一种基于 NFV 的检测 OSPF 双 LSA 攻击的方法

李鹏飞 陈 鸣 邓 理 钱红燕
(南京航空航天大学计算机科学与技术学院 南京 211106)

摘 要 OSPF 协议是因特网中使用最广泛和最成功的内部网关路由协议之一。尽管当前对 OSPF 协议的安全性已有许多研究,但仍缺乏有效的检测路由欺骗攻击的方法,难以保证网络中 OSPF 路由的安全性。通过研究 OSPF 双链路状态通告(LSA)攻击方法的原理,给出了用于确定攻击者的 3 个必要条件,提出了一种检测 OSPF 双 LSA 攻击的方法。基于网络功能虚拟化(NFV)技术,设计实现了检测中间盒与分析服务器用于检测攻击与消除路由污染。检测中间盒负责从各链路捕获相关 OSPF 分组,将 trace 记录发送给分析服务器;分析服务器调用检测算法分析处理接收到的 trace 记录流,若检测到攻击则告警,同时指令检测中间盒来恢复污染路由。原型系统的实验结果表明,所提方法能够在 IP 网络或 NFV 网络中准确高效地检测出 OSPF 双 LSA 攻击,并且实现的系统具有性价比高、易于部署等优良特点。

关键词 OSPF,路由协议攻击,网络安全,网络功能虚拟化,检测方法
中图法分类号 TP393 **文献标识码** A

NFV Based Detection Method Against Double LSAs Attack on OSPF Protocol

LI Peng-fei CHEN Ming DENG Li QIAN Hong-yan
(Department of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China)

Abstract The OSPF protocol is one of the most widely used and successful interior gateway routing protocols in the Internet. Although there have been lots of investigations on the security of the OSPF protocol, there is still a lack of effective detection methods against the route spoofing attacks, so it is difficult to ensure the security of the OSPF routing in networks. By studying the principle of the double link state advertisements (LSAs) attack on the OSPF protocol, this paper presented three necessary conditions that are used to detect the attack, and proposed a detection method against the double LSAs attack on the OSPF protocol. Then, a corresponding detection middle box and analysis server used to detect attacks and clear up their routing pollution were designed and implemented based on the network function virtualization (NFV) technology. The detection middle box is responsible for capturing relevant OSPF packets from various links, sending the trace records to the analysis server, and receiving instructions from the analysis server to restore the polluted routes. The analysis server invokes the detection algorithm to analyze and process the trace record stream, and an alarm is given and an instruction is sent to the detection middle box to restore the contaminated routes if an attack is detected. The experimental results of the prototype show that the proposed method can detect the OSPF double LSAs attack in both IP networks or NFV networks accurately and efficiently, and the prototype has excellent characteristics such as high cost performance and easy to deploy.

Keywords OSPF, Routing protocol attack, Network security, Network function virtualization, Detection method

1 引言

随着互联网的快速发展,社会进入大数据时代,这对网络安全提出了巨大挑战。路由协议安全是网络安全的重要组成部分[1],路由选择协议是路由器决定分组传输路径的关键协议。一旦数据分组传输路径上的某台路由器的路由信息出错,网络中的分组就无法传输到正确的目的地,严重影响了数据分组的正常传输。

开放式最短路径优先(Open Shortest Path First, OSPF)路由协议[2-4]是一个广泛使用的内部网关协议。然而,OSPF 协议也存在安全漏洞,攻击者容易利用协议的缺陷对其进行攻击,并且不易被人发现。目前,对于 OSPF 协议有多种攻击方法[5-9],双 LSA 攻击这种路由欺骗攻击是其中较为新颖和典型的[5]。针对这一重要的安全威胁,本文提出了一种检测 OSPF 典型路由欺骗攻击的方法,设计实现了一种经济有效的检测技术,提升了网络路由协议的安全性。

本文第 2 节概述了相关工作;第 3 节分析了 OSPF 双 LSA 攻击的特点和必要条件;第 4 节提出了一种检测这种攻

本文受国家自然科学基金项目(61772271,61379149)资助。

李鹏飞(1993-),男,硕士,主要研究方向为 NFV、计算机网络,E-mail:lipfeinj@163.com;**陈 鸣**(1957-),博士,教授,CCF 高级会员,主要研究领域为计算机网络、无人机网络、网络测量、未来网络,E-mail:mingchen@nuaa.edu.cn(通信作者);**邓 理**(1996-),男,硕士,主要研究方向为 NFV、计算机网络;**钱红燕**(1973-),女,博士,副教授,CCF 会员,主要研究方向为计算机网络、信息安全。

击的方法，并基于 NFV 设计实现了攻击检测；第 5 节在 NFV 环境下对原型系统进行了验证；最后总结全文。

2 相关工作

2.1 安全机制以及攻击技术

OSPF 协议具有较为完善的安全机制[2-3]，包括协议包认证、过程化检查和约束、洪泛机制、自反击机制等。其中，自反击机制是指，当路由器收到一个自己的 LSA 实例时对其进行判断，若该 LSA 实例与其当前数据库的内容不一致，它将立即通告一个包含正确链路状态的新实例。自反击机制和泛洪的结合确保了每当路由器发现恶意 LSA 时，就会立刻被更新的 LSA 所覆盖，使攻击者难以篡改其他路由器中的链路状态数据库和路由表。

在 OSPF 网络中，建立了邻接关系的路由器之间发生的攻击为内部攻击[5-9]，其主要分为两类：路由欺骗攻击和消耗路由器资源攻击。消耗路由器资源攻击主要有最大年龄攻击和序列号增加攻击，会大量消耗路由器的资源，造成拒绝服务。路由欺骗攻击主要有双 LSA 攻击、邻接欺骗攻击、单路径注入攻击、远程虚假链接等[8-9]。双 LSA 攻击是指攻击者利用 OSPF 协议判断 LSA 新旧规则的漏洞，篡改链路状态数据库中的真实 LSA，从而达到路由欺骗、中间人攻击等效果，对网络的危害很大。远程虚假链接是指攻击者远程与网络中的路由器建立虚假的邻接关系，然后再注入虚假的路由造成流量黑洞等危害。

2.2 检测方法

目前，对于 OSPF 攻击的检测技术仅限于检测消耗资源类攻击。对于 OSPF 路由欺骗的检测方法几乎没有，并且对检测到的 OSPF 攻击进行恢复的方法的研究也较少。文献[10]设计一种工具来检查 OSPF 口令强度并执行多种测试。此方法从加强密钥认证的强度出发，虽然能增大外部攻击的难度，但是不能防御 OSPF 的内部攻击。文献[11]提出了基于软件包分析的攻击检测系统，其获取网络路由器的 OSPF 路由协议报文，当检测到伪造异常的 OSPF 报文时，就产生告警信息。本文提供了检测攻击的基本思路，但文献没有具体提出如何检测攻击，并且不能检测路由欺骗攻击。

2.3 网络功能虚拟化技术

网络功能虚拟化(Network Functions Virtualization，NFV)[12]是一种基于虚拟化技术，利用软件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，可降低对专用硬件的依赖，减少网络设备的成本，加快网络新业务的部署以及网络的创新。本文利用 NFV 技术，在宿主服务器上基于轻量级 Linux 容器(LXC)[13-14]构建一个使用 OSPF 协议的网络，并且该网络也能够与实体 OSPF 路由器互联互通。

3 OSPF 双 LSA 攻击分析

为了检测 OSPF 路由欺骗，首先分析双 LSA 攻击的工作原理。

3.1 攻击原理

OSPF 协议根据 LSA 的序列号、时限、校验和来判断 LSA 的新旧。若当两个 LSA 的序列号、校验和相同，且其 LS 时限差小于 15 min 时，系统就认为两者相同。由此，Nakibly 等提出了一种 OSPF 双 LSA 攻击方法来篡改特定路由器的路由[5]。

图 1 所示为一次典型 OSPF 双 LSA 攻击过程，攻击者(可以是路由器或运行 OSPF 协议的主机)通过先后发送触发 LSA 报文和抗反击 LSA 报文，来篡改区域内其他路由器链路状态数据库中关于路由器 R_4 的信息，其中 R_4 为受害路由器。

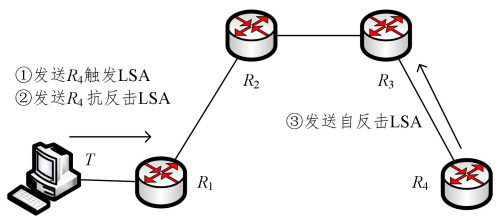


图 1 双 LSA 攻击过程

由于系统认为抗反击 LSA 和自反击 LSA 相同，因此先到的 LSA 会被保存，后到的 LSA 会被丢弃，故对触发 LSA 和抗反击 LSA 的发送间隔有要求。LSA 最短达到时间是指协议进程接收 LSA 新实例之间的时间间隔，系统默认为 1 s。LSA 最短生成时间是指协议进程构造一个新 LSA，并将其发送出去的最小间隔，系统默认为 5 s。因此在忽略 OSPF 的更新以及洪泛时间的情况下，触发 LSA 和抗反击 LSA 的发送间隔为 1～5 s，且间隔时间越接近 1 s，被污染的区域就越大。

3.2 时序分析

图 2 显示了图 1 攻击过程的时序关系。简明起见，图 2 忽略了路由器中更新的 LSA 数据分组。

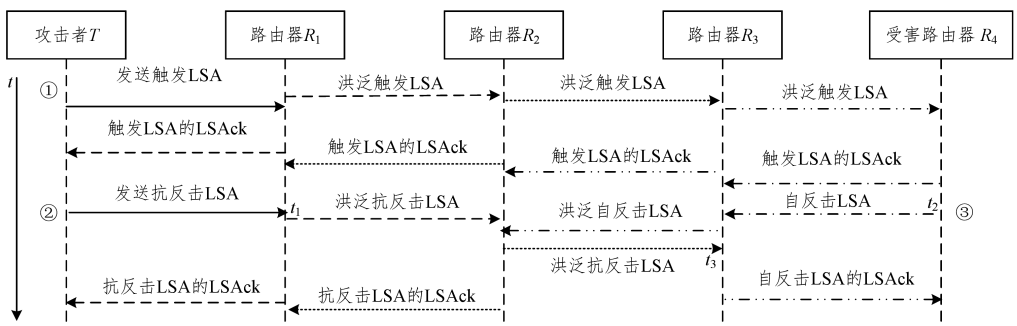


图 2 双 LSA 攻击时序图

下面分几个阶段进行讨论。

1)攻击者 T 向 R_1 发送受害路由器 R_4 的触发 LSA。其序列号比 R_4 链路状态数据库中对应的序列号大，R_1 接收后洪泛该 LSA。OSPF 协议检验该 LSA 合法之后，各个路由器

分别回复 LSAck 包。

2）攻击者在 t_1 时刻向 R_1 发送抗反击 LSA，其序列号比触发报文大 1。它的 R_2 接收后洪泛抗反击 LSA。t_3 时刻，R_3 收到该抗反击 LSA。然而，由于 R_3 在先于 t_3 的 t_2 时刻收到了自反击 LSA，因此它会将该抗反击 LSA 丢弃。因此，除了 R_3，其他路由器分别回复 LSAck 包。

3）R_4 收到触发 LSA 后，在 t_2 时刻引发自反击。R_3 收到自反击 LSA 后，将它洪泛给 R_2 并回复 R_4 一个自反击 LSA 的 LSAck 包。但由于 R_2 链路状态数据库已经存放抗反击 LSA，因此丢弃自反击 LSA。

实际网络中，可能网络拓扑不同，导致路由污染情形不同，但是图 2 中这些报文出现的因果关系类似。仅当攻击者发送触发 LSA 和抗反击 LSA 后，后继路由器才会向其他链路转发该双 LSA 攻击报文，因此如果能够检测到所有这些报文对，其中与最先出现这种报文对的链路相连的主机或路由器就是攻击者。因此，确定网络中某台路由器或主机是 OSPF 双 LSA 攻击者 T 的 3 个必要条件是：

1）按序发送合法的触发 LSA 与抗反击 LSA；

2）这两条报文产生的时间间隔为 1～5 s；

3）这两条报文的产生时间为全网中最早的。

4　OSPF 双 LSA 攻击的检测机制与系统

3.2 节得到了确定双 LSA 注入攻击者的必要条件。本节提出了一种基于 NFV 的检测机制和相应的系统实现方案：在所有可能产生攻击 OSPF 行为的地方安装检测中间盒来收集 OSPF 报文信息，将收集到的相关信息送交给特定的分析服务器，分析处理 OSPF 报文踪迹，确定攻击者并通知检测中间盒恢复攻击的不良影响。

4.1　基于 NFV 的检测系统

若每台路由器都具有收集和分析 OSPF 报文的功能，则必须重新设计实现路由器，代价太高。因此，考虑在 NFV 与 IP 技术混合的网络环境下或在 NFV 网络环境下，设置专用中间盒设备来收集和处理相关信息。

图 3 给出了系统运行场景，其中的所有路由器都是虚拟的，设置如图 3 所示的检测中间盒 MB_1 — MB_3，它由在如 LXC 这样的虚拟机中运行特定的虚拟网络功能（VNF）程序构成，用于收集 OSPF 双 LSA 攻击信息，并发送给分析服务器，该中间盒也可用于真实路由器。只要这些虚拟机的相关端口映射到宿主服务器的某个外接端口（如以太网接口）上，并且通过二层交换机与实际路由器的特定端口相连，就能够获得所需的相关报文。

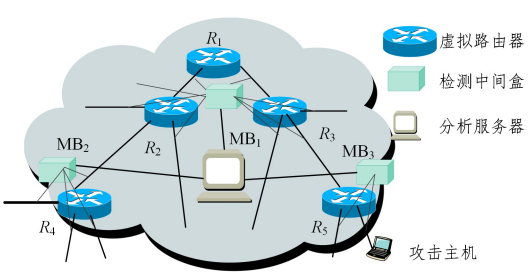
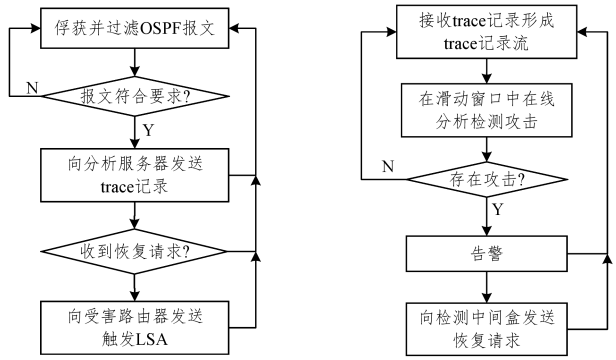


图 3　一种基于 NFV 的检测系统场景



（a）检测中间盒工作流程　　（b）分析服务器工作流程

图 4　OSPF 攻击检测系统两部件的工作流程

该系统由检测中间盒和分析服务器两个主要部件构成。图 4 分别给出了该检测系统两个部件的工作流程图。

4.2　检测中间盒的设计

检测中间盒由运行在 LXC 中、具有特定收集功能的 VNF 构成。该 VNF 的主要工作过程包括：基于 libpcap 在被监测端口的数据链路层增加一个旁路接口，当 Linux 内核通过驱动程序直接从网卡获取数据时，libpcap 将通过创建 AF_PACKET 类型的 Socket 获得分组拷贝；然后定义 BSD Packet Filter（BPF）规则来获得所需类型的分组，对收集的报文进行过滤；再将符合条件的分组传递给上层的程序。

由于各个中间盒的 libpcap 函数接口返回的是分组的字节数组，无法得知 OSPF 报文及其相互关系，需要将其送到分析服务器进行处理。

VNF 的通信模块负责将相关报文发送给分析服务器。在初始化阶段，该模块打开一个 UDP socket，用于发送 OPSF 分组和接收来自分析服务器的指令，一旦接收到指令，构造一个特定的 OSPF 触发 LSA 报文并将其发送给受害路由器，以快速恢复被污染的路由。

4.3　分析服务器的设计

分析服务器同样是由运行在 LXC 中具有特定分析功能的 VNF 构成。该 VNF 主要具有两个功能：1）从指定端口接收从检测中间盒发送的 trace 记录；2）利用分析检测算法分析由 trace 记录构成的流，若检测到攻击则发出告警，并设法恢复相关路由器中被污染的路由信息。

每条 trace 流主要包括下列字段：时间戳、链路 ID、IP 目的地址、IP 源地址、OSPF 分组类型、路由器 ID、区域号、LSU 的序列号、链路状态（Link State）ID 等。时间戳取自分析服务器的时钟，用于解决各个路由器、中间盒时钟不同步的问题，以保证检测逻辑的正确性。

算法 1 给出了分析服务器检测 OSPF 双 LSA 攻击的算法。该算法的核心就是按照 3.2 节提出的 3 个必要条件进行判断。

算法 1　分析服务器检测算法

输入：trace 记录流

输出：系统安全情况

1. next_begin←0 //检测起始参数

2. for p←next_begin+1 to trace_num do;//p 为当前检测的位置

3.　rec_a←0，rec_c←0 //判断告警是否重复，初始值设为 0

```
4.  for index←p to trace_mxnum do;//滑动窗口大小为:trace_mxnum
5.    if ospf_type∈{router LSA} then
6.      记录序列号 a、时间戳 b、lsid c 、链路号 d、源地址 e、lsa 位置 y←index
7.      if ∃t∈(b,b+2) 链路 d 上出现序列号为 a、lsid 为 c、目的地址为 e 的 LSAck then
8.  if ∃t∈(b+1,b+5) 链路 d 上出现 router LSA then
9.        记录序列号 e、时间戳 f、lsid g、源地址 h
10.       if g=c&&e=a+1&&e=h then
11.         if ∃t∈(f,f+2)链路 d 上出现序列号为 e、lsid 为 g、目的地址为 h 的 LSAck then
12.           if rec_a=0&rec_b=0 then//与初始值比较
13.             告警,rec_a←a,rec_b←b,next_begin←y,break
14.           else if a≠rec_a||b≠rec_b then
15.             告警,rec_a←a,rec_b←b,next_begin←y,break
16. end for
17. trace_mxnum←trace_mxnum+next_begin;//保证滑动窗口大小固定
18. end for
```

该算法设计了一种滑动窗口机制来在线分析 trace 记录流,窗口包括了具有报文数量约束的报文序列,以便检测分析报文是否合法等。检测到触发 LSA 后,该窗口的后沿停留在该报文处不动,而其前沿就会根据需要向前移动,以包含后继的报文;直至窗口中的分析得到结论,释放窗口中的报文信息,窗口向前滑动。

4.4 攻击恢复方法

一旦分析服务器检测到 OSPF 双 LSA 攻击,就能通过分析抗反击 LSA 得知受害路由器信息。由于攻击不会影响分析服务器与检测中间盒子之间的链路,因此指令能够达到检测中间盒。同理,中间盒发送的新的触发 LSA 能够到达受害路由器。由于攻击不会影响受害路由器的路由表,只会篡改其他路由器路由表中关于受害路由器的信息,因此在攻击后,受害路由器的自反击报文能够到达所有路由器。分析服务器根据网络拓扑决定由某个检测中间盒发送一个有关受害路由器的触发 LSA,让其序列号大于抗反击 LSA 的序列号,必定再次引发受害路由器的自反击机制,让检测的攻击失效。

5 实验及其分析

5.1 实验环境搭建

NFV 技术的特点是在保证网络高逼真的同时,大大降低实验硬件成本。实验中的元件均为虚拟的,只需一台服务器来承载 LXC,iperf 等开源软件,将 LXC 运行 quagga、NETEAM 等配置成虚拟路由器或虚拟主机,保证了此方法的经济性。搭建的原型系统如下:宿主服务器 ThinkServer RD550(内存 8GB,CPU 4 核)上构建一个 NFV 网络[15],虚拟路由器配置 OSPF 路由协议[16]。图 5 给出了用于实验的 NFV 网络,其包含:10 台 OSPF 路由器 r_1 — r_{10};3 个区域 Aera0、Aera1 和 Aera2;5 台虚拟主机 h_1 — h_5。

设置两个虚拟检测中间盒和一个虚拟分析服务器。中间盒 1、2 分别收集 r_4 左边、右边所有的链路上的数据包,过滤出 OSPF 分组;逐个添加链路 ID 字段;利用 UDP 协议发送到分析服务器的 8888 号端口;接收服务器指令后进行相应的故障恢复。分析服务器与 r_9、中间盒 1、2 直连,负责接收 trace 记录,加上时间戳形成 trace 流;调用检测算法对 trace 流进行实时检测,告警后给检测中间盒发送指令以恢复污染路由。

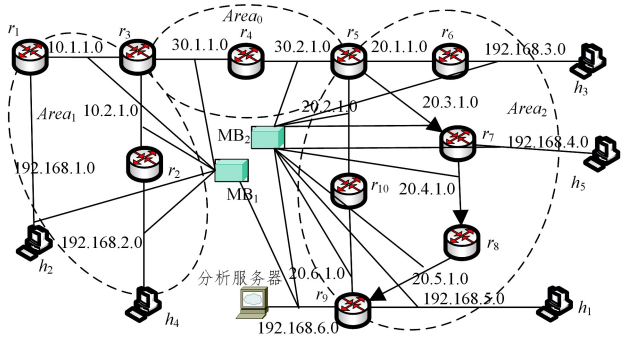


图 5 实验用的 NFV 网络

5.2 实验过程

5.2.1 攻击和告警

为了验证检测系统的有效性,实验设置密集的攻击,每隔 1 s 发起一次攻击,一共 4 次。将攻击 1 中发送触发 LSA 的时间设为 0。攻击 1:运行在 r_7 上的攻击程序在时刻 0 s 向 r_5 注入关于 r_{10} 的触发 LSA,在时刻 2 s 注入抗反击 LSA;攻击 2:运行在 r_2 上的攻击程序在时刻 1 s 向 r_3 注入关于 r_1 的触发 LSA,在时刻 3 s 注入抗反击 LSA;攻击 3:运行在 r_5 上的攻击程序在时刻 2 s 向 r_7 注入关于 r_6 的触发 LSA,在时刻 4 s 注入抗反击 LSA;攻击 4:运行在 r_8 上的攻击程序在时刻 3 s 向 r_9 注入关于 r_{10} 的触发 LSA,在时刻 5 s 注入抗反击 LSA。表 1 和表 2 分别列出了 r_3 在受到路由欺骗前和后路由表表项的主要参数。其他路由器受到路由欺骗后,其路由表也发生了变化,文中没有一一列举。

表 1 路由器 r_3 被攻击前的路由表项

目的地址	网关	Metric
192.168.1.0	10.1.1.1	20
192.168.2.0	10.2.1.2	20
192.168.3.0	30.1.1.4	40
192.168.4.0	30.1.1.4	40
192.168.5.0	30.1.1.4	50

表 2 路由器 r_3 被攻击后的路由表项

目的地址	网关	Metric
192.168.2.0	10.2.1.2	20
192.168.3.0	30.1.1.4	40
192.168.4.0	10.1.1.1	20
192.168.5.0	30.1.1.4	50

由表 1 可知:r_3 未受攻击时,去往 192.168.4.0 的流量都会转发到 r_4 的 30.1.1.4 端口,并且存在去往 192.168.1.0 网段的路径。由表 2 可知:受攻击后,r_3 中去往 192.168.4.0 的流量转发给 r_1,但由于 r_1 在物理上不与该网段相连,r_1 接收后会将数据包丢弃,导致了流量黑洞。而且路由表中不含 192.168.1.0 的表项,攻击也造成其他主机无法与 h_2 通信。

图 6 给出了分析服务器过滤出的攻击 2 的 trace 记录。记录 1 是触发 LSA,根据 LS ID、序列号、目的地址可以判断记录 2 是其 LSAck 包。根据序列号等字段判定记录 3 的是抗反击 LSA;记录 4 为其 LSAck 包。可判断 trace 记录中的报文满足必要条件 1。比较记录 1 和 3 的时间戳,判断满足

必要条件 2。由于算法中重复的告警会忽略，因此 trace 记录也满足必要条件 3。据此，能够及时准确地告警：链路 lbr2 上存在双 LSA 攻击，攻击源为 r_2。

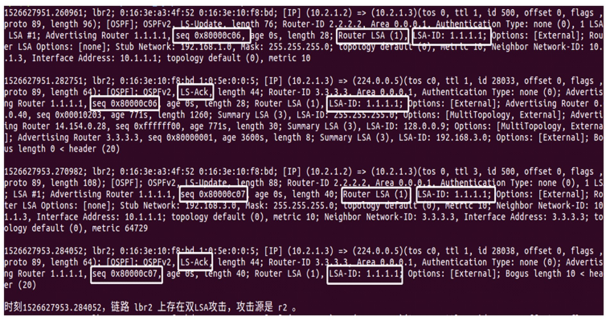


图 6　trace 记录流中的攻击

5.2.2　恢复污染路由

系统设计分析服务器检测到攻击后，它以接收到抗反击 LSA 的时间戳为标准，推迟 5 s 启动检测中间盒，发送新的触发 LSA。实验中，分析服务器检测到攻击 1 并告警后，它在时刻 7s 发送指令启动检测中间盒 1，由检测中间盒 1 立即向路由器 r_{10} 发送新的触发 LSA。当分析服务器检测到攻击 2 并告警后，它在时刻 8 s 发送指令启动检测中间盒 2，由检测中间盒 2 立即向路由器 r_1 发送新的触发 LSA。同理，所有的污染路由都可以得到恢复。

在攻击结束的一段时间后，再检查路由器 r_3、r_5、r_7、r_9 路由表，被污染的表项已经得到了恢复。上述实验结果表明：

1）本文提出的检测方法不仅可以准确地判断出 OSPF 双 LSA 攻击的存在，而且能够确定攻击者的位置；

2）本文提出的基于 NFV 的检测系统能够实时在线地工作，它不仅能够经济有效地检测 OSPF 双 LSA 攻击，而且能够及时恢复被攻击污染的路由。

结束语　本文基于 NFV 技术，提出了一种经济高效的检测防护 OSPF 双 LSA 攻击的方法，并研发了相应的原型系统。通过检测中间盒，从 OSPF 路由器端口检测关键 OSPF 报文序列，并将 trace 记录汇集到分析服务器处。通过分析服务器对 trace 记录流进行分析处理，完成了该攻击的鉴别、告警和恢复等操作。原型系统实验结果表明了本文方法及其系统的可行性和可用性。下一步，我们将研究把本文的基本方法用于检测与防护其他网络攻击的工作中。

参 考 文 献

[1] JIN L, XIE L. Internet network security [J]. Computer Engineering And Design, 2003, 24(2): 19-22.

[2] MOY J. OSPF version 2. RFC 2328 [S]. Fremont, CA: IETF, 1998.

[3] MOY J T. OSPF: Anatomy of an Internet routing protocol[J]. IEEE Network, 1998, 12(6): 4.

[4] JAYAKUMAR M, REKHA N R S, BHARATHI B. A comparative study on RIP and OSPF protocols[C]// Proceedings of International Conference on Innovations in Information, Embedded and Communication Systems. NJ: IEEE, 2015: 1-5.

[5] NAKIBLY G, KIRSHON A, GONIKMAN D, et al. Persistent OSPF attacks [C]// Proceedings of the 19th Annual Network and Distributed System Security Symposium. San Diego: Internet Society, 2012.

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

[7] NAKIBLY G, KIRSHON A, GONIKMAN D, et al. Owning the Routing Table-New OSPF Attacks[C]// Proceedings of Black Hat . USA: Black Hat, 2011.

[8] 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.

[9] SONG Y, GAO S, HU A, et al. Novel attacks in OSPF networks to poison routing table[C]// ICC 2017-2017 IEEE International Conference on Communications. IEEE, 2017: 1-6.

[10] KASAMSUWAN P, VISOOTTIVISETH V. OSV: OSPF vulnerability checking tool[C]// Proceedings of International Joint Conference on Computer Science and Software Engineering. NJ: IEEE, 2017: 1-6.

[11] WANG M H. The Security Analysis and Attacks Detection of OSPF Routing Protocol[C]// Proceedings of International Conference on Intelligent Computation Technology and Automation. NJ: IEEE, 2015: 836-839.

[12] MIJUMBI R, SERRAT J, GORRICHO J L, et al. Network Function Virtualization: State-of-the-art and Research Challenges[J]. IEEE Communications Surveys & Tutorials, 2017, 18(1): 236-262.

[13] MICHALSKI M, CIESLAK K, POLAK M. The system for large networks emulation with OSPF/BGP routers based on LXC[C]// IEEE, International Conference on High PERFORMANCE Switching and Routing. IEEE, 2016: 1-4.

[14] BEMSTEIN D. Containers and Cloud: From LXC to Docker to Kubernetes[J]. IEEE Cloud Computing, 2015, 1(3): 81-84.

[15] JAKMA P, LAMPARTER D. Introduction to the quagga routing suite[J]. IEEE Network, 2014, 28(2): 42-48.

[16] DUMITRACHE C G, PREDUSCA G, CIRCIUMARESCU L D, et al. Comparative study of RIP, OSPF and EIGRPprotocols using Cisco Packet Tracer[C]// Proceedings of International Symposium on Electrical and Electronics Engineering. NJ: IEEE, 2017: 1-6.