

# ARSAO:一种通用的检测与防御 OSPF 路由欺骗的机制

李鹏飞,陈 鸣,钱红燕

(南京航空航天大学 计算机科学与技术学院,江苏 南京 211106)

**摘 要:**OSPF 路由欺骗对 OSPF 路由协议构成严重的安全威胁,目前还没有全面有效的攻击检测和防御方法。文中首先分析比较了目前主要的 OSPF 路由欺骗攻击,将攻击分为引起反击和不引起反击两类,由此提出了两类 OSPF 路由欺骗攻击的检测算法和防御机制 ARSAO(against the routing spoofing attacks on the OSPF protocol);其次,提出了一种通用的系统结构,能够支持检测与防御这两类 OSPF 路由欺骗攻击;并且基于网络功能虚拟化(NFV)技术设计实现了具有上述系统架构的原型系统。实验结果表明,在网络时延和丢包非极端的情况下,该系统和相关技术不仅能够准确、高效地检测出多种 OSPF 路由欺骗攻击,并且能够及时防御与恢复污染路由;基于 NFV 的 ARSAO 系统具有经济性、灵活性和易于部署等优点,能够用于 NFV 网络以保障该网络 OSPF 协议的安全性。

**关键词:**OSPF 路由欺骗攻击;检测与防御方法;系统结构;网络功能虚拟化

中图分类号:TP393                      文献标识码:A                      文章编号:1673-629X(2019)10-0120-07  
doi:10.3969/j.issn.1673-629X.2019.10.025

## ARSAO: A General Detection and Defense Mechanism Against Routing Spoofing Attacks on OSPF Protocol

LI Peng-fei, CHEN Ming, QIAN Hong-yan

(School of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics,  
Nanjing 211106, China)

**Abstract:**OSPF route spoofing poses a serious security threat to OSPF routing protocols. Currently, there is no comprehensive and effective attack detection and defense method yet. We first analyze and compare the current major OSPF route spoofing attacks, and separate the attacks into having counterattacks and having no counterattacks respectively, and then propose two types of OSPF route spoofing attack detection algorithms and defense mechanisms ARSAO (against the routing spoofing attacks on the OSPF protocol). Secondly, a general system structure is proposed to support both detection and defense OSPF route spoofing attacks. Third, a prototype system with the above system architecture is designed based on network function virtualization (NFV) technology. The experiment shows that in the case of network delay and packet loss are not extreme, the system and related technologies can not only detect multiple OSPF route spoofing attacks accurately and efficiently, but also defend and recover pollution routes in time. The NFV-based ARSAO system is economical, flexible and easy to deploy, which can be used in an NFV network to secure the OSPF protocol of the network.

**Key words:**OSPF route spoofing attack; detection and defense method; system structure; network function virtualization

### 0 引 言

路由选择协议对于因特网至关重要,决定着数据分组的转发路径,保证了分组能够跨越网络正确、高效地到达目的地。开放式最短路径优先(open shortest path first, OSPF)路由协议<sup>[1-2]</sup>是因特网自治系统中最

常用的内部网关协议之一,尽管有一定的安全保护措施,OSPF 仍受到许多攻击者的觊觎<sup>[3-4]</sup>。

OSPF 是一种典型的链路状态路由选择协议,每当链路的状态发生变化(如开销的变化或连接/中断状态的变化)或经过一定时间,路由器就会利用链路

状态通告 (link state advertisement, LSA) 广播链路状态信息。LSA 是描述网络拓扑的分组,记录相邻路由器信息,在相邻路由器中交换<sup>[5-6]</sup>,所有有效的 LSA 会被存放在链路状态数据库中,路由器根据链路状态数据库计算得到路由表。因此,LSA 上的路由信息的真实性和准确性至关重要,一旦被篡改,虚假的路由将会导致整个网络陷于混乱。路由欺骗<sup>[7-11]</sup>是一种利用协议漏洞伪造 LSA 篡改路由信息的攻击方法。一旦攻击者实施路由欺骗攻击,会严重影响网络的安全,造成分组无法到达目的地、路由环路、流量黑洞、网络瘫痪等严重后果。而路由选择中的洪泛机制会进一步增强路由欺骗攻击的破坏力<sup>[12]</sup>。此机制虽然在功能上是必要的,但同时会在整个网络中洪泛虚假的 LSA,导致大面积的路由污染<sup>[13]</sup>。

文中通过对目前已存在的多种 OSPF 路由欺骗攻击进行分析和分类,提出了有针对性的检测算法;设计了一种通用的检测和防御系统,基于网络功能虚拟化 (NFV) 实现了原型系统,并通过实验证明了该系统和相关技术的有效性。

### 1 相关工作

目前为止,针对攻击方法的研究,主要在于新型路由欺骗攻击的发现。文献[7]提出了一种新型的路由欺骗攻击,利用协议处理 LSA 头部时,不检查链路状态 ID 和路由器标识的一致性,成功躲过反击机制,同时该文献还提出了三种预防的方法。文献[8]发现了两种逃避反击机制的新攻击,分别为邻接欺骗攻击和单路径攻击。文献[9-10]发现了两种危害性很大的路由欺骗攻击,分别为双 LSA 注入攻击和远程邻接攻击。文献[11]在双 LSA 注入攻击的基础上提出了双 LSA 远程多注入攻击。这些文献提出的路由欺骗攻击都是利用了协议缺陷或者漏洞,逃避反击机制对路由器进行攻击。

关于 OSPF 协议安全性的研究主要集中在攻击分析、消耗资源类攻击的检测以及防范。文献[14]提出一种冗余的网络系统架构,降低 LSA 伪造攻击对网络的影响,提高 OSPF 网络系统的生存能力。文献[15]设计一种模型来分析验证 OSPF 协议中关键漏洞的存在,并通过此方法提出并验证了一个新漏洞。文献[16]引入了一种渗透工具来检查 OSPF 口令强度,增加网络的安全性,但该工具受到了路由器硬件和操作系统版本的限制。文献[17]对 OSPF 协议进行安全性分析,并建议将基于软件包分析的入侵检测功能加入规范。文献[18]利用路由器嵌入的 TPM 模块和内部的动态度量模块防止遭受操作系统层面的入侵,利用系统处理攻击报文的流程来判断是否受到最大年龄攻

击等三种攻击。该方法将整个系统存在于路由器内部,能够经济有效地检测这三种攻击。文献[19]设计了一个通用、多模式的 OSPF 协议脆弱性检测系统,利用网络受到资源消耗攻击时,CPU 满载无法处理 SNMP (simple network management protocol) 请求的特点,采用 SNMP 和旁路监听相结合的方法实现检测结果的实时监控,有效地检测出消耗资源类的攻击。

网络功能虚拟化 (network functions virtualization, NFV)<sup>[20]</sup>是一种利用通用硬件以及虚拟化技术,承载多种功能的软件来代替传统硬件,实现各种网络功能或网络设备的技术。通过 NFV 技术,使网络功能不再依赖专用硬件,减少了网络设备的成本,实现网络新业务的快速开发与部署,为网络发展注入新的动力。

## 2 OSPF 路由欺骗攻击分类及其检测算法

### 2.1 路由欺骗攻击分类

表 1 列出了目前主要欺骗方法的特点。通过进一步分析发现,当欺骗攻击不引起反击机制时,尽管欺骗攻击的原理不同,但有着以下的共同特性,且与网络拓扑无关:

- (1)攻击者发送一个恶意的路由器 LSA。“恶意”指它的 LSA 部分与链路状态数据库中真实的 LSA 不同;
- (2)攻击者会收到一个 LSAck 包,表明恶意 LSA 通过了协议的校验和检查;
- (3)由于协议的缺陷等原因,恶意的 LSA 并不会引起反击机制,使其篡改了真实的 LSA 达到欺骗的效果。

表 1 攻击特点

| 攻击种类        | 引起反击机制 | 逃避反击机制 | 攻击与网络结构相关 |
|-------------|--------|--------|-----------|
| 双 LSA 注入攻击  | 是      | 是      | 无         |
| 双 LSA 远程多注入 | 是      | 是      | 无         |
| 邻接欺骗        | 否      | 是      | 有         |
| 远程邻接欺骗      | 否      | 是      | 有         |
| 单路径注入攻击     | 否      | 是      | 有         |
| LSA 覆盖攻击    | 否      | 是      | 无         |

当某种欺骗攻击引起反击机制时,尽管具体方式有所不同,但它们欺骗原理相似<sup>[9]</sup>,且实现的攻击均具有以下特性:

- (1)攻击者按序向路由器发送触发 LSA 和抗反击 LSA,且抗反击 LSA 与链路状态数据库中真实的 LSA 不同;
- (2)这两条报文的时间间隔在 1 ~ 5 s,并且攻击者都收到两个报文的 LSAck 包;
- (3)触发 LSA 引起了反击机制,然而由于抗反击

LSA 和反击 LSA 的校验和、序列号相同,且时间差在 15 min 以内,这两种报文先到的被保存,后到的被丢弃。

由此,将这六种路由欺骗攻击分为两大类:第一类为引起反击类攻击,第二类为不引起反击类攻击。

2.2 检测算法

对于引起反击和不引起反击的两类路由欺骗攻击,分别设计了相应的检测算法。

2.2.1 算法 I: 不引起反击类攻击的检测算法

邻接欺骗、远程邻接欺骗、单路径注入、LSA 覆盖等不会引起 OSPF 协议反击机制,根据它们的特性设计算法 I。

算法 I: 检测不引起反击类攻击的算法。

Input: 路由器的 OSPF 报文流

Output: OSPF 欺骗存在与否

```
1:for position←next_begin+1 to trace_num do //position 为
检测的当前报文位置
2:for index←position to window_size do//window_size 为滑
动窗口大小
3:if 此条报文是 router LSA do
4:if LSAs ∈ |LS Database| then
5:记录时间戳、链路号等参数
6:if 存在 LSAck 包 then
7:if 存在合法的反击 LSA then
8:break
9:else if 未告警 then
10:告警
11:end for
12:滑动窗口+1
13:end for
```

算法 I 先解析流中的每条路由器 LSA,记录下捕获报文的时间戳、报文所在网桥号、序列号等参数,与链路状态数据库的链路信息对比,判断其是否为恶意;若不是,跳出流程,反之,继续执行,判断其是否合法、是否引起反击机制。合法指该 LSA 通过了协议的过程化检查与约束,之后进程会回复一个 LSAck 报文。由反击机制特点可知:反击 LSA 的序列号比恶意 LSA 的序列号大 1,链路状态 ID 和恶意 LSA 的相同,链路状态信息和真实的链路状态数据库中的相同。据此判断恶意 LSA 是否引起反击机制。若出现,跳出流程,从下一条报文重新执行流程。反之,由于所有洪泛的恶意 LSA 之间的链路状态 ID 和序列号都相同,比较两次告警恶意 LSA 的链路状态 ID 和序列号可判断告警是否重复,找出最先发送恶意 LSA 报文的路由器或主机。

2.2.2 算法 II: 引起反击类攻击检测算法

目前引起反击类攻击仅有双 LSA 注入攻击和双 LSA 远程多注入攻击两种。根据特性设计算法 II。

算法 II: 检测引起反击类攻击的算法。

Input: 路由器的 OSPF 报文流

Output: OSPF 欺骗存在与否

```
1:for position←next_begin+1 to trace_num do
2:for index←position to window_size do
3:if 此条报文是 router LSA do //触发 LSA
4:保存时间戳、链路号等参数
5:if 存在 LSAck then
6:if 存在抗反击 LSA then
7:if 存在抗反击 LSA 的 LSAck then
8:if LSAs ∈ |LS Database| then
9:break
10:else if 未告警 then
11:告警
12:end for
13:滑动窗口+1
14:end for
```

与算法 I 相同的是解析路由器 LSA 时都会记录下捕获的时间戳、报文所在网桥号等参数。但是它们算法流程并不相同,后者将采集到的路由器 LSA 作为触发 LSA 执行算法流程,依次判断其是否合法、是否出现抗反击 LSA 以及抗反击 LSA 是否合法是否恶意、告警是否重复。

3 基于 NFV 的通用 OSPF 路由欺骗攻击的检测算法和防御机制 (ARSAO)

尽管两类路由欺骗攻击篡改某些路由器的路由表,但不会影响受害路由器的反击 LSA 到达所有路由器。所以检测到欺骗攻击后,向路由器发送一条序列号更大的 LSA,刻意引起它的反击机制,将使攻击失去效果。基于该原理,本节提出了 OSPF 路由欺骗攻击的防御机制,能够有效地防御大部分 OSPF 路由欺骗攻击。但邻接欺骗攻击和远程邻接欺骗攻击,因它们通过伪装成路由器,发送关于自身的虚假 LSA,即使再次引起反击机制,洪泛的依旧是虚假路由,所以不能通过激发协议的反击机制进行防御。这两种攻击需要通知管理员处置。

3.1 支撑 ARSAO 的系统结构

文中基于 NFV 提出了通用的系统架构,如图 1 所示,该架构主要分为采集层和分析层。

采集层主要包含若干中间盒,以及采集、通信和防御实施三大模块。采集模块功能主要包括:捕获流经路由器各端口的 OSPF 分组;过滤掉与欺骗攻击无关的 OSPF Hello 报文;解析协议报文。通信模块将解析完的报文发送给分析服务器以及接收分析服务器的防御指令。防御实施模块接收分析服务器的防御指令后,构造新的路由器 LSA 后发送给路由器。



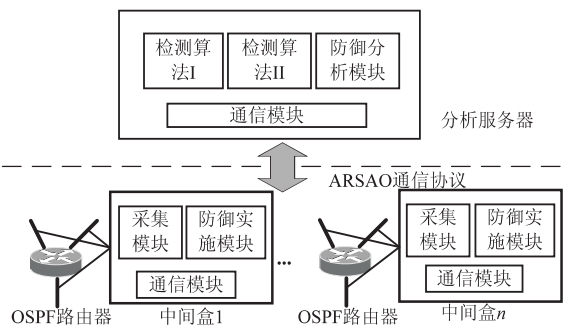


图 1 ARSAO 的系统架构

分析层包含一个分析服务器,由通信、防御分析两大模块组成。通信模块接收来自中间盒的协议报文和发送防御指令。防御分析模块将协议报文加上链路号和时间戳形成 trace 记录流;获取每条协议报文的核心参数;调用两类检测算法多线程检测 trace 记录流;检测到攻击后告警并构造防御指令。

考虑到开销、效率、实时性等因素,分析服务器和中间盒之间采用 UDP 协议进行通信。

3.2 中间盒设计

中间盒是指在 Linux 容器(LXC)中运行具有特定检测与防御功能的虚拟网络功能(VNF)。它通过网桥连接到路由器之间,用软件实现中间盒是文中的研究点之一。它的程序设计基于 socket 编程,利用了 libpcap、tcpdump、libnet 技术。中间盒各个模块的工作流程如图 2 所示。

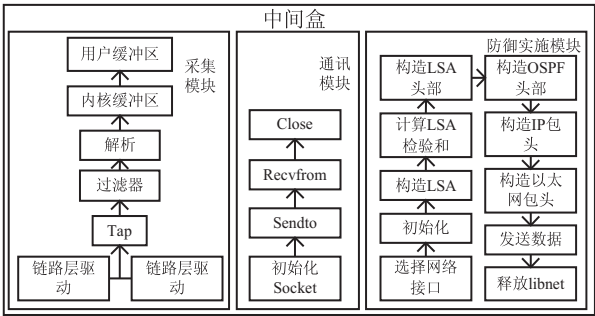


图 2 中间盒工作流程

通信模块在初始化阶段,打开一个 UDP socket,利用 send to 函数向分析服务器发送数据包,recvfrom 函数接收分析服务器的防御指令。

采集模块在监测接口的数据链路层增加一个旁路处理,基于 libpcap 利用原始套接字从链路层驱动程序中获取数据包的拷贝,通过 Tap 函数将数据包发送给 BSD Packet Filter (BPF) 过滤器。定义过滤规则对数据包进行逐一匹配,符合条件的使用 tcpdump 中的对应函数对报文进行解析,之后存放入内核缓冲区,并传递给用户缓冲区。

防御实施模块每当其接收到分析服务器的防御指令后,调用 libnet 函数库自底层向上层构造新的触发 LSA。

3.3 分析服务器设计

分析服务器是指在 LXC 中具有特定分析功能的 VNF,它通过一个网桥桥接所有的中间盒,确保及时地接收中间盒发送来的协议报文。它的工作过程如下:程序初始化阶段打开 UDP socket,监听端口,等待连接请求,利用 recvfrom 函数接收协议报文。接收报文后,对每条报文添加网桥 ID 和时间戳,存入接收缓冲区,利用正则表达式过滤读取参数,存入 trace 记录中,然后使用 pthread\_create 函数开启两个线程,分别调用两类检测算法对流检测,判断是否存在攻击。若存在,生成告警信息,存入日志文件,并且生成防御指令。最后利用 sendto 函数发送防御指令。

trace 记录的结构如图 3 所示。时间戳占 2 个字节,表示协议报文被捕获的时间;网桥 ID 占 2 个字节,标识报文所在的网桥;LSA 类型占 1 个字节,表示 LSA 类型,当 OSPF 分组类型不为 LSU 时,自动填充 0;链路数占 2 个字节,表示路由器接口活动的数量;链路 ID 占 4 个字节,表示路由器接口所连接的对象;链路数据占 4 个字节,为 IP 地址掩码或接口的 IP 地址。时间戳取自宿主服务器的时钟,解决各个路由器、中间盒时钟不同步问题,保证检测逻辑的正确性。



图 3 trace 记录结构

防御指令中包含:恶意 LSA 序列号、链路状态 ID、区域 ID、中间盒 IP 地址、目标路由器 IP 地址。这些参数用于中间盒构造 LSA。

4 原型系统实验与分析

4.1 实验环境

为了验证 ARSAO 系统的功能和性能,对该系统进行实验测试。实验设备和环境配置如下:宿主服务器为 ThinkServer RD550(内存 32 GB、Xeon(R) CPU4 核、x5647 @ 2.93 GHz);服务器的操作系统为 Ubuntu 16.04,以 LXC 作为虚拟机构建 NFV 网络作为测试原型系统的环境<sup>[21-22]</sup>。

原型系统的 NFV 网络如图 4 所示。该网络是由 17 台配置 OSPF 协议的路由器  $R_1-R_{17}$  组成,它分为 5 个区域  $Aera_0-Aera_4$ 。包含虚拟主机 6 台  $H_1-H_6$ 。网段的掩码皆为 255.255.255.0。此外原型系统设置了 5 个检测中间盒和 1 个分析服务器。

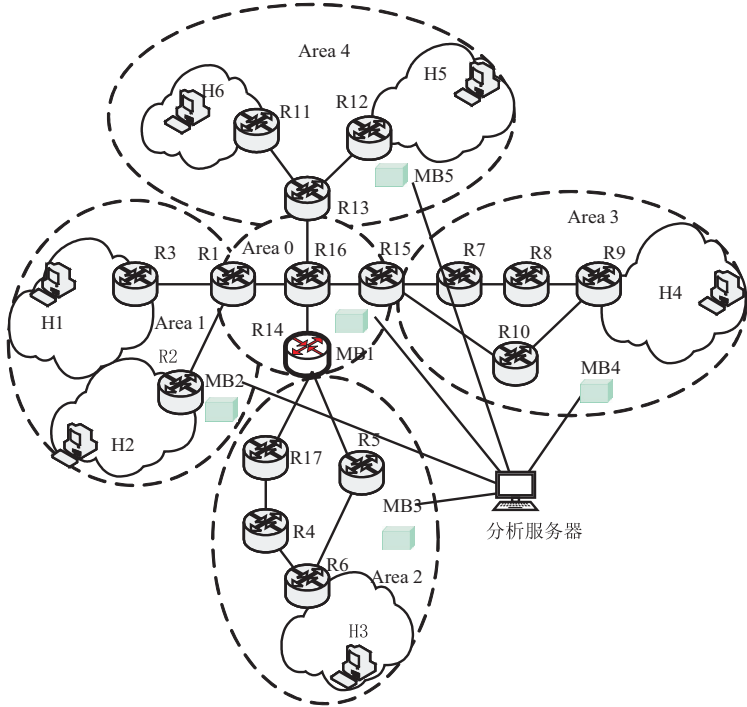


图 4 测试原型系统的 NFV 网络

4.2 系统的功能验证

由于双 LSA 远程多注入攻击与双 LSA 注入攻击类似以及邻接欺骗攻击与远程邻接欺骗攻击类似,实验选择对邻接欺骗攻击、双 LSA 注入攻击、LSA 攻击覆盖攻击、单路径注入攻击这四种路由欺骗攻击行为进行验证,测试系统的检测功能和防御功能。分别在  $Area_1$ 、 $Area_2$ 、 $Area_3$ 、 $Area_4$  依次进行这四种攻击(时间间隔 1 s)。

$Area_1$  内,攻击者  $H_2$  发送所构造的 Hello 报文,与

$R_2$  建立邻接关系,之后注入恶意的攻击报文。 $Area_2$  内,攻击者从  $R_{17}$  向  $R_{14}$  注入触发 LSA 和抗反击 LSA 报文; $Area_3$  内,攻击者从  $R_7$  向  $R_{15}$  发送覆盖攻击的 LSA 报文, $Area_4$  内,攻击者从  $R_{11}$  向  $R_{13}$  注入关于  $R_{12}$  的恶意 LSA 报文。攻击前,记录  $R_2$ 、 $R_{14}$ 、 $R_{15}$ 、 $R_{13}$  的路由表。攻击后,再次查看受害路由器的路由表,对比可得路由表项被篡改。表 2 为  $R_2$  被攻击后的路由表项列表,最后一行为多出的恶意的路由信息。

表 2 路由器  $R_2$  被攻击后的路由表项

| 目的地址            | 网关       | 开销 |
|-----------------|----------|----|
| 100.100.1.0(H1) | 20.2.1.3 | 30 |
| 100.100.2.0(H2) | *        | 0  |
| 100.100.3.0(H3) | 20.2.1.3 | 60 |
| 100.100.4.0(H4) | 20.2.1.3 | 60 |
| 100.100.5.0(H5) | 20.2.1.3 | 50 |
| 100.100.6.0(H6) | 20.2.1.3 | 50 |
| 144.144.144.0   | *        | 0  |

图 5 中的日志文件显示了 ARSAO 系统对攻击特征的报文进行了告警,并且准确找出了攻击源。检测到攻击的 5 s 后,再次查看受害路由器的路由表,大部分路由器的路由表已经恢复,未恢复的  $R_2$  则由管理员进行处置。

实验表明:ARSAO 系统能够检测出这两大类路由



图 5 日志文件

欺骗攻击、准确找到攻击源、防御其中的大部分攻击。  
(邻接欺骗攻击、远程邻接欺骗攻击除外)

4.3 系统的性能验证与分析

为了测试系统的性能,选择双 LSA 注入攻击和单路径攻击进行实验,选取检测时间、防御时间、误报率和漏报率作为指标。公式如下:

$$t_{\text{检测时间}} = t_{\text{检测到攻击的时刻}} - t_{\text{攻击的时刻}} \tag{1}$$

$$t_{\text{防御时间}} = t_{\text{检测到构造的触发 LSA 报文时刻}} - t_{\text{检测到攻击的时刻}} \tag{2}$$

$$p_{\text{误报率}} = n_{\text{误报}} / n_{\text{攻击}} \tag{3}$$

$$p_{\text{漏报率}} = n_{\text{漏报}} / n_{\text{攻击}} \tag{4}$$

为了更好地模拟真实的网络环境,利用流量发生软件 Iperf 设置背景流量,流量控制软件 Netem 设置丢包率和时延。在不同的丢包率和时延下,在 Area<sub>1</sub>、Area<sub>2</sub>、Area<sub>3</sub>、Area<sub>4</sub>内分别间隔 1 s 进行双 LSA 注入攻击和单路径注入攻击。一共进行 10 轮实验,每轮一类欺骗攻击 100 次,检测时间、防御时间是 1 000 次实验的平均值,误报率和漏报率为 10 轮实验的平均值。实验结果见图 6 ~ 图 9。

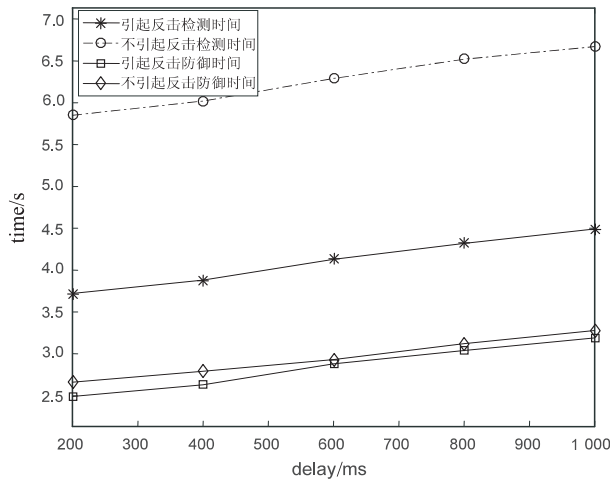


图 6 时延对检测时间和防御时间的影响

由图 6 可知,两类攻击的检测需都要一定的时间。200 ms 时延下,引起反击类的检测时间与防御时间分别为 3.72 s 和 2.49 s,不引起反击类的检测时间与防御时间分别为 5.85 s 和 2.66 s。不引起反击类攻击的检测时间明显大于引起反击类攻击的检测时间,防御时间两类攻击相差不多,两类攻击的检测时间和防御时间随着网络时延基本呈线性增加。

图 7 显示的是丢包率对检测时间和防御时间的影响。这两类攻击的检测时间与防御时间随着丢包率的增大有一定的波动,但并没有明显影响。

图 8 给出了不同时延下两类攻击的漏报率和误报率。从图 8 可知,当时延较小时,时延的增加不会使系统产生误报,而当时延高于一定的值  $\alpha$  (1 ~ 1.5 s) 时,系统开始出现漏报,且漏报率随着时延的增大逐渐增大。

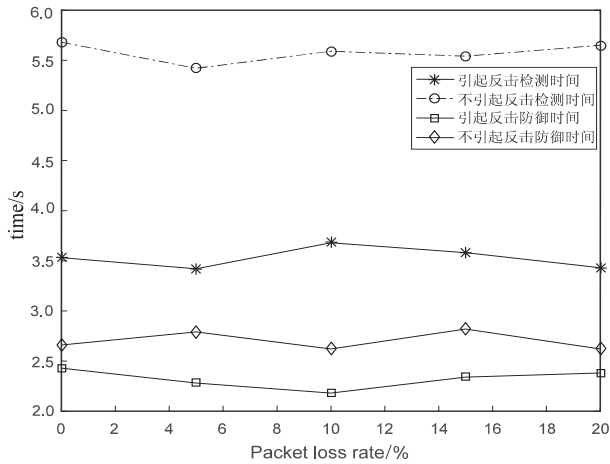


图 7 丢包率对检测时间和防御时间的影响

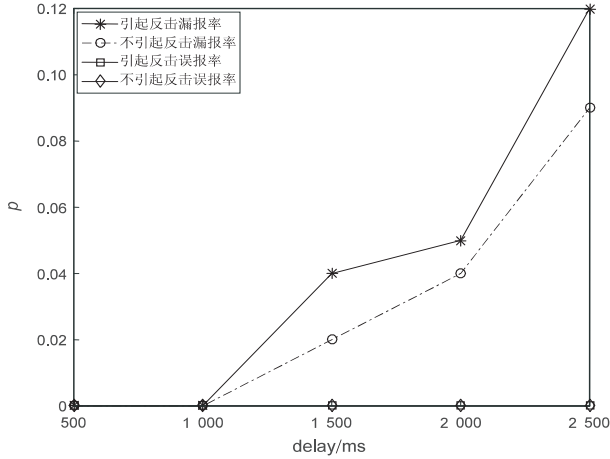


图 8 时延对漏报率和误报率的影响

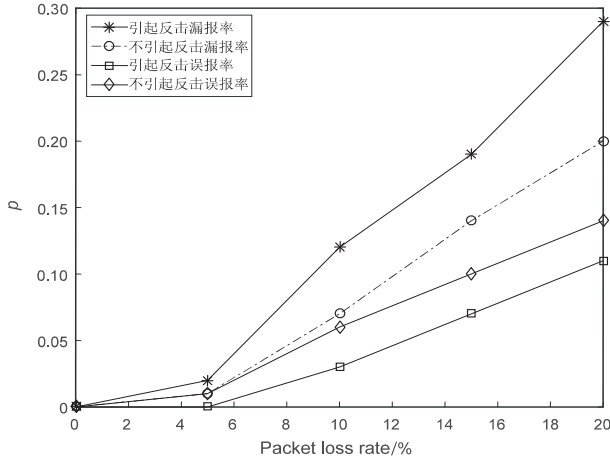


图 9 丢包对漏报率和误报率的影响

图 9 给出了不同丢包率下两类攻击的漏报率和误报率,两者皆随着丢包率的增加急剧升高。一旦网络出现丢包,网络出现的情况有很多,可能是因出现恶意 LSA 的确认报文丢失导致系统出现攻击的漏报;也有可能引起反击类攻击的反击 LSA 报文丢失,导致系统将把这类攻击误判成另一类攻击。同一丢包率下,引起自反击类攻击的误判率低于另一类,漏判率高于另一类。因为反击类攻击检测算法步骤较多,其中任何一个步骤的报文不正确,都会导致漏判,所有步骤都满

足,才会误判。

上述实验结果表明,网络时延和丢包对 ARSAO 系统的性能产生了一定的影响,但在非极端的网络时延和丢包的情况下,该系统能够用统一的通用设施快速有效地检测出各种 OSPF 欺骗攻击并能够进行及时防御,检测具有低误报率和低漏报率,提升了 NFV 网络的安全性和健壮性。由于采用通用基础设施,系统也具有经济性。

## 5 结束语

目前对于出现的多种 OSPF 路由欺骗攻击仍缺乏有效的检测和防御方法。文中在深入研究 OSPF 路由欺骗攻击的基础上,将它们分为两类,提出了两类 OSPF 路由欺骗攻击的 ARSAO 机制。基于 NFV 技术,提出并实现了一种通用的支持检测与防御的系统。原型系统实验表明,ARSAO 具有经济性、灵活、易于部署等特点,能够准确快速地检测出除邻接欺骗攻击和远程邻接欺骗攻击外的 OSPF 的路由欺骗攻击,并能迅速地进行故障恢复达到防御的效果,提高 NFV 网络的安全性。下一步,将该研究扩展到检测与防御其他类型网络攻击的工作中。

### 参考文献:

- [1] GUPTA M, MELAM N. Authentication/confidentiality for OSPFv3[S]. [s. l.]:[s. n.],2006.
- [2] MOY J. OSPF version 2[S]. Fremont,CA:IETF,1998.
- [3] JOU Y F, GONG F, SARGOR C, et al. Design and implementation of a scalable intrusion detection system for the protection of network infrastructure[C]//Proceedings of the DARPA information survivability conference and exposition. Los Alamitos,CA;IEEE,2000:69-83.
- [4] JONES E, MOIGNE O L. OSPF security vulnerabilities analysis[EB/OL]. 2006-06-16. <https://tools.ietf.org/html/draft-ietf-rpsec-ospf-vuln-02.txt>.
- [5] BOUILLARD A, JARD C, JUNIER A. Some synchronization issues in OSPF routing[C]//International conference on data communication networking. Reykjavik, Iceland;IEEE,2013:1-10.
- [6] CARIA M, JUKAN A. Link capacity planning for fault tolerant operation in hybrid SDN/OSPF networks[C]//IEEE global communications conference. Washington, DC, USA;IEEE,2016:1-6.
- [7] NAKIBLY G, SOSNOVICH A, MENAHEM E, et al. OSPF vulnerability to persistent poisoning attacks: a systematic analysis[C]//30th annual computer security applications conference. New Orleans, Louisiana, USA;ACM,2014:336-345.
- [8] SONG Y, GAO S, HU A, et al. Novel attacks in OSPF networks to poison routing table[C]//International conference on communications. Paris, France;IEEE,2017:1-6.
- [9] NAKIBLY G, KIRSHON A, GONIKMAN D, et al. Owing the routing table - new OSPF attacks[C]//Proceedings of Black Hat. USA;Black Hat,2011.
- [10] NAKIBLY G, KIRSHON A, GONIKMAN D, et al. Persistent OSPF attacks[C]//Proceedings of the 19th annual symposium on network and distributed system security. San Diego, USA;the Internet Society,2012.
- [11] 夏云峰. 基于 OSPF 路由协议的路由欺骗分析[D]. 南京:东南大学,2014.
- [12] ANU G P, VIMALA S. Optimization of OSPF LSA flooding process using clustering technique[C]//10th international conference on intelligent systems and control. Coimbatore, India;IEEE,2016:1-5.
- [13] COHEN R, HESS-GREEN R, NAKIBLY G. Small lies lots of damage: a partition attack on link-state routing protocols[C]//IEEE conference on communications and network security. Florence, Italy;IEEE,2015:397-405.
- [14] DANIEL S. Using protocol redundancy to enhance OSPF network system survivability[C]//Proceedings of Southeast-Con. St. Petersburg, USA;IEEE,2018:1-7.
- [15] NIARI S T, JAHANGIR A H. Verification of OSPF vulnerabilities by colored petri net[C]//Proceedings of 6th international conference on security of information and networks. Aksaray, Turkey;ACM,2013:102-109.
- [16] KASEMSUWAN P, VISOOTTIVISETH V. OSV: OSPF vulnerability checking tool[C]//14th international joint conference on computer science and software engineering. Nakhon Si Thammarat;IEEE,2017:1-6.
- [17] WANG Minghao. The security analysis and attacks detection of ospf routing protocol[C]//7th international conference on intelligent computation technology and automation. Changsha, China;IEEE,2015:836-839.
- [18] 覃遵颖, 李国栋, 李卫, 等. OSPF 协议脆弱性分析与检测系统的设计和实现[J]. 通信学报, 2013, 34(z2):58-63.
- [19] 徐壮壮. 基于可信路由器的 OSPF 攻击和异常检测系统[D]. 北京:北京工业大学,2014.
- [20] MIJUMBI R, SERRAT J, GORRICHIO J L, et al. Network function virtualization: state-of-the-art and research challenges[J]. IEEE Communications Surveys & Tutorials, 2017, 18(1):236-262.
- [21] MICHALSKI M, CIESLAK K, POLAK M. The system for large networks emulation with OSPF/BGP routers based on LXC[C]//16th international conference on high performance switching and routing. Budapest, Hungary;IEEE,2015:1-4.
- [22] BERNSTEIN D. Containers and cloud: from LXC to Docker to Kubernetes[J]. IEEE Cloud Computing, 2015, 1(3):81-84.