基于重叠网的IPv6网络拓扑保护模型

刘慧生 王振兴 张连成 侯 毅
(解放军信息工程大学 郑州 450002)

摘 要 与IPv4不同,IPv6具有端到端通信、层次化地址结构等新特性,基于NAT掩蔽等手段的网络拓扑传统保护技术不再适用于IPv6环境。然而,现有的IPv6网络拓扑结构保护机制存在破坏端到端特性、难以适用网络层加密等问题。借鉴"隐真"和"示假"的军事思想,提出基于重叠网的IPv6网络结构保护模型。首先提出"重叠隐蔽网"的设计,即通过构建一个具有真实网络前缀的逻辑子网实现对网络真实结构的隐藏,然后给出重叠隐蔽网拓扑动态生成算法,以实现重叠隐蔽网的拓扑结构的动态变化。理论分析与实验测试结果表明,所提模型可有效隐蔽网络真实拓扑结构,并可通过虚假的拓扑结构欺骗攻击者,消耗其攻击资源。

关键词 IPv6,结构保护,重叠网,拓扑动态生成
中图法分类号 TP393 **文献标识码** A

Overlay Network Based IPv6 Network Architecture Protection Model

LIU Hui-sheng WANG Zhen-xing ZHANG Lian-cheng HOU Yi
(PLA Information Engineering University, Zhengzhou 450002, China)

Abstract Different from IPv4, IPv6 has some new properties, such as end-to-end communication, hierarchical address structure. Traditional network architecture protection schemes based on network address translation (NAT) are not in point as before. However, the proposed schemes for IPv6 network architecture protection have some shortages, such as destroying the end-to-end property of the Internet, which leads to prevent the use of IPSec. Motivated by "showing falsity" and "hiding truth" in military tactics, an overlay network based network architecture protection model in IPv6 (ON-NTPM6) was proposed. Firstly, an "Overlay Masking Network" design was presented, which is used to hide the true network architecture by deploying a virtual subnet with true allocated network prefix in the site. Then a topology dynamically generating algorithm was proposed, which is used to dynamically and randomly generate the topology of overlay masking network. Theoretical and empirical analysis results demonstrate that ON-NTPM6 can effectively conceal the true architecture of protected network, and further deceive adversaries and consume their attack resources with virtual overlay network topology.

Keywords IPv6, Architecture protection, Overlay network, Topology dynamically generating

IPv4环境中,人们广泛部署NAT(Network Address Translation,网络地址转换)[1]机制,通过隐蔽网络内部拓扑结构,减少网络的可探测信息,从而有效提高网络防护能力。然而,随着网络技术的不断发展,互联网即将全面过渡至IPv6。考虑到上层应用需要、网络传输效率等因素,IPv6恢复了端到端通信,同时摒弃了NAT机制。IPv4中,基于NAT的网络隐蔽技术已不再适用于IPv6[2]。

摒弃NAT机制后,IPv6提出了临时地址生成机制、NPTv6(Network Prefix Translation version 6)和基于移动IPv6的拓扑保护等机制,以尽可能隐蔽网络结构信息。然而,这些机制都存在一些问题:IPv6地址随机生成机制难以隐蔽网络拓扑层次;NPTv6破坏了IPv6端到端的特性,难以适用于IPsec加密等机制;移动IPv6标准尚在改进,路由优化等改进特性的不断加入,使得基于移动IPv6的拓扑保护机制难以实际部署。

对此,借鉴"隐真"和"示假"的思想,本文提出一种基于重叠网的IPv6网络拓扑保护模型(Overlay Network Based Network Topology Protection Model in IPv6, ON-NTPM6)。首先提出"重叠隐蔽网"(Overlay Masking Subnet, OMS)的概念,为机密网络内部需要与外部网络进行交互的节点构建一个具有真实网络前缀的逻辑子网。这些节点在与外部网络通信时,采用从该逻辑子网获得的前缀,以隐蔽网络内部真实拓扑结构,保护网络拓扑安全。然后给出拓扑动态调整机制,对重叠网的拓扑结构动态随机调整,实现了重叠隐蔽网拓扑的层次化、动态化,以进一步干扰攻击者的探测。

本文第1节介绍相关研究工作和国内外进展情况;第2节讨论所提模型的基本结构;第3节重点介绍拓扑动态生成算法;第4节对所提方案的安全性进行理论分析;第5节通过仿真分析对模型进行验证。

1 相关工作

(1)IPv6网络结构保护

到稿日期:2012-08-27 返修日期:2012-12-01 本文受国家重点基础研究发展计划(2007CB307102)资助。
刘慧生 博士生,主要研究方向为网络信息安全,E-mail:giamo@mspil.edu.cn。

在 IPv6 网络结构保护方面，目前已提出的方案主要有 3 种：临时地址机制、NPTv6 机制和基于移动 IPv6 的 IPv6 拓扑保护机制。

Narten 等提出了临时地址生成机制[3]，利用临时地址生成算法，动态地生成一个具有时效性的主机地址。无状态地址自动配置是 IPv6 的典型特性之一，当用户采用基于主机的 MAC 地址生成地址中的 64 位接口标识时，攻击者可以通过对网卡厂商的分析，极大地缩短主机可能的地址范围，从而有效降低发现 IPv6 主机的难度。而临时地址生成机制可以有效地降低此类安全风险。然而该方法作用有限，攻击者仍可以通过扫描探测等手段探测得到网络的真实拓扑层次等信息。

NPTv6 机制[4]是 IPv6 网络的地址转换机制，与 NAT 原理类似。虽然 IPv6 具有巨大的地址空间，然而管理员出于方便管理等考虑，仍有可能部署地址翻译机制。与 IPv4 的 NAT 不同，NPTv6 的外部地址和内部地址是一对一映射的，外部地址采用全球单播地址，在内部采用只能在本地范围使用的唯一本地地址(Unique Local Addresses，ULA)。NPTv6 机制虽然隐藏了真实地址，但是网络拓扑结构的相关信息如拓扑深度等仍然直接暴露给攻击者，而且 NPTv6 的使用破坏了 IPv6 端到端通信的设计，将导致无法使用 IPsec 加密通信等问题。

还有一种 IPv6 拓扑保护机制是基于移动 IPv6 的 IPv6 网络结构保护机制[5]。移动 IPv6 被设计用于为 IPv6 提供移动性支持。然而在某种程度上，其也可以看成是一种利用了家乡代理进行通信的秘密隧道机制。移动节点将真实的地址作为转交地址(Care-of-Address，CoA)，同时虚构出一个新的家乡地址(Home-of-Address，HoA)作为与外部节点通信的地址，通信数据包则利用家乡代理(Home Agent，HA)通过隧道模式进行传输，由此实现对真实网络结构的保护。然而，在 IETF 的 MIPv6 的协议规范中，为了提高路由的转发效率，进一步设计了路由优化机制，以实现移动节点直接与通信对端节点通信。当开启该功能时，位于外部网络的通信对端节点将同时获知移动节点的 CoA 和 HoA 地址，由此节点的真实地址被暴露在外。

(2)基于重叠网的网络防御

重叠网技术在网络防御方面已得到了一定的应用[6]。其基本原理是将真正的服务器隐藏于重叠网之后，外部的服务请求需经由重叠网里代理服务器传递至内部的真实服务器。因为所有服务是通过代理服务器提供的，所有攻击者想要阻断服务器的服务就必须要攻陷代理服务器。该技术借此将攻击隔离于代理服务器，从而保护真实服务器的安全。Keromytis 等提出的 SOS(Secure Overlay Services)[7,8]是典型的使用重叠网来防御 DDoS 的技术，当使用者需要服务时，必须经由特点的入口点(Access Point)在重叠网中转发至特定主机(Secret Servlet)，再通过这些特定主机转发至真实服务器(Server)。MOVE[9]是另一种类似的技术，差别在于，其通信时是通过服务转移的方式，将 Secret Servlet 和 Server 的通信通过跳板(Stepping Stone)转移至另一台迁移服务器(Migration Server)。

已有的基于重叠网的网络防御技术都是构建应用层的重叠网，以实现对网络服务程序安全性的保护，但是代理服务器的真实 IP 地址等信息仍直接暴露在外部，攻击者仍然可以通过扫描等手段定位到真实目标，从而渗透入代理网络发起攻击。

借鉴“隐真”和“示假”的军事思想，本文提出的 ON-NTPM6 构建了一个独立于物理链路的网络级的重叠网，暴露于外部的地址都是动态的、不真实的地址，从而实现对 IPv6 网络内部结构的保护。

2 基于重叠网的 IPv6 网络结构保护模型

ON-NTPM6 的基本思想是：受保护站点网络首先为所有需与外部通信的节点提供一个独立于物理链路的重叠网，然后周期性地动态变化重叠网的拓扑结构，从而进一步迷惑攻击者，消耗其攻击资源。

首先定义 ON-NTPM6 中的几个重要概念。

定义 1(重叠隐蔽网，OMS)　一个独立于物理链路的逻辑子网；具有独立于其他真实子网的真实网络前缀；由重叠隐蔽网服务器及站点内需与外部通信的节点组成。

在部署重叠隐蔽网时，逻辑子网将被分配一个小于 64 位的网络前缀。这是因为：与 IPv4 中标识子网的位数是可变的约定不同，在通常的 IPv6 部署中没有可变长度子网前缀的表示法。在目前定义的单播 IPv6 地址的单个 IPv6 子网层中，用于区分子网的位数固定为 64 位。而 ON-NTPM6 为了提高对攻击者的干扰能力，需要实现网络的层次化，所以给逻辑子网分配的网络前缀需小于 64 位，而且需要实现的层次越多，分配的前缀就得越小。

定义 2(重叠隐蔽网服务器，OMS Server)　用以控制重叠隐蔽网运行的服务器，是 ON-NTPM6 的核心之一，用以完成站点内节点地址的分配管理等功能。

定义 3(重叠隐蔽网节点(OMS Node)　加入了重叠隐蔽网的节点，是秘密站点内需与外部通信的主机。路标节点(Route Flag Node，RFN)OMS Node 中被选出执行路由器转发行为的节点。一旦节点被指定为路标节点，其除需转发数据外，还需对向外转发的数据包 IP 头的 TTL 值进行－1 处理。

定义 4(重叠隐蔽网配置有效期，OMS Configure Period，OCP)　OMS Server 重新配置重叠隐蔽网拓扑的周期。当配置有效期到期后，需根据在有效期收到的拓扑配置信息重新配置本节点属性等相关信息。

ON-NTPM6 模型的基本结构如图 1 所示。

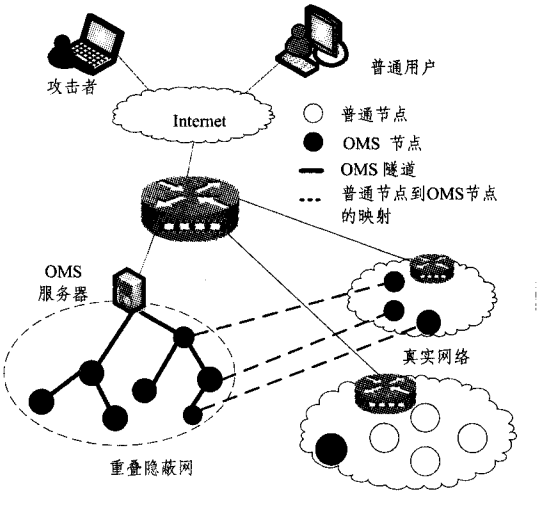

图 1　ON-NTPM6 结构示意图

其中，OMS 内部的数据传递通过 IPv6-in-IPv6 隧道完成。OMS 节点上安装有一个虚拟的网络适配器（与主机网卡上的 IPv6 过渡隧道的接口功能类似），用以通过 IPv6-in-IPv6 隧道发送和接收 OMS 数据。

2.1 基本工作流程

其基本工作流程包括拓扑配置流程和通信流程。

1. 拓扑配置流程

(1)以 OCP 为周期，周期性地从 OMS Server 开始逐层执行重叠隐蔽网拓扑动态生成算法（见第 3 节）。

(2)OMS 节点根据收到的拓扑配置通告，设置下一 OCP 内用于重叠网通信的地址，并通知通信对端节点。

2. 基本通信流程

(1)内部节点向外发送数据

当 OMS 节点需与外部网络通信时，使用 OMS 分配的逻辑子网地址进行通信。通信数据包利用基于真实 IP 地址的 IPv6-in-IPv6 隧道，在重叠隐蔽网中通过若干路标节点逐层转发至 OMS 服务器。

OMS 服务器收到来自 OMS 节点的数据包后，剥除隧道封装，以其中所含的逻辑子网所分配地址作为通信数据包的源地址，将数据包转发至外部网络的目的节点处。

(2)内部节点从外部接收数据

当 OMS 服务器收到来自外部的以重叠隐蔽网地址为目标的数据包时，将其按隧道格式封装，然后利用基于真实 IP 地址的 IPv6-in-IPv6 隧道，在重叠隐蔽网内将其通过路标节点逐层转发至目标节点处。

2.2 通信保持策略

为有效地迷惑攻击者，OMS 的网络拓扑会周期性地随机变化，而内部节点的重叠网地址也会因此发生变化，由此可能导致通信会话的中断。

对此，ON-NTPM6 采用了“过保留”策略，即设置切换时限（Change TTL）。OMS 内的节点在收到新的拓扑通知后，开始启用新地址，但旧的地址以及拓扑在切换时限内仍可使用。即拓扑切换前，部分未结束的会话仍然可以使用旧的地址和拓扑进行通信直到其结束，而新会话则必须使用新地址。当切换时限到期后，不管是否有会话尚未结束，旧地址和拓扑结构都将强行中止使用。

3 重叠隐蔽网拓扑动态生成算法

ON-NTPM6 的核心是动态变化重叠隐蔽网的结构。本节给出重叠网拓扑动态生成算法。通过周期性地从 OMS Server 开始执行该算法，随机逐层生成拓扑结构，从而实现重叠隐蔽网拓扑的动态性且无规律性。

重叠隐蔽网拓扑动态生成算法（Overlay Masking Subnet Topology Dynamically Generating，OMSTDG）是一个随机生成拓扑的算法，通过动态地分配节点实现拓扑的随机化。其中，α 和 h 由管理员在部署 OMS 时指定，RFNnet 是指各路标节点控制的相应重叠子网，n 为路标节点控制的重叠子网内节点总数。

```
OMSTDG(v0,N,α,h)
Input: v0:执行算法的节点
       N:待分配节点集 N={ v1,v2,…,vn}
       α:生成路标节点的概率
       h:剩余拓扑深度
Proc:
(1)Select randomly n·α nodes for composing RFNset,
   //形成 n·α 个下层子网，为每个子网分配下层前缀
(2)Allcoate the rest n·(1-α) nodes into n·α+1 subnets;
   //包括 n·α 个下层子网以及与自己直接连接的子网中；
(3)Send advertise message to vi∈RFNset:Ni,h-1;
   //Ni 是 vi 所辖的节点集合，h-1 是可用的剩余拓扑深度；
(4)For each node vi in RFNset
(5)OMSTDG(vi,Ni,α,h-1);
Proc End
```

4 安全性分析

1. 抗远程探测能力

主动攻击者在发起攻击前，一般需要对网络结构进行探测。其主要通过 ICMPv6 或 TCP 探测节点的存活性，通过 Traceroute 探测网络拓扑[10]。

设攻击者在某个时刻通过其控制的节点对 OMS 所在的站点 A 进行探测，A 中有 m 个存活节点，这些节点在当前网络拓扑的拓扑深度分别为 $Dep_1, Dep_2, \cdots, Dep_m$。

根据 Traceroute 探测过程可知，从探测点到目标点路径上的每个节点都将被 ICMPv6 探测报文请求一次。对于每个探测路径上属于站点 A 的节点，将攻击者探测该目标节点所耗费的时间作为攻击者的探测开销，用 t 表示。

假设攻击者可获知全部存活节点地址，目标是探明具体拓扑，则攻击者在探测站点 A 过程中，探测点所花费的总开销为

$$\sum_{k=1}^{m} Dep_k \cdot t \tag{1}$$

而 ON-NTPM6 方案中，拓扑具有时效性，即任意拓扑结构都只能保存 OCP（重叠网配置有效期）的时间。

所以攻击者成功实施攻击的条件是

$$\sum_{k=1}^{m} Dep_k \cdot t \leqslant OCP \tag{2}$$

由上分析可得：

结论 1 攻击者在采用远程探测的方式对受 ON-NTPM6 保护的站点网络进行攻击时，攻击者成功实施攻击的概率与其探测每个节点所花费的开销以及重叠隐蔽网的拓扑深度有关，且生成的拓扑深度越大，攻击者总开销越大，越难以攻击成功。

2. 抗流量分析能力

被动攻击者主要通过对数据包载荷信息的截获进行分析，获知其中的 IP 地址以及报文各字段值，从而推断出网络拓扑结构以及节点操作系统等信息。受 ON-NTPM6 保护的站点内部节点，在与外部网络通信时，使用的 IP 地址是由 OMS 临时分配的，并不是主机真实的 IP 地址，且其有效期与 OCP 有关，而不是长期有效。由此可得：

结论 2 攻击者无法通过流量截获分析得到主机的真实地址，无法通过被动攻击的手段得到目标网络的真实拓扑结构。

3. 抗渗透攻击能力

假设攻击者已通过其他途径（如社会工程学等）成功发现节点 i 的地址，但不知道其他节点的地址。然后开始对网络内的节点开始攻击、渗透。下面本文将分析在此情况下，系统的安全程度。设拓扑隐蔽网共有节点 M 个，拓扑深度为 h，如图 2 所示。

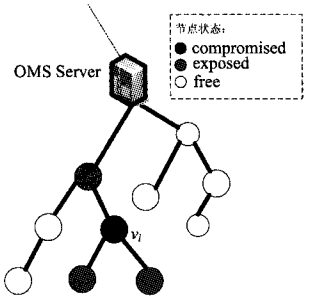

图 2　OMS 受攻击示意图

首先给出节点的 3 种状态：free 表示节点安全，未被攻击者发现；exposed 表示因其下层或上层节点被攻击者控制导致自身真实 IP 地址暴露；compromised 表示该节点被攻击者控制。且因其负责下层节点的转发，所以该节点在当前拓扑中的上层节点和下层全部节点的 IP 地址全部暴露给攻击者，即状态从 free 转换为 exposed。

设攻击者可攻击任意处于 exposed 状态的节点，消耗时间为 t，成功控制目标节点（使节点状态变为 compromised）的概率是 p。

所提方案保护网络失败的条件是：攻击者在 OCP（重叠网配置有效期）内成功使节点集合中比例为 a 的节点处于 exposed 状态时，攻击者已可推知目标站点网络内的全部真实拓扑。

攻击开始时，节点 i 被控，设节点 i 所辖节点共有 m_0 个，拓扑深度为 h_i。

此时，包括 i 及其上、下层节点，被攻击者获知真实地址的节点共有 $S_0=2+m_0$ 个。

假设攻击者已在可忽略的极短时间内从地址缓存等获知 i 和其下层节点的真实地址，接着攻击者将尝试通过攻击上层节点，以期进一步发现节点。

t 时间后，攻击者将以 p 的概率成功拿下 i 的上层节点。

此时，被攻击者获知真实 IP 地址的节点为：

$$S_1=\begin{cases}2+m_1, & \text{where } P=p\\ S_0, & \text{where } P=1-p\end{cases}$$

式中，m_1 表示节点 i 的上层节点 i_1 所辖节点数。

$2t$ 时间后，攻击者将以 p 的概率成功控制 i 的上层节点。

此时，被攻击者获知真实 IP 地址的节点为：

$$S_2=\begin{cases}2+m_2, & \text{where } P=p\\ S_1, & \text{where } P=1-p\end{cases}$$

式中，m_2 表示节点 i_1 的上层节点 i_2 所辖节点数。

由此可推得，kt 时间后：

$$S_k=\begin{cases}2+m_k, & \text{where } P=p\\ S_{k-1}, & \text{where } P=1-p\end{cases} \tag{3}$$

而攻击者停止的条件有 2 种：

(1)可用时间内，发现的节点数目达到 aM 个，攻击成功。

此时，$2+m_k>aM$，即 $a\leqslant\frac{2+m_k}{M}$。

(2)可用时间耗光，即攻击了 OCP 的时间，节点数目仍未达到要求，攻击失败。

此时，$OCP\leqslant kt$。

由上分析可得：

结论 3　目标站点网络的安全程度和 OCP 有关，OCP 越小，即网络拓扑变化越快，攻击者可以实施攻击的时间越有限，也越容易失败。

5　实验分析

本文在 Linux Fedora 13 平台上，实现了 ON-NTPM6 的原型系统，其中 OSM Node 通过部署于主机的客户端实现，利用 OMS Server 分配的地址，通过虚拟出的网卡（OMS Interface）收发通信数据包，如图 3 所示。

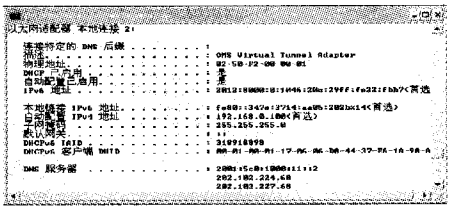

图 3　OMS 虚拟网卡

为了验证 ON-NTPM6 的实际性能，构建测试环境进行实验分析。测试环境如图 4 所示。

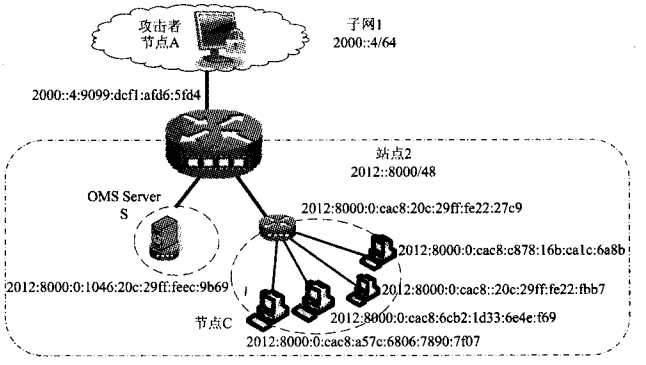

图 4　实验环境拓扑结构示意图

主要由同一路由器连接的两个子网（2012:8000::/48 和 2000:4::/64）组成。其中 2012:8000::/48 为使用 OMS 进行安全防护的站点，2000:4::/64 为攻击者所处的外部网络，2000:4::9099:dcf1:afd6:5fd4 为攻击者 IP 地址。此外，假设攻击者可以获知站点内的全部存活节点的地址信息。

首先分析 ON-NTPM6 为节点通信带来的额外时间开销。在节点 A 处分别部署基于 Apache 和 Xlight 的 IPv6 HTTP 和 IPv6 FTP 服务器，在节点 C 处分别通过 HTTP 和 FTP 远程访问 A 节点上的测试文件，并记录传输时间开销，结果如图 5 所示。

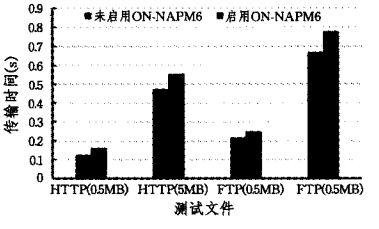

图 5　ON-NTPM6 对节点通信的影响

由实验结果可知，ON-NTPM6 的使用给节点的通信带来了一定的额外时间开销，但开销稳定，约为 15%～18%。这是由于在启用 ON-NTPM6 后，数据在重叠隐蔽网内逐层转发，因此产生了一定的额外时间开销。

然后，测试 ON-NTPM6 的拓扑欺骗情况。首先不对目标网络采用 ON-NTPM6 保护，通过 NMAP v5.91[11] 对目标站点进行探测，探测所得拓扑如图 6 所示。

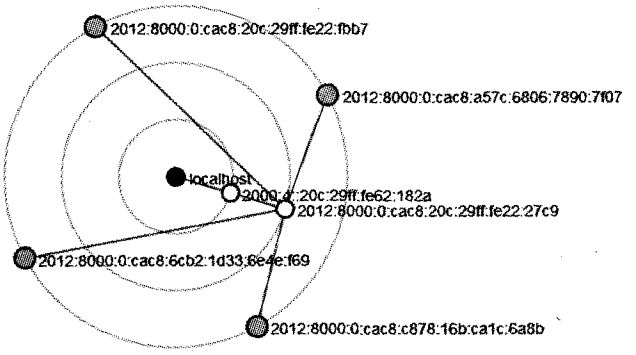

图 6　启用 ON-NTPM6 前 NMAP 拓扑探测结果

由结果可知，在未采取保护措施时，攻击者在获得站点内所有节点信息的情况下，通过探测得到的拓扑结构与网络的真实情况相同。

接着采用 ON-NTPM6 对站点网络进行保护。由于实验节点较少，设置欺骗拓扑深度 $h=2$，生成路标节点的概率为 0.25。再次使用 NMAP v5.91 对目标站点进行探测，探测所得拓扑如图 7 所示。

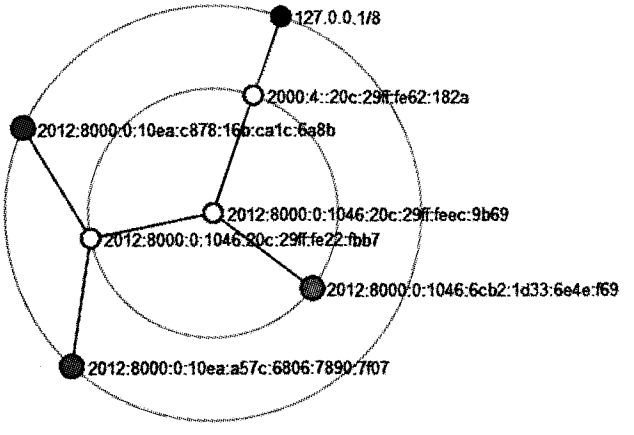

图 7　启用 ON-NTPM6 后 NMAP 拓扑探测结果

由结果可知，当采用 ON-NTPM6 对网络进行保护后，即使攻击者获得了当时全部存活主机的位置信息，但仍然只能得到一个虚假的拓扑结构，如主机节点（地址为 2012:8000:0:cac8:20c:29ff:fe22:fbb7）在启用 ON-NTPM6 后，攻击者通过拓扑探测，认为其是一个路由节点（地址为 2012:8000:0:1046:20c:29ff:fe22:fbb7）。也就是说，ON-NTPM6 能够有效地欺骗攻击者，从而保护目标站点的网络结构安全。

结束语　IPv6 的部署已全面展开。与 IPv4 相比，IPv6 并不是一次简单的协议升级，而是具有了许多改进的特性，如实现了网络层的身份认证、恢复了端到端通信等。这些新特性使得现有的以 NAT 机制为主的网络拓扑保护技术已不再适用。

借鉴“隐真”和“示假”的思想，本文提出了基于重叠网的 IPv6 网络结构保护模型（ON-NTPM6），首先提出“重叠隐蔽网”的设计，通过构建一个具有真实网络前缀的虚拟子网来实现对真实拓扑的隐藏，然后给出重叠隐蔽网拓扑动态生成算法，实现了重叠隐蔽网的拓扑结构的动态变化。理论分析与实验结果表明，所提出的模型可有效隐蔽网络真实拓扑结构，而且能够以虚假的复杂拓扑结构欺骗攻击者，消耗其攻击资源。

参 考 文 献

[1] Srisuresh P, Egevand K. Traditional IP network address translator (traditional NAT)[M]. IETF RFC 3022, Network Working Group, Jan. 2001

[2] Groat S, Dunlop M, Marchany R, et al. IPv6: nowhere to run, nowhere to hide[C]// Proceeding of the 44th International Conference on System Sciences. Hawaii, 2011: 1-10

[3] Narten T, Draves R, Krishnan S. Privacy extensions for stateless address autoconfiguration in IPv6[M]. IETF, RFC 4941, Network Working Group, Sep. 2007

[4] Wasserman M, Baker F. IPv6-to-IPv6 network prefix translation [M]. IETF, RFC 6296, Network Working Group, June 2011

[5] De Velde G V, Hain T, Droms R, et al. Local network protection for IPv6[M]. IETF, RFC 4864, Network Working Group, May 2007

[6] Beitollahi H, Geert Deconinck G. An Overlay Protection Layer against Denial-of-Service Attacks[C]// Proceeding of IEEE International Symposium on Parallel and Distributed Processing. 2008: 1-8

[7] Keromytis A D, Misra V, Rubenstein D. SOS: An Architecture for Mitigating DDoS Attacks[J]. IEEE Journal on selected areas in communications, 2004, 22(1): 176-188

[8] Keromytis A D, Misra V, Rubenstein D. SOS: Secure Overlay Services[C]// Proceeding of ACM SIGCOMM. 2002: 61-72

[9] Stavrou A, Keromytis A D, Nieh J, et al. MOVE: An End-to-End Solution to Network Denial of Service[C]// Proceeding of the ISOC Symposium on Network and Distributed System Security. 2005

[10] 杨柳，李振宇，张大方，等. 冗余最小化的 IPv6 拓扑发现方法[J]. 计算机研究与发展，2007，44(6)：939-946

[11] Lyon G F. Nmap Network Scanning. The Official Nmap Project Guide to Network Discovery and Security Scanning[M]. USA, 2009

（上接第 48 页）

[18] Courtois N, Klimov A, Patarin J, et al. Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations[C]// Proceedings of International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT). Lecture Notes in Computer Science. 1807, Belgium: Springer, 2000: 392-407

[19] Ding J, Buchmann J, Mohamed M S, et al. MutantXL[C]// Proc. Symbolic Computation and Cryptography. Beijing, 2008: 16-22

[20] Mohamed M S, Mohamed W S, Ding J, et al. MXL2: Solving polynomial equations over GF(2) using an improved mutant strategy[C]// J. Buchmann, J. Ding, eds. Post-Quantum Cryptography-PQCrypto 2008 (Cincinnati, 2008). Lect. Notes Comput. Sci. 5299. Berlin: Springer, 2008: 203-215

[21] Mohamed M S E, Cabarcas D, Ding Jin-tai, et al. MXL3: An efficient algorithm for computing Gröbner bases of zero-dimensional ideals[C]// Proceedings of ICISC 2009. Lect. Notes Comput. Sci. 5984. Springer, 2010: 87-100

[22] Webster A, Tavares F, Stafford E. On the design of S-boxes[C]// Advances in Cryptology-Crypto'85. Lecture Notes in Computer Science 218. New York, NY: Springer-Verlag, 1985: 523-534