 IPv6 网络环境中进行了模拟 DoS 攻击实验。经过对实验结果的分析,得出了“DoS 攻击对移动 IPv6 网络性能造成很大的影响”的结论。

如何解决移动 IPv6 网络中的 DoS 攻击问题是我们需要进一步研究的方向。

参考文献:

[1] JOHNSON D, PERKINS C, ARKKO J. RFC 3775, Mobility support in IPv6[S], 2004.

[2] AURA T, ARKKO J. MIPv6 BU Attacks and Defenses, Draft-aura-mipv6-bu-attacks-01.txt[R]. IETF, 2001.

[3] NARTEN T, DRAVES R. RFC 3041, Privacy extensions for stateless address auto-configuration in IPv6[S], 2001.

[4] ARKKO J, DEVARAPALLI V, DUPONT F. Using IPSec to protect mobile IPv6 signaling between mobile nodes and home Agents, Draft-ietf-mobileip-mipv6-ha-IPSec-06.txt[R]. IETF, 2003.

[5] NIKANDER P, AURA T, ARKKO J, *et al*. Mobile IP version 6 route optimization security design background, Draft-nikander-mobileip-v6-ro-sec-00.txt[R]. IETF, 2003.

[6] CHEN TIAN-WEI, SCHAFER G, FAN CHANG-PENG, *et al*. Denial of service protection for optimized and QoS-aware handover based on localized cookies [C]// Proceedings of 5th European Wireless Conference. Barcelona: Springer-Verlag, 2004: 155 – 161.

[7] 徐雷鸣,庞博, 赵耀. NS 与网络模拟[M]. 北京:人民邮电出版社,2003.

[8] Mobiwan: NS-2 extensions to study mobility in wide-area IPv6 networks[EB/OL]. [2007 – 03 – 15]. http ://www. inrialpes. fr/planete/Mobiwan.