doi :10.3969/j.issn.1671-1122.2020.07.005

一种基于软件定义网络的主机指纹抗探测模型

张涛[1,2]，芦斌[1,2]，李玎[1,2]，何康[1,2]

（1. 信息工程大学网络空间安全学院，郑州 450001；2. 数学工程与先进计算国家重点实验室，郑州 450001）

摘　要：针对主机指纹探测防御困难的问题，文章提出基于软件定义网络的主机指纹抗探测模型。模型构造包含虚假指纹信息的虚拟节点，通过识别指纹探针，按照指纹模板构造响应报文，实现对指纹探测攻击的欺骗。随后提出蜜罐映射与流量牵引技术，结合蜜罐技术将指向虚拟节点的攻击流量重定向到蜜罐，实现对攻击行为的捕获分析。为了分析模型对网络安全带来的收益，建立该模型防御效能的概率模型，量化了探测次数、虚拟节点数量、蜜罐映射规则数、允许损失数、虚拟节点欺骗率和蜜罐检测率等参数对攻击成功概率的影响。最后结合 DPDK 技术基于 X86 平台搭建原型系统，实验结果表明该模型与典型的抗识别工具 IPMorph 相比具备更高的欺骗成功率，且带来的额外性能开销低于 5%。

关键词：主机指纹；网络探测；蜜罐；网络欺骗

中图分类号：TP309　**文献标志码：**A　**文章编号：**1671-1122（2020）07-0042-11

中文引用格式：张涛，芦斌，李玎，等 .一种基于软件定义网络的主机指纹抗探测模型 [J]. 信息网络安全，2020，20（7）：42-52.

英文引用格式：ZHANG Tao, LU Bing, LI Ding, et al. A Host Fingerprint Anti-detection Model Based on SDN[J]. Netinfo Security, 2020, 20(7): 42-52.

A Host Fingerprint Anti-detection Model Based on SDN

ZHANG Tao[1,2], LU Bing[1,2], LI Ding[1,2], HE Kang[1,2]

(1. *Cyberspace Security Institute*, *Information Engineering University*, *Zhengzhou* 450001, *China*; 2. *State Key Laboratory of Mathematical Engineering and Advanced Computing*, *Zhengzhou* 450001, *China*)

Abstract: Point at the difficulty of host fingerprint detection defense, a host fingerprint anti-detection model based on SDN is proposed. The model constructs virtual nodes that contain fake fingerprint information. By identifying fingerprint probes and constructing response messages according to the fingerprint template, it can deceive fingerprint detection attackers. Then put forward honeypot mapping and traffic traction technology, combined with honeypots, redirect the attack traffic directed to the virtual node to the honeypot, and realize the capture and analysis of aggressive behavior. To analyze the benefits of the model for cybersecurity, a probabilistic model of the proposed model's defense effectiveness was established. The influence of parameters such as the number of detections, the number of virtual nodes, the number of honeypot mapping rules,

收稿日期：2019-12-15

基金项目：国家自然科学基金 [61601517]

作者简介：张涛（1995—），男，山东，硕士研究生，主要研究方向为信息安全、移动目标防御；芦斌（1981—），男，山西，副教授，博士，主要研究方向为人工智能、网络空间安全；李玎（1992—），男，河南，博士研究生，主要研究方向为网络与信息安全、流量分析；何康（1992—），男，山东，博士研究生，主要研究方向为深度学习、网络空间安全。

通信作者：张涛 1019032076@qq.com

the number of allowable losses, the virtual node spoofing rate, and the honeypot detection rate on the probability of attack success is quantified. Finally, the DPDK technology is used to build a prototype system based on the X86 platform. The experimental results show that the proposed model has a higher success rate of deception than the typical anti-recognition tool IPMorph, and the additional performance overhead is less than 5%.

Key words: host fingerprint; reconnaissance; honeypot; cyber deception

0 引言

随着网络攻击技术的发展，网络安全问题日益严峻。网络攻击有一般规律可循，洛克希德马丁公司提出网络攻击的杀伤链模型，包括侦察探测、武器化、交付、利用、部署、命令与控制以及目标达成7个阶段[1]。其中侦察探测是大多数网络攻击行为的第一阶段，攻击者需要收集目标相关信息以发现目标的脆弱性和可利用资源，进而采取针对性的攻击方式。因此，侦察探测是攻击杀伤链中极为重要的一步，所占整个攻击过程时长的比重往往超过50%[2]。攻击者通过侦察探测获得的目标信息越多，可利用的攻击资源越丰富，可采用的攻击手段就越多样。因此如何在攻击的侦察探测阶段采取防御措施，阻止攻击者获取目标信息或诱骗攻击者获取错误信息，进而干扰攻击者的攻击行为，达成防御目标是网络安全领域的研究热点之一。

主机指纹是网络节点的信息集合，包含节点网络服务的特征信息、网络拓扑的特征信息以及操作系统的特征信息等，是攻击者进行探测的重要目标信息。围绕主机指纹的防护国内外研究人员开展了相关工作。SHAMSI[3]等人提出通过修改出站入站数据报文的方式对系统指纹信息进行修改，进而迷惑探测者。文献[4]提出了IPMorph方法，通过实现用户态的TCP/IP协议栈完成实时流量监控与数据包修改，从而欺骗攻击者。文献[5]提出增强型Anti-Xprobe2工具，通过构造探针响应报文实现对Xprobe探测工具的欺骗。KAMPANAKIS[6]等人利用SDN技术伪造操作系统指纹，迷惑攻击者，该方法仅随机修改数据包中的指纹特征，缺少针对性的修改策略。上述工具或方法均是通过对节点出入站流量的修改进行的操作系统信息防护，需要在每个节点上进行部署，部署方式繁琐冗余，难以对网络整体进行统一的防御，若网络内某一节点未实施保护，易被攻击者作为跳板进行横向渗透。

蜜罐是一种常用的抵抗指纹探测的网络欺骗方式[7]，防御者通过部署蜜罐引诱攻击者进行指纹探测等攻击行为并加以捕获分析，从而对抗攻击者。HAN[8]等人利用SDN细粒度流量控制能力，将攻击流量发送至多个蜜罐，选择最优应答发送给攻击者，可以充分利用蜜罐资源。文献[9]提出基于博弈论的蜜罐最优防御方法，将攻防双方的行为建模为不完全信息的贝叶斯博弈，研究攻击行为存在频率阈值，当达到阈值以上时，攻防双方都将采取欺骗性行动；在阈值以下时，防御者可以采取混合防御策略，以实现较低的攻击成功率。FAN[10]等人提出一种基于SDN的蜜罐部署方式，提供了高度的可编程性，搭建原型系统验证方法的可行性和有效性。SHI[11]等人结合区块链技术分散部署动态蜜罐平台，提升了蜜罐部署的安全性，同时验证了在防范网络攻击方面的有效性。蜜罐部署方式的丰富以及与SDN技术的结合，提高了蜜罐防御技术的灵活性与可用性，但是上述研究缺少对蜜罐防御效果的形式化评估。

针对当前静态网络固有的主机指纹信息保护困难问题，本文结合移动目标防御技术中动态、异构、冗余的思想[12]，提出基于虚拟节点的主机指纹抗探测模型。结合网络欺骗技术，改变检测拦截的事后防御方式，在探测行为发起之前，通过生成虚拟节点制造虚假主机指纹信息，保护真实节点；结合蜜罐映射与流量牵引技术，通过虚拟节点将攻击流量牵引至蜜罐节点进行捕获分析，从而阻止攻击行为；结合瓮模型建立防御效能模型，量化探测次数、虚拟节点数量、蜜罐映射规则数量等条件对攻击成功概率的影响；通过建立原型系统验证防御模型的有效性和可用性。

1 防御模型

网络攻击可划分为多个阶段，攻击者大多从侦察探测阶段发起攻击行为。指纹探测能够根据目标主机的流量判断目标主机的操作系统类型、版本号等信息，易被攻击者利用，挖掘漏洞实施攻击，给网络安全带来严重威胁。基于获取信息的方式可划分为两种：被动指纹识别和主动指纹识别。被动指纹识别通过嗅探、监听等方式分析目标主机的流量进行指纹识别。主动指纹识别类似于雷达的工作方式，通过主动发包的方式向目标主机发送设计构造的探针，收集分析主机的响应报文进行指纹识别。相对于被动指纹识别，主动指纹识别收集信息丰富、时效性强、识别准确率高，更为攻击者所青睐，研究价值也更高，典型工具如Nmap和Xprobe2等。本文的研究重点是主动指纹识别防御，在生产环境中正常用户不会对网络内其他用户开展主动指纹识别，通过对主动指纹探针的识别可区分正常用户流量与指纹探测流量。简化的典型攻击流程如图1所示，攻击者探测获取节点信息，随后发起关联攻击行动，因此攻击者十分依赖探测阶段获取的信息，在探测阶段采取防御措施收效也更显著。本文重点研究在攻击者主动探测阶段建立防御模型，对节点主机指纹信息进行保护。

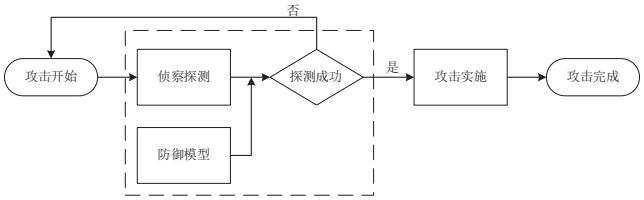

图 1 网络攻击流程示意图

定义1 主机指纹信息 F $F=\{ip,mac,ports,ostype\}$，其中，$ip$为节点的网络地址，$mac$为节点的物理地址，节点的开放端口集合为$ports=\{port_1,port_2,\cdots,port_n\}$，$ostype$为节点的操作系统特征信息。

本文研究场景如图2所示。外部攻击者通过主动发送探针的方式对目标网络进行主机指纹探测，获取目标网络内各节点的主机指纹信息，发现目标网络内活跃节点及节点脆弱性资源，以支撑网络攻击杀伤链的下一环节。根据探测顺序将探测流程划分为3个阶段。

1）节点发现阶段，攻击者通过发送ICMP探针寻找目标网络内的活跃节点；

2）端口探测阶段，针对目标网络内的活跃节点，攻击者通过TCP CONNECT、TCP FIN、TCP ACK等端口扫描探测方法确定活跃节点的开放端口集合；

3）操作系统探测阶段，攻击者利用ICMP、TCP、UDP等协议构造多个数据包探针，对活跃节点进行操作系统探测，通过分析节点返回的响应报文，结合活跃节点的开放端口信集合，获取节点的操作系统特征信息。

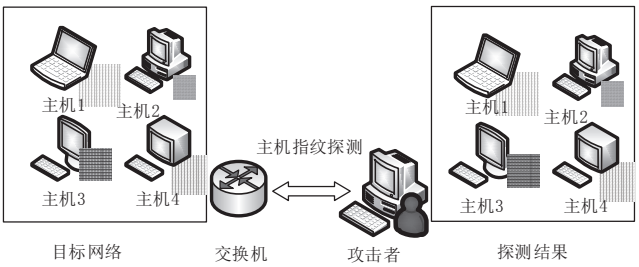

图 2 主机指纹探测场景示意图

1.1 虚拟节点防御模型

定义2 虚拟节点 V $V=\{F_v,T\}$，其中，$F_v=\{ip_v,mac_v,ports_v,ostype_v\}$，为虚拟节点的主机指纹信息；$T$为虚拟节点信息的再配置周期。

虚拟节点实质上是由模型生成的包含一组主机指纹信息及重配置周期的无实体网络节点。为了与目标网络内的原有节点进行区分，称目标网络内原有节点为真实节点。虚拟节点防御模型在目标网络地址空间内生成若干虚拟节点，当收到主机指纹探测报文后，依据虚拟节点的主机指纹信息构造响应报文，从而欺骗攻击者，隐藏真实节点指纹信息。

虚拟节点防御模型基本原理如图3所示，在目标网络上行出口处结合SDN交换机部署模型。目标网络的上下行流量均通过SDN交换机，通过分析上下行流量，模型可捕获其中的主机指纹探测探针。模型为保护真实节点的主机指纹信息，生成与真实节点IP地址相同的虚拟节点，当攻击者对该IP地址进行探测时，

仅能获取F_v而非真实节点指纹信息F。除此之外，模型在目标网络地址空间选取未使用的IP地址，生成若干虚拟节点迷惑攻击者。若仅静态生成若干数量的虚拟节点，则并未改变传统网络的固有的静态性、不变性等易受攻击的特点。模型采用了移动目标防御理论中的动态思想，为每个虚拟节点设置重配置周期T，动态更新虚拟节点的主机指纹信息，构造复杂多变的网络环境，干扰攻击者的探测行动，阻碍攻击者获取节点指纹信息，提升目标网络的安全性。

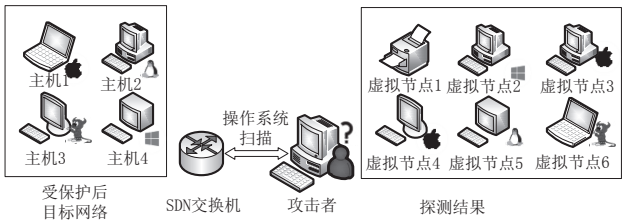

图 3 虚拟节点防御模型基本原理示意图

虚拟节点防御模型的基本工作流程如图4所示。

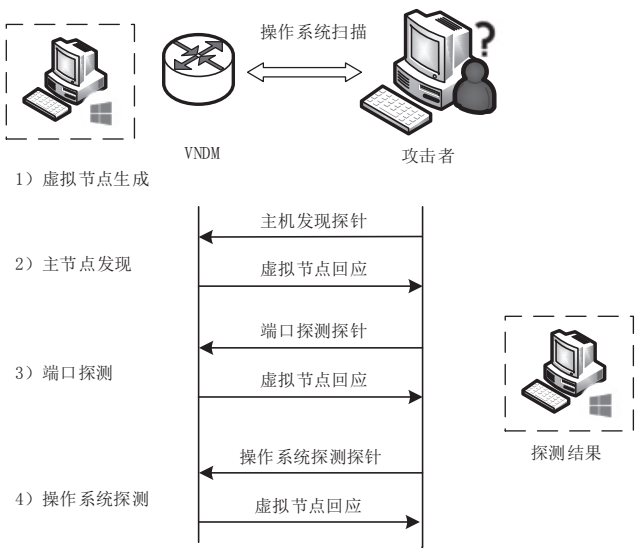

图 4 虚拟节点防御模型工作流程示意图

1）虚拟节点生成，构建虚拟节点的主机指纹F_v，设置虚拟节点的动态配置周期T，生成虚拟节点V，每经过一个再配置周期T后，重新构建虚拟节点$V'=\{F_v',T'\}$；

2）节点发现，攻击者在目标网络地址空间进行活跃节点探测，当目标IP地址是ip_v时，生成响应报文；

3）端口探测，攻击者对虚拟节点进行端口探测，匹配探测端口是否在$ports_v$中，命中则构造端口响应报文；

4）操作系统探测，攻击者发送操作系统探测探针，模型从流量中捕获识别探针，依据虚拟节点的操作系统特征信息$ostype_v$，构造响应报文，攻击者收到响应报文后结合节点的端口开放情况，分析得到操作系统信息。

1.2 虚拟节点-蜜罐防御模型

虚拟节点-蜜罐防御模型可有效降低攻击者获取真实节点主机指纹信息的成功率，本文给出了具体的分析验证。攻击者通过对目标网络进行长时间探测，发现目标网络防御方法的规律，采取针对性措施避开防御措施，达到攻击目标。针对这一局限性，结合蜜罐防御技术对模型进行改进，提出虚拟节点-蜜罐防御模型。蜜罐本质上是一种对攻击者的网络欺骗技术，通过部署诱饵节点、敏感信息或相关服务，诱惑攻击方实施攻击，从而捕获和分析攻击行为[13]。传统的蜜罐部署方式中，蜜罐节点常采用固定的网络地址，与真实节点部署在同一目标网络之中。蜜罐节点在捕获分析攻击行为的同时，也易被攻击者发现并规避。攻击者可通过设置探测白名单的方式规避蜜罐节点的检测，致使蜜罐防御失效[14]。

本文模型基于SDN精细的流量控制能力[15]实现蜜罐映射与流量牵引，达到虚拟节点和蜜罐节点的联合防御效果。该技术设置蜜罐映射规则，当攻击者对设定规则后的虚拟节点进行主机指纹探测或者访问连接时，依据规则将流量牵引到蜜罐节点进行捕获分析。虚拟节点-蜜罐防御模型基本原理如图5所示。由于攻击者对生成有虚拟节点的目标网络拓扑不具备先验知识，无法区分虚拟节点和真实主机，而正常用户不会对虚拟节点进行扫描探测，因此本文模型仅对未对应真实主机的虚拟节点设置蜜罐映射与流量牵引规则，真实主机间的正常通信流量不会被重定向，攻击者对虚拟节点的攻击流量会被诱导至蜜罐进行捕获分析。

本文模型的基本工作流程分为5个阶段。

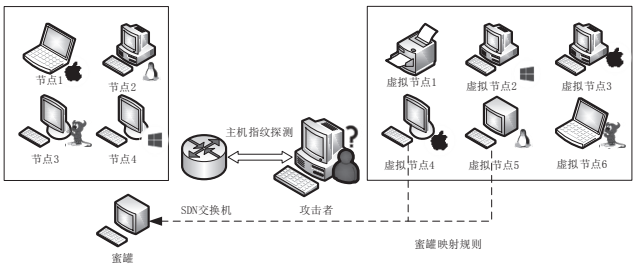

图 5 虚拟节点-蜜罐防御模型基本原理示意图

1）虚拟节点生成阶段，构建虚拟节点的主机指纹F_v及动态配置周期T，生成虚拟节点$V=\{F_v,T\}$，设置映射规则f，经过一个再配置周期T后，重新构建F_v；

2）节点发现阶段，攻击者探测目标是虚拟节点的IP地址时，根据虚拟节点ip_v生成响应报文；

3）端口探测阶段，虚拟节点收到端口探测报文，查询探针探测的端口是否命中开放端口集合，命中则构造端口响应报文，同时根据映射规则f将攻击探针数据包牵引至H；

4）操作系统探测阶段，攻击者对已发现的节点发送操作系统探测探针，模型识别探针根据映射规则f将探针数据包牵引至H，同时依据虚拟节点的$ostype_v$构造响应报文，攻击者接收到响应报文结合端口探测结果，分析获得虚拟节点的操作系统特征信息；

5）攻击者获取虚拟节点的主机指纹信息F_v后发起攻击行为，模型依据映射规则f将攻击流量牵引至H进行分析。

2 防御效能模型

本章主要工作是建立1.2节提出的防御模型对抗探测攻击的效能模型，主要是多种防御模型下攻击成功的概率模型，这对研究探测防御模型的表现以及模型改进有重要的指导借鉴意义。假设攻击者有两种攻击成功场景：1）立足点攻击，当攻击者的目标节点受到如防火墙等保护措施无法从外部直接发起攻击时，攻击者就需要控制一个和目标节点在同一网络内的节点，以此作为立足点绕过防火墙对目标节点横向渗透；2）网络控制攻击，攻击者的目标不是获取单个节点的控制权，而是需要控制目标网络内一定阈值数量的节点才视为攻击成功，典型场景如组建僵尸网络、拓展僵尸节点[16]。

结合Urn模型与多维超几何分布模型，构建一个由真实节点、虚拟节点、蜜罐节点组成的目标网络。外部攻击者对其进行探测攻击，参数如下：

1）网络中真实节点的数量为m，未采取防护措施时，攻击者可通过指纹探测获取指纹信息进而控制该节点；

2）系统在网络中生成v个虚拟节点，其中，m个对真实节点进行保护，配置有蜜罐映射规则的虚拟节点数为h；

3）攻击者可进行指纹探测的活跃节点数为$N=\max\{v,m\}$；

4）攻击者进行k次不重复探测；

5）攻击者指纹探测被虚拟节点的主机指纹成功欺骗的概率为虚拟节点欺骗率α；

6）攻击者指纹探测被蜜罐节点成功检测发现的概率为蜜罐检测率β；

7）当攻击者获取一个及以上的真实节点的主机指纹信息时即认为立足点攻击成功；

8）当攻击者获取网络内一半以上真实节点的主机指纹信息时即认为网络控制攻击成功。

结合Urn模型将目标网络视为装有N个带颜色小球的盒子，用颜色标识不同类型节点。其中用m个红色小球代表真实节点，h个黄色小球代表配置有蜜罐映射规则的虚拟节点，$v–m–h$个绿色小球代表除去真实节点和配置有蜜罐映射规则的虚拟节点的节点，抽取绿色小球对攻击者来说毫无价值。将攻击者的连续k次探测行为等效为在此盒子中连续不放回抽取k个小球，根据抽取结果的概率分布刻画攻击成功的概率分布。

2.1 无防御模型概率分布

为了有明确的防御效果对比，首先考虑不采取任何安全措施的无防御模型。攻击者通过遍历网络地址空间即可发现全部活跃节点$N=m$，可直接探测获得真

实节点的主机指纹信息。因此对于给定k次主机指纹探测，成功x次的概率与数学期望如公式（1）和公式（2）所示。

$$P(X_k=x)=\begin{cases}1 & x=k\\ 0 & x\neq k\end{cases} \quad (1)$$

$$E(X_k)=k \quad (2)$$

2.2 虚拟节点防御模型概率分布

考虑虚拟节点防御模型，在m个真实节点的目标网络内生成v个虚拟节点，攻击者可进行探测的活跃节点数$N=v$。由于采用虚拟节点对真实节点进行保护，当攻击者对受虚拟节点保护的真实节点进行探测时，获取到虚拟节点主机指纹的概率为α，获取真实节点信息的概率为$1-\alpha$。对于给定k次主机指纹探测获得x个真实节点主机指纹的概率，结合小球投盒问题，在盒子中共有v个小球，其中包括m个红色小球，$v-m$个绿色小球。从盒子中不放回地抽取k个小球，求成功取到x个红色小球的概率。需要指出的是由于虚拟节点的保护，每抽到红色小球时有α概率使此次抽取失败，即虚拟节点成功欺骗攻击者。因此，对于给定k次主机指纹探测，结合二维超几何分布，可得攻击成功节点数x的概率分布与数学期望如公式（3）和公式（4）所示。

$$P(X_k=x)=\sum_{i=\max\{x,k+m-v\}}^{\min\{k,m\}}\frac{C_{v-m}^{k-i}C_m^iC_i^x(1-\alpha)^x\alpha^{i-x}}{C_v^k} \quad (3)$$

$$E(X_k)=k\frac{m(1-\alpha)}{v} \quad (4)$$

立足点攻击的成功概率与网络控制攻击的成功概率分别如公式（5）和公式（6）所示。

$$P(X_k\geq 1)=1-P(X_k=0)=1-\sum_{i=\max\{0,k+m-v\}}^{\min\{k,m\}}\frac{C_{v-m}^{k-i}C_m^i(1-\alpha)^i}{C_v^k} \quad (5)$$

$$P(X_k\geq[\frac{m+1}{2}])=\sum_{x=[\frac{m+1}{2}]}^{m}\sum_{i=\max\{x,k+m-v\}}^{\min\{k,m\}}\frac{C_{v-m}^{k-i}C_m^iC_i^x(1-\alpha)^{i-x}\alpha^x}{C_v^k} \quad (6)$$

2.3 虚拟节点-蜜罐防御模型概率分布

考虑虚拟节点-蜜罐防御模型，当攻击者对虚拟节点的攻击流量被牵引至配置映射规则的蜜罐节点进行捕获分析时，防御者可采取封堵拦截等防御措施挫败攻击者的行动，因此当攻击行为被蜜罐节点发现时即可认为攻击失败。需要注意的是，蜜罐节点对攻击行为的检测率会直接影响攻击成功概率，通过检测成功率β来刻画蜜罐节点对攻击行为的检测能力。结合Urn模型，m个红色小球、h个黄色小球，以及$v-m-h$个绿色小球分别代表受虚拟节点保护的真实节点、蜜罐映射规则的虚拟节点和其他虚拟节点。对于给定k次非重复探测，考虑虚拟节点欺骗成功率α和蜜罐节点检测成功率β的影响，计算攻击者成功扫描x次且未被蜜罐发现的概率如公式（7）所示。

$$P(X_k=x,Y_k=0)=\sum_{i=\max\{x,k+m-v\}}^{\min\{k,m\}}\sum_{j=\max\{0,k+m+h-v-i\}}^{\min\{h,k-i\}}\frac{C_{v-m-h}^{k-i-j}C_m^iC_i^x(1-\alpha)^{i-x}\alpha^xC_h^j(1-\beta)^j}{C_v^k} \quad (7)$$

立足点攻击的成功概率和网络控制攻击的成功概率如公式（8）和公式（9）所示。

$$P(X_k\geq 1,Y_k=0)=P(Y_k=0)-P(X_k=0,Y_k=0) \quad (8)$$

$$P(X_k\geq[\frac{m+1}{2}],Y_k=0)=\sum_{x=[\frac{m+1}{2}]}^{m}\sum_{i=\max\{x,k+m-v\}}^{\min\{k,m\}}\sum_{j=\max\{0,k+m+h-v-i\}}^{\min\{h,k-i\}}\frac{C_{v-m-h}^{k-i-j}C_m^iC_i^x(1-\alpha)^{i-x}\alpha^xC_h^j(1-\beta)^j}{C_v^k} \quad (9)$$

在虚拟节点-蜜罐防御模型中，攻击者被蜜罐节点检测发现后即认为攻击失败，但是实际上经验丰富的攻击者可以允许一定的探测损失[17]。即攻击者利用多个攻击节点发起探测且允许Y个攻击节点被蜜罐节点捕获。对于给定k次操作系统指纹扫描，攻击者成功扫描x次且不多于Y个节点被蜜罐欺骗的概率如公式（11）所示。

$$P(X_k=x,Y_k=y)=\sum_{i=\max\{x,k+m-v\}}^{\min\{k,m\}}\sum_{j=\max\{y,k+m+h-v-i\}}^{\min\{h,k-i\}}\frac{C_{v-m-h}^{k-i-j}C_m^iC_i^x(1-\alpha)^{i-x}\alpha^xC_h^jC_j^y(1-\beta)^{j-y}\beta^y}{C_v^k} \quad (10)$$

$$P(X_k=x,Y_k\leqslant Y)=\sum_{y=0}^{Y}P(X_k=x,Y_k=y) \quad (11)$$

立足点攻击成功概率和网络控制攻击成功概率如公式（12）和公式（13）所示。

$$P(X_k\geqslant 0,Y_k\leqslant Y)=P(Y_k\leqslant Y)-P(X_k=0,Y_k\leqslant Y) \quad (12)$$

$$P(X_k\geqslant[\frac{m+1}{2}],Y_k\leqslant Y)=\sum_{x=[\frac{m+1}{2}]}^{m}\sum_{y=0}^{Y}\sum_{i}\sum_{j}\frac{C_{v-m-h}^{k-i-j}C_m^iC_i^x(1-\alpha)^{i-x}\alpha^xC_h^jC_j^y(1-\beta)^{j-y}\beta^y}{C_v^k} \quad (13)$$

3 模型分析

本章旨在通过定量分析多个参数对攻击成功概率的影响，找到影响防御模型性能的重要因素，进而指导防御模型和防御策略进一步优化。

3.1 探测次数

探测次数是分析攻击成功概率的重要参数。考虑目标网络内存在10个真实节点，生成100个虚拟节点，对应真实节点的虚拟节点10个，配置蜜罐映射规则的虚拟节点5个，蜜罐节点检测率为80%，虚拟节点欺骗率为90%。考虑立足点攻击场景如图6所示，虚拟节点防御模型随着探测次数的增加，攻击成功率随之提高，当对全部活跃节点进行主机指纹探测后攻击成功率约为60%。因此攻击者可花费更多时间，通过多次遍历活跃节点的方式提高扫描成功率。虚拟节点-蜜罐防御模型下，攻击成功率随探测次数的增加呈现出先增后减的趋势，峰值为8%。这是由于探测次数的增加提高了被蜜罐捕获的概率，因此当遍历全部活跃节点时，攻击成功概率降至0.1%。当攻击者允许损失节点数为2时，攻击成功率得到了较大的提升，最高为26%。网络控制攻击如图7所示，由于攻击者需要控制网络内半数以上节点，攻击成功率较立足点攻击降低幅度较大，均不高于2%。

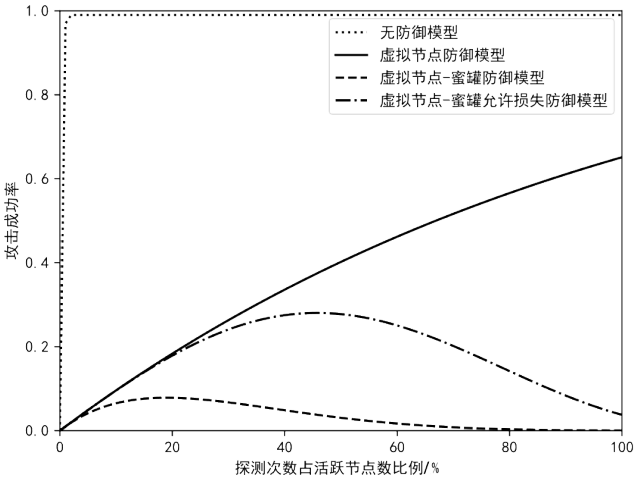

图 6 不同防御模型下探测次数对立足点攻击成功概率影响

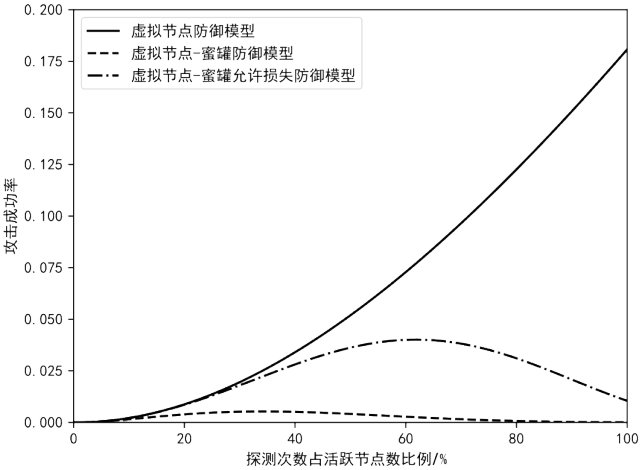

图 7 不同防御模型下探测次数对网络控制攻击成功概率影响

3.2 虚拟节点数量

虚拟节点数量直接影响攻击者探测的活跃节点总数，进而影响攻击成功率。网络内存在10个真实节点，采用虚拟节点防御模型生成虚拟节点，虚拟节点欺骗率为90%。绘制不同虚拟节点数下探测次数与立足点攻击成功率曲线，如图8所示。对于40次探测，100个虚拟节点比40个虚拟节点攻击成功率下降39%。生成的虚拟节点数量越多，在相同探测次数下攻击成功率越低，防御效果越好。换言之，当攻击者主机指纹探测速率存在上限时，可通过生成大量虚拟节点增加可探测的活跃节点总数，从而迫使攻击者消耗更多攻击资源。

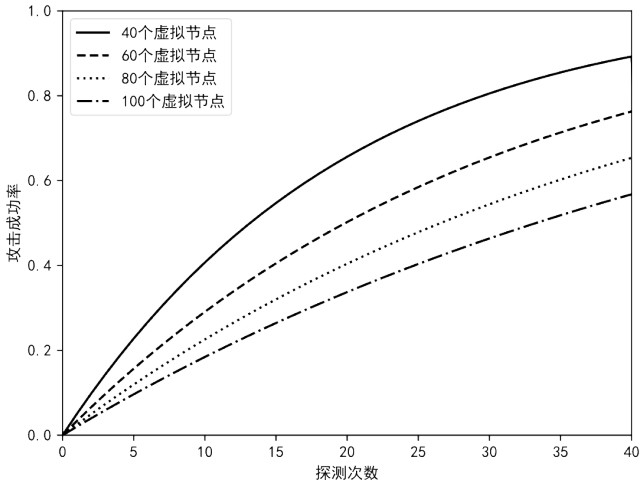

图 8 虚拟节点数量对攻击成功概率影响示意图

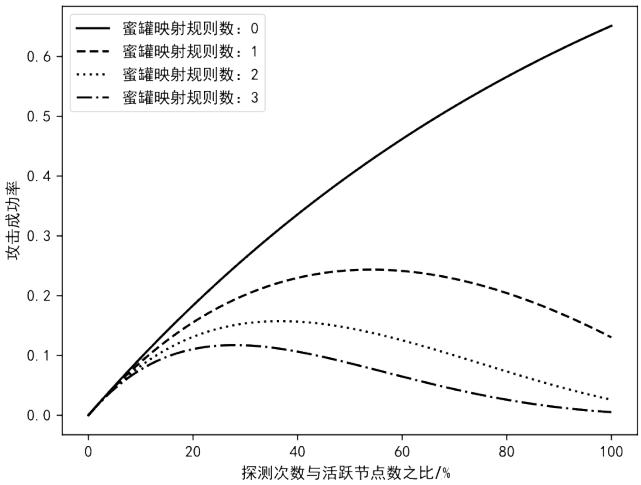

图 9 不同蜜罐映射规则数下探测次数与攻击成功率曲线图

3.3 蜜罐映射规则数

假设攻击者的目标是在不被蜜罐发现的情况下探测真实主机指纹信息，攻击成功概率将受到网络中蜜罐映射规则数的影响。为了简化概率模型，假设一次完整探测行为完成前即便被蜜罐发现，攻击者也将继续探测行动。考虑一个目标网络，存在10个真实节点，100个虚拟节点，对应真实节点的虚拟节点10个，攻击者可探测的活跃节点数N=100，蜜罐节点检测率为80%，虚拟节点欺骗率为90%，绘制不同蜜罐映射规则数下探测次数与攻击成功概率曲线，如图9所示。固定的探测次数情况下，蜜罐映射规则数越多，攻击成功率越低，即便仅配制1条规则，攻击成功率也下降较多。当探测比例为60%，设置3条蜜罐映射规则比仅设置1个的攻击成功率下降14%。相较于传统的蜜罐部署方式，虚拟节点-蜜罐防御模型通过蜜罐映射与流量牵引技术，支持蜜罐节点与虚拟节点一对多的映射关系。一个蜜罐节点支持多个虚拟节点的映射规则，通过配置多条映射规则的方式放大蜜罐防御能力。

3.4 允许损失数

对于攻击者而言，如果目标节点的价值极高，可接受部分攻击节点的损失来完成对目标的攻击。考虑一个包括10个真实节点、100个虚拟节点以及蜜罐映射规则数为5的目标网络。攻击者可探测的活跃节点数N=100，探测次数固定为50次，蜜罐节点检测率为80%，虚拟节点欺骗率为90%，绘制不同蜜罐映射规则数下允许损失数与攻击成功概率的关系曲线，如图10所示。需要注意到在相同允许损失数时，网络内部署蜜罐映射规则的数量越多，攻击成功率越低。当允许损失数为2时，部署3条蜜罐映射规则比仅部署1条的攻击成功率下降了35%。网络内未配置蜜罐映射规则时，攻击成功率不受允许损失数影响，部署蜜罐映射规则后，随着允许损失数的增加，攻击成功率逐渐提高至与未配置蜜罐映射规则相同。

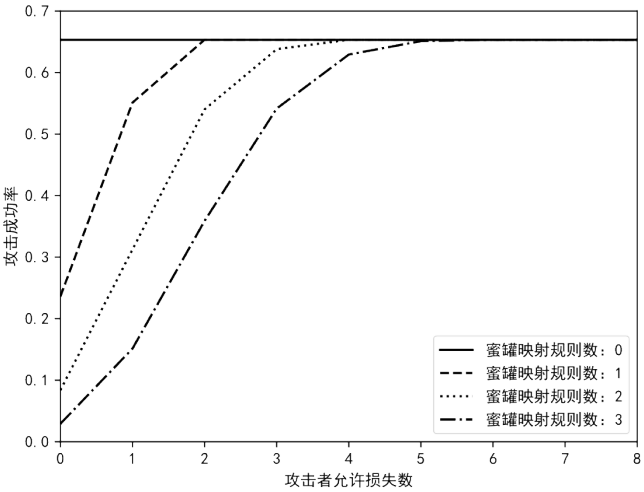

图 10 不同蜜罐映射规则数下允许损失数与攻击成功率曲线

3.5 虚拟节点欺骗率

虚拟节点防御模型和虚拟节点-蜜罐防御模型通过生成与真实节点IP地址相同的虚拟节点，来欺骗攻

击者获取到虚拟节点主机指纹F_v。虚拟节点的欺骗能力受到指纹探针响应构造能力、攻击者探测方式等因素影响。采用虚拟节点欺骗成功率α进行刻画，欺骗失败则认为攻击者能够成功探测真实节点的指纹信息。

如图11所示，考虑目标网络内存在10个真实节点，虚拟节点防御模型生成100个虚拟节点，则对应有真实节点的虚拟节点为10个，绘制立足点攻击场景下不同虚拟节点欺骗成功率α下探测次数与攻击成功概率曲线。当探测次数确定时，α越大，攻击成功率越低。理想状态下当α=1时，攻击成功率为0，虚拟节点可完全欺骗攻击者，攻击者无法获取受保护真实节点的主机指纹信息，因此提高虚拟节点欺骗成功率可有效提升防御性能。

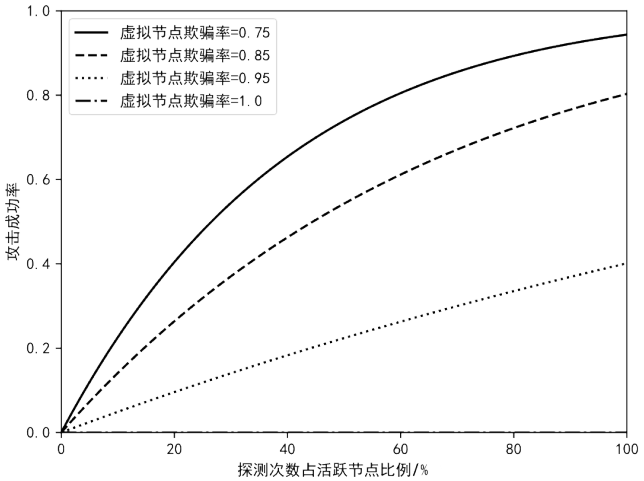

图 11 不同虚拟节点欺骗率下探测次数与攻击成功率曲线图

3.6 蜜罐节点检测率

虚拟节点-蜜罐防御模型结合蜜罐映射与流量牵引技术，通过配置蜜罐映射规则，将探测攻击流量牵引至蜜罐节点进行分析，采用蜜罐节点检测率β刻画蜜罐节点对攻击行为的检测能力，进而影响攻击者的攻击成功率。如图12所示，考虑网络内存在10个真实节点，防御模型生成100个虚拟节点，对应真实节点的虚拟节点10个，虚拟节点欺骗率为90%，配置5条蜜罐映射规则，绘制不同蜜罐检测率下探测次数与攻击成功率关系曲线。当探测次数确定时，β越大，攻击成功率越低，当探测次数所占比例为20%时，β=0.9比β=0.7攻击成功率降低了3%，因此提高虚拟节点欺骗成功率可提升防御性能。相较于蜜罐映射规则数量，检测率对攻击成功率影响较小。

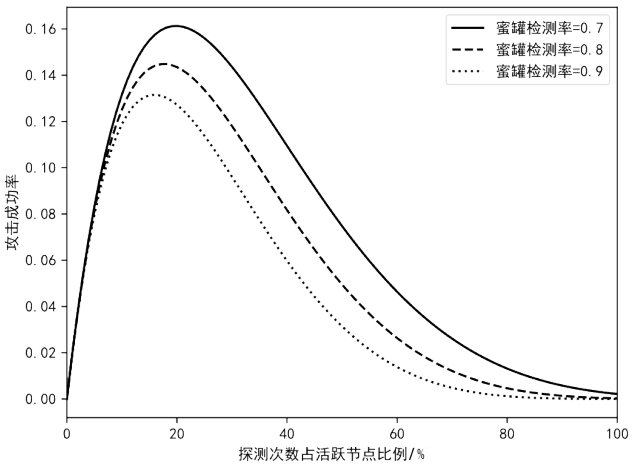

图 12 不同蜜罐检测率下探测次数与攻击成功率曲线图

4 实验结果分析

4.1 防御能力分析

本文设计实现了模型的原型系统，并在SDN交换机上进行部署，采用Intel的DPDK（Data Plane Development Kit）[18]在X86平台上实现，如图13所示，搭建目标网络对模型进行分析验证。其中攻击者IP地址为172.14.96.181，Win7操作系统，开放22、23、3389服务端口。主机A为Centos7操作系统，IP地址172.14.96.177，主机B为Win10操作系统，IP地址为172. 14.96.178，主机A、B均接入部署原型系统的SDN交换机。通过控制器进行虚拟节点配置，包括虚拟节点数量、虚拟节点配置周期。实验环境选择生成20个虚拟节点，重配置周期设置为5分钟，虚拟节点端口、MAC、操作系统均为随机选择，并对主机A进行保护，不保护主机B。将IP地址为172.14.96.179的虚拟节点C的端口设置为22、80、8080、MAC地址设置为00:21:CC:CD:24:37，操作系统设置为Linux3.10。使用KVM平台搭建了蜜罐仿真原型系统，部署了虚拟机级别的高仿真Web服务蜜罐，开启22、80、8080端口，开启了SSH与Web服务。

攻击者使用Nmap工具对主机A和主机B所在子网进行两次指纹探测获得的结果如表1所示。两次

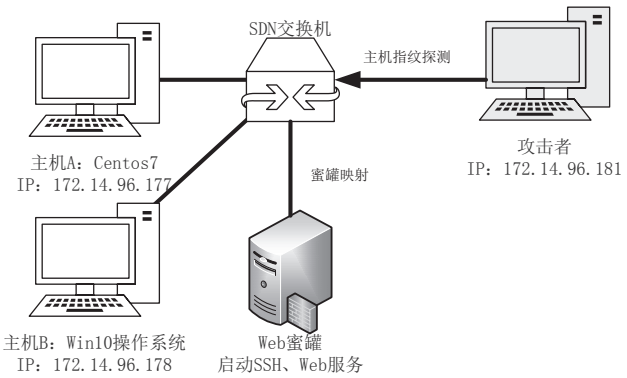

图 13 实验环境拓扑结构示意图

扫描获得的活跃节点数量均为23个，重点关注攻击者、主机A、主机B的扫描结果，同时选择IP地址为172.14.96.179的虚拟节点作为虚拟节点的代表进行对比。对于攻击者来说，由于是探测发起者，所以网络距离为0跳，扫描结果与实际配置环境吻合。对于主机B，距离攻击者的网络距离为1跳，扫描获得指纹信息与主机B信息吻合，表明当不采取保护措施时，攻击者可轻易获取主机指纹信息。两次扫描结果对比，主机A的端口、MAC以及操作系统信息均发生了跳变且与现实配置环境不同，证明虚拟节点可有效对真实节点的主机指纹信息进行保护。对于虚拟节点C，其指纹信息不受跳变影响，两次探测结果与设置吻合。

表 1 指纹探测结果

命令	IP	MAC	操作系统	端口	网络距离
2019/12/13 9:20 nmap -O 172.14.96.0/24	172.14.96.177	00:21:85:FD:C1:D2	Linux 2.7.3	80/443/1025/8080	1
	172.14.96.178	8C:89:A5:0F:17:D4	Windows 10	23/443/3389	1
	172.14.96.179	00:21:CC:CD:24:37	Linux 3.10	22/80/8080	1
	172.14.96.181	2C:53:4A:03:CF:BC	Windows 7	22/23/3389	0
2019/12/13 9:37 nmap -O 172.14.96.0/24	172.14.96.177	08:00:CD:68:31:38	Windows Server 2012 R2 Update1	22/110/3389/1433	1
	172.14.96.178	8C:89:A5:0F:17:D4	Windows 10	23/443/3389	1
	172.14.96.179	00:21:CC:CD:24:37	Linux 3.10	22/80/8080	1
	172.14.96.181	2C:53:4A:03:CF:BC	Windows 7	22/23/3389	0

设置蜜罐映射与流量诱导规则，将虚拟节点C的流量映射至蜜罐，攻击者在获得虚拟节点C的扫描结果后，发现节点C开启了22、80、8080端口且为Linux3.10操作系统，尝试对虚拟节点C进行访问和连接。使用Firefox浏览器访问虚拟节点C的Web服务，使用Securecrt工具访问虚拟节点C的SSH服务，在服务器上创建txt文件。如图14所示，攻击者对虚拟节点的访问被诱导至部署的高仿真蜜罐，并可在蜜罐管理界面捕获记录攻击行动，包括SSH登录记录、文件读写日志以及Web访问记录等行为。

图 14 攻击行为捕获记录

将模型与目前较为典型的指纹欺骗工具IPMorph进行对比，在不启用防御模型情况下在主机A上部署IPMorph工具，选定30种常见指纹类型设置模板进行探测。随后关闭IPMorph工具，启用本文模型，仍选用同样的30种指纹类型进行探测，重复3次，探测结果如表2所示。相较于IPMorph，本文模型取得了更优的欺骗效果。这是由于IPMorph的欺骗机制基于主机探测响应报文的修改，如果主机存在防火墙等防御工具，会屏蔽部分扫描探针，不会产生部分响应报文，因而无法构造虚假响应报文，导致指纹欺骗失败。本文模型则是根据虚拟指纹信息直接构造响应报文，不依赖于主机响应包，与IPMorph相比欺骗机制独立，具备更高的灵活性。

4.2 性能分析

分析本文模型导致的网络性能的额外开销，使用

表 2 探测结果对比

防御方式	探测结果与欺骗模板匹配数		
IPMorph	26	26	27
虚拟节点 - 蜜罐防御	30	29	30

思博伦测试仪上下行口连接SDN交换机，设置随机包长64~1500字节并以100Mbps速度发包，测量10次计算平均时延与标准差，结果如表3所示。与未采用防御模型的SDN交换机相比，本文模型带来的额外性能开销低于4%，同时生成虚拟节点数量对网络性能的额外开销影响极小。

表 3 时延对比

部署方式	平均时延 /μs	标准差
无虚拟节点	23.17	0.63
生成 100 个虚拟节点	24.22	0.72
生成 150 个虚拟节点	24.19	0.77
生成 200 个虚拟节点	24.25	0.73

5 结束语

本文提出一种基于软件定义网络的主机指纹抗探测模型，针对主机指纹信息保护困难的问题，通过动态生成包含主机指纹信息的虚拟节点，实现主机指纹混淆欺骗，结合蜜罐映射与流量牵引技术，将指向虚拟节点的攻击流量重定向到蜜罐进行捕获分析。建立防御效能的概率模型，量化了探测次数、虚拟节点数量、蜜罐映射规则数、允许损失数、虚拟节点欺骗率和蜜罐节点检测率等因素对攻击成功概率的影响。通过与典型指纹欺骗工具IPMorth进行对比，验证了本文模型具备更好的指纹欺骗效果，同时额外的性能开销低于5%。（责编 程斌）

参考文献：

[1] ZHUANG R, DELOACH S A, OU X. Towards A Theory of Moving Target Defense[C]//ACM. Proceedings of the First ACM Workshop on Moving Target Defense, November 3, 2014, Scottsdale, Arizona, USA. New York: ACM, 2014: 31–40.

[2] DAVID J, THOMAS C. Efficient DDoS Flood Attack Detection Using Dynamic Thresholding on Flow–based Network Traffic[J]. Computers & Security, 2019, 82(7): 284–295.

[3] SHAMSI Z, NANDWANI A, LEONARD D, et al. Hershel: Single–Packet OS Fingerprinting[J]. ACM SIGMETRICS Performance Evaluation Review, 2014, 42(1): 195–206.

[4] PRIGENT G, VICHOT F, HARROUET F. IpMorph: Fingerprinting Spoofing Unification[J]. Journal in Computer Virology, 2010, 6(4): 329–342.

[5] MA Junliang, WANG Xili, HE Juhou, et al. Research and Design of Enhanced Anti–Xprobe2[J]. Computer Engineering and Applications, 2012, 48(32): 1–4.
马君亮，汪西莉，何聚厚，等. 增强型 Anti–Xprobe2 的研究与设计 [J]. 计算机工程与应用，2012，48（32）：1–4.

[6] KAMPANAKIS P, PERROS H, BEYENE T. SDN–based Solutions for Moving Target Defense Network Protection[C]//IEEE. The Fifteenth International Symposium on a World of Wireless, Mobile and Multimedia Networks, Jun 16–19, 2014, Sydney, Australia. New York: IEEE, 2014: 1–6.

[7] JIA Zhaopeng. Research on Defense Oriented Network Spoofing Technology[D]. Beijing: Beijing University of Posts and Telecommunications, 2018.
贾召鹏 . 面向防御的网络欺骗技术研究 [D]. 北京：北京邮电大学，2018.

[8] HAN W, ZHAO Z, DOUPÉ A, et al. Honeymix: Toward Sdn–based Intelligent Honeynet[C]//ACM. Proceedings of the 2016 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, March 9–11, 2016, New Orleans Louisiana USA. New York: ACM, 2016: 1–6.

[9] LA Q D, QUEK T Q S, LEE J, et al. Deceptive Attack and Defense Game in Honeypot–enabled Networks for the Internet of Things[J]. IEEE Internet of Things Journal, 2016, 3(6): 1025–1035.

[10] FAN W, DU Z, CREASEY M, et al. HoneyDOC: An Efficient Honeypot Architecture Enabling all–round Design[J]. IEEE Journal on Selected Areas in Communications, 2019, 37(3): 683–697.

[11] SHI L, LI Y, LIU T, et al. Dynamic Distributed Honeypot Based on Blockchain[EB/OL]. https://ieeexplore.ieee.org/document/8727529, 2019–11–15.

[12] JAFARIAN J H, NIAKANLAHIJI A, AL–SHAER E, et al. Multi–dimensional Host Identity Anonymization for Defeating Skilled Attackers[C]//ACM. Proceedings of the 2016 ACM Workshop on Moving Target Defense, October 24, 2018, Vienna, Austria. New York: ACM, 2016: 47–58.

[13] ZHUGE Jianwei, TANG Yong, HAN Xinhui, et al. Honeypot Technology Research and Application[J]. Journal of Software, 2013, 24(4): 825–842.
诸葛建伟，唐勇，韩心慧，等. 蜜罐技术研究与应用进展 [J]. 软件学报，2013，24（4）：825–842.

[14] LI Yan. Design and Implementation of Honeynet Active Defense System Based on SDN[D]. Beijing: Beijing University of Posts and Telecommunications, 2019
李俨 . 基于 SDN 的蜜网主动防御系统设计与实现 [D]. 北京：北京邮电大学，2019.

[15] BONFIM M S, DIAS K L, FERNANDES S F L. Integrated NFV/SDN Architectures: A Systematic Literature Review[J]. ACM Computing Surveys (CSUR), 2019, 51(6): 1–39.

[16] HERWIG S, HARVEY K, HUGHEY G, et al. Measurement and Analysis of Hajime, A Peer–to–peer IoT Botnet[EB/OL]. http://www.cs.umd.edu/~smherwig/pub/18–imc/hajime–poster.pdf, 2019–10–15.

[17] CERON J M, STEDING J K, HOEPERS C, et al. Improving Iot Botnet Investigation Using An Adaptive Network Layer[J]. Sensors, 2019, 19(3): 727.

[18] PONGRÁCZ G, MOLNÁR L, KIS Z L. Removing Roadblocks from SDN: OpenFlow Software Switch Performance on Intel DPDK[C]//IEEE. 2013 Second European Workshop on Software Defined Networks, October 10–11, 2013, Berlin, Germany. New York: IEEE, 2013: 62–67.