融合多协议的网络层拓扑发现算法研究

周长建[1] 邢金阁[1] 刘海波[2]
(东北农业大学现代教育技术与信息中心 哈尔滨 150030)[1]
(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)[2]

摘 要 随着信息技术的不断发展,以及国家对网络空间安全的重视程度越来越高,现有的网络安全产品已经难以满足用户越来越广泛的网络安全需求。通过分析网络拓扑发现对网络安全的重要性,以及现有网络拓扑发现的优缺点,改进原有的网络层的拓扑发现算法,同时改进网络层的 OSPF 和 SNMP 拓扑发现规则,实现一种结合 SNMP 和 OSPF 共同优点的网络拓扑算法,实验证明该算法取得了不错的效果。

关键词 网络拓扑,SNMP,OSPF,网络安全,态势感知
中图法分类号 TP393.02 **文献标识码** A

Research on Network-layer Topology Discovery Algorithm Based on Multi-protocol

ZHOU Chang-jian[1] XING Jin-ge[1] LIU Hai-bo[2]
(Modern Educational Technology and Information Center, Northeast Agricultural University, Harbin 150030, China)[1]
(Department of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China)[2]

Abstract With the continuous development of information technology, and the cyberspace security obtains more and more value, the existing network security products have been difficult to meet the user's demand, which has more and more extensive network security. This paper analyzed the importance of network topology discovery in the area of network security and the advantages and disadvantages of the existing network topology, and improved the original topology discovery algorithm of network-layer. Though improving OSPF and SNMP topology discovery rules of network-layer, a network topology algorithm combining the common advantages of SNMP and OSPF was achieved. Experimental results prove that it has a good performance.

Keywords Network topology, SNMP, OSPF, Network security, Situation awareness

1 引言

网络拓扑发现能够为网络安全态势感知提供有效的服务,网络安全态势感知需要对管理目标进行实时监控,主要包括各个节点设备和中转设备等,这就需要网络拓扑发现方法具有一定的鲁棒性,同时需要多层次的拓扑发现方法的部署,目前在网络层比较流行的拓扑发现协议有 SNMP,ARP,ACMP,OSPF 等[1]。本文主要分析这几种拓扑发现协议的优缺点,结合 SNMP 协议目标明确的优点以及设备要求高、路径繁琐等缺点,同时包括 OSPF 协议效率高速度快的优点及严重依赖路由协议,对不使用 OSPF 协议的路由器禁止获取其他路由器的链路状态等缺点。本文主要对这两种协议的不足进行改进,使用基于 SNMP 的拓扑方法,并采用 OSPF 方法作为辅助,既能够弥补基于 SNMP 的拓扑方法不能访问未开启 SNMP 协议路由器的缺点,又能够解决 OSPF 方法严重依赖路由的弊端,结合这两种协议的特点进行优化改进。实验证明,这种方法能够有效提高拓扑发现的能力。

2 现有网络拓扑发现方法

网络拓扑发现常用的协议有 SNMP[2],ARP[3],ACMP[4] 和 OSPF[5] 等,根据这几种协议标准,采用网络层的拓扑方法获取各节点的路由器信息及中转设备信息,本节首先分析几种常见的拓扑发现协议,然后根据协议信息分析目前常用的拓扑发现方法。

2.1 拓扑发现协议

每种协议都有自己独特的功能和优缺点,本小节主要分析 SNMP 和 OSPF 2 种网络层协议的主要工作原理和适用范围[6]。

2.1.1 SNMP 协议

SNMP(Simple Network Management Protocol)即简单网络管理协议,该协议可以为不同的网络设备提供一致的数据接口,大大简化了网络管理的难度和复杂性,提高了工作效率。网络中的设备只要支持并开启 SNMP 服务协议,管理人员就可以通过 SNMP 协议对对应设备进行管理和维护[7]。

本文受国家自然科学基金项目(41306086),中央高校基本科研业务费自主项目(HEUCF100606)资助。
周长建(1984—),男,硕士,工程师,主要研究方向为网络空间安全、机器学习,E-mail:zhouchangjian@neau.edu.cn;邢金阁(1972—),男,硕士,高级工程师,主要研究方向为网络空间安全、教育信息化;刘海波(1976—),男,博士,副教授,主要研究方向为模式识别、计算机视觉。

2.1.2 ICMP 协议

ICMP 协议(Internet Control Message Protocol)通过向目标网络主机发送探测报文消息来探测网络是否拥堵及其连通性等信息。该协议是 IP 协议的组成部分,报文都需要 ICMP 作为支撑。其中 Ping 是 ICMP 最常用的工具之一。Ping 命令的目的是能够探测网络节点主机的存活,当网络设备发送 Ping 包以后,若节点主机存活,则会返回一个 ICMP 应答包,否则主机会很长时间才能收到目的超时报文,这种状况非常影响使用 Ping 命令进行工作的效率。为弥补 Ping 这一不足,采用异步方式进行探测,可以提高探测速度并降低网路拥堵的可能,但是有可能会造成网络阻塞,有些网络设备不支持这种方式。ICMP 协议还有一个工具是 TraceRoute,同样可以用作网络探测工作的网络拓扑发现,当用来检测网络连通性时,会得到源点与目的节点之间的路由路径。由于从源节点到目的节点的路径很可能存在多条,因此多次使用 TraceRoute 命令进行路径发现时,有可能存在多条不同的路径,可以针对这一特点进行网络拓扑发现,但是 TraceRoute 命令的网络拓扑发现方法存在着使用时间长、占用带宽较大、消耗资源较多等缺点[8]。

2.1.3 OSPF 协议

OSPF 协议即开放式段路径优先(Open Shortest Path First)协议,其作用范围是一个自治网络系统,在该系统内部有动态的网关路由功能。其优势是能够实时探测自治网络系统内部拓扑的变化,并根据链路状态的变化情况,动态实时计算网络内部最短路径,同时更新自制系统内部路由路径的最佳方式。OSPF 协议所作用的自治系统可以分为多个小区域,每个小区域都包括独立的路由器和主机,每个小区域都存在一个边界路由器,该路由器也存在多个端口连接多个区域,并且可以为所有相邻网络边界维护一份完整的网络拓扑信息资源库。OSPF 协议的主要作用在于连接不同的小区域,在不同的小区域间交互路由等信息。由此构成了整个网络的主干区域[9]。

2.2 网络拓扑发现方法

网络层拓扑发现方法的主要原理是采用网络层拓扑方法,从而获得路由器及与其相互连接的各个网络设备信息和子网信息[10]。网络层拓扑发现主要采用广度优先算法对网络层设备进行遍历。如以网络系统中某路由器为起点,采用 SNMP 协议及其他协议搜索该路由器临近的路由器,接着再依次访问与它们分别相邻的所有节点,依次类推。网络层拓扑发现方法主要有基于 SNMP 和 OSPF 两种协议的方法,每种方法都有其优缺点及适应环境,需要具体问题具体分析,才能够利用适用于本网络系统的安全态势感知拓扑发现方法。

2.2.1 基于 SNMP 的拓扑方法

基于 SNMP 的拓扑方法的主要工作原理是通过 SNMP 协议访问路由器路由表 ipRouteTable 信息,找到 ipRouteType 为 direct 的路由,下一跳地址 ipRouteNetHop 就是直连的路由器。从路由表 ipRouteTable 中得到的ipRou-teDest和 ipRoutemask 进行“与”运算得到对应的网络地址。随后从 ipRouteTable 表中得到 ipRouteType 项,得到子网类型,从而偏于网络拓扑的绘制工作[11]。

基于 SNMP 的拓扑发现方法的优点是:目标明确、效率高、速度快,以及对网络带来的负载小、系统开销低等;并且可以通过 SNMP 协议直接从路由表中获取下一跳路由器地址等信息,能较方便地获取完整的网络拓扑结构[12]。在网络安全态势感知中,同样使用 SNMP 协议进行网络系统监测,基于 SNMP 的拓扑发现方法可以非常便利地与网络安全态势感知系统进行深度融合[13]。但该拓扑方法也有一些明显的缺点,具体描述如下:

(1)对路由设备的要求较高,该协议要求路由器必须开启 SNMP 协议,否则无法获取到拓扑发现所需要的信息。

(2)通过该协议访问路由设备 MIB 库时,必须事先知道设备 MIB 库的 community 值,否则无法访问。

(3)ipRouteTable 表的索引是 IP 地址,但路由器每个端口都有一个 IP 地址,所以存在同一路由器的多个端口的 ipRouteTable 表信息较为冗杂的情况。

2.2.2 基于 OSPF 协议的拓扑方法

OSPF 是一种基于优先开放最短路径链路状态选择的协议。使用 OSPF 协议的各个路由器之间通过交换路由信息来共享网络的链路状态。由于每个路由器都保存有链路信息,因此可以通过分析路由表中保存的链路信息得到网络的拓扑结构[14]。该协议具有高效的路由工作速率和较低的网络资源占有率等优点,适用于较大规模的网络拓扑发现。网络中每个开启 OSPF 的路由器都会保存一个 OSPF MIB 库,通过访问 MIB 库获得链路信息,最终得到网络拓扑结构信息,也可以通过获取 OSPF 的 LSU 报文,以及分析报文信息的方式得到拓扑结构[15]。基于 OSPF 协议的拓扑发现方法的优点是效率高、速度快,但是该方法严重依赖路由协议,对不使用 OSPF 协议的路由器禁止获取其他路由器的链路状态。

3 改进的拓扑发现方法

为克服以上几种拓扑发现方法的缺点,本文提出了一种融合以上两种拓扑方法进行网络层拓扑发现的方法。其核心思想是使用基于 SNMP 的拓扑方法,并使用 OSPF 方法作为辅助[16]。这样既能够弥补基于 SNMP 的拓扑方法不能访问未开启 SNMP 协议路由器的缺点,又能够解决 OSPF 方法严重依赖路由的弊端。

3.1 改进算法的主要流程

算法主要流程如下。

(1)初始化 ipRouteTable,加入拓扑初始路由器信息;

(2)if ipRouteTable 为空,转到(8),否则转到(3);

(3)提取 ipRouteTable 中的 1 条路由信息,存入 Router__tmp;

(4)if Router_tmp 支持 SNMP 协议,执行(5),否则转到(6);

(5)使用 SNMP 协议获取直连的路由信息,并存入 ipRouteTable 和 XML 文件的 Router-SNMP 中,同时将连接关系存入 Link-R;

(6)使用 OSPF 协议获取直连的路由信息,并存入 ipRouteTable 和 XML 文件 Router-OSPF 中,同时连接关系存入到 Link-R,并执行(2);

（7）将 Router-SNMP 和 Router-OSPF 中的信息写入 Routers；

（8）结束。

3.2　改进 SNMP 拓扑算法

基于改进型的 SNMP 协议拓扑方法的主要算法如下：

（1）初始化路由表中的子网队列、路由器信息队列和连接队列；

（2）将缺省网关的 IP 地址添加到路由器 ipRouteTable 队列；

```
while(ipRouteTable){
if(ipRouteType=4){
ipRouteNextHop IP 加入网关队列；
添加 R-R 关系；
}
if(ipRouteType=3){
ipRouteTable 和 ipAddrTable 匹配，获得子网信息；
ipRouteDest 和 ipRouteMask 加入到子网队列；
添加 R-R 关系；
}
CurrentRouter 加入队列中。
}
}
```

（3）在对应的拓扑信文件库中记录路由器队列和连接队列、子网队列。

表 1 是一张 ipRouteTable 表。

表 1　ipRouteTable 表

ipRoute Dest	ipRouteIf Index	ipRoute NextHop	ipRoute Type	ipRoute Proto
10.1.1.0	4	10.1.5.0	indirect	local
10.1.2.0	3	10.1.6.0	direct	ospf
10.1.3.0	5	10.1.7.0	direct	ospf
10.1.4.0	4	10.1.8.0	indirect	ospf

其中，ipRouteDest 是 ipRouteTable 路由索引，ipRouteDest表征路由器目的地址，ipRouteMask 表示子网掩码，通过 ipRouteDest 和 ipRouteMask 得到子网信息。将 IP 数据包中的地址与 ipRouteMask 进行与运算，如果等于 ipRouteDest 地址，说明该 IP 能够在本路由器中找到对应的路由，同时按照本条路由信息对 IP 数据包进行转发。ipRouteIndex 是路由端口的索引值，该值与 ifTable 表对应，IP 数据包通过该接口转发给下一路由 ipRouteType 表示路由类型：当 ipRouteType 的值为 indirect 时，意味着该路由是间接路由；当 ipRouteType 为 direct 时，意味该路由是直接路由。ipRouteDest 表示目标网络地址，ipRouteNextHop 表示该子网需通过的路由器端口地址，ipRouteProto 表示本条路由的建立协议，可以通过 OSPF 建立，也可以手动添加（local）。通过分析 ipRouteTable 的信息，可以得到路由器的连接关系，也能得到直连的子网信息。通过 ipRouteTable 表的 ipRouteNextHop 字段，可以得到与该路由器相连的其他路由器相关信息，同时通过 ipRouteDest 和 ipRouteMask 的信息判断 ipRouteNextHop 是否在 ipRouteDest 的子网中。

3.3　改进 OSPF 拓扑算法

OSPF 协议路由器可以通过开启 OSPF 协议的路由器相互之间发送链路状态信息来获得网络的拓扑结构[17]。可以通过获取并分析链路状态（LSA）的方法进行网络拓扑发现，LSA 封装在 LSU 报文中，故可以通过分析 LSU 报文，得到网络拓扑信息[18]。该算法的主要代码如下：

```
初始化 LSAList，CONList；
while(LSAList){
  取出一条记录，；
if(该记录是 Router LSA){
for(Router LSA){
判断链路类型；
switch (link Type){
case 1：
以 routerId，linkId，linkData 初始化 CON 对象，设置 linkType=point-to-point，加入到 CONList 队列；break；
case 2：
将 advRouter 和 linkId 加入 transitMapA；break；
case 3：
routerId，linkId，linkData 初始化 CON 对象，设置 linkType=stub，加入到 CONList 队列；break；
case 4：
routerId，linkId，linkData 初始 CON 对象，设置 linkType=virtual link，该对象加入 CONList 队列；break；
}
}
} else if (Network LSA){
linkStateId 和 networkMask，计算出与 DR 直连的地址 transitAddress；
linkStateId 和 transitAddress 加入 transitMapB；
}
}
while(transitMapA){
取出一条记录；
if(transitMapB. linkStateId==transitMapA. linkId)
{
transitAddress；
advRouter，linkId 和 transitAddress 初始化 CON 对象，设置linkType=transit，该对象加入 CONList 队列；
}
}
}
```

3.4　融合多协议的网络层拓扑发现协议模块设计

网络层拓扑采集模块主要获取网络层拓扑信息并将该信息存储到网络拓扑库。该模块的设计方式主要基于 SNMP 和 OSPF 两种协议的网络拓扑发现算法，其中以 SNMP 协议为主，OSPF 协议为辅。最后将获得的有路由的拓扑信息存入网络拓扑信息库。该采集模块的工作流程如图 1 所示。

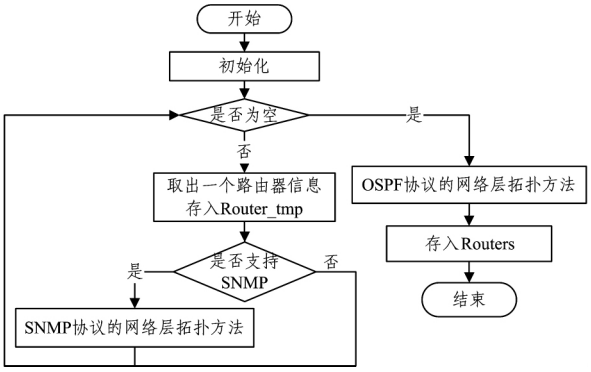

图 1　网络层拓扑采集模块的工作流程图

首先初始化 ipRouteTable 队列，读取 ipRouteTable 的配置信息，判断该路由器是否支持 SNMP 协议，若支持，则用 SNMP 协议拓扑模块进行拓扑信息采集，否则使用 OSPF 协议拓扑模块将采集到的信息存入 ipRouteTable，继续遍历 ipRouteTable，直到 ipRouteTable 为空。

SNMP 协议拓扑模块的伪代码如下：

```
初始化路由器队列，链接队列，子网队列；
缺省网关 IP 地址加入 ipRouteTable 队列；
while(ipRouteTable){
if(ipRouteType=4){
下一跳地址插入待访问网关队列；
连接关系加入到链接队列；
}
if(ipRouteType=3){
    ipRouteTable 和 ipAddrTable 匹配，获取子网地址
ipRouteDest 和 ipRouteMask 加入子网队列；
连接关系加入链接队列；
}
CurrentRouter 加入路由器队列；
}
}
更新路由器队列、链接队列和子网队列；
```

OSPF 协议拓扑模块的伪代码如下：

```
初始化 LSAList，CONList；
while(LSAList){
  取出一条记录；
if(该记录是 RouterLSA){
for(RouterLSA){
判断链路类型；
switch (linkType){
case 1：
routerId，linkId，linkData 初始化 CON 对象，设置 linkType=point-to-point，加入 CONList 队列；break；
case 2：
advRouter 和 linkId 加入 transMapA；break；
case 3：
routerId，linkId，linkData 初始 CON 对象，设置 linkType=stub，加入 CONList 队列；break；
case 4：
routerId，linkId，linkData 初始化 CON 对象，设置 linkType=virtual link，加入 CONList 队列；break；
}
}
} else if (Network LSA){
linkStateId 和 networkMask，计算直连传输网地址 transitAddress；
linkStateId 和 transitAddress 加入 transMapB 中；
}
}
while(transMapA){
取出一条记录；
if(transMapB. linkStateId==transMapA. linkId)
{
   transMapB 中 linkId 对应的 transitAddress；
   advRouter，linkId 和 transitAddress 初始 CON 对象，设置 linkType=transit，加入 CONList 队列；
}
}
}
```

4 实验结果及分析

本实验测试环境是由 6 台路由器{R1，R2，R3，R4，R5，R6}和一个主机节点主机构成，如图 2 所示。其目的是验证经改进后的融合多协议的网络层拓扑算法对现实网络环境的适应情况。

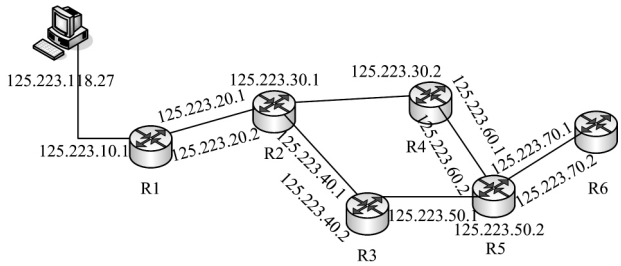

图 2 网络层拓扑发现方法的实验环境示意图

实验配置如表 2 所列。

表 2 实验配置表

路由器名称	OSPF 协议	SNMP 服务
R1	使用	开启
R2	不使用	开启
R3	使用	开启
R4	使用	开启
R5	使用	开启

实验过程如下：分别在每个节点主机开启 SNMP、OSPF 方法以及 SNMP 和 OSPF 结合的网络层拓扑方法测试程序，进行拓扑发现测试操作。图 3－图 5 示出了根据这几种方法测试所得到的网络拓扑信息。

```
〈?xml version="1.0" encoding="UTF-8"?〉
-〈xml-fragment version="1.0"〉
-〈Router〉
 〈RouterID〉1〈/RouterID〉
 〈RouterIP〉125.223.10.1〈/RouterIP〉
 〈/Router〉
-〈Router〉
 〈RouterID〉2〈/RouterID〉
 〈RouterIP〉125.223.20.2〈/RouterIP〉
 〈/Router〉
-〈Router〉
 〈RouterID〉3〈/RouterID〉
 〈RouterIP〉125.223.30.2〈/RouterIP〉
 〈/Router〉
-〈Router〉
 〈RouterID〉4〈/RouterID〉
 〈RouterIP〉125.223.40.2〈/RouterIP〉
 〈/Router〉
-〈Router〉
 〈RouterID〉5〈/RouterID〉
 〈RouterIP〉125.223.50.2〈/RouterIP〉
 〈/Router〉
-〈Router〉
 〈RouterID〉6〈/RouterID〉
 〈RouterIP〉125.223.60.2〈/RouterIP〉
 〈/Router〉
〈/xml-fragment〉
```

图 3 基于 SNMP 协议的网络层拓扑方法获得的网络层拓扑信息

```
〈?xml version="1.0" encoding="UTF-8"?〉
-〈xml-fragment version="1.0"〉
-〈Router〉
 〈RouterID〉1〈/RouterID〉
 〈RouterIP〉125.223.10.1〈/RouterIP〉
 〈/Router〉
-〈Router〉
 〈RouterID〉2〈/RouterID〉
 〈RouterIP〉125.223.20.2〈/RouterIP〉
 〈/Router〉
〈/xml-fragment〉
```

图 4　基于 OSPF 协议的网络层拓扑方法获得的网络层拓扑信息

```
〈?xml version="1.0" encoding="UTF-8"?〉
-〈xml-fragment version="1.0"〉
-〈Router〉
 〈RouterID〉1〈/RouterID〉
 〈RouterIP〉125.223.10.1〈/RouterIP〉
 〈/Router〉
-〈Router〉
 〈RouterID〉2〈/RouterID〉
 〈RouterIP〉125.223.20.2〈/RouterIP〉
 〈/Router〉
-〈Router〉
 〈RouterID〉3〈/RouterID〉
 〈RouterIP〉125.223.30.2〈/RouterIP〉
 〈/Router〉
-〈Router〉
 〈RouterID〉4〈/RouterID〉
 〈RouterIP〉125.223.40.2〈/RouterIP〉
 〈/Router〉
-〈Router〉
 〈RouterID〉5〈/RouterID〉
 〈RouterIP〉125.223.50.2〈/RouterIP〉
 〈/Router〉
-〈Router〉
 〈RouterID〉6〈/RouterID〉
 〈RouterIP〉125.223.60.2〈/RouterIP〉
 〈/Router〉
-〈Router〉
 〈RouterID〉7〈/RouterID〉
 〈RouterIP〉125.223.70.2〈/RouterIP〉
 〈/Router〉
〈/xml-fragment〉
```

图 5　SNMP 和 OSPF 协议相结合的网络层拓扑改进方法获得的网络层拓扑信息

通过分析实验数据可知，SNMP 协议的网络层拓扑方法得到 6 条路由信息，OSPF 协议的网络层拓扑方法得到 2 条路由信息，SNMP 和 OSPF 协议相结合的改进方法得到 7 条拓扑信息。由于本次实验实际只有 6 条路由信息，通过分析实验数据可以发现，125.223.50.2 和 125.223.60.2 属于同一台路由器的不同端口地址，即同名 IP 问题，需要拓扑信息分析才能够解决。所以可以得出结论：在本实验环境下，SNMP 和 OSPF 协议相融合的网络层拓扑改进方法具有更大的网路拓扑发现范围，对网络环境的适应性较好。

结束语　基于网络拓扑协议的网络态势感知技术越来越受到学术界的关注，网络空间安全技术在未来将会承担更加重要的工作，未来计算机网络信息的发展不再是单一和孤立的工作环境，融合多协议的网络拓扑发现技术利于 SNMP 协议和 OSPF 协议的优点组合，实现了网络层的拓扑发现算法，取得了不错的效果。在未来的工作中，可以尝试在链路层协议的融合及跨层融合方法，相信会有更多优秀成果出现。

参 考 文 献

[1] BASS T. Multisensor data fusion for next generation distributed intrusion detection systems[C]// Proc. of the '99 IRIS National Symp. on Sensor and Data Fusion. Laurel, 1999: 24-27.

[2] BASS T. Intrusion systems and multisensor data fusion [J]. Communications of the ACM, 2000, 43(4): 99-105.

[3] 龚正虎，卓莹. 网络态势感知研究[J]. 软件学报，2010，21(7)：1605-1619.

[4] CHEN X Z, ZHENG Q H, GUAN X H, et al. Quantitative hierarchical threat evaluation model for network security[J]. Journal of Software, 2006, 17(4): 885-897.

[5] EI Y, LIAN Y F, FENG G D. A network security situational awareness model based on information fusion[J]. Journal of Computer Research and Development, 2009, 46(3): 353-362.

[6] WEI Y, LIAN Y F. A network security situational awareness model based on log audit and performance correction[J]. Chinese Journal of Computers, 2009, 32(4): 763-772.

[7] 庄锁法，龚俭. 网络拓扑发现综述[J]. 计算机技术与发展，2007，17(10)：80-91.

[8] 李明江. SNMP 简单网络管理协议[M]. 北京：电子工业出版社，2007.

[9] MASSEY D, WU C L, ZHANG L X, et al. On design and evaluation of "intention-driven" ICMP traceback[C]// Tenth International Conference on Computer Communications and Networks, 2011. Scottsdale, AZ, 2011: 159-165.

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

[11] PLUMMER D C. Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48bit Ethernet address for transmission on Ethernet hardware[M]. RFC Editor, 1982.

[12] 张干. 基于 OSPF 路由协议的实时网络拓扑搜索的研究与实现[D]. 北京：北京邮电大学，2016：31-39.

[13] 凌军，曹阳，等. 基于 ARP 和 SNMP 的网络拓扑自动发现算法[J]. 武汉大学学报(理学版)，2001，47(1)：67-70.

[14] 何鹏，邱建林. 几种网络拓扑搜获方法的分析研究[J]. 微机发展，2015，15(7)：17-23.

[15] 闫兴篡，殷建平，蔡志平. 网络拓扑发现算法综述[J]. 计算机工程与应用，2007，43(14)：131-135.

[16] 陈旭. 一种基于 SNMP 的以太网拓扑自动发现算法[J]. 太原理工大学学报，2006，37(1)：116-118.

[17] 李延冰，马跃，王炜，等. 基于生成树的链路层拓扑发现算法[J]. 计算机工程，2006，32(4)：109-113.

[18] 姜誉，胡铭曾，方滨兴，等. 一个 Internet 路由器级拓扑自动发现系统[J]. 通信学报，2002，23(12)：54-62.