doi:10.3969/j.issn.1000-436x.2013.z2.012

OSPF 协议脆弱性分析与检测系统的设计和实现

覃遵颖[1,2]，李国栋[1,3]，李卫[2,3]，黄旭昌[2]

（1. 西安交通大学 网络中心，陕西 西安 710049；2. 西安交通大学 电子与信息工程学院，陕西 西安 710049；
3. 通讯网信息传输与分发技术重点实验室，河北 石家庄 050081）

摘 要：在分析和研究 OSPF 协议脆弱性的基础上，设计实现了一个通用的、多模式的 OSPF 协议脆弱性检测系统，包括了使用伪造实体路由器方法实现拒绝服务攻击模型和使用零拷贝技术实现中间人攻击模型，并采用 SNMP 和旁路监听相结合的方法实现了检测结果的实时监控。最后，在测试环境中对不同种类的路由设备进行了脆弱性验证，并对脆弱性的危害进行了定量的分析。

关键词：OSPF；LSA；脆弱性攻击模型；路由攻击；脆弱性检测

中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2013)Z2-0058-06

Design and implementation of OSPF vulnerability analysis and detection system

QIN Zun-ying[1,2], LI Guo-dong[1,3], LI Wei[2,3], HUANG Xu-chang[2]

(1. Center of Network, Xi'an Jiaotong University, Xi'an 710049, China;
2. School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China;
3. Science and Technology on Information Transmission and Dissemination in Communication Networks Laboratory, Shijiazhuang 050081, China)

Abstract: A universal and multi-mode OSPF vulnerability detection system was designed based on analysis and research of OSPF vulnerability. The system implements denial of service attack model with the method of forging entity router and man-in-middle attack model with zero-copy technology. The method combining SNMP and bypass monitoring was adopted to achieve real-time monitoring of test results. Finally, the system proves the vulnerability of different types of routing equipments in the test environment and the vulnerability hazards were analyzed quantitatively.

Key words: OSPF; LSA; vulnerability attack model; routing attack; vulnerability detection

1 引言

互联网络的高速发展使其成为承载当今人类社会信息传递交流的重要基础设施，如何保障网络安全、稳定、可靠运行以及确保信息安全是互联网发展面临的巨大挑战。路由协议作为互联网络最重要的基础协议之一，负责在路由器间交换、发现和维护关于网络的拓扑信息，寻找网络数据分组交换的最佳路径，实现对网络数据的转发。正确的路由信息是网络报文正确高效传输的前提，路由信息的错误或混乱，严重时会造成网络的瘫痪和秘密信息的泄露。

OSPF（open shortest path first）协议作为当前应用最为广泛的内部网关协议，为自治系统内部的主机提供动态路由选择。多年来国内外的学者和研究人员不断对 OSPF 协议的安全缺陷和顽健性进行研究，并提出了多种检测模型和方法[1~4]。本文在分析和研究 OSPF 协议脆弱性的基础上，设计实现了一个通用的、多模式的 OSPF 脆弱性检测系统，并利用该系统对不同种类的路由设备进行了多种安全缺陷的验证，对比了不同安全缺陷对不同种类路由设备的影响，最后对安全缺陷的危害进行了定量分析。

收稿日期：2013-09-06
基金项目：通信网信息传输与分发技术重点实验室开放课题基金资助项目（ITD-U11001）
Foundation Item: The Open Subject of Science and Technology on Information Transmission and Dissemination in Communication Networks Laboratory(ITD-U11001)

2　OSPF 协议脆弱性分析

OSPF 路由协议是基于链路状态的协议，它的运行机制使 OSPF 自治区域能够快速收敛并进行 SPF 计算得到路由表。在网络状态发生变化时，它能够快速响应，使路由设备及时更新路由信息[5]。OSPF 协议采用了安全保护机制、可靠的扩散机制、一致性校验、分层路由等机制来增加其协议安全性[6]，使 OSPF 路由协议具有一定的自我保护能力，但这并不足够安全，其协议本身仍然存在着许多漏洞，利用这些漏洞可发起针对 OSPF 的路由攻击。

首先，由于 OSPF 是通过 LSA 机制来广播路由信息，通过篡改 LSA 对 OSPF 发动攻击，将会使区域内的路由产生震荡，导致拓扑混乱和网络异常。其次，在实际运营的网络环境中，路由器的安全保护机制也仅限于使用密码认证，大多数路由器甚至于使用空认证或者明文认证。当 OSPF 使用空验证和简单口令验证时，其路由报文将很容易被截获，根据明文传输的路由信息可以生成伪造的路由信息或利用它分析网络拓扑和流量模式；加密身份认证可防范修改路由消息及阻塞协议报文传输等攻击，但是外部攻击者仍可通过发送使用加密验证的恶意报文来进行 DoS 攻击[7]。最后，OSPF 协议细节上也存在着缺陷，如 OSPF 协议的一致性验证只包含 OSPF 头部检验，而没有包含 IP 分组头；OSPF 根据 LSA 序列号判断 LSA 的新旧，可以通过篡改 LSA 设计序列号加一攻击、最大序列号攻击、最大年龄攻击等[8,9]。

3　系统设计与实现

3.1　脆弱性攻击模型

在对 OSPF 协议脆弱性深入分析和总结的基础上，本文建立了相应的攻击模型用于检测这些脆弱性，根据采用的技术方案和实现目标的不同，分成拒绝服务攻击模型和中间人攻击模型 2 类。

拒绝服务攻击模型包括如下几个模型。

1) DR/BDR 篡改攻击，攻击者通过将 Hello 报文中的指定路由器和备份指定路由器字段置零后发送到域内，引发指定路由器和备份指定路由器的重选，引起局部网络的不稳定。

2) LSR 报文伪造攻击，攻击者向目标路由器高速发送 LSR 链路状态请求报文，使得路由器不停地响应 LSR 报文，占用路由器大量的 CPU 周期，使其无法提供转发服务。

3) 序列号加 1 攻击，不断的将收到的 LSA 数据分组序号加一或更多后，重新计算校验和发送出去。源路由器将会不断地发送具有更大链路序号的数据分组去纠正错误信息，导致网络带宽消耗、拓扑震荡，甚至引起网络不可用。

4) 最大序列号攻击，将 LSA 数据分组的链路序号设为最大值 0x7FFFFFFF，重新计算校验和后发送出去，效果与序列号加 1 攻击类似。

5) 最大年龄攻击，在其捕获到一个 LSA 数据分组后，将链路年龄设为最大，重新发送出去，效果与序列号加 1 攻击类似。

中间人攻击模型通过篡改 LSU 报文中的 AS External LSA（autonomous system external LSA）完成攻击。

3.2　系统总体架构

本文旨在设计一个通用的、多模式的 OSPF 脆弱性检测系统，根据此设计目标，本系统的架构如图 1 所示，分为 3 个子系统：攻击子系统、监控子系统和可视化子系统。

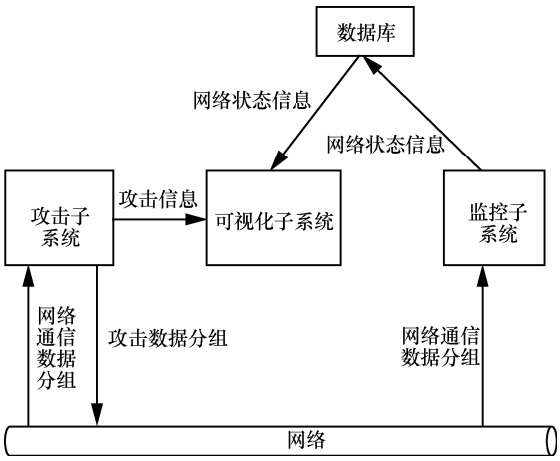


图 1　OSPF 协议脆弱性检测系统架构

攻击子系统首先捕获被攻击网络的流量，通过各路由器所发出的路由信息分析当前路由器状态，根据状态值的不同产生相应的攻击数据分组，实施路由攻击。

监控子系统采集网络状态信息和攻击信息并与攻击子系统通讯，在获得信息的基础上对数据进行融合、分析，生成网络状态相关信息，并将状态信息发送给可视化显示子系统。

可视化子系统读取攻击子系统的攻击信息和监控子系统存储的信息，可视化地显示当前网络状态、攻击过程和结果。

3.3　攻击关键技术

拒绝服务攻击模型的主要目标是通过向被攻击者发送大量伪造报文，从而消耗被攻击者的资源或者产生网络拥塞，造成路由和网络的不可用。实验发现如果仅仅是发送单一的攻击报文，此报文会被路由器直接丢弃。对 OSPF 进行有效的路由攻击必须维护 OSPF 的状态机，因此攻击者必须要伪造成一个合法的实体路由器。

伪造路由器的方法通过改造 Quagga 实现。Quagga/Zebra 是一款基于 Linux 平台下的开源路由软件，它具有使用的广泛性、易用性和功能完备性等特点。Quagga 包含一个核心守护进程 Zebra，它作为 Linux 底层核心的一个抽象层，为上层模块化的路由协议的实现提供系统级的服务。OSPF 作为其中一个独立模块，它与 Zebra 守护程序交换路由更新信息。不同的攻击只有在特定的路由状态下才能有效，本文的攻击模型都设计在 Full 状态下。通过设计和选择不同的 OSPF 状态机，在攻击需要的对应状态下篡改和伪造 OSPF 报文完成不同的攻击。系统中 OSPF 的状态机如图 2 所示。

OSPF 数据分组的收发在 ospf_packet.c 文件中定义，因此系统的各个攻击也需要在这个文件中定义相应的处理函数。OSPF 拒绝服务攻击主要函数说明如表 1 所示。

表 1　OSPF 拒绝服务攻击主要函数说明

函数名	说明
ospf_make_hello	伪造 Hello 报文，将 DR 和 BDR 字段清零，并设置高优先级
ospf_make_fake_ls_req	伪造 LSR 报文并发送
lsa_related_attack	与 LSA 相关的攻击，包括序列号加 1、最大序列号、最大年龄

中间人攻击模型的主要目标是通过连接在 2 个路由器之间，获得它们路由信息的同时进行篡改，从而达到改变路由、影响网络拓扑的目的。为了达到这个目的，攻击者需要高效地捕获、过滤并转发数据分组。如果转发效率不够高，数据分组延时较大，则可能引起重传等问题。另一方面，中间人不能产生一些无用分组干扰正常的通信。经过研究，利用 NTZC 可以有效实现中间人攻击。零拷贝技术（NTZC）是通过将若干连续的内核空间 mmap 到用户空间，减少数据分组拷贝次数，达到提高效率的目的。作为中间人，攻击者可以获得两端路由器间通信的所有报文，方便窃取路由信息和其他通讯信息。中间人攻击的过程如图 3 所示。

其攻击流程如下。

1) 等待捕获存在 AS External LSA 的 LSU 报文。

2) 根据步骤 1)中捕获的 LSU 报文伪造一个 LSU 报文，将该 LSA 的 link state ID 字段设置为需要改变的路由（设为 *R*）的目的 IP 地址，advertising router 字段设置为路由 *R* 希望被引导到的 IP 地址，即所有去往 link state ID 地址的数据分组都要经过 advertising router 这个地址。同时设置该 LSA 的 metric 值，令其小于当前网络中存在的其他到达 *R* 的

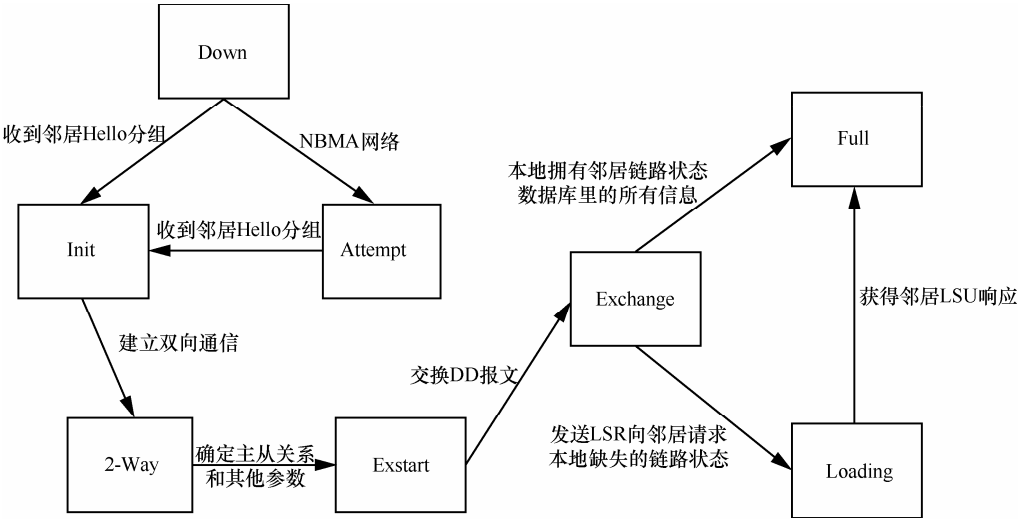


图 2　OSPF 状态机转换

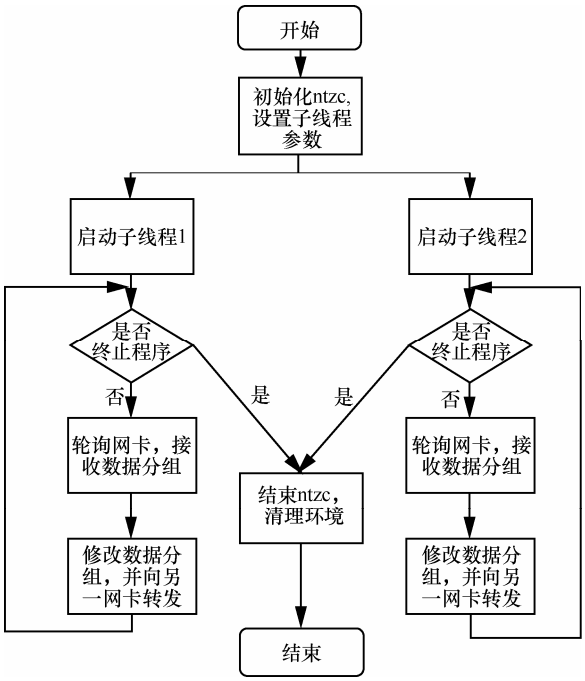


图 3　中间人攻击流程

目的地址的所有路由的 metric 值。

3) 接收路由器对伪造的 LSU 报文的响应，但不转发这个响应报文。

3.4　SNMP 与旁路方式相结合的网络监控

在攻击检测的过程中，需要监控网络中所有路由器状态的变化情况，用以对脆弱性的危害进行定量分析。当网络中存在攻击，设备的 CPU 将满负荷运行，无法处理 SNMP 请求，监控系统将无法捕获设备的运行状态和信息。因此，本文采用 SNMP 和旁路监听相结合的方式实现网络监控。系统通过设置定时器，定时向路由器发出 SNMP 请求，获得 CPU 利用率、内存利用率等路由器状态信息。旁路监听方式使用路由交换设备的端口流量镜像功能将网络流量旁路到监控服务器上，在服务器上使用 WinPcap 对接收到的端口出入流量进行实时采集，对流量数据进行过滤，丢弃那些无用数据，对有用数据（路由协议数据分组）进行分析，得到当前路由器状态和网络状态，从而监控网络的异常变化，且不会对网络产生任何影响。

4　系统测试

为了比较 OSPF 脆弱性对不同路由设备危害程度，针对国内外设备厂商，使用实际的硬件物理设备搭建 2 套检测环境（思科 3900 和锐捷 5750 路由器）分别对系统进行测试。系统的测试环境如图 4 所示。

通过本系统的检测，得到脆弱性检测结果如表 2 所示。

表 2　　脆弱性检测结果

序号	被检测攻击类型	检测结果
1	DR/BDR 篡改攻击	2 种测试环境下均无效
2	LSR 报文伪造攻击	2 种测试环境下均无效
3	序列号加 1 攻击	2 种测试环境下均有效
4	最大序列号攻击	2 种测试环境下均有效
5	最大年龄攻击	锐捷路由器有效，思科路由器无效
6	中间人攻击	2 种测试环境下均有效

其中，DR/BDR 篡改攻击和 LSR 报文伪造攻击都没有成功实现。可见，思科 3900 和锐捷 5750 路

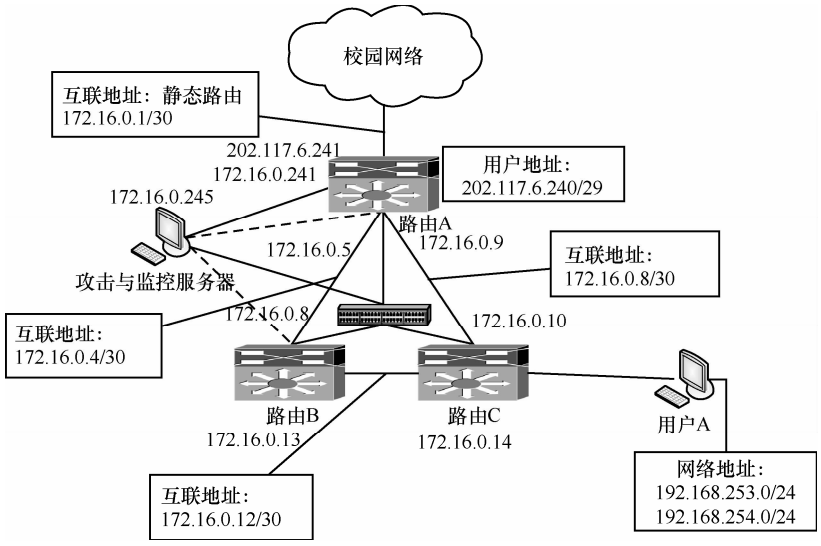


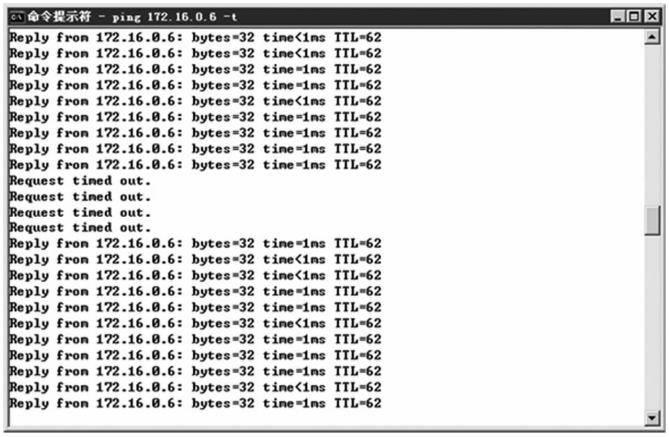
图 4　系统测试环境示意

由器对 DR/BDR 重选机制进行了改进；对于 LSR 报文伪造攻击，通过分析发现，由于受制于 OSPF 的状态机和定时器，系统无法连续高速地发送 LSR 报文，进而路由器的 CPU 占用率也没有大的变化。

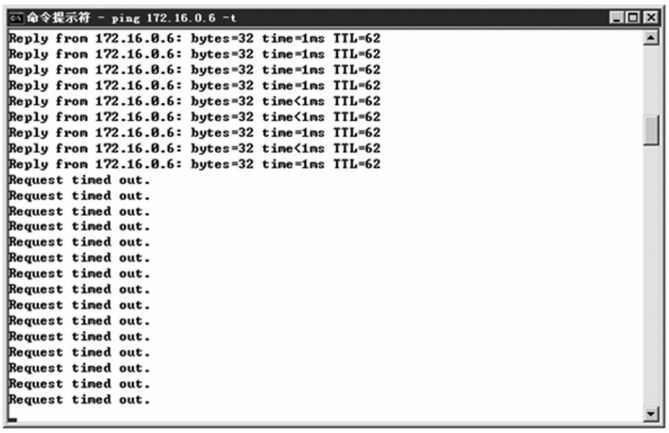
序列号加 1 攻击利用了 OSPF 协议泛洪机制和 LSA 头部字段方面存在的脆弱性，攻击后引起自治域内产生大量更新报文。通过理论分析和检测结果，攻击后自治域内产生的 LSA 更新的数量与攻击时序列号加 1 的 LSA 数量成正比。正常情况下，测试环境中的路由数据分组数量为 1.2 个每秒。测试中，当序列号加 1 的 LSA 的数量为 8（受制于自治域内存在的 LSA 总量），攻击后自治域内路由数据分组数量上升为平均 2.07 个每秒。每发送一个序列号加 1 的 LSA，自治域内就将产生至少 57 byte 的数据，当发送 1 000 个序列号加 1 的 LSA 后，这个数据将达到 57 000 byte，且不包含以太网头部，IP 分组头部和 OSPF 头部。当网络规模比较大时，序列号加 1 攻击将占用不少宝贵的网络带宽。

最大序列号攻击的目标为引起路由的间断性失效以及令自治域内产生大量 LSA 更新，在图 5(a)中可以看到，被检测路由器在攻击中路由失效，在攻击结束后恢复了正常。最大年龄攻击模型利用了 OSPF 协议泛洪机制和 LSA 头部字段方面存在的脆弱性，结果为引起自治域内存在大量更新报文，同时引起网络路由间断性不可用，它的测试结果如图 5(b)所示。

OSPF 中间人攻击的目标为改变网络中的路由，监控子系统通过 traceroute 方法监测路由的变化情况。在测试环境中，路由器 *C* 拥有到达 192.168.253.0/24 网络的路由，并且通过 OSPF 协议，路由器 *A* 和 *B* 都学习到了这条路由。中间人在转发 *A* 与 *B* 间的数据分组时，修改目的地址为 192.168.253.0 的 LSA 中的 metric 字段，令 *A-B-C* 链路的 metric 值小于 *AC* 链路的 metric 值。结果表明，到达 192.168.253.0/24 网络的路由因此而发生改变，攻击模型检测成功。



(a) 最大序列号攻击结果



(b) 最大年龄攻击结果

图 5 路由攻击测试结果

5　结束语

本文根据 OSPF 协议存在的安全威胁和漏洞建立路由攻击模型，设计脆弱性检测系统对攻击模型进行实现来验证多个安全漏洞。近年来，虽然国内外研究人员致力于通过改进保护机制等方法来增强其协议安全性，但从研究结果可以看出，OSPF 协议本身仍存在不足，一旦被恶意攻击，将导致网络不可用或者信息的泄露。因此，在以后的研究中对本文检测出的 OSPF 安全漏洞进行改进势在必行。

参考文献：

[1] HARTMAN S, ZHANG D. Analysis of OSPF Security According to KARP Design Guide[S]. 2011.

[2] JAVVIN. TCP/IP network vulnerability and security[EB/OL]. http://www.javvin.com/networksecurity/tcpipnetwork.html.

[3] JONES E, MOIGNE O. OSPF Security Vulnerabilities Analysis[S]. 2006.

[4] BARBIR A, MURPHY S, YANG Y. Threats to Routing Protocols[S]. RFC 4593, 2006.

[5] MOY J. OSPF Version 2[S]. 1998.

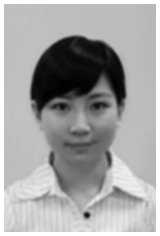
[6] 陈海燕, 季仲梅, 李鸥等. OSPF 路由协议安全性分析及其攻击检测[J]. 微计算机信息, 2005, 5: 234-235.
CHEN H Y, JI Z M, LI O, *et al*. OSPF routing protocol security analysis and attacks detection[J]. Microcomputer Information, 2005, 5: 234-235.

[7] 蔡朝权. OSPF 路由协议的攻击分析与安全防范[J]. 计算机工程与技术, 2007, 28(23): 5618-5620.
CAI Z Q. OSPF routing protocol attacks analysis and security precaution[J]. Computer Engineering, 2007, 28(23): 5618-5620.

[8] 高峥, 李林涛. OSPF 协议安全性分析[J]. 黑龙江科技信息, 2011, 11: 78.
GAO Z, LI L T. OSPF protocol security analysis[J]. Heilongjiang Science and Technology Information, 2011, 11: 78.

[9] VETTER B, WANG F, WU S. F. An experimental study of insider attacks for OSPF routing protocol[A]. IEEE 1997 International Conference on Network Protocols[C]. Atlanta, Georgia, USA, 1997. 293-300.

作者简介：



覃遵颖（1985-），女，陕西安康人，西安交通大学博士生、工程师，主要研究方向为网络安全。

李国栋（1974-），男，山西长治人，西安交通大学博士生、高级工程师，主要研究方向为网络安全。

李卫（1967-），男，陕西榆林人，博士，西安交通大学副教授，主要研究方向为计算机网络安全与管理。

黄旭昌（1986-），男，福建福州人，西安交通大学硕士生，主要研究方向为网络安全。