OSPF 虚幻路由假邻接研究

王云霄，徐国爱
（北京邮电大学信息安全中心，北京 100876）

摘要：虚幻路由假邻接是针对 OSPF 邻接关系建立过程发起的一种新型的攻击，此类攻击会对配置了 OSPF 路由协议的网络基础设施会造成路由黑洞、路径劫持、流量窃听等严重的影响。本文对远程假邻接的原理进行了深入分析，在其基础上提出了一种在局域网内假邻接的攻击方法，并且在仿真平台上对两种攻击方法分别做仿真验证，获取攻击参数及实验结果，给出了两种攻击方法在持续时间，攻击成本，窃听流量等方面的对比，最后提出了针对虚幻路由假邻接的防御方法。

关键词：网络安全；OSPF 虚幻路由；假邻接；路由黑洞；仿真验证
中图分类号：TP393

The Research of OSPF Phantom Route False Adjacency

Wang Yunxiao, Xu Guoai
(Information Security Center,Being University of Post and Teleommunication,Beijing 100876)

Abstract: Phantom route false adjacency is OSPF adjacency-Targeted new attack，this type of attack will have serious impact on network infrastructure,such as blackhole,route hijacking,traffic eavesdropping and so on .In this paper,we make a deep analysis of the remote false adjacency,on this basis, we propose lan false adjacency, two kinds of attack methods were simulated, and the results were obtained on the simulation platform.We give a comparison of two methods of attack, such as duration, cost, and so on.At last,a method of defending this kind of attack is proposed.

Key words: Cyber Security; OSPF phantom route;False adjacency;Blackhole; Simulation

0 引言

OSPF（Open Shortest Path First，开放式最短路径优先）是目前最主要的 IGP（Interior Gateway Protocol，内部网关协议），其由 IETF（The Internet Engineering Task Force，国际互联网工程任务组）于 1988 年专门为 TCP/IP 网络研发，已经经过一次大的版本更新，目前全球网络中广泛使用的 OSPF 协议是定义在 RFC（Request For Comment）2328 中的 OSPF 第二版。OSPF 协议是基于 IP 层的协议，协议号为 89。不同于 EIGRP、RIP 等内部网关协议，OSPF 是一个链路状态协议，它支持大规模网络；启用 OSPF 协议的网络节点通过发送 LSA（链路状态更新报文）来同步更新，并且可以通过 Dijkstra 算法绘制以自己作为根节点的整个区域的网络拓扑树；同时支持区域的概念，对网络拓扑进行合理的区域规划可以达到地址汇总，网络分层的目的；另外，OSPF 还支持区域认证，通过设置网络接口密钥或者区域密钥保障网络运行安全。

OSPF 被广泛应用在互联网运营商，企业内网以及家庭办公小型组网中，所以针对 OSPF 协议的网络攻击也层出不穷，Cohen 等人在文献[1]中介绍了一种基于 AS 的 OSPF 分割攻击方法；伪造 LSA 报文攻击是另一种较为常见的针对 OSPF 协议的攻击方法，一般伪造 LSA 报文攻击会触发 OSPF 协议的 fight-back 安全防护机制以致攻击效果不明显，Esmail 等人在文献[2]中介绍了一种利用 OSPF 二义性[3]从而不会触发 fight-back 安全防护机制的伪造 LSA

作者简介：王云霄（1991-），男，北京邮电大学硕士研究生，主要研究方向：网络安全
通信联系人：徐国爱（1972-），男，北京邮电大学教授，主要研究方向：软件安全、信息安全管理和密码学. E-mail: xga@bupt.edu.cn

报文攻击；Michael 等人在文献[4]中介绍了基于抢占 DR 角色攻击导致网络中断或者造成长路由的攻击方法；文献[5][6]中介绍了针对 OSPF 的重放攻击方法。

以上介绍的几种常见的针对 OSPF 路由协议的攻击，攻击者都没有与受害路由建立邻居关系，因此攻击时间较短，攻击效果有限。2011 年 8 月，在美国拉斯维加斯举办的黑帽大会（Black Hat Conference）上，Dr. Gabi Nakibly 中提出了一种针对 OSPF 协议的伪造虚幻路由攻击，对在 OSPF 区域中，普通路由器在与指定路由器建立邻接关系过程中存在的安全缺陷进行了研究，发现了 OSPF 远程假邻接造成的虚幻路由安全威胁。

本文对 Nakibly 在研究中提出的安全缺陷利用场景进行了仿真复现，对攻击参数及结果进行研究更正，并且首先提出了一种局域网内假邻接导致流量窃听的方法，并对两种攻击方法在多个维度做了对比分析，最后提出了一种针对远程假邻接攻击的防御方法。

本文的组织结构安排如下：第二节描述 OSPF 邻接关系建立过程；第三节分析 OSPF 虚幻路由假邻接安全缺陷；第四节复现虚幻路由假邻接安全缺陷场景并仿真实验；第五节虚幻路由假邻接的防御。

1 OSPF 邻接关系建立过程

待建立 OSPF 邻接关系的双方的 Hello 报文间隔，Dead 时间间隔，区域 ID，认证密钥四个字段都保证一致是成功建立 OSPF 邻接关系的前提[7]，另外，正常邻接关系的建立需要 Hello，DBD，LSR，LSU，LSACK 五类 OSPF 报文的参与，如图 1 所示。

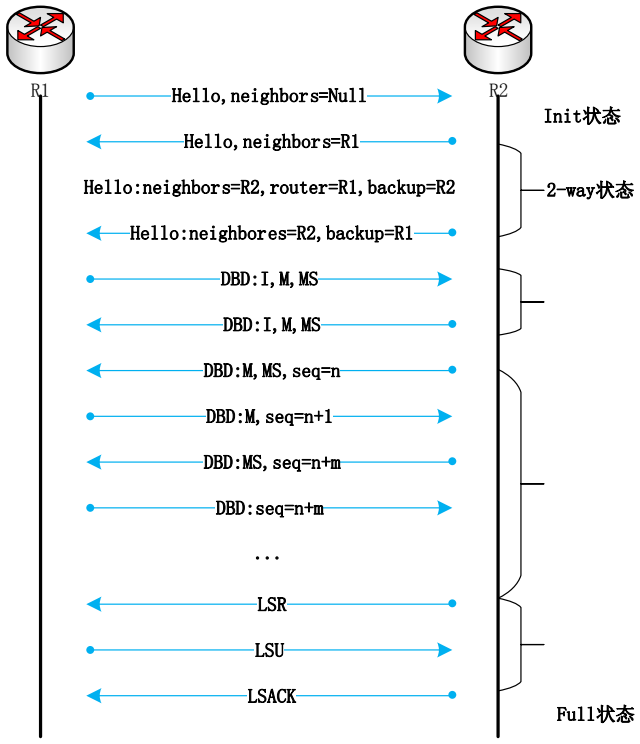

图 1 OSPF 邻接关系建立过程

Fig.1 OSPF adjacency building process

（1）Hello（Hello 报文），用于与邻居建立邻居或者邻接关系。

（2）DBD（Database Description，数据库描述报文），链路状态数据库内容的索引信息。

（3）LSR（Link State Request，链路状态请求报文），根据自身没有的链路状态请求邻居的特定项。

（4）LSU（Link State Update，链路状态更新报文），向建立邻接关系的路由器发送链路状态通告

（5）LSACK（Link State Acknowledge，链路状态确认），保障 OSPF LSU 报文传输的可靠性。

具体邻接关系建立过程可以分为七个阶段，分别为：

（1）Init 状态，双方互相发送 Hello 报文，选举 DR/BDR 角色。

（2）Exstart 状态，双方互相发送 DBD 报文，决定 Master/Slave 关系。

（3）Exchange 状态，以 Exstart 状态下决定的 Master/Slave 关系为基础进行 DBD 数据库信息交换。

（4）Loading 状态，双方根据对方 DBD 报文的内容互相发送 LSR 报文请求路由链路通告信息，双方分别回复对方请求的 LSU，并对对方响应的 LSU 报文回复 LSACK 报文进行显式确认。

（5）Full 状态，OSPF 邻接关系建立完成的标志。

基于 OSPF 邻接关系的这些建立过程，在 DBD 报文交换部分中其实存在着假邻接安全缺陷，使邻接关系可以跳过 Loading 状态直接进入 Full 状态，达到虚幻路由的目的。

2 OSPF 虚幻路由假邻接安全缺陷分析

Nakibly 在研究[8][9]中提出了远程假邻接的攻击方法。根据 RFC 2328 Sec.10.8，对 OSPF 协议建立邻接关系中的交换 DBD 报文部分有如下描述：由在 Exstart 状态下选举的 Master/Slave 角色来决定在 Exchange 状态下建立邻接关系的双方决定谁率先发起 DBD 报文交换。在 Exstart 状态，双方同时发送带有 I（Initialize，第一个 DBD 报文），M（More，后续还有内容发送）和 MS（Master，指定自己为 Master）选项的 DBD 报文，此报文不包含任何 LSA Header，双方会根据 DBD 报文中的 Router-id 的大小决定 Master/Slave 关系，Router-id 大的 OSPF 路由器接口将会成为 Master 角色，对端相应的将成为 Slave 角色，接下来双方 DBD 报文中的 I 位置将会被置为 0，Master 的 MS 字段置为 1，Slave 的 MS 字段置为 0，进而进入 Exchange 状态，由 Master 来决定 DBD 报文的序列号，双方按照 Master 决定的 DBD 报文序列号开始交换带有 LSA Header 的报文。当收到 DBD 报文中 M 位为 0 时说明对方已经将 DBD 报文发送完毕，邻接状态将进入 Loading 状态。DBD 报文格式如图 2 所示。

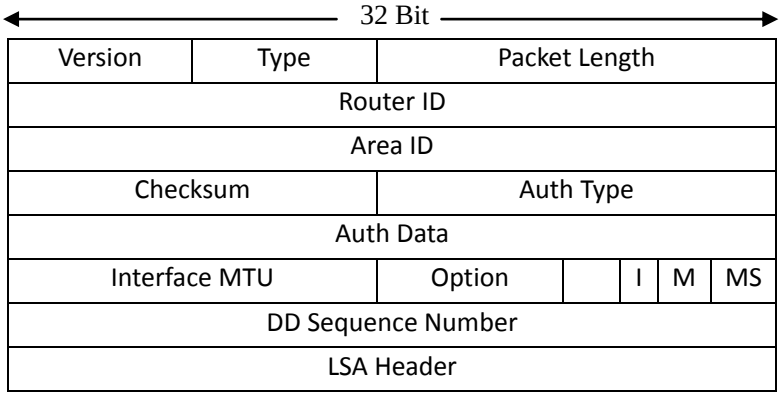

图 2 DBD 报文格式

Fig.2 DBD packet format

本文经过实验发现，在 Slave 路由器没有 Master 路由器的 MAC 地址的情况下，导致 Slave 无法给 Master 发送 DBD 报文，但是双方依然可以建立起邻接关系。Nakibly 在研究中将此

类现象归纳为，Master 路由器在不处理 Slave 路由器发送的报文的情况下可以与 Slave 路由器建立邻接关系，这种说法并不准确。本文现将此类远程假邻接攻击总结如下，由于处于 Slave 角色的路由器没有对 Master 路由器是否真正可达做验证，只通过 OSPF 的邻接关系建立完成错误地判定邻接路由器的真实性，所以导致虚幻路由的产生。利用这一点，可以通过虚幻路由的方式与受害路由器建立远程假邻接的关系。此攻击的前提是受害路由器必须为指定路由器，因为只有指定路由器才会对网络中新的 Hello 包做出发送 DBD 报文的回应。攻击者发送伪造 Hello 包，使受害路由器进入 2-way 状态，进而发送 Router-id 较大的 DBD 报文，在 Extart 状态中让自己成为 Master，因为在 Exchange 状态中，Slave 需要发送 DBD 报文逐条回应 Master 发送的 DBD 报文，序列号为 Master DBD 报文序列号+1，由于是远程假邻接，攻击者如果是 Slave 角色，则无法收到受害路由所发送的 DBD 报文，也就无法获知 DBD 报文的序列号，导致邻接状态卡顿在 Extart 状态，邻接关系建立失败。攻击者成为 Master，从而控制整个邻接建立过程，Slave 对 Master 可达性并没有做验证，所以邻接关系可以成功建立，之后攻击者则可以发送恶意的 LSU 报文造成路由黑洞，最短路径劫持等威胁。另外如果攻击者和受害路由器处于同一局域网中，则可以通过伪造虚幻路由器 MAC 地址实施 ARP 欺骗，进而进行流量窃听。

具体攻击步骤如图 3 所示，为了简化邻接关系的建立，降低攻击成本，将 Master 发送的 DBD 报文中的 LSA Header 一直置为空，Slave 在 Master 发送的 DBD 报文中没有发现自己所需要的 LSA 信息，Slave 也就不需要发送 LSU 请求报文，从而跳过交换 LSU 报文的 Loading 状态，直接进入 Full 状态，邻接关系建立完成。通过这个过程，可以发现 Master 是在 Extart 和 Exchange 状态中占有绝对的主导地位，Slave 只是被动的收发 DBD 报文。

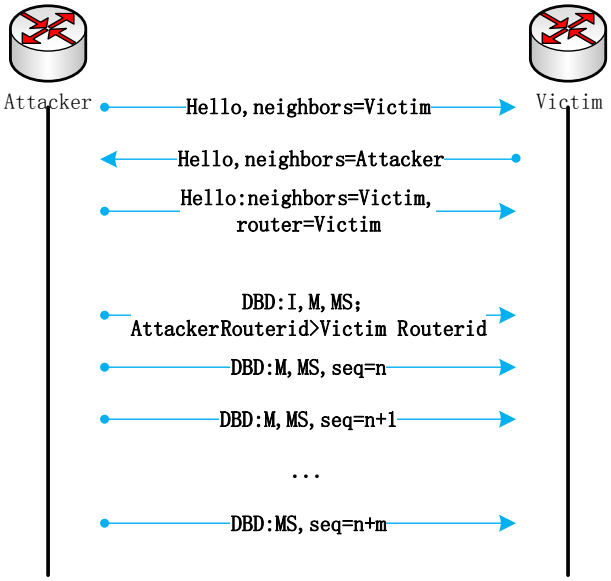

图 3 远程假邻接具体攻击流程

Fig.3 Specific attack step of remote false adjacency

为了使假邻接关系成功建立，需要在以下几个关键点选择合适的参数：

（1）获知被攻击网络的 OSPF Hello 时间间隔、Dead 时间间隔以及区域 ID 号码，否则邻接关系会因为以上参数不匹配而建立失败，通常情况下，网络管理员不会修改以上参数，否则会极大的增加网络管理成本；

（2）不抢占原有指定路由器角色，攻击者成为 DROther，如果攻击者抢占指定路由器角色，则需要与区域内其他路由器分别建立邻接关系，导致攻击成本显著增加；

（3）攻击者的 Router-id 大于指定路由器的 Rouer-id，用于在 Exstart 状态协商 Master/Slave 时占据 Master 角色，决定 Exchange 状态下的序列号；

（4）如果被攻击区域配置了消息加密认证，则需要知悉密钥，如果攻击者处于被攻击网络，可以通过嗅探抓取 OSPF 加密报文，并结合使用 John The Ripper 报文破解工具爆破 OSPF 密钥；

（5）需要攻击者始终以小于默认 Dead 时间的间隔发送 Hello 报文维持邻居关系存活；

（6）为了使攻击持续时间更长，在局域网内假邻接的情况下需要回复 LSACK 报文来确认受害路由器发送的 Network LSA。

3 虚幻路由假邻接安全缺陷场景及仿真实验

3.1 远程假邻接虚幻路由—路由黑洞

攻击者可以在启用 OSPF 协议网络中的任何位置通过创建虚幻路由器，并通过虚幻路由器宣告此网络中已经存在的子网，由于 OSPF 协议的特点，造成此条恶意路由被整个区域学习，区域内每个路由器根据 Dijistra 算法计算最短路径，将这条恶意路由与正常路由表项做比较，如果将恶意路由被选为最优路径的话，则此路由器所有发往正常子网的流量则会被发往虚幻路由器，由于虚幻路由器所在局域网的网关并不知道虚幻路由器的 MAC 地址，导致流量全部拥挤在网关，进而造成路由黑洞。

在仿真平台上搭建图 4 所示的实验拓扑场景，此实验拓扑总共包含六台路由器和一台终端设备，包含六个网段并且所有网络设备都处于同一个自治系统内，并且设计了局域网部分，能够更加直观的看出远程假邻接虚幻路由所造成的现象。

拓扑中的设备型号均为思科 7200，版本号均为 15.0(1)M，本次实验对受害路由的担当 DR 接口的 OSPF 优先级调至 10，其他路由器接口 OSPF 依然保持默认为 1，这儿会使得虚幻路由器并不会抢占受害路由的 DR 接口的角色，将接口的优先级调高是在网络配置人工指定 DR 接口的常用手段。

终端设备的操作系统 Centos，通过云模块接入仿真平台，并且在系统中通过 NetworkConnection 设置静态 IP 地址，并将网关地址设置为直连路由器接口的 IP 地址，从而保证终端操作系统可以与仿真平台中的网络设备通信。由于攻击者处于整个被攻击网络的外部，所以此攻击方法被称之为远程假邻接虚幻路由攻击。

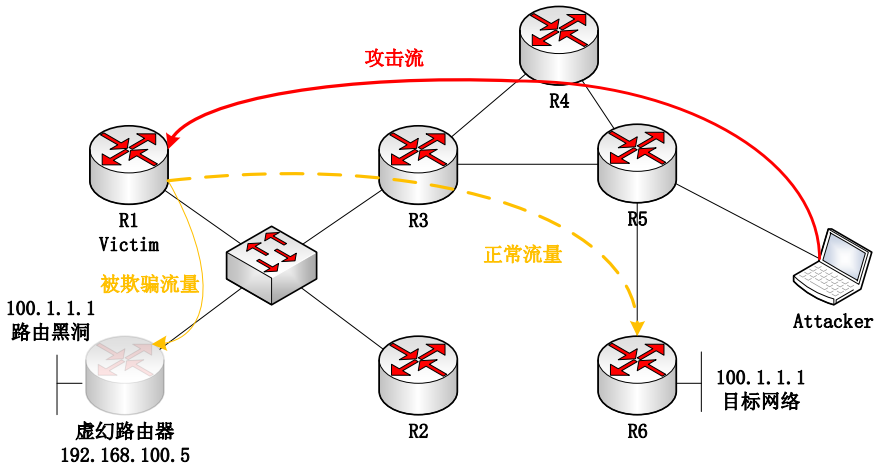

图 4 路由黑洞实验拓扑

Fig.4 Lab topology of route blackhole

本次实验中硬件只需要一台接入网络的主机即可，并不需要一台被控制的路由器即可完成攻击，软件工具使用 Scapy，Scapy 是 Python 语言编写的一个功能强大的交互式数据包处理程序，可用来发送、嗅探、解析和伪造多种网络数据包。本文使用 Scapy 进行 OSPF Hello、OSPF DBD、OSPF LSU、OSPF LSACK 及 ARP 响应等数据包的构造及发送，使用 Python 脚本语言编写整个攻击脚本的编写。本次实验伪造出 IP 地址为 192.168.100.5，掩码为 24 位的虚幻路由器，通过和指定路由器 R1 建立远程假邻接关系，进而通告网络中已经存在的路由子网造成路由黑洞。

OSPF 邻居建立的第一步是发送 Hello 包，将以太网 Ether 的源地址和目的地址都设置为 None，因为 Scapy 会自动帮助填写数据链路层信息，源 IP 地址设置为 192.168.100.5，目的 IP 地址设置为 192.168.100.1。通常情况，OSPF Hello 包文的 IP 目的地址为组播地址 225.0.0.5，又由于攻击者不处于被攻击网络中，通过实验使用 OSPF Hello 单播报文同样可以达到效果。将虚幻路由器的 Router-id 设置为 55.5.5.5，OSPF Hello 中的 hello interval 和 dead interval 保持默认值，router 字段设置为指定路由器的 IP 地址，backup 字段设置为备用路由器的 IP 地址，并且在 neighbors 字段设置为指定路由器的 Router-id，目的是为了使指定路由器通过此 Hello 报文发现虚幻路由器，直接进入 2-way 状态，并且由于受害路由为指定路由器，所以受害路由率先发送 DBD(I,M,S)包，进入 ExStart 状态。

另外需要注意的是，IP 的 chksum 字段和 OSPF Header 的 chksum 字段都需要设置为 None，Scapy 才会重新计算校验和，否则会出现校验出错的情况。

当指定路由器发送 DBD(I,M,S)报文后，攻击者构造 DBD(I,M,S)报文回应，Scapy 报文截图如图 5 所示：

```
###[ IP ]###
     version= 4L
     ihl= 5L
     tos= 0xc0
     len= 80
     id= 332
     flags=
     frag= 0L
     ttl= 128
     proto= ospf
     chksum= None
     src= 192.168.100.5
     dst= 192.168.100.1
     \options\
###[ OSPF Header ]###
        version= 2
        type= Hello
        len= 48
        src= 55.5.5.5
        area= 0.0.0.0
        chksum= None
        authtype= Null
        authdata= 0x0
###[ OSPF Hello ]###
           mask= 255.255.255.0
           hellointerval= 10
           options= E+L
           prio= 1
           deadinterval= 40
           router= 192.168.100.1
           backup= 192.168.100.3
           neighbors= ['1.1.1.1']
```

```
###[ IP ]###
     version= 4L
     ihl= 5L
     tos= 0xc0
     len= 52
     id= 60989
     flags=
     frag= 0L
     ttl= 128
     proto= ospf
     chksum= None
     src= 192.168.100.5
     dst= 192.168.100.1
     \options\
###[ OSPF Header ]###
        version= 2
        type= DBDesc
        len= 32
        src= 55.5.5.5
        area= 0.0.0.0
        chksum= None
        authtype= Null
        authdata= 0x0
###[ OSPF Database Description ]###
           mtu= 1500
           options= E
           dbdescr= MS+M+I
           ddseq= 1446637115
           \lsaheaders\
```

图 5 OSPF Hello 和 DBD 伪造报文

Fig.5 False packets of OSPF Hello and DBD

将首个 DBD 报文中的 dbdescr 设置为”MS+M+I”，第二至十个 DBD 报文中的 dbdescr 都设置为”MS+M”，将最后一个 DBD 报文中的 dbdscr 设置为”MS”。这个过程中需要以小于

死亡时间的时间间隔定时的发送 OSPF Hello 包以维持受害路由与虚幻路由器的邻接关系，当攻击者将 OSPF Database Description 报文发送完毕后，在 R1 上通过 show ip ospf neighbor 命令，截图如图 6 所示。

```
*Nov 11 21:58:55.527: %OSPF-5-ADJCHG: Process 1, Nbr 55.5.5.5 on Ethernet1/0 from LOADING to FULL, Loading Done
R1#sh ip os nei

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DROTHER    00:00:37    192.168.100.2   Ethernet1/0
3.3.3.3           1   FULL/BDR        00:00:37    192.168.100.3   Ethernet1/0
55.5.5.5          1   FULL/DROTHER    00:00:34    192.168.100.5   Ethernet1/0
```

图 6 OSPF 邻居表

Fig.6 OSPF neighbor table

这说明 R1 已经与虚幻路由器建立了邻居关系，并且将虚幻路由器加入到自己的 LSA database 中，虚幻路由器的角色为 Drother。构造 OSPF Router LSA，Scapy 报文截图如图 7 所示。

```
###[ OSPF Link State Update ]###
          lsacount= 1
          \lsalist\
           |###[ OSPF Router LSA ]###
           |  age= 1
           |  options= E+DC
           |  type= 1
           |  id= 55.5.5.5
           |  adrouter= 55.5.5.5
           |  seq= 0x80000011
           |  chksum= None
           |  len= 60
           |  flags=
           |  reserved= 0
           |  linkcount= 3
           |  \linklist\
           |   |###[ OSPF Link ]###
           |   |  id= 100.1.1.1
           |   |  data= 255.255.255.255
           |   |  type= stub
           |   |  toscount= 0
           |   |  metric= 1
           |   |###[ OSPF Link ]###
           |   |  id= 55.5.5.5
           |   |  data= 255.255.255.255
           |   |  type= stub
           |   |  toscount= 0
           |   |  metric= 1
           |   |###[ OSPF Link ]###
           |   |  id= 192.168.100.1
           |   |  data= 192.168.100.5
           |   |  type= transit
           |   |  toscount= 0
           |   |  metric= 10
```

图 7 OSPF Router LSA 伪造报文

Fig.7 False packet of OSPF Router LSA

将 OSPF Link State Update 中的 linkcount 设置为 3，因为构造的 LSA 中包含了 3 部分的更新内容，将 R5 在 OSPF 区域中宣告的 100.1.1.1 这条路由设置为 stub 更新，stub 更新的 id 字段为 IP 网段，data 字段为掩码；并且还需要将一条正确的 transit 路由更新包含在内，transit 区域即为被攻击的局域网，以至于使得 R1 相信此虚幻路由确实处于同一个局域网中， id 字段设置为 DR 路由器的 IP 地址，data 字段设置为虚幻路由器的 IP 地址。将此 LSA 报文单播发送给 R1。在 R1 中通过 show ip route 命令，对比发送 LSA 报文前后的路由表项，截图如图 8、图 9 所示。

```
R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
C        1.1.1.1 is directly connected, Loopback0
      2.0.0.0/32 is subnetted, 1 subnets
O        2.2.2.2 [110/11] via 192.168.100.2, 00:09:06, Ethernet1/0
      3.0.0.0/32 is subnetted, 1 subnets
O        3.3.3.3 [110/11] via 192.168.100.3, 00:08:56, Ethernet1/0
      4.0.0.0/32 is subnetted, 1 subnets
O        4.4.4.4 [110/21] via 192.168.100.3, 00:08:46, Ethernet1/0
      5.0.0.0/32 is subnetted, 1 subnets
O        5.5.5.5 [110/21] via 192.168.100.3, 00:07:41, Ethernet1/0
      6.0.0.0/32 is subnetted, 1 subnets
O        6.6.6.6 [110/31] via 192.168.100.3, 00:07:15, Ethernet1/0
      34.0.0.0/24 is subnetted, 1 subnets
O        34.1.1.0 [110/20] via 192.168.100.3, 00:08:46, Ethernet1/0
      35.0.0.0/24 is subnetted, 1 subnets
O        35.1.1.0 [110/20] via 192.168.100.3, 00:08:46, Ethernet1/0
      45.0.0.0/24 is subnetted, 1 subnets
O        45.1.1.0 [110/30] via 192.168.100.3, 00:08:46, Ethernet1/0
      56.0.0.0/24 is subnetted, 1 subnets
O        56.1.1.0 [110/30] via 192.168.100.3, 00:08:46, Ethernet1/0
      100.0.0.0/32 is subnetted, 1 subnets
O        100.1.1.1 [110/31] via 192.168.100.3, 00:01:37, Ethernet1/0
      192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.100.0/24 is directly connected, Ethernet1/0
L        192.168.100.1/32 is directly connected, Ethernet1/0
```

图 8 R1 路由表（攻击前）

Fig.# R1 route table(Before attack)

```
R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
C        1.1.1.1 is directly connected, Loopback0
      2.0.0.0/32 is subnetted, 1 subnets
O        2.2.2.2 [110/11] via 192.168.100.2, 00:16:34, Ethernet1/0
      3.0.0.0/32 is subnetted, 1 subnets
O        3.3.3.3 [110/11] via 192.168.100.3, 00:16:24, Ethernet1/0
      4.0.0.0/32 is subnetted, 1 subnets
O        4.4.4.4 [110/21] via 192.168.100.3, 00:16:14, Ethernet1/0
      5.0.0.0/32 is subnetted, 1 subnets
O        5.5.5.5 [110/21] via 192.168.100.3, 00:15:09, Ethernet1/0
      6.0.0.0/32 is subnetted, 1 subnets
O        6.6.6.6 [110/31] via 192.168.100.3, 00:14:43, Ethernet1/0
      34.0.0.0/24 is subnetted, 1 subnets
O        34.1.1.0 [110/20] via 192.168.100.3, 00:16:15, Ethernet1/0
      35.0.0.0/24 is subnetted, 1 subnets
O        35.1.1.0 [110/20] via 192.168.100.3, 00:16:15, Ethernet1/0
      45.0.0.0/24 is subnetted, 1 subnets
O        45.1.1.0 [110/30] via 192.168.100.3, 00:16:15, Ethernet1/0
      55.0.0.0/32 is subnetted, 1 subnets
O        55.5.5.5 [110/11] via 192.168.100.5, 00:00:03, Ethernet1/0
      56.0.0.0/24 is subnetted, 1 subnets
O        56.1.1.0 [110/30] via 192.168.100.3, 00:16:15, Ethernet1/0
      100.0.0.0/32 is subnetted, 1 subnets
O        100.1.1.1 [110/11] via 192.168.100.5, 00:00:13, Ethernet1/0
      192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.100.0/24 is directly connected, Ethernet1/0
L        192.168.100.1/32 is directly connected, Ethernet1/0
R1#
```

图 9 R1 路由表（攻击后）

Fig.9 R1 route table(After attack)

R1 如果发送到目的 IP 为 100.1.1.1 的包，会将其发送给虚幻路由 192.168.100.5，并不会发送给 192.168.100.3，并且查看 R4 的路由表，也通过 OSPF 学习到了此虚幻路由。

实验结果表明，区域内的所有路由器都会通过动态路由协议 OSPF 学习到此虚幻路由，

会利用 OSPF 的 Dijkstra 算法选出最优的路径，等待收敛完成后，被感染的路由则会陷入路由黑洞，导致目的流量被大量劫持到并不存在的虚幻路由。另外还会导致受害路由所处局域网的边界路由器的负担加重，影响数据包处理速度等。

表 1 路由黑洞影响范围

Tab.1 Influence range of blackhole

R1	R2	R3	R4	R5	R6
感染	感染	感染	携带	正常	正常

实验结果如表 1 所示，远程假邻接中，受害路由器在进入 Full 状态之后，根据 OSPF 路由协议 RFC，作为指定路由器，会向虚幻路由器发送一条 Network LSA，由于受害路由器无法获知虚幻路由器的 MAC，导致报文无法发出，从而攻击者也无法发送 LSACK 来确认此 Network LSA，受害路由器在经过 24 个重传间隔后会将虚幻路由器邻接关系改成 down。在 3.2 章节中提出了一种，利用 ARP 欺骗，在局域网中假邻接的攻击方法，使得受害路由器可以将 Network LSA 发出，攻击者通过嗅探并回应此 LSA，使得假邻接持续时间延长。

3.2 局域网内假邻接虚幻路由—流量窃听

攻击者在自己所在局域网中攻击指定路由器，使虚幻路由与指定路由器建立假邻接关系，并且伪造虚幻路由的 MAC 地址，与远程假邻接类似，同样伪造虚幻路由器宣告恶意路由，等待整个区域收敛完成后，将此恶意路由加入路由表的路由器会将发送目标网络的流量发送到攻击者所在的子网，由于 MAC 地址在此局域网中并不存在，利用交换设备遇到未知 MAC 地址会泛洪的特点或者集线器的广播报文的特点，攻击者可以嗅探到被恶意导流的流量。

当攻击者处于受害者同一个局域网中时，将以上实验拓扑调整为如图 10 所示。

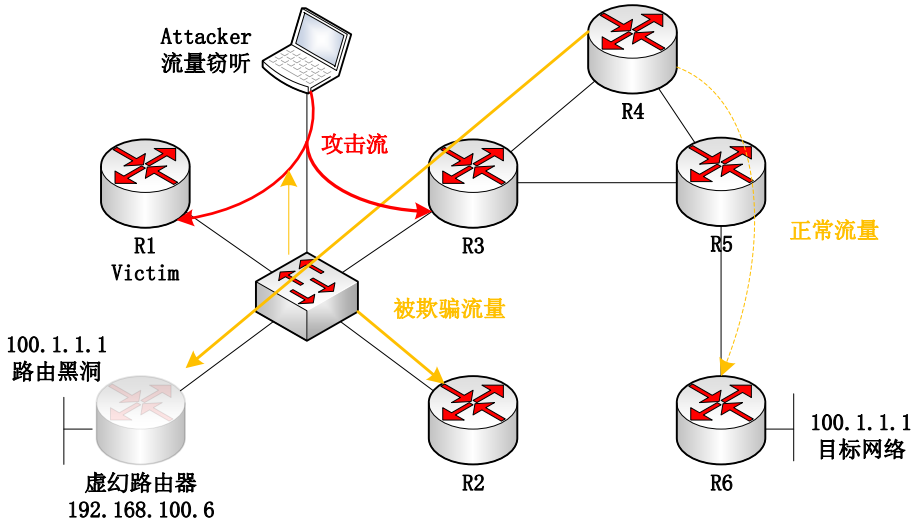

图 10 流量窃听实验拓扑

Fig.10 Lab topology of route eavesdropping

攻击者的 IP 地址设置为 192.168.100.5/24，伪造的虚幻路由器的 IP 地址为 192.168.100.6/24，Router-id 为 66.6.6.6，其他的路由器的配置保持不变。由实验可知，当攻击者与受害路由建立假邻接关系之后，受害路由会向虚幻路由器发起一次 Network LSA 报文，以 5s 的时间间隔进行重传，如果在 115s 之后没有收到此 LSA 报文的 ACK 报文，受害路由将断开与虚幻路由的邻居关系，使得之前宣告的路由失效，Wireshak 截图如图 11 所示。

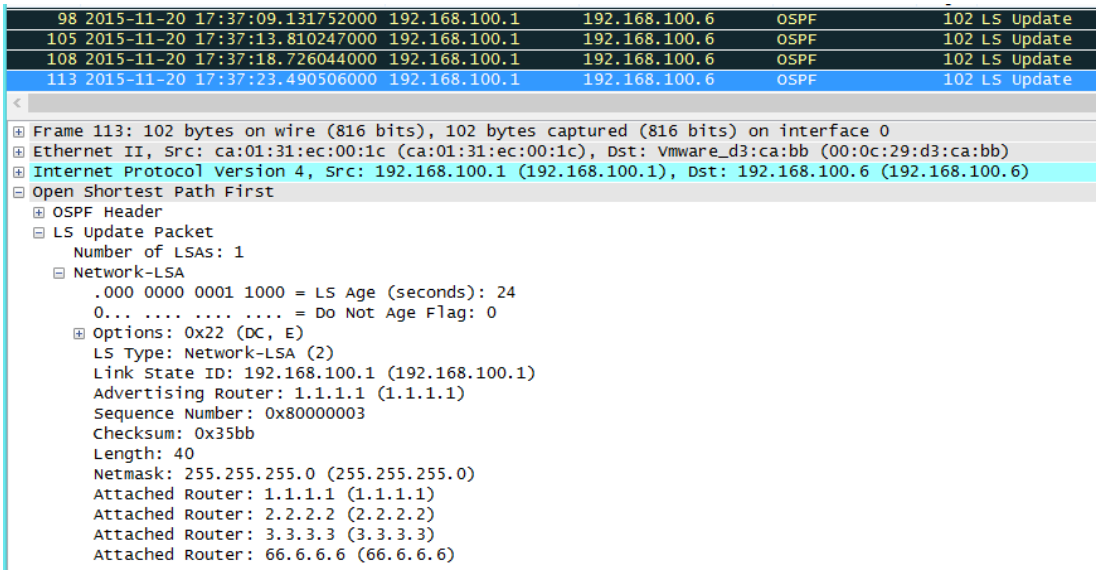

图 11 OSPF Network LSA 重传报文

Fig.11 Retransmission of OSPF Network LSA

在发送 LSA 之前，受害路由器需要知道虚幻路由器的 MAC 地址，攻击者可以伪造一个局域网中并不存在的 MAC 地址，由于交换机遇到 ARP 表中不存在的 MAC 地址会在局域网广播泛洪，所以我们才可以窃听到受害路由给虚幻路由器发送的 LSA 报文以及后续窃取到发送到虚幻路由的流量。向受害路由单播应答伪造虚幻路由的 ARP 报文，使得受害路由会向这个伪造的 MAC 地址发送 Network LSA，此时，攻击者嗅探并回应此 LSA。使用 Scapy 伪造 ARP 响应包和伪造 LSACK 报文，Scapy 报文截图如图 12 所示。

图 12 ARP 和 LSACK 伪造报文

Fig.12 False packets of ARP and LSACK

OSPF LSA Header 区域中的 seq 和 chksum 字段需与受害路由发送的 Network LSA 中的对应字段保持一致才能够使受害路由器接收此 LSACK 并停止重传 Network LSA，至此邻居关系建立完成。之后，发送恶意 LSA 报文，宣告虚幻路由器可以去往目的子网，等待整个区域都学习到这条虚幻路由之后，攻击者就会窃听到受到感染的路由器发往目的 IP 地址的流量。

表 2 两种假邻接对比

Tab.2 Comparison of two false adjacency

	持续时间（s）	攻击成本	窃取流量
远程假邻接	115	高	否
局域网内假邻接	3600	低	是

表 2 为远程与局域网内假邻接在持续时间、供给成本和窃取流量三个方面的对比。

在持续时间方面，远程假邻接由于受到重传次数的限制，而且攻击者并不会收到受害路由发送的 LSA，邻接关系并没有完全建立，所以等待重传次数到达上限之后，邻接关系就会失效，在持续 115s 之后，邻接关系会从 Full 变为 Down，宣告的恶意虚幻路由就被会路由表剔除，再经过 60s 之后，邻接关系彻底失效，但是恶意虚幻路由拓扑信息依然存在于受害路由器的 ospf database 中，老化时间为一个小时，在此一小时之内，可以重放邻接关系建立过程进行攻击，并不需要重新发送 LSU 报文；而局域网内假邻接，可以通过回复 LSACK，与受害路由器建立完全的邻接关系，因为 OSPF 协议的老化时间为 60 分钟，30 分钟会和所有激活邻居进行强制 DBD 更新，所以虚幻路由可以持续 30 分钟。

在攻击成本方面，远程假邻接不了解局域网情况，可能存在 IP 冲突，而且与受害路由处于不同局域网中，可控性较差；局域网内假邻接，攻击者与受害路由处于相同局域网中，可以方便的进行 ARP 欺骗，流量窃听，攻击成本较低。

在能否窃取流量方面，远程假邻接能够对受到感染的路由器只能造成路由黑洞的影响，受害路由器会发现大量的超时丢包；局域网内假邻接可以通过伪造出的虚幻路由器在造成路由黑洞的同时，还可以窃听到受感染的路由器发往目标 IP 地址的流量，正是利用了攻击者可以伪造 ARP 响应包、LSACK 确认报文，并且交换机遇到目的 MAC 未知的报文会广播泛洪的特性。

4 虚幻路由假邻接攻击的防御

基于第三节对虚幻路由原理的分析，产生远程虚幻假邻接的原因是 Slave 路由器没有验证 Master 路由器可达性，仅凭 OSPF 邻接关系的建立即确定邻接关系。本节在 OSPF 协议栈与 OSPF 安全配置两个方面提出了虚幻路由防御的方法。

4.1 OSPF 协议栈防御

建立正常 OSPF 邻接关系的两台路由器接口都必须处于同一个局域网中，相应的双方路由器的 ARP 表中必然存在对方的 ARP 信息，对于虚幻路由器远程假邻接，攻击者与受害路由器不在同一个局域网中，由于 MAC 地址在整个网络路径中是逐跳不断的解封装和封装，所以伪造 OSPF 报文的 MAC 地址与受害路由所处网络网关的 MAC 冲突，所以受害路由器的 ARP 表项中并没有攻击者伪造虚幻路由器 IP 的 MAC 地址，如图 13 所示。

可以通过修改 OSPF 协议栈进行防御，在回应 OSPF 协议 Hello 报文之前加入目标地址可达性验证。对目标路由器可达性的认证可以通过检查 ARP 表项中是否存在邻接关系对方

的 MAC 地址信息。

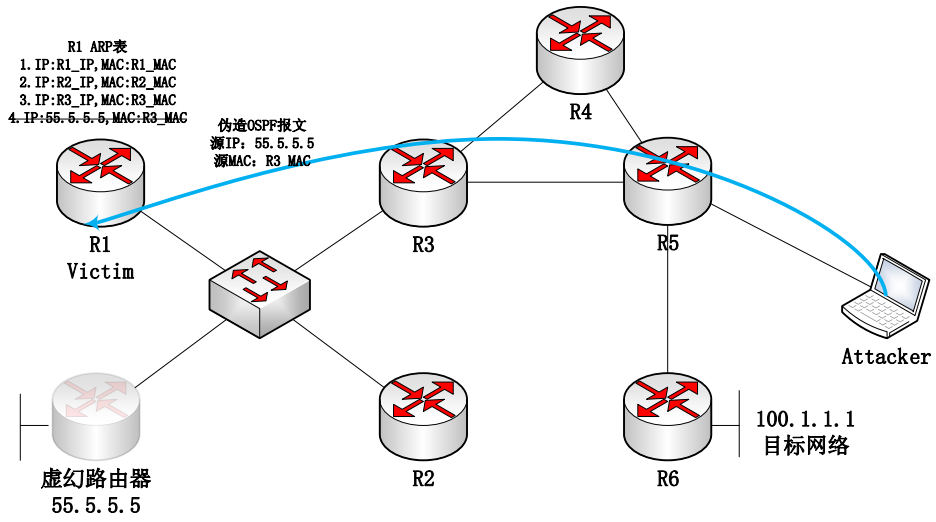

图 13 远程假邻接的防御

Fig.13 Defence of remote false adjacency

4.2 OSPF 安全配置防御

可以通过目前 OSPF 协议存在的安全加固方式进行防御，在建立邻接关系方面，可以通过修改默认的 Hello 时间间隔、Dead 时间间隔，增加建立邻接关系的难度，此项加固需要修改局域网中所有启用 OSPF 协议路由器的配置参数，否则正常的 OSPF 邻接关系也无法建立；在加密认证方面，尽量避免空密钥和明文密钥进行链路验证或者区域验证，推荐使用密文消息验证，并且加强密钥强度，增加爆破攻击的难度。

5 结论

本文基于 Nakibly 的研究构思，使用仿真平台来绘制搭建针对 OSPF 协议虚幻路由的安全研究实验场景，并在此实验环境中复现了针对 OSPF 在创建邻接关系的过程中存在虚幻路由的隐患，并首先提出了一种通过伪造 OSPF 报文配合 ARP 欺骗的方式进行局域网内假邻接的攻击方法，通过对比攻击步骤和实验结果参数，得出此方法相对远程假邻接的攻击方法在攻击效果上效率更高，攻击持续时间更长，成本更低，攻击效果更明显的结论，并提出了远程假邻接的防御方法。未来将继续研究加密链路 OSPF 虚幻路由攻击及攻击效果分析。

[参考文献] (References)

[1] Cohen R, Hess-Green R, Nakibly G. Small Lies, Lots of Damage: a Partition Attack on Link-State Routing Protocols[J]. IEEE CNS, 2015, 20(3): 100-108.
[2] Esmail Kaffashi, Ahmad Madadi Mousavi. A new attack on link-state database in open shortest path first routing protocol[J]. Journal of Electrical and Electronic Engineering, 2015, 3(2-1): 39-45.
[3] 郑庆棠. 基于仿真平台的典型动态路由协议攻击技术研究[D]. 北京：北京邮电大学，2013.
[4] Michael Sudkovitch, David I.Roitman, OSPF Securiy Project[OL]. [2010-10-1]. http://webcourse.cs.technion.ac.il/236349/Spring2013/ho/WCFiles/2009-2-ospf-report.pdf
[5] 康威, 罗守山, 辛阳. OSPF 路由协议安全性分析与研究[D]. 北京：北京邮电大学大学，2010.
[6] Jones E, Moigne O. OSPF security vulnerabilities analysis[J]. Work in Progress, 2006. 30(2): 11-38.
[7] Wendell Odom. CCNP ROUTE 642-902[M]. Indiana：Cisco Press，2011.
[8] Gabi Nakibly, Alex Kirshon, Dima Gonikman. Persistent OSPF Attacks[A]. Gabi Nakibly. The forum of NDSS 2012[C]. San Diego: NDSS Press, 2012. 10-21.
[9] Gabi Nakibly, Adi Sosnovich, Eitan Menahem. OSPF Vulnerability to Persistent Poisoning Attacks:A Systematic Analysis[A]. Gabi Nakibly. The forum of the 30th Annual Computer Security Applications Conference.[C]. New Orleans: ACM Press, 2014. 336-345.