文章编号:1673-9469(2011)04-0093-04

一种新的IPv6安全协议-有限制发送协议

胡清桂
(内江师范学院 现代教育技术中心,四川 内江 641112)

摘要:介绍了安全协议IPsec的不足,并针对IPsec无法解决的安全隐患提出了一种新的网络安全协议—有限制发送协议。在新的协议中,如果主机向网络发送大量的具有攻击性的数据包时,其发送权利将会受到限制,从而保证网络的安全。采用了OPNET仿真软件对新的协议进行了仿真,仿真结果表明,采用新的协议时,网络性能要好。采用新的协议时,平均HTTP响应时间为0.013 s;不采用新的协议时,平均HTTP响应时间为0.032 s。

关键词:IPsec;OPNET仿真;HTTP响应时间;缓存表
中图分类号:TP393.1 **文献标识码**:A

One new kind of IPv6 security protocol: Limited transmission protocol

HU Qing-gui
(Department of Modern Education Technology Center, Neijiang Teachers College, Sichuan Neijiang 641112, China)

Abstract: Firstly, IPsec is introduced and its shortage is analyzed. Secondly, as a new Protocol, the limited transmission protocol is put forward. In the new protocol, if many data packets are transmitted into the network by a computer, the computer would be limited to transmit data packets in order to assure the security of the network. Then, the performance of the new protocol is simulated with OPNET software, which shows the new protocol could enhance the network performance. For example, the average of HTTP object response time is 0.013s when the new protocol is adopted in the network. When the new protocol is not adopted, it is 0.032s.

Key words: IPsec; OPNET simulation; HTTP response time; buffer table

随着计算机技术和通信技术的不断发展,网络中信息的安全获取和传递对于人类的生活和发展变得越来越重要。而现实的网络又存在着各种各样的安全威胁,网络攻击的方式越来越多,IPv6作为下一代互联网通信协议,其安全性显得尤为重要。目前,IPv6安全协议主要是IPsec[1],它由认证协议(AH),封装安全载荷(ESP),Internet密钥交换协议(IKE)三个协议构成,它们分别提供认证、数据完整性和机密性三种保护。

认证协议(AH)即分组头认证协议主要提供数据源身份认证,数据完整性和重放攻击的保护功能[2]。封装安全载荷(ESP)主要是为IP层提供加密保证,数据源身份认证,数据完整性[3]。密钥交换协议(IKE)主要是对密钥交换进行管理,它主要包括对使用的协议,加密算法和密钥进行协商。与同类安全协议相比,IPsec具有很多优点,系统开销小,透明性好,实现起来更方便,管理也更方便等,但它也有其的局限性。

1 IPv6安全协议无法解决的安全隐患

以IPv6协议的子协议移动IPv6协议(MIPv6)为例,它也采用IPSec体系中认证协议(AH),封装安全载荷(ESP),Internet密钥交换协议(IKE)来提供认证、数据完整性和机密性保护。

但是,当黑客源源不断地向某一个服务器发送大量的TCP连接请求这样的数据分组,服务器

收稿日期:2011-08-30
作者简介:胡清桂(1973-),男,四川泸县人,硕士,从事网络技术研究。

不得不处理这些请求,并为每一个请求分配一块内存和其他资源,最后,服务器的CPU忙于处理这些无用的数据分组耗尽内存,而无法响应其它有用信息,造成拒绝服务攻击[4]。因为目前的单播数据分组的路由只依赖于目的地址,并不一定要查看源地址,因此黑客可以将数据分组的源地址设置成一个不存在的地址或一个合法的地址来欺骗对方服务器。

到目前为止,这样的安全隐患还没有较好的解决方法。"包过滤技术"(packet filtering)可以减轻这类攻击造成的威胁,包过滤技术原理在于监视并过滤网络上流入流出的IP包,拒绝发送可疑的IP包。但"包过滤技术"在处理这些无用的数据分组时,也要占用CPU资源,当黑客发送的无用的数据分组实在太多时,"包过滤技术"也无能为力。

实际上,在现行的IPv4网络中,类似的安全隐患也是存在的。以校园局域网为例,某一台计算机中"ARP"病毒后,它疯狂地向其他主机以及服务器发送大量的ARP数据包,欺骗其他主机,当它发送的欺骗数据包实在太多时,足以让三层交换机处理不过来而死机,造成网络瘫痪的局面。

2 有限制发送协议

针对上面介绍的IPsec无法解决的安全隐患,笔者提出一种新的网络安全协议—有限制发送协议。新协议的工作原理是这样的:

1)任何节点都有权利向网络发送数据分组,不附加任何限制条件。

2)当某一服务器或者客户机重复多次收到无用的数据分组时,就向发送数据包的源节点发送"恶意节点"消息。

3)接收方服务器接收到含有"恶意节点"消息的数据分组时,将对应的节点添加到事先创建的"黑名单"缓存中。

4)接收方服务器发现"黑名单"缓存中的源节点确实在向网络发送大量的数据分组时,立即限制其发送权利,让它只享有"平均发包率"权利。这里所说的"平均发包率"权利是指服务器下属的其它节点在单位时间内平均每个节点发送了N个数据包,那么被限制的节点在单位时间内也只能发送N个数据包。

5)一段时间后,如果接收方服务器依然被告知"黑名单"中的"恶意节点"依旧是"恶意节点",那么服务器将进一步限制其发送权利,让它只享有"平均发包率"一半的发送权利。

6)再过一段时间,如果接收方服务器依然被告知"黑名单"中的"恶意节点"依旧是"恶意节点",那么服务器将彻底限制其发送权利,不再允许它发送数据包。

7)再过一段时间,服务器恢复"恶意节点"部分发送权利,让它享有"平均发包率"一半的发送权利。

8)再过一段时间,如果接收方服务器依然被告知"黑名单"中的这一"恶意节点"依旧是"恶意节点",那么服务器将再次彻底限制其发送权利,不再允许它发送数据包。相反,如果接收方服务器没有被告知"黑名单"中的这一"恶意节点"依旧是"恶意节点",那么就进一步恢复它的发送权利,让它享有"平均发包率"权利。

9)再过一段时间,如果接收方服务器再次被告知"黑名单"中的这一"恶意节点"依旧是"恶意节点",那么服务器将再次限制其发送权利,让它享有"平均发包率"一半的发送权利。相反,如果接收方服务器没有被告知"黑名单"中的这一"节点"依旧是"恶意节点",那么就进一步恢复它的发送权利,不再限制它的发送权利,将这一节点信息从"黑名单"中删除。

这一新的协议既可以在未来的IPv6网络中工作,也可以在目前的IPv4网络中工作。另外,它既可以在服务器上工作,也可以在客户机上工作。但在客户机上工作与在服务器上工作是有一定区别的,在客户机上工作时,由于客户机不知道其它节点发送数据包的情况,所以它需要询问服务器其它节点的"平均发包率",然后再对自身主机发送数据包的频率进行限制。该协议在客户机上工作时,它可以被集成到Internet协议中,作为Internet协议的一个子协议。当这一协议被集成到Internet协议中工作时,我们可以理解成Internet协议限制主机盲目大量的发送数据包。

如果这一新的协议能够在网络中得到应用,那么,所有主机都不能盲目大量的发送数据包,这样,网络中的压力将会大大减轻。

3 "黑名单"缓存表的设计

假设这一新的协议是在服务器上工作,可以这样设计"黑名单"缓存表。

假设服务器接收到一个"举报"信息,怀疑IP

为 192.168.10.7 的主机盲目大量的发送攻击性数据,该主机是从 2 号端口连接服务器的。此时,如果被“举报”的主机并没有大量发送数据包,那么,服务器可以暂时不信任这一“举报”信息。相反,如果被“举报”的主机确实正在向网络大量发送数据包,那么,服务器就信任这一“举报”信息,限制可疑主机发送数据包权利,让它只享有“平均发包率”权利,并将这一信息添加到“黑名单”缓存表中,假设限制时间定为 600 s。“黑名单”缓存表内容如下所示。

<192.168.10.7,2,N,600 s>

需要说明的是,此时可疑主机只享有“平均发包率”权利,如果它不再大量发送数据包,那么,它的正常网络连接不受影响。

等待一段时间后,如果服务器还接收到针对该主机的“举报”信息,那么,将进一步限制其发送权利,让它只享有“平均发包率” 一半的发送权利,相应地,“黑名单”缓存表作如下变化。

<192.168.10.7,2,N/2,600 s>

等待一段时间后,如果服务器继续接收到针对该主机的“举报”信息,那么,将进一步限制其发送权利,也就是停止它发送权利,相应地,“黑名单”缓存表作如下变化。

<192.168.10.7,2,0,600 s>

10 min 限制时间满后,如果服务器没有接收到针对该主机的“举报”信息,那么,服务器将放宽其发送权利,让它只享有“平均发包率” 一半的发送权利,相应地,“黑名单”缓存表作如下变化。

<192.168.10.7,2,N/2,600 s>

10 min 限制时间满后,如果服务器还是没有接收到针对该主机的“举报”信息,那么,服务器将进一步放宽其发送权利,让它只享有“平均发包率”的发送权利,相应地,“黑名单”缓存表作如下变化。

<192.168.10.7,2,N,600 s>

上面简要举例说明新协议在服务器上工作时“黑名单”缓存表变化过程,这是“黑名单”缓存表中只有一个节点的情况,有些时候,缓存表中完全可能出现多个节点。

4 使用 OPNET 软件对新协议的仿真

OPNET 是最常用的网络仿真软件之一,它采用三层建模机制,分别为进程模型,节点模型和网络模型,这种建模方式和协议、设备、网络对应,可以全面反映网络的相关特性[5-6]。使用 OPNET 进行网络建模仿真大体上可以分为以下几个步骤,配置网络拓扑(topology),节点模型和进程的设计,配置业务(traffic),运行仿真(simulation),最后发布仿真报告(report)[7]。

4.1 配置网络结构模型和节点模型

为了对改进后的移动 IPv6 协议进行仿真,笔者配置了如下简单的网络结构模型,3 个路由器 Router A, Router B, Router C 相互连接,每一个路由器连接一个无线收发机 Access Point, 每一个无线收发机旁边有 2 个无线上网设备 wkstn,如图 1 所示。

在这一网络中,让路由器 Router C 连接的无线收发机下面的无线上网设备 wkstn 1 不断地向路由器 Router B 下面 wkstn 6 发送大量的 TCP 连接请求。

同时,让其它无线上网设备与 wkstn 6 通信,对比采用新协议和不采用新协议两种情况下 wkstn 6 对其它无线上网设备的平均响应时间。

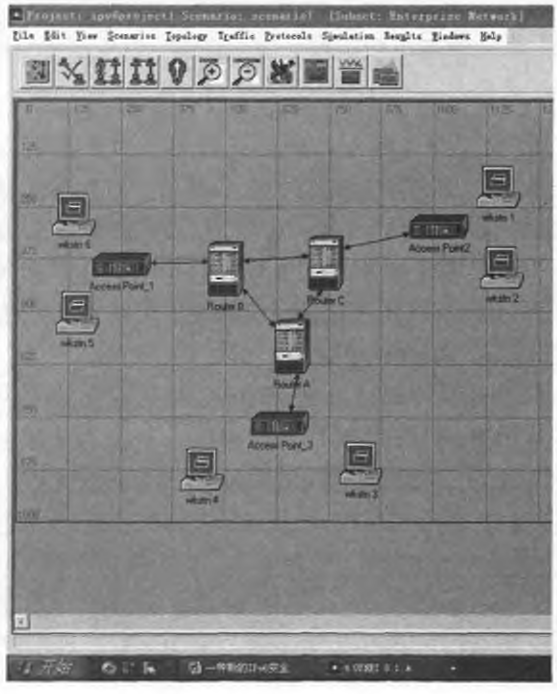

图1 网络拓扑结构

Fig. 1 The topology of the network

面 1 网络结构模型中,客户端 wkstn 节点模型采用 OPNET 软件现有的名为 wlan_station_adv 的节点模型,如图 2 所示。

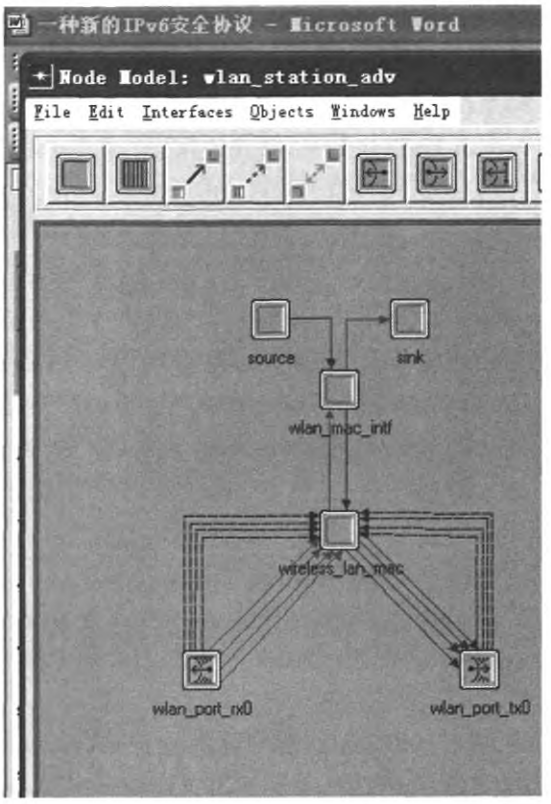

图2 Wlan_station_adv节点模型

Fig. 2 The model of the node wlan_station_adv

4.2 业务量配置和仿真

完成网络拓扑结构配置以及节点模型设计后,开始配置业务量和确定统计量。对于配置业务量,本文采用的方法是在 traffic 选项中再选择 Import conversation pairs 选项进行相关参数的配置[8]。配置业务量时,让 wkstn 1 不断地向 wkstn 6 发送大量的 TCP 连接请求。同时,让其它无线上网设备与 wkstn 6 通信。

下面的仿真结果是 wkstn 6 对其它无线上网设备作出的 HTTP 平均响应时间。从仿真结果上可以看出,不采用新协议时,wkstn 6 对其它无线上网设备作出的 HTTP 平均响应时间在 0.03 s 之上,大约是 0.032 s。

采用新协议时,wkstn 6 对其它无线上网设备作出的 HTTP 平均响应时间在 0.012 5 s 之上,大约是 0.013 s。

由仿真结果可以看出,不采用新协议时,wkstn 6 对其它无线上网设备作出的 HTTP 平均响应时间要慢,这是因为 wkstn 1 不断地向 wkstn 6 发送大量的 TCP 连接请求时,耗费了 wkstn 6 的 CPU 资源,使 wkstn 6 来不及响应其它的服务请求。相反,采用新协议后,当 wkstn 1 不断地向 wkstn 6 发送大量无用的 TCP 连接请求时,其发送数据包的权利受到限制,从而 wkstn 6 对其它的服务请求响应要快。

5 结束语

在新的协议中,如果主机向网络发送大量的具有攻击性的数据包时,其发送权利将会受到限制,从而保证网络的安全。对新的方案进行了仿真,仿真结果表明,在新的协议情况下,目标客户机平均响应时间要快。但这只是理论分析的结果,实际上,要真正实现这一新的协议,还有许多问题需要解决,比如,"恶意节点"的具体判定标准,采用何种方法举报"恶意节点"等。

参考文献:

[1] 杨文超,贾世楼. 改善层次化 MAP 的移动 IP 切换时延的方法[J]. 北京邮电大学学报,2007,30(2):127-131.

[2] 胡 晓,宋俊德,宋 梅. 分级移动 IPv6 中一种新的自适应 MAP 选择算法[J]. 计算机应用研究,2006(10):229-231.

[3] 李娟娟, 钱德沛. 基于 P2P 的无线传感器网络应用架构研究[J]. 微电子学与计算机, 2006, 23(9): 13-19.

[4] 孙飞燕, 张朝阳, 仇佩亮. HFC 接入网络 MAC 层随机访问机制静态特性及动态稳定性分析[J]. 电路与系统学报, 2003, 8(2): 33-38.

[5] 张 涌,钱乐秋. 基于扩展有限状态机测试中测试输入数据自动选取的研究[J]. 计算机学报, 2003, 26(10):1295-1303.

[6] 管明祥,郭 庆,李 陆. 基于临近空间通信网络混合业务的 MAC 协议[J]. 华南理工大学学报:自然科学版, 2008, 36(5): 65-69.

[7] 梁 俊,田 斌,仝海波,等. 一种支持 QoS 的 D-TDMA 协议性能分析与仿真[J]. 空军工程大学学报: 自然科学版, 2010, 11(1): 59-63.

[8] JUAN JUAN LI, DE PEI QIAN. A P2P-based application architecture for wireless sensor networks[J]. Micro Electronics & Computer, 2006, 23(9):13-19.

(责任编辑 刘存英)