基于网络特征混淆的欺骗防御技术研究

赵金龙，张国敏，邢长友
（陆军工程大学指挥控制工程学院，江苏 南京 210001）

摘　要：网络攻击之前通常有侦查阶段，攻击者通过流量分析和主动扫描等技术获取目标系统的关键信息，从而制定有针对性的网络攻击。基于网络特征混淆的欺骗防御是一种有效的侦查对抗策略，该策略干扰攻击者在侦查阶段获取的信息，从而使攻击者发动无效的攻击。对现有混淆欺骗防御方案的技术原理进行了分析，给出了网络混淆欺骗的形式化定义，并从 3 个层次对现有的研究成果进行了讨论，最后分析了混淆欺骗防御技术的发展趋势。

关键词：网络侦查防护；拓扑混淆；侦查欺骗；欺骗防御
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.2096−109x.2021045

Research on deception defense techniques based on network characteristics obfuscation

ZHAO Jinlong, ZHANG Guomin, XING Changyou
Command & Control Engineering College, Army Engineering University, Nanjing 210001, China

Abstract: There is usually a reconnaissance stage before a network attack, the attacker obtains the key information of the target system through techniques such as traffic analysis and active scanning, to formulate a targeted network attack. Deception defense techniques based on network characteristics obfuscation is an effective strategy to confront network reconnaissance, which makes the attacker launch an ineffective attack by thwarting the attacker's reconnaissance stage. The technical principle of the existing obfuscation defense solutions was analyzed, the formal definition of network obfuscation was given, the existing research works were discussed from three aspects, and finally the development trend of the obfuscation deception defense technique were analyzed.

Keywords: network reconnaissance protection, topology obfuscation, reconnaissance deception, deception defense

收稿日期：2020−06−06；**修回日期：**2021−01−20
通信作者：张国敏，zhang_gmwn@163.com
基金项目：国家自然科学基金（61572521）；武警工程大学科研创新团队科学基金（KYTD201805）
Foundation Items: The National Natural Science Foundation of China (61572521), The Scientific Foundation of the Scientific Research and Innovation Team of Engineering University of PAP (KYTD201805)

论文引用格式：赵金龙, 张国敏, 邢长友. 基于网络特征混淆的欺骗防御技术研究[J]. 网络与信息安全学报, 2021, 7(4): 42-52.
ZHAO J L, ZHANG G M, XING C Y. Research on deception defense techniques based on network characteristics obfuscation[J]. Chinese Journal of Network and Information Security, 2021, 7(4): 42-52.

1　引言

大量研究表明，网络攻击之前通常伴有侦查阶段。有研究指出 70%的攻击活动之前都存在侦查行为[1]，一次网络攻击中平均 45%的时间用在了在侦查阶段[2]。因此，在网络杀伤链[3]等研究定义的攻击模型中，都将网络侦查作为网络攻击的第一个阶段，如图 1 所示。网络侦查能够帮助攻击者有效地识别潜在目标及其漏洞，为其提供战术优势[4-5]。攻击者通常采用各种扫描器或定制化工具去扫描目标网络和系统，以获取相关信息，包括网络拓扑（节点关系、链路带宽、路由表、MAC 地址、IP 地址、操作系统）和服务及服务依赖关系等，并依赖这些网络的特征信息来识别可供利用的主机和漏洞，从而制定高效的攻击方案。例如，高级持续威胁 APT，社会工程学攻击等网络攻击的实施都依赖于网络侦查结果[6-7]。

因此，缓解网络侦查是一种有效的防御策略。然而，传统的计算机网络的静态特性使对抗网络侦查面临着很大的挑战。一方面，攻击者可以在发起攻击前几天或几年对目标系统的防御进行侦查，侦查面[8]的静态性使攻击者能够不断进行网络侦查和攻击尝试，以识别能被利用的漏洞；另一方面，在网络侦查期间，攻击者一般会采取躲避侦查的措施，尽量使用合法的工具和命令、低速的探测流量，从而使恶意探测活动难以与合法活动区分开来。一些被动式的侦查方案，如网络窃听[8]、流量分析[9]等由于其隐身的特点，更加难以被察觉。

为了应对这种攻防不对称引起的安全防御问题，学术界和产业界提出了主动防御的解决方案，包括移动目标防御[10]、拟态防御[11]、欺骗防御[12]等，欺骗防御解决方案因为其有效性和便捷性受到广泛的关注。欺骗防御技术利用攻击者依赖收集到的信息制定下一步的攻击计划这一特点，为攻击者提供错误的信息来迷惑攻击者，从而误导攻击者的行为。从博弈论的角度也可以证明对入侵者实施欺骗要比在发现入侵时直接驱逐入侵者获取的收益要高[13-14]。因而，在侦查阶段对攻击者实施欺骗是很有必要的。

基于网络特征混淆的欺骗防御技术正是用于应对网络杀伤链的侦查阶段，旨在防止攻击者获取关于网络结构的真实知识，防范主机探测[15]、拓扑发现[16]、指纹扫描[17]等网络侦查技术。本文梳理了近年来关于对抗网络侦查技术的混淆欺骗防御方案，结合已有的描述给出了网络混淆欺骗防御的形式化定义，分析了网络混淆欺骗防御设计中面临的关键问题和常用的技术原理，并从 3 个层面介绍了不同方案的特点，最后总结分析了这一研究可能的发展方向。

2　网络混淆欺骗防御的形式化定义

基于网络特征混淆的欺骗是欺骗防御的一种形式，旨在防止攻击者探查网络结构的真实信息，以保护网络中的关键链路、关键节点和服务。按照 Yuill[18]给出的计算机安全欺骗的定义，网络混淆欺骗防御是为了误导攻击者对网络结构的认知而采取的行动，以提升网络的安全。

现有的一些研究工作中，也给出了关于网络混淆欺骗防御的定义。Kelly 等[19]提出网络混淆类的欺骗表示在网络不同节点上设置虚假但可操作的视图，以便在扫描器成功之前检测到它，利用欺骗性的路由信息将扫描流量定向到一个诱饵节点上，使扫描变慢或无用。Achleitner 等[7]提出了应对内部攻击者的网络混淆欺骗防御的形式化定义：利用动态地址转换、路由突变、恶意流动态检测等操作，将一组网络特征集合 NF = {TL=主机在拓扑中位置，NH=主机数量，AH=主机地址，CH=主机间连接，LB=链路带宽，HD=主机时延}映射到另一组网络特征集合 NF'，从而使攻击者获得错误的网络信息集 T'，最小化 T' 的可用性。

网络混淆欺骗防御是攻防双方对网络侦查面的配置和认知的一个交互过程，上述的定义针对的是特定的场景，不够清晰和全面。因此，为了

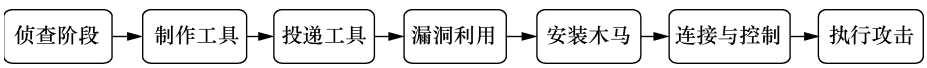

图 1　攻击链模型
Figure 1　Kill chain model

进一步明确网络混淆欺骗防御的含义，结合文献[20]中对欺骗防御的形式化定义，本文对上述的定义进行补充和完善，给出更准确的网络混淆欺骗防御的形式化定义。

定义网络的基本特征为 NF，NF 是一个包含节点集合 S 和节点关系集合 C 的集合， NF= {S, C}。其中 $S=\{s_1, s_2, \cdots, s_n\}$，$s_i$ 代表单独的一个网络节点，是一个包含所有和构建网络侦查面有关的信息的集合，包含节点的 IP 地址、MAC 地址、节点在网络中的位置、节点开放的端口、运行的操作系统和服务及其版本等信息。C 表示节点间的连接关系、转发关系、链路带宽、时延等和链路拓扑有关的信息。

定义网络信息的侦查者为 Viewer，表示通过观察网络信息来获取关于网络的知识的操作者，Viewer= {Defender，User，Attacker}。其中防御者（Defender）拥有关于系统的所有权限，可以配置、修改网络特征的表现形式。普通用户（User）只使用防御者分配给他的功能，防御者要考虑修改网络特征对普通用户的影响。攻击者（Attacker）对网络进行侦查，企图获取关于网络的更多真实信息。

定义由基本的网络特征 NF 构成的系统侦查面为 RS，RS 代表一个侦查者 Viewer 可以获取的关于网络特征的信息集合 T。当侦查者 Viewer 代表防御者时，RS = NF，防御者可以完全获取系统的所有信息。一个普通的侦查者（普通用户或者攻击者）可以观察到的侦查面 RS 是 NF 的一个子集或者一个与 NF 存在部分交集的集合 T'。对一个攻击者而言，在极端情况下，集合 T'为空集。

定义网络混淆策略为 Trick，防御者通过一系列技术手段，如 IP 地址跳变、拓扑突变、设置蜜罐等，操纵网络特征的表现形式，构成虚假的侦查面 RS，可以表示为 RS = Trick(NF)，尽可能地误导或者延缓攻击者获取网络特征的真实信息，从而达到保护己方系统的目的。

基于以上的定义，可以将网络拓扑混淆欺骗防御形式化定义为四元组形式：Obfuscation- deception=(NF，Viewer，Trick，RS)。攻击者的目标是根据对系统暴露的侦查面 RS 的侦查分析，获得关于目标网络特征的最大信息集合，防御者通过混淆手段展示出虚假的侦查面，降低攻击者获取的信息集的可用性，这是一个攻防双方不断博弈的过程，如图 2 所示。

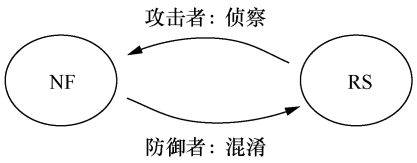

图 2 网络混淆欺骗防御模型

Figure 2 Cyber obfuscation deception defense model

3 网络混淆欺骗防御设计

网络混淆欺骗防御的根本目标是通过修改网络特性，控制攻击者通过网络侦查收集到的信息集，最大限度地降低这些信息的可用性。因此，如何有效地修改网络特征是各项研究考虑的重点。混淆方案的设计必须满足安全属性要求。一方面要保证安全性，即防御者要对系统中各个用户的行为完全可分辨可控制，系统不能被非法修改、非法利用，不能被当作入侵真实系统的跳板，而攻击者无法分辨真假信息，不能访问被防护的信息。另一方面，混淆方案要保证系统的可用性，对合法用户和正常业务的影响要在可接受的范围，这是反映混淆方案好坏的一个重要指标。在这些安全属性约束的约束下，混淆方案的设计过程中面临的主要挑战有以下 3 点。

（1）混淆方案的有效性

混淆欺骗防御的基本方法是隐藏某些真实信息或者显示虚假信息，但可用性是网络安全防御的基本需求。混淆不应该影响正常业务的使用，这就必须要求在使用欺骗的时候显示某些真实的信息，如邮件服务器的域名。因此，设置混淆方案的关键是如何在真实的信息中混合虚假的信息，保证虚假信息的可信性，使攻击者难以将真实信息和虚假信息区分开来。

（2）混淆方案的可控性

虚假信息越多，攻击者分辨真伪所花费的时间也就越多。但大量采用虚假信息来混淆网络特征将不可避免地对合法用户产生影响。虚假信息可以诱使攻击者采取行动，但合法用户和服务也可能对一条虚假信息做出响应。而误报不仅会增

加防御者的工作负担，还会降低警报的效用。因此防御者需要控制注入虚假信息的成本，即混淆方案造成的影响要在可控的范围内。因而，防御者要在有效性和可控性之间做出权衡。

（3）混淆方案的生存周期

攻击者会观察与网络环境的交互情况，并动态调整攻击策略。即攻击者对网络特征真实信息的推测伴随着攻击的整个过程，因此，混淆方案必须能够根据对手意图动态地、自主地进行更改。然而，关于混淆方案的动态调整周期和调整时机，学术界目前并没有明确的解决方案。过于频繁的变化会带来不可接受的性能损耗和潜在的拒绝服务攻击隐患，过长的周期又会造成防御方案泄露的风险。

为了应对混淆欺骗防御设计中的挑战，学术界提出了各种解决方案。目前，常用的混淆方案按照其技术原理基本可以分为 3 类，如表 1 所示。

（1）诱饵式混淆

通过设置有诱惑价值的虚假节点（一般指含有漏洞的节点）来吸引攻击者的注意力，诱使攻击者访问这些虚假节点，从而达到延缓攻击者侦查速度或预警的目的。这类方案通过少量高价值的虚假信息来控制混淆的有效性和可控性，并通常在较长的周期内保持不变。最常见的是蜜罐技术[21]，通过混淆网络的结构，在扩大节点空间的同时改变网络中节点的价值分布。例如，高交互蜜罐技术，通过伪装有漏洞的主机或服务来吸引攻击者[22]，如图 3 所示。诱饵式混淆方案通常用于收集攻击者的信息情况，高价值的诱饵节点需要高昂的配置成本。此外，防御者要确保诱饵节点的安全性，因为含有漏洞的诱饵节点容易被攻击者当作渗透的跳板。

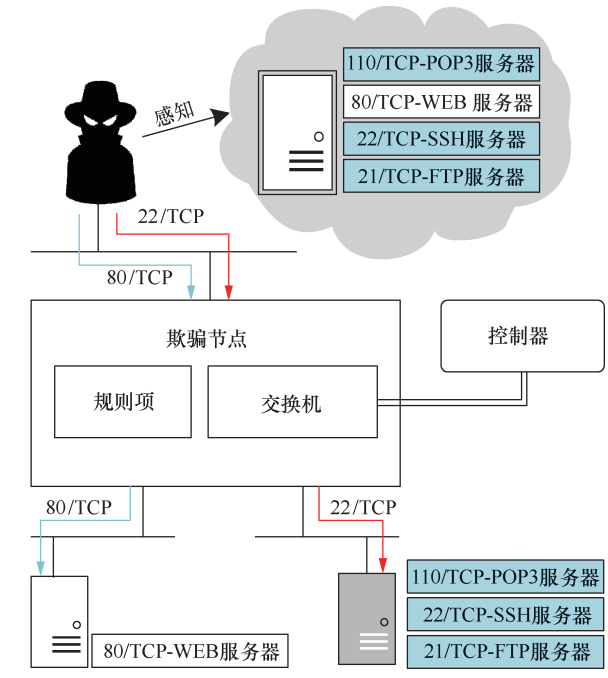

图 3　利用高交互蜜罐来保护关键节点的混淆方案

Figure 3　Obfuscation scheme using high-interaction honeypots to protect key nodes

（2）空间类混淆

通过设置大量低价值的虚假资源，如 IP 地址、开放端口号等来提供一个巨大的攻击面[23]，增大攻击者的搜索和判断空间，从而隐藏真实资源，以延缓攻击者攻击速度，降低其攻击成功的概率。与诱饵式混淆相反，这类方案通过大量轻量级的虚假信息来混淆真实信息，而合法用户一般对这类虚假信息不感兴趣，因此不会对合法用户造成较大干扰。同样地，这类方案也会在较长的周期内保持不变。如开源软件 Honeyd[24]可以让一台主机在网络中模拟多达 65 536 个地址，FORMALTECH 公司的防御方案 CyberChaff[25]，通过在网络中引入数百甚至数千个虚假的轻量级

表 1　网络混淆欺骗防御的基本方案

Table 1　Typical methods of cyber obfuscation deception defense

混淆方案	原理	方法	典型研究
诱饵式混淆	设置有诱惑价值的虚假节点，改变网络的节点价值分布	蜜罐、蜜饵、蜜标	DressUp[22], SDhoneynet[26]
空间类混淆	设置大量轻量级的虚假资源，扩大真实资源的分布空间	轻量级虚拟机、大量开放端口、活跃 IP 地址	Honeyd[24]，CyberChaff[25]
动态变化混淆	展示错误的或者动态变化的信息，增加系统的不确定性	指纹伪装、拓扑突变、IP 地址随机化	NetShifter[27], PLD-Logic[28]

节点来混淆真实主机的位置，如图 4 所示。部署空间类混淆方案需求的资源较小，易于部署，但通常只有大量的虚假节点才能达到防护的效果，在路由跳变空间等可选空间受限的情况下则难以部署。

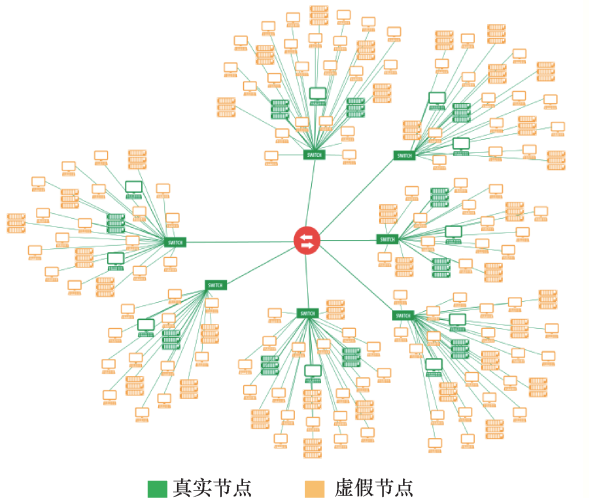

图 4　CyberChaff 混淆方案
Figure 4　Obfuscation solution of CyberChaff

（3）动态变化混淆

通过向攻击者披露错误的或者动态变化的系统信息来增加不确定性从而提升侦查难度，拓扑突变、IP 地址随机化等技术都是通过动态变换系统信息来迷惑攻击者。动态变化或错误的信息可以有效混淆真实信息，但对合法用户的影响也更加显著。因此为了更好的混淆效果，通常需要牺牲一部分合法用户的利益。这类方案通常有明确的变化周期，如随机变化[27]或者基于事件[28]来变化策略。伪蜜罐[29]通过使真实系统具有蜜罐的特征从而吓退攻击者，操作系统混淆方案[28]通过更改或者隐藏操作系统的特征来隐藏操作系统的真实信息。例如，文献[28]通过依照概率来随机应答攻击者的扫描探测，让攻击者无法获取准确的操作系统和服务的信息，从而提升侦查难度。这类方案通常会对合法用户造成较大影响，动态变化的信息会对系统性能造成很大的损耗，而错误的信息可能会影响合法用户的操作。

4　网络混淆方案分类

4.1　分类方法

针对网络欺骗防御技术，各类文献中提出了多种分类方法[30-32]。一种常用的方式是按照欺骗所采用的方法的属性进行分类，文献[20]从欺骗环境构建的角度将欺骗方法分为了掩盖、混淆、伪造、模仿 4 类。这里的混淆是指通过更改系统资源的特征使系统资源看上去像另外的资源，如拟态防御。由于混淆欺骗防御往往包含多个方面，这种分类方式并不能清晰地区分已有的研究工作的特点。文献[12]中作者提出从欺骗的目标、欺骗的单元、应用欺骗的层及其部署模式 4 个维度进行分类的方法，综合考虑了欺骗技术的各个方面。但这样的方式过于复杂，不能突出各种技术的主要思想。

另一种常见的分类方式是根据欺骗技术部署的位置进行分类。Cohen[31]提出根据应用欺骗的位置，从最低的硬件层到最高的应用程序层，对欺骗技术进行分类。Pingree[32]等进一步提出了一个 4 层的分类方式，即网络层、系统层、应用程序层和数据层欺骗。文献[20]也采用了同样的分类方式划分了欺骗技术的层次结构。按照这类分类方式，基于网络特征混淆的欺骗技术则属于网络层的欺骗技术，通过网络可以直接访问的技术，是不依赖于特定的主机的，考虑的是欺骗节点和节点特征在己方网络中的部署问题和资源的隐藏问题。

按照上述讨论，需要更细粒度的划分方式来分析已有研究工作的相似性和差异性，以便为往后的工作提出指导。基于网络特征混淆的欺骗防御技术主要用于防止攻击者侦查网络结构信息，而网络结构体系包含 3 个层次：表示网络节点间连接关系的拓扑，网络节点和节点上运行的系统和提供的服务。各个层次的组成和功能有很大差异，特征信息也不相同，因而针对各个层面的防护方案也各不相同（如表 2 所示）。以系统指纹来统一指代节点上运行的系统和提供的服务，则在层次法划分的基础上，按照网络结构体系，可以将基于网络特征混淆的欺骗防御技术分为基于拓扑和基于端节点、基于系统指纹 3 个层面。

4.2　拓扑混淆

网络拓扑指的是节点的连接关系和转发关系，是构建网络基础功能、进行网络诊断和故障定位所需的基本信息。然而，网络拓扑知识也可

表 2　网络混淆欺骗防御方案概述
Table 2　Overview of cyber obfuscation deception defense solutions

层次结构	防护目标	应对的威胁	典型工具	防御方案
拓扑防护	关键链路、网络拓扑	LFA、拓扑推断	Traceroute、RIPE atlas	报文重路由[6,26,33]，覆盖网络[34-35]，拓扑突变[36-39]
端节点防护	关键资源、端节点的角色和位置	主机扫描、网络窃听、端口扫描	Sniff、ping、Iris、Nmap	Honey-X 技术[40-43]，主机虚拟视图[7, 44-46]，报文随机化[47-53]
系统指纹防护	节点运行的操作系统和服务及其版本	指纹扫描、漏洞探测	SinFP3、p0f、Nessus	高交互蜜罐[22, 54-55]，动态信息响应[56-59]

以被攻击者用来规划更精确更有效的攻击，如链路泛洪攻击（LFA，link-flood attack）[60-61]。因此针对拓扑的混淆欺骗防御的主要目的是保护拓扑的关键链路等信息免于被攻击者发现，防范拓扑推断和链路洪范等攻击。

LFA 攻击要求攻击者了解目标网络的拓扑结构和转发行为, 利用网络的链路图来确定目标链路。典型的缓解 LFA 攻击的主动防御技术是重路由 traceroute 探测分组。如 Trassare 等[6]构造了一种基于智能路由器的欺骗网络，其关键思想是确定网络中关键的节点，通过添加虚拟链接使该节点的中心度最小化，然后由智能路由器在边界响应 traceroute 包，伪装虚拟节点的应答，以欺骗恶意的 traceroute 探测并影响攻击者推断的网络结构。Kim 和 Shin[26]提出了一种基于 SDN 的蜜网 SDHoneyNet，通过向攻击者提供虚假链路图来主动地、预防性地缓解 LFA。它通过将 traceroute 数据包重定向到虚拟网络拓扑，防止恶意流量到达瓶颈链路来达到隐藏关键链路的目的。WANG 等[33]中提出了一种链路混淆算法，将潜在的 LFA 目标链接隐藏起来，防止被攻击者发现。隐藏目标链接的方法也是改变来自恶意攻击节点的 traceroute 包的路由，使目标链接不出现在路径中，并向对手提供伪造的具有很高流量密度的链接映射，从而使攻击者误以为某些诱饵链路是目标链路。

这种基于报文重路由的方案，对没有足够冗余路径的拓扑的保护程度有限。因此，文献[62]提出将网络功能虚拟化应用到网络中，以扩展网络拓扑的多样性。通过向网络中添加虚拟阴影网络（VSN），以虚假的拓扑信息欺骗攻击者，而不暴露真实的网络拓扑和特征，以解决可用的备选路由受网络拓扑限制的问题。

基于重路由 traceroute 包的解决方案难以应对流量统计分析技术，因此一些文献提出通过构建虚拟覆盖网络来隐藏真实网络结构。如文献[34]提出了一个链路拓扑混淆框架 NetHide 来应对 LFA 攻击，NetHide 通过在数据平面上直接拦截和修改路径跟踪分组来混淆拓扑，它在保持路径跟踪工具的实用性的同时，减轻了 LFA。NetHide 的关键思想是将网络混淆描述为一个多目标优化问题，允许在安全性和可用性之间进行灵活的权衡。与之类似的还有文献[35]，作者通过引入网络掩码器来混淆分布式系统的真实网络拓扑，防止攻击者发现和滥用分布式信息系统的节点。

此外，还有利用 MTD 技术来应对拓扑发现攻击的技术，包括频繁的 IP 地址变换、网络配置自适应、网络拓扑突变、路由信息动态变化等，这些方法都旨在网络级别迷惑攻击者。典型的拓扑突变技术如图 5 所示，在探测到 traceroute 包后，将随机变化这些包的路由，如红色线路所示，防止攻击者获取网络真实的转发路径。文献[27]提出了一种基于 SDN 的全面的多维网络混淆和欺骗解决方案 NetShifter，该方案利用 SDN 和虚拟化技术，集成了报文头部随机化、主机/服务器 IP 地址突变、路由/流突变、拓扑突变技术，同时变异和随机化网络配置的多个方面，每个方面都增加了网络攻击者必须分析的复杂性维度，并利用 GRE/VPN 隧道技术解决了拓扑突变空间受物理子网限制的问题。文献[36]提出了一种应对针对关键链路的间接 DDoS 攻击的解决方案 MoveNet，通过使用虚拟网络（VN）提供对关键网络资源的持续、动态、威胁感知分配，增加多个 VN 的关键链路的不确定性，以此来欺骗攻击

者对关键网络资源的探测。其他路由跳变技术参考文献[37-39]，文献[37]提出了一种基于覆盖网络的路由随机化方法，文献[38]中提出可以通过使用 SDN 来实现高效、可定制的路由随机化方案，文献[39]中描述了一个通过不断重路由流量来避免链路攻击的防御系统。

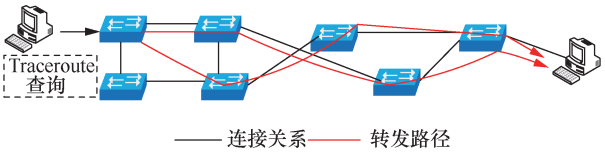

图 5　典型的拓扑突变技术
Figure 5　Typical topology mutation technique

4.3　端节点混淆

网络中端节点指代终端主机和服务器，作为承载重要数据和提供服务的重要载体，一直是网络攻击的重点。DDoS 攻击和网络渗透都依靠关键节点的角色识别和真实 IP 地址确认，攻击者通过流量窃听[8]和主机扫描[15]、端口扫描[63]等手段确定活跃主机 IP 地址和重要节点。因此，针对端节点的混淆欺骗防御的主要目的是保护关键节点和节点特征免于被攻击者发现，主要防御主机发现和端口、指纹探测等攻击。

典型的混淆方案是通过 honey-X 技术来伪装对攻击者的扫描查询的应答，从而吸引攻击者的注意力。如文献[40]提出使用蜜罐网络来延缓攻击者的渗透速度，依据计算机网络的逻辑布局，通过在网络的关键点上添加分散注意力的集群和相互连接的虚拟机集合来修改网络拓扑，引诱对手去探索无用的信息，降低入侵者到达目标主机的概率。Openfire[41]使用防火墙将不需要的消息转发给诱饵机，使所有端口看起来都是打开的，从而诱使攻击者将目标对准虚假服务。此外，Honeyd[24]和 DTK[30]工具都可以通过生成多个虚假服务和网络 IP 地址来欺骗攻击者，使他们攻击虚假目标。

蜜网技术则是通过构建一个安全可控的环境，通过高交互蜜罐响应攻击者的侦查扫描，伪装漏洞服务，从而吸引攻击者的注意力。文献[42]则提出了一种嗅探反射技术，通过在网络入口利用 Snort 入侵检测系统来检测可能的网络侦查数据包，并将其转发到影子网络。在影子网络中，生成扫描响应以混淆攻击者对网络的探查。而文献[43]则关注攻击者入侵内网的主机后并试图进一步侦查感染网络时，将通信重定向到具有相同配置的欺骗网络，从而最大限度地减少对操作数据和资产的进一步破坏。类似的，通过沉洞（sinkholing）攻击[41]，将恶意流量重定向到模拟真实终端行为的粘性蜜罐（tarpits）[64]上，创建粘性连接来减缓或阻止自动扫描，并迷惑对手。

大量的文献研究通过为主机分配虚拟视图来延缓主机探测攻击。Achleitner 等[7]提出了一种基于软件定义网络的侦查欺骗系统（RDS）来防止网络内部的攻击者获取网络的更多信息，通过仿真网络拓扑和物理特性，为不同节点分配不同的虚拟视图来欺骗恶意主机发现攻击，限制攻击者获取到的真实网络的细节，如图 6 所示。该方案旨在

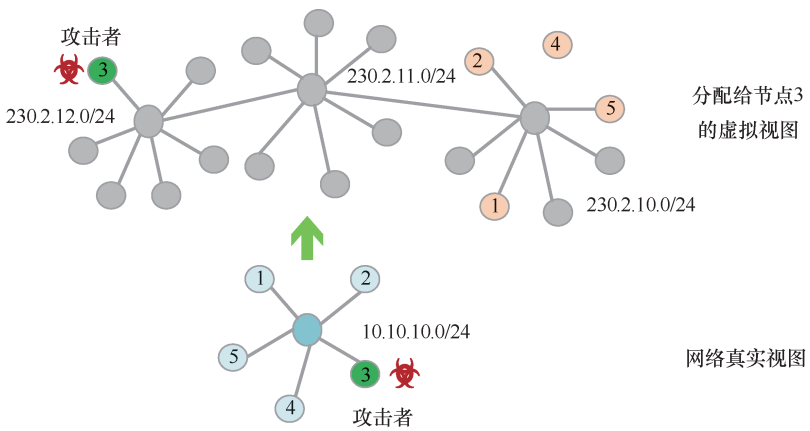

图 6　Achleitner 等提出的虚拟视图方案
Figure 6　The virtual view scheme proposed by Achleitner et al

限制性能对良性网络流量的影响的同时，有效延迟敌方发现脆弱主机的过程，并在网络中识别敌方侦查的来源。在此基础上，XU 等[44]提出将真实网络拓扑按照物理结构划分为不同的分组，分别实施不同欺骗策略，解决了文献[7]中由于单台欺骗服务器在网络规模变大时带来的性能约束。Kelly 等[19]在文献[7]的基础上，利用遗传算法分析了防御方和攻击方的最优配置策略，为提供有效的欺骗视图指出了指导。

与文献[7]类似，Robertson 等[45]提出了一种定制信息网络 CINDAM，同样为网络上的每个主机创建一个临时的虚拟网络视图，从而将网络的恒定拓扑结构转换为欺骗性的、可变的和个性化的拓扑结构，防止攻击者探测主机信息。文献[46]描述了一种自适应网络欺骗系统 ACyDS，ACyDS 为企业网络中的每个主机提供一个唯一的虚拟网络视图，并且可以动态生成和改变每个主机的网络视图，防止入侵者入侵网络中的主机。

随机化技术也是一种主要的端节点的混淆欺骗防御手段。网络地址空间随机化（NASR）[47]通过修改动态主机配置协议（DHCP）服务器，频繁改变系统 IP 地址。自屏蔽动态网络结构（SDNA）[48]通过重写进入和离开操作系统的数据包，以防止从主机观察到网络中的真实地址。类似的 IP 地址跳转解决方案还有 OF-RHM[5]，SDN Shuffle[49]。

为了应对网络窃听，流量分析等手段引起的通信双方身份识别，关键节点定位等攻击，还有大量关于匿名通信系统的研究。基于 SDN 交换机的 IP 地址变换策略如图 7 所示，通过在入网节点对主机的 IP 地址进行映射，来达到隐藏主机真实 IP 地址的目的[27]。文献[50]中，作者提出了一种利用 IPv6 承载加密的真实 IPv4 地址的匿名通信系统 SPINE，来防止数据包在通过不可信网络时泄露通信方的信息。文献[51]中提出了一种匿名系统 iTAP，在网络边缘将报文头部重写为可变的随机标识符，防止大型局域网中网络窃听。文献[52]中提出了在数据中心网络中隐藏通信方真实身份、防止攻击者推断关键节点的匿名系统 MIC。文献[53]中研究了无线网络中节点角色的隐藏问题，防止攻击者通过流量分析识别出网络中的关键节点。

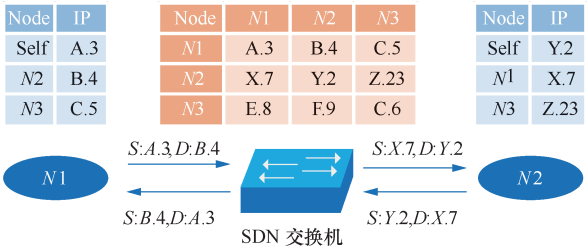

图 7　基于 SDN 交换机的 IP 地址变换策略

Figure 7　IP address mutation strategy based on SDN switch

4.4　系统指纹混淆

由于大多数安全漏洞依赖于操作系统，因此攻击者在确定攻击目标在网络中的位置和 IP 地址后，需要了解目标系统的操作系统版本、应用版本和配置，以便制定进一步的攻击策略。攻击者可以通过被动嗅探、收集和分析主机间传送的数据包，也可以主动向目标主机发送精心设计的数据包并分析响应来实现系统指纹分析[17]。针对系统指纹的混淆主要目的是保护节点特征免于被攻击者发现，防御指纹探测类攻击。

防御指纹探测常用的方式通过伪装有漏洞的主机或服务，并通过这些服务的特征混淆真实系统的特征，最常见的是高交互蜜罐技术。如文献[22]通过设置含有多个漏洞服务的影子服务器来干扰攻击者对真实系统服务的判断。文献[54-55]利用了代理服务器来实现保护 Web 服务的欺骗框架，来防止对 Web 应用程序的探测和攻击。

另一种常用的技术是通过向攻击者展示错误的或者动态变化的信息来迷惑攻击者。典型的如伪蜜罐[29]通过修改系统特征，从而使真实系统具有蜜罐的特征从而吓退攻击者。Jajodia 等[28]提出了一种基于概率逻辑理论（PLD-Logic，probabilistic logic of deception）的欺骗防御方案来防护企业网，通过为各种扫描查询提供真假混合的响应，来增加攻击者的攻击时间和成本，并通过计算给定约束条件下回答攻击者扫描查询的最佳方法，来最大化欺骗的效果。文献[23]将给定系统的设备、设备间的连通性、设备提供的服务等信息形式化为系统视图，并定义了不同视图之间的距离，通过创建满足指定视图距离等期望的最优虚拟视图来防御攻击者对系统指纹的探测攻击。具体如图 8 所示，通过将外向数据包中所有可能泄露操作系统有关信息的特定域修

改为欺骗性的签名，使攻击者通过 Sinfp3 等工具探测时获取到错误的结果，如图中将服务器识别为打印机。Watson[56]等为了避免暴露特定信息，限制攻击者探测受保护主机操作系统的能力，采用了协议过滤器来修改网络实现的特征，与之相似的还有文献[57]。Malecot[58]介绍了一种通过随机连接跳转和流量伪造来随机化指纹探测的技术，从而达到迷惑攻击者的目的。文献[59]提出了一种欺骗防御架构 CHAOS, 通过使用主机突变混淆、端口混淆和基于诱饵服务器的混淆，灵活地转发和修改网络中的数据包，模糊攻击面，降低攻击者嗅探网络流量的能力，防止目标主机的真实信息泄露。

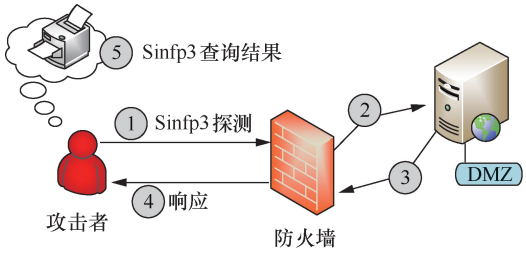

图 8　操作系统指纹混淆方案

Figure 8　Operating system fingerprint obfuscation scheme

5　未来研究方向

虽然现在已围绕网络特征混淆欺骗防御做了大量的研究工作，提出了很多有效的系统框架和解决方案，但网络攻击呈现出多样化、复杂化、规模化等特点，攻防对抗的形势日趋严峻，在此情况下，有必要从以下 3 方面加强网络特征混淆欺骗防御技术的研究。

（1）基于人工智能的自适应、智能化的混淆框架研究。攻击者的侦查时间和手段多变，网络侦查技术日渐复杂，需要更加复杂的混淆策略来应对不同的防护场景。因此，利用机器学习、人工智能技术，研究能够自适应调整混淆策略，智能化响应攻击者行为的混淆欺骗防御框架十分有必要。

（2）基于 SDN 等新兴网络技术的可定制化、可伸缩性的部署方案研究。不同的业务环境和防护需求使部署混淆方案变得十分不便，如何基于 SDN 可编程网络平台、微服务、网络功能虚拟化等新兴网络技术解决按照用户需求和使用场景定制混淆方案、弹性可伸缩的部署混淆方案将是未来的重要研究方向。

（3）量化的混淆效果评定。目前欺骗防御缺乏明确的评价指标和测试方法，导致在实际部署中存在大量冗余，难以达到最优效果。学术界也在积极探索量化评价欺骗防御方案效果的方法，但一套完整可靠、明确有效的量化指标和评测方案仍有待更深一步的研究。

6　结束语

网络侦查在网络攻击中扮演着重要的角色，对抗网络侦查可以有效缓解网络攻击。而基于网络特征混淆的欺骗防御技术是一种应对网络侦查的有效手段，受到学术界和产业界的高度重视，产生了大量的研究成果和商业产品。本文首先介绍了利用混淆欺骗防御方案应对网络侦查的必要性，并给出了网络混淆欺骗防御的形式化定义，最后给出了网络拓扑混淆欺骗防御技术的分类方案并介绍了目前的研究状况。

网络混淆欺骗防御是一个很有前景的研究方向，仍处于成熟过程的早期阶段。现有方案的配置集受到静态物理拓扑的限制，还必须考虑其安全属性的约束，在挫败攻击者进行侦查、发动攻击和窃取情报方面仍有不足之处。目前也缺乏对混淆效果的度量，很难从技术上了解攻击者对混淆方案的想法。为了应对各种网络攻击带来的威胁，仍然需要一种全面、动态、高效的混淆欺骗防御方案。

参考文献：

[1] PANJWANI S, TAN S, JARRIN K M, et al. An experimental evaluation to determine if port scans are precursors to an attack[C]//2005 International Conference on Dependable Systems and Networks (DSN'05). 2005: 602-611.

[2] KEWLEY D, FINK R, LOWRY J, et al. Dynamic approaches to thwart adversary intelligence gathering[C]//Proceedings DARPA Information Survivability Conference and Exposition II DISCEX'01. 2001, 1: 176-185.

[3] HUTCHINS E M, CLOPPERT M J, AMIN R M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains[J]. Leading Issues in Information Warfare Security Research, 2011, 1(1): 80.

[4] AL-SHAER E, DUAN Q, JAFARIAN J H. Random host mutation for moving target defense[C]//International Conference on Security and Privacy in Communication Systems. 2012: 310-327.

[5] JAFARIAN J H, AL-SHAER E, DUAN Q. Openflow random host mutation: Transparent moving target defense using software de-

fined networking[C]//Proceedings of the First Workshop on Hot Topics in Software Defined Networks. 2012: 127-132.

[6] TRASSARE S T, BEVERLY R, ALDERSON D. A technique for network topology deception[C]//2013 IEEE Military Communications Conference. 2013: 1795-1800.

[7] ACHLEITNER S, LA PORTA T F, MCDANIEL P, et al. Deceiving network reconnaissance using SDN-based virtual topologies[J]. IEEE Transactions on Network and Service Management, 2017, 14(4): 1098-1112.

[8] CHIANG C-Y J, VENKATESAN S, SUGRIM S, et al. On defensive cyber deception: a case study using SDN[C]//2018 IEEE Military Communications Conference (MILCOM). 2018: 110-115.

[9] ERIKSSON B, DASARATHY G, BARFORD P, et al. Efficient network tomography for internet topology discovery[J]. IEEE/ACM Transactions on Networking (TON), 2012, 20(3): 931-943.

[10] JAJODIA S, GHOSH A K, SWARUP V, et al. Moving target defense: creating asymmetric uncertainty for cyber threats [M]// Advances in information security. 2011.

[11] 邬江兴. 网络空间拟态防御研究[J]. 信息安全学报, 2016, 1(4): 1-10.
WU J X. Research on cyber mimic defense[J]. Journal of Cyber Security, 2016, 1(4): 1-10

[12] XIAO H, KHEIR N, BALZAROTTI D. Deception techniques in computer security: a research perspective[J]. ACM Computing Surveys, 2018, 51(4): 1-36.

[13] BAO N, MUSACCHIO J. Optimizing the decision to expel attackers from an information system[C]//2009 47th Annual Allerton Conference on Communication Control and Computing (Allerton). 2009: 644-651.

[14] HORÁK K, ZHU Q, BOŠANSKÝ B. Manipulating adversary's belief: a dynamic game approach to deception by design for proactive network security[C]//International Conference on Decision and Game Theory for Security. 2017: 273-294.

[15] JAFARIAN J H, AL-SHAER E, DUAN Q. Adversary-aware ip address randomization for proactive agility against sophisticated attackers[C]//2015 IEEE Conference on Computer Communications (INFOCOM). 2015: 738-746.

[16] SPRING N, MAHAJAN R, WETHERALL D. Measuring ISP topologies with rocketfuel[J]. ACM Sigcomm Computer Communication Review, 2002, 32(4): 133-145.

[17] TROWBRIDGE C. An overview of remote operating system fingerprinting[EB].

[18] YUILL J J. Defensive computer-security deception operations: Processes, principles and techniques[D]. Raleigh: North Carolina State University, 2006.

[19] KELLY J, DELAUS M, HEMBERG E, et al. Adversarially adapting deceptive views and reconnaissance scans on a software defined network[C]//2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). 2019: 49-54.

[20] 贾召鹏, 方滨兴, 刘潮歌, 等. 网络欺骗技术综述[J]. 通信学报, 2017, 38(12): 128-143.
JIA Z P, FANG B X, LIU C G, et al. Survey on cyber deception[J]. Journal on Communications, 2017, 38(12): 128-143.

[21] 石乐义, 李阳, 马猛飞. 蜜罐技术研究新进展[J]. 电子与信息学报, 2019, 41(2): 249-259.
SHI L Y, LI Y, MA M F. Latest research progress of honeypot technology[J]. Journal of Electronics & Information Technology, 2019, 41(2): 249-259.

[22] STOECKLIN M P, ZHANG J, ARAUJO F, et al. Dressed up: baiting attackers through endpoint service projection[C]//Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization. 2018: 23-28.

[23] ALBANESE M, BATTISTA E, JAJODIA S. Deceiving attackers by creating a virtual attack surface[M]//Cyber Deception. 2016: 167-199.

[24] PROVOS N. Honeyd-a virtual honeypot daemon[C]//10th DFN-CERT Workshop, Hamburg, Germany. 2003: 4.

[25] Cyberchaff[EB].

[26] KIM J, SHIN S. Software-defined honeynet: towards mitigating link flooding attacks[C]//2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W). 2017: 99-100.

[27] AL-SHAER E, WEI J, HAMLEN K W, et al. Netshifter: a comprehensive multi-dimensional network obfuscation and deception solution[M]//Autonomous Cyber Deception. 2019: 125-146.

[28] JAJODIA S, PARK N, PIERAZZI F, et al. A probabilistic logic of cyber deception[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(11): 2532-2544.

[29] ROWE N C, DUONG B T, CUSTY E J. Fake honeypots: a defensive tactic for cyberspace[C]//IEEE Workshop on Information Assurance. 2006: 223-230.

[30] COHEN F. A note on the role of deception in information protection[J]. Computers & Security, 1998, 17(6): 483-506.

[31] COHEN F. The use of deception techniques: honeypots and decoys[J]. Handbook of Information Security, 2006, 3(1): 646-655.

[32] PINGREE L. Emerging technology analysis: Deception techniques and technologies create security technology business opportunities[R]. Gartner Inc, 2015.

[33] WANG Q, XIAO F, ZHOU M, et al. Linkbait: active link obfuscation to thwart link-flooding attacks[J]. arXiv: Networking and Internet Architecture, 2017.

[34] MEIER R, TSANKOV P, LENDERS V, et al. Nethide: secure and practical network topology obfuscation[C]//27th USENIX Security Symposium (USENIX Security 18). 2018: 693-709.

[35] MAXIMOV R V, IVANOV I I, SHARIFULLIN S R. Network topology masking in distributed information systems[C]//Selected Papers of the VIII All-Russian Conference with International Participation" Secure Information Technologies". 2017: 83.

[36] GILLANI F, AL-SHAER E, LO S, et al. Agile virtualized infrastructure to proactively defend against cyber attacks[C]//IEEE Conference on Computer Communications. 2015: 729-737.

[37] DUAN Q, AL-SHAER E, JAFARIAN H. Efficient random route mutation considering flow and network constraints[C]//2013 IEEE Conference on Communications and Network Security (CNS). 2013: 260-268.

[38] KAMPANAKIS P, PERROS H, BEYENE T. SDN-based solutions for moving target defense network protection[C]//Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014. 2014: 1-6.

[39] LIASKOS C, KOTRONIS V, DIMITROPOULOS X. A novel framework for modeling and mitigating distributed link flooding attacks[C]//IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications. 2016: 1-9.
[40] SHAKARIAN P, KULKARNI N, ALBANESE M, et al. Keeping intruders at bay: a graph-theoretic approach to reducing the probability of successful network intrusions[C]//International Conference on E-Business and Telecommunications, Cham. 2014: 191-211.
[41] BORDERS K, FALK L, PRAKASH A. Openfire: Using deception to reduce network attacks[C]//International Conference on Security & Privacy in Communications Networks & the Workshops. 2007: 224-233.
[42] WANG L, WU D. Moving target defense against network reconnaissance with software defined networking[C]//International Conference on Information Security. 2016: 203-217.
[43] SHIMANAKA T, MASUOKA R, HAY B. Cyber deception architecture: covert attack reconnaissance using a safe SDN approach[C]//Proceedings of the 52nd Hawaii International Conference on System Sciences. 2019: 1-10.
[44] XU M, GAO Y, FENG C. DDS: a distributed deception defense system based on SDN[C]//2018 14th International Conference on Computational Intelligence and Security (CIS). 2018: 430-433.
[45] ROBERTSON S, ALEXANDER S, MICALLEF J, et al. Cindam: customized information networks for deception and attack mitigation[C]//IEEE International Conference on Self-adaptive & Self-organizing Systems Workshops. 2015: 114-119.
[46] CHIANG C-Y J, GOTTLIEB Y M, SUGRIM S J, et al. Acyds: an adaptive cyber deception system[C]//2016 IEEE Military Communications Conference. 2016: 800-805.
[47] ANTONATOS S, AKRITIDIS P, MARKATOS E P, et al. Defending against hitlist worms using network address space randomization[J]. Computer Networks, 2007, 51(12): 3471-3490.
[48] YACKOSKI J, XIE P, BULLEN H, et al. A self-shielding dynamic network architecture[C]//Military Communications Conference. 2011: 1381-1386.
[49] MACFARLAND D C, SHUE C A. The SDN shuffle: Creating a moving-target defense using host-based software-defined networking[C]//Proceedings of the Second ACM Workshop on Moving Target Defense. 2015: 37-41.
[50] DATTA T, FEAMSTER N, REXFORD J, et al. {spine}: Surveillance protection in the network elements[C]//9th USENIX Workshop on Free and Open Communications on the Internet (FOCI 19). 2019.
[51] MEIER R, GUGELMANN D, VANBEVER L. ITAP: In-network traffic analysis prevention using software-defined networks[C]//Proceedings of the Symposium on SDN Research. 2017: 102-114.
[52] ZHU T W, FENG D, WANG F, et al. Efficient anonymous communication in SDN-based data center networks[J]. IEEE-ACM Transactions on Networking, 2017, 25(6): 3767-3780.
[53] LU Z, WANG C, WEI M. A proactive and deceptive perspective for role detection and concealment in wireless networks [M]//Cyber Deception. 2016: 97-114.
[54] FRAUNHOLZ D, RETI D, DUQUE ANTON S, et al. Cloxy: a context-aware deception-as-a-service reverse proxy for web services[C]//Proceedings of the 5th ACM Workshop on Moving Target Defense. 2018: 40-47.
[55] HAN X, KHEIR N, BALZAROTTI D. Evaluation of deception-based web attacks detection[C]//Proceedings of the 2017 Workshop on Moving Target Defense. 2017: 65-73.
[56] WATSON D, SMART M, MALAN G R, et al. Protocol scrubbing: network security through transparent flow modification[J]. IEEE/ACM Transactions on Networking, 2004, 12(2): 261-273.
[57] SMART M, MALAN G R, JAHANIAN F. Defeating TCP/IP stack fingerprinting[C]//Usenix Security Symposium. 2000: 17.
[58] MALÉCOT E L. Mitibox: Camouflage and deception for network scan mitigation[C]//Usenix Conference on Hot Topics in Security. 2009: 4.
[59] SHI Y, ZHANG H, WANG J, et al. Chaos: an SDN-based moving target defense system[J]. Security and Communication Networks, 2017.
[60] STUDER A, PERRIG A. The coremelt attack[C]//European Symposium on Research in Computer Security, 2009: 37-52.
[61] KANG M S, LEE S B, GLIGOR V D. The crossfire attack[C]//2013 IEEE Symposium on Security and Privacy. IEEE, 2013: 127-141.
[62] AYDEGER A, SAPUTRO N, AKKAYA K. Utilizing NFV for effective moving target defense against link flooding reconnaissance attacks[C]//2018 IEEE Military Communications Conference(MILCOM). 2018: 946-951.
[63] GADGE J, PATIL A A. Port scan detection[C]//2008 16th IEEE International Conference on Networks. 2008: 1-6.
[64] LISTON T. Labrea: “Sticky” honeypot and ids[EB].

[作者简介]

赵金龙（1994− ），男，甘肃静宁人，陆军工程大学硕士生，主要研究方向为网络安全、欺骗防御、软件定义网络。

张国敏（1979− ），男，江苏南京人，博士，陆军工程大学副教授，主要研究方向为软件定义网络、网络安全、网络测量和分布式系统。

邢长友（1982− ），男，江苏南京人，博士，陆军工程大学副教授，主要研究方向为网络安全、软件定义网络、网络度量和网络功能虚拟化。