基于网络攻击面自适应转换的移动目标防御技术

雷 程[1),3)] 马多贺[2)] 张红旗[1),3)] 杨英杰[1),3)] 王利明[2)]

[1)](信息工程大学密码工程学院 郑州 450001)

[2)](中国科学院信息工程研究所信息安全国家重点实验室 北京 100093)

[3)](河南省信息安全重点实验室 郑州 450001)

摘 要 移动目标防御是一种改变网络空间攻防对抗格局的革命性技术,它通过动态改变攻击面使得目标网络更具弹性.网络跳变作为有效抵御主动扫描的防御方法,是实现移动目标防御的关键技术之一.现有跳变机制由于在空间上采用随机选取方法并在时域采用固定跳变周期,极大降低了跳变防御的不可预测性和时效性;与此同时,由于跳变实施过程缺乏约束且跳变部署复杂度高,因此增加了网络开销,降低了跳变防御的可用性和可扩展性.针对以上问题,文中提出了一种基于网络攻击面自适应转换的移动目标防御技术.为了实现网络跳变收益的最大化,在分层跳变的架构上设计了一种网络自适应跳变算法.它由网络威胁感知和跳变策略生成两部分组成.通过设计基于 Sibson 熵的威胁感知机制分析扫描攻击策略,以指导网络跳变机制的选择;基于网络攻击面和网络探测面定义了网络视图和视图距离,通过设计基于视图距离的跳变策略生成算法,选取使得视图距离最大的跳变端信息集合,以最大化跳变的不可预测性;此外,通过采用跳变周期自拉伸策略保证跳变的时效性.从而通过基于视图距离的跳变策略选取与可变的跳变周期制定实现网络攻击面时空二维的自适应转换,最大化防御收益.为了解决网络资源有限条件下的跳变实施问题,利用可满足性模理论形式化描述跳变实施的约束条件,以保证跳变实施的可用性;通过设计启发式跳变实施部署算法以提高部署效率,以保证跳变防御的可扩展性.最后,理论与实验分析了该技术抵御扫描攻击的能力和跳变成本,通过以不同类型的扫描攻击为例证明了该技术在保证网络服务质量的同时可有效抵御 92.1%以上的主动扫描攻击.

关键词 移动目标防御;网络攻击面;网络探测面;网络欺骗;网络视图;启发式跳变部署

中图法分类号 TP393 **DOI 号** 10.11897/SP.J.1016.2018.01109

Moving Target Defense Technique Based on Network Attack Surface Self-Adaptive Mutation

LEI Cheng[1),3)] MA Duo-He[2)] ZHANG Hong-Qi[1),3)] YANG Ying-Jie[1),3)] WANG Li-Ming[2)]

[1)](*Cryptography Engineering Institute, Information Engineering University, Zhengzhou* 450001)

[2)](*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093)

[3)](*Henan Key Laboratory of Information Security, Zhengzhou* 450001)

Abstract Moving target defense is a revolutionary technology which has the capability of game-changing. It can dynamically shift the attack surface, making the targeted system more difficult for attackers to strike. As an effective method against malicious scanning and sniffer, network mutation is one of the key point in moving target defense research. Since existing network mutation mechanisms mainly adopt random selection method in mutation space and set fixed period mutation, the unpredictability and timeliness of network mutation are poor. Besides,

收稿日期:2016-11-26;在线出版日期:2017-08-19.本课题得到国家"九七三"重点基础研究发展规划项目(2011CB311801)、国家"八六三"高技术研究发展计划项目(2015AA016106)、郑州市科技领军人才(131PLKRC644)资助.**雷 程**,男,1989 年生,博士研究生,主要研究方向为网络与信息安全、移动目标防御、数据安全交换.E-mail:leicheng12150@126.com.**马多贺**(通信作者),男,1982 年生,博士,助理研究员,主要研究方向为网络与信息安全、移动目标防御、云安全.E-mail:maduohe@iie.ac.cn.**张红旗**,男,1962 年生,博士,教授,博士生导师,主要研究领域为网络与信息安全、等级保护、信息安全管理.**杨英杰**,男,1971 年生,博士,副教授,主要研究方向为数据挖掘、态势感知和信息安全管理.**王利明**,男,1978 年生,博士,副研究员,主要研究方向为可信网络、云计算安全等.

existing mechanisms have low usability and poor expandability due to the lack of constraints and high complexity in the implementation of network mutation. In order to achieve maximizing mutation defense benefit on the basis of ensuring the network service quality, a novel of moving target defense technique based on network attack surface self-adaptive mutation is proposed. On one hand, hierarchical mutation architecture is used so as to increase the flexibility of network mutation. Based on it, self-adaptive endpoint mutation algorithm is designed. It consists of network threat awareness mechanism and mutation strategy algorithm. Firstly, network threat awareness mechanism based on Sibson entropy is proposed, thus guiding the selection of network mutation mechanism through perceiving malicious scanning strategies. What's more, network view and view distance are defined based on attack surface and exploration surface. Based on it, mutation strategy algorithm is proposed. It selects mutation endpoint information set which can maximize network view distance, thus improving the unpredictability of network mutation. Besides, in order to guarantee the timeliness of network view, mutation period stretch strategy is adopted. As a result, by adopting endpoint mutation selection based on network view and changeable mutation period, network attack surface transforms in a self-adaptive way by the combination of spatial and temporal mutation, in which maximizes the defensive benefit. On the other hand, virtual endpoint mutation is used in order to decrease the overhead of network mutation. Based on it, satisfiability modulo theory is used to solve the lack of mutation constraints problem in the limited network resource during network mutation. Since solving satisfiability modulo theory problem is non-deterministic polynomial problem, heuristic mutation deployment algorithm is designed so as to optimize the computational efficiency, thus ensuring the expandability of network mutation implementation. Moreover, in order to guarantee the consistency of net-flow table update, the "delete in sequential order, and add in reversed order" policy is adopted. Therefore, by adopting heuristic method based on satisfiability modulo theory and proposing net-flow table update policy, it ensures availability of network mutation. Theoretical and experimental analysis show the ability of resisting scanning attacks and mutation cost. Compared with existing typical endpoint mutation mechanisms such as Random Host Mutation and Spatial and Temporal Random Host Mutation, the proposed method can disrupt more than 92.1% of different types of scanning strategies in network attacks. Besides, the flow table size of the proposed method decreases 69.24%, and the packet drop rate also decreases 64.13%. Consequently, it verifies the proposed technique can not only ensures the network service quality, but also be effectively perceiving and resisting different types of scanning strategies in network attacks.

Keywords moving target defense; network attack surface; network exploration surface; cyber deception; network view; heuristic mutation deployment

1 引 言

随着网络应用的不断普及和深化,互联网一方面正在深刻影响着人们的生活方式,孕育着社会运转的新常态;另一方面也成为国家战略性关键基础设施,支撑着国家重要领域的有效运转.然而,近年来以高级先进持久威胁为代表的网络攻击手段层出不穷,互联网安全面临严峻挑战.尽管现有以"堵漏洞、打补丁、筑高墙"为代表的防御机制力求消除缺陷、填补不足、降低损害[1].根据国家互联网应急中心发布的《2015 年中国互联网网络安全报告》统计表明,2015 年网络安全事件 126916 起,同比 2014 年增长了 125.9%[2].网络攻防的核心是围绕资源脆弱性的利用和预期网络状态的实现开展的.从攻击方的角度分析,攻击过程可分为离线和在线两个阶段.离线阶段主要是侦测和剖析目标系统,通过侦测目标系统发掘和锁定可被利用的资源脆弱性,依据侦测信息研究

和制定相应的攻击方法；在线阶段主要是实施攻击，依据制定的策略开展相应攻击行动，通过让目标系统达到预期的状态以实现攻击目的. 攻击者可通过长期侦测，收集目标网络系统的配置信息并发掘网络资源的脆弱性. 漏洞一旦被确认，攻击者可以通过继续安装定制的后门来长期控制、威胁网络系统. 从防御方的角度分析，现有以“堵漏洞、打补丁、筑高墙”为代表的防御方法主要可分为嵌入阻塞和重塑结构两种方式. 重塑结构的防御方法针对系统固有的漏洞，通过放插件、打补丁等方法使资源脆弱性不可用；嵌入阻塞的防御方法则针对系统运维的缺陷，通过访问控制、入侵检测等方法使不合规的系统状态不可达.

虽然现有防御方法已经发展的相当成熟，但是认知的局限性使重塑结构的防御方式难以发掘所有的脆弱性信息；机制的固定性使阻塞嵌入的防御方法难以抵挡攻击方离线阶段的持续侦测和长期分析，互联网安全面临易攻难守的严峻挑战. 究其根源，可归结为：(1) 网络系统体系结构上存在固有安全缺陷，实践中工程链诸环节的安全性难以证明，设计的缺陷和安全漏洞往往在所难免，攻防双方存在信息不对称的特性；(2) 网络组成的确定性和结构的静态性为网络杀伤链的执行提供了所需的依存环境，攻防双方存在时间不对称特性；(3) 网络空间要素的单一性加剧了攻防态势的不平衡，攻防双方存在成本不对称的特性. 因此，在网络攻击趋向组合化、自动化的态势下，现有防御方法难以有效应对愈加复杂和智能的渗透式网络入侵，攻防双方地位的不对称日益加剧.

为了“改变游戏规则”，移动目标防御(Moving Target Defense，MTD)[3] 应运而生. 它针对攻防双方地位的不对称性和目标系统缺乏弹性的问题，以防御者可控的方式对网络系统进行多层次的主动变迁，通过动态、随机地改变网络配置属性，多样化网络要素组成，从而构建一种持续动态、多样的网络环境，以破坏攻击链对运行环境确定、单一特质的依赖. 研究表明，攻击者有 95% 的时间用于收集目标网络信息并策划攻击方法. 因此，网络扫描作为各种攻击手段的先导技术和初始阶段，为网络攻击的有效实施发挥着不可替代的作用[4]. 端节点信息，即 IP 地址和端口信息，作为网络层攻击面[5] 的有机组成部分和网络扫描的主要对象，成为了亟需被防护的重要网络属性. 因此，网络跳变[6] 作为实现移动目标防御的重要机制之一被广泛研究.

在分析总结现有研究的基础上，针对跳变防御收益和网络服务质量难以平衡的问题，提出了基于网络攻击面自适应转换的移动目标防御技术(Moving Target Defense based on Network Attack Surface Self-Adaptive Mutation Technique，NAS-SAMT). 该技术在保证网络服务质量的前提下最大化防御收益，具有以下创新性：

(1) 基于威胁感知触发跳变策略，提高网络跳变策略选取的针对性：针对网络跳变策略选择存在盲目性的问题，在构建安全威胁模型的基础上，设计基于 Sibson 熵的威胁感知机制. 针对盲扫描、半盲扫描和跟随扫描策略的特点，利用假设检验分析并判断，从而指导下一步跳变策略的选择.

(2) 基于视图距离自适应变换网络攻击面，提高网络跳变的不可预测性和时效性：针对网络跳变空间有限的问题，提出基于视图距离的跳变策略生成方法. 依据网络攻击面和网络探测面的视图距离，选取使得不同跳变策略下视图距离最大的跳变端信息，从而提高网络跳变的不可预测性. 与此同时，通过跳变周期拉伸策略保证网络端信息变换的时效性，从而最大化防御收益.

(3) 基于启发式跳变部署限制和降低跳变实施性能开销，提高网络跳变的可用性和可扩展性：针对网络资源有限且网络跳变实施缺乏约束的问题，采用基于可满足性模理论[7](Satisfiability Modulo Theories，SMT) 的启发式算法，通过 SMT 形式化描述跳变所需满足的性能约束；采用启发式算法实现网络跳变的高效部署，从而降低跳变实施过程中的网络性能开销，保证网络服务质量.

本文第 2 节介绍网络跳变的背景知识和相关工作；第 3 节构建威胁模型；第 4 节设计网络自适应跳变方案，它由基于 Sibson 熵的威胁感知、基于视图距离的跳变策略生成和基于 SMT 的启发式跳变部署三部分组成；第 5 节构建基于自适应跳变的网络移动目标防御架构，给出通信协议与跳变更新策略；第 6 节和第 7 节通过理论分析和仿真实验对比 NAS-SAMT 与现有典型跳变机制的防御收益与防御开销；最后，总结全文工作.

2　背景知识与相关工作

2.1　软件自定义网络与 OpenFlow

软件定义网络[8](Software-Defined Network，SDN) 是基于逻辑控制和数据转发分离设计思想，将路由器和交换机等网络设备的控制功能从数据转发功能中解耦处理的网络架构. 它由一个可编程的逻辑集中式控制器管理整个网络；由底层转发设备实

现数据转发功能. SDN 集中控制的特点使得控制器可以在线获取网络性能指标,并在此基础上及时调配资源、实施全局决策. OpenFlow 协议则是控制器管理和配置底层网络设备的主流通信协议. 在基于 OpenFlow 的 SDN 网络中,各应用依据网络管理者定制的策略生成规则,控制器将形成的规则逻辑视图映射到物理交换机中形成规则物理视图,OpenFlow 协议则将规则以流表形式下发到交换机上,从而确定数据包的转发路径.

随着网络拓扑规模不断扩大、组成愈加复杂,现有 OpenFlow 交换机每秒可新增的流表项仅为 150 条~750 条左右. 若采用高速三态内容寻址存储器(Ternary Content Addressable Memory, TCAM)提高交换机寻址速率. 基于 TCAM 的 OpenFlow 交换机每秒可新增的流表项为 2000 条~4000 条左右[9].

2.2 移动目标防御的设计原则

移动目标防御(Moving Target Defense, MTD)是由移动目标的思想发展而来. 2011 年美国总统行政办公室国家科学与技术委员会发布的《可信网络空间:联邦网络空间安全研究与发展项目战略计划》①报告中对移动目标防御的定义为:"一种通过创建、分析、评估和部署多样化、随时间持续变换的机制或策略,增加攻击者实施攻击的复杂度和成本,限制和降低系统脆弱性曝光程度和被攻击概率,提高系统弹性的防御手段."

由移动目标防御定义可知[10],移动目标防御机制要具有不可预测性、时效性、可用性和可扩展性:

(1)不可预测性. 由于移动目标防御需要通过不断改变攻击面和探测面以增加攻击者的侦测空间、破坏网络攻击对网络杀伤链的依赖.

(2)时效性. 由于网络资源脆弱性无法被全部转移,因此依然存在被暴露的攻击面,移动目标防御需要通过适宜的跳变频率以压缩攻击者的侦测时间、提高网络攻击的成本开销.

(3)可用性. 由于移动目标防御需要不断变换攻击面和探测面,因此需要通过选取适宜的变换要素和变换频率保证合理的防御开销.

(4)可扩展性. 由于移动目标防御需要不断更新部署信息,因此实施过程应将目标网络系统作为"黑盒"处理,并保证部署的效率.

2.3 网络跳变的相关工作

现有网络跳变研究根据所依托的网络架构可分为以下两类:

(1)传统网络架构下的端信息跳变. Kewley 等人[11]提出了一种动态网络地址变换的方法(Dynamic Network Address Translation, DYNAT). 它通过变换 TCP/IP 报头信息欺骗攻击者对目标网络的扫描,从而只有合法用户通过正确变换报文信息才能与服务器进行安全交互. Fink 等人[12]提出了一种自同步的动态地址转换方法,它在 TCP 三次握手的过程中协商会话通信的跳变地址,并在每次跳变更新时进行认证,从而实现会话过程中的端信息跳变. Antonatos 等人[13]则提出了基于网络地址空间随机化的自主式防御方法(Network Address Space Randomization, NASR). NASR 通过分析潜在被感染的端节点,利用动态主机设置协议(Dynamic Host Configuration Protocol, DHCP)改变端节点信息,以规避可能存在的蠕虫攻击. Badishi 等人[14]则提出了一种轻量级的端口跳变方法,在区分正常用户和攻击者的情况下通过跳变端口以实现对攻击者的欺骗. MT6D[15]利用 IPv6 地址空间大的特性实施 IP 地址的跳变. 该方法在每个跳变周期内通过哈希函数和当前交互标识(Interface Identifier, IID)、共享对称密钥以及系统时间戳计算通信双方的下一跳 IP 地址. 与此同时,为了提高跳变的安全性,MT6D 的跳变周期是随机改变的. 林楷等人[16]通过额外开放前后两个跳变时隙对应的 IP 和端口实现对同步失败数据包的接收,以提高同步的成功概率. 由于实际端信息跳变需要消耗大量节点资源,因此极大地降低了跳变实施的可用性. 由于虚拟跳变是通过构建真实端信息与虚拟端信息映射关系,从而在不改变节点实际端信息的情况下实现网络跳变的方法,因此可有效降低跳变产生的开销. Jia 等人[17]提出了 MOTAG 架构,通过在云服务周围部署隐蔽代理变换通信路径. 当 DDoS 对代理实施攻击时,MOTAG 通过切换代理的方式削减 DDoS 攻击对目标系统的影响,并保证用户的正常使用. 为了进一步提高跳变 IP 地址的随机性,Sun 等人[18]提出了一种基于虚拟机的无缝端信息跳变方法. 通过虚拟化技术实施端信息跳变和蜜罐动态生成,从而提高攻击者的视在不确定性. Al-Shaer 等人[19]提出了随机端信息跳变方法(Random Host Mutation, RHM),它采用了双层跳变机制,其中低频跳变周期是预先设定的,它包含了整数倍的高频跳变周期;每个节点的高频跳变周期则是依据端节点的重要程度设定的. 然而,该方法中

① Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program https://www.nitrd.gov/SUBCOMMITTEE/csia/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf

高频跳变周期是随机确定的，因此盲目的跳变会增加网络跳变的成本，难以适用于资源有限的网络情况. 与此同时，传统网络架构下的网络跳变存在路由同步的问题. Hari 等人[20]在随机端口跳变(Random Port Hopping，RPH)的基础上引入离散马尔可夫链以提高通信双方的通信成功率. Malathi[21]通过设计 HOPERAA 算法，解决了线性时钟漂移对网络跳变同步的影响. 由于传统网络中分布式路由不易于管理，它一直是阻碍端信息跳变有效实施的关键瓶颈.

(2)软件定义网络架构下的端信息跳变. 由于 SDN 网络具有逻辑控制与数据转发相分离的特性，这为解决分布式路由难以有效协同管理的问题带来了新思路. 基于 SDN 的网络跳变可动态修改跳变周期和跳变规则，可有效提高网络跳变的可管理性. SDNA[22]通过在每个子网内部署一个超级管理节点将实际 IP 地址转换为虚拟 IP 地址，实现对端节点的虚拟跳变，以防止外部攻击者对内部网络节点的扫描. 然而每个端节点在建立链接时都要流经对应子网内的管理节点进行身份认证和地址转换，极大增加了管理节点的负载和跳变的实施成本，降低了跳变的可用性. OF-RHM[23]是一种基于 OpenFlow 的 IP 转换机制，通过每次会话时将实际 IP 转换虚拟 IP 实现端地址跳变. 该方法通过形式化描述选取 IP 所需满足的约束，在此基础上利用平均概率或者权值的方法选取跳变的 IP 地址实施跳变. 然而，OF-RHM 中每个子网内的端节点跳变周期是相同的，极大地限制了网络跳变的随机性. MacFarland 等人[24]提出了基于 SDN 的端信息混淆机制，SDN 控制器在每个连接建立时利用端节点的真实 IP 和 MAC 地址获得合成 IP(synthesis IP，sIP)，从而防止端节点真实地址泄露. 然而，该方法利用控制器实施网络跳变，易造成控制器负载过大而导致跳变机制可用性差. Wei 等人[25]提出了基于 OpenFlow 的重定向跳变方法，通过增加额外的交换代理将可信的正常用户和可疑用户进行区分，并在此基础上通过交换代理动态迁移抵御 DDoS 攻击. 然而，该方法由于需要在 SDN 网络中部署大量的额外交换代理，因此防御成本过高，实用性差. 针对该问题，Debroy 等人[26]提出了一种基于 SDN 的低频跳变方法. 它利用虚拟机作为隐蔽交换代理实施动态迁移，并通过分析目标网络的安全态势确定跳变的周期，从而降低跳变的成本. Ma 等人[27]提出了一种基于可满足性模理论的端信息跳变方法. 该方法利用可满足性模理论形式化描述网络跳变所需满足的要求，从而有效降低跳变实施的性能开销. 然而，由于 SMT 求解是 NP 问题，因此部署实施的复杂度随着约束条件的增多而增加. Wang 等人[28]则提出了一种基于嗅探反射器的恶意侦测防御方法. 它基于 SDN 构造影子网络，通过反馈随机生成的目标网络信息迷惑攻击者，从而抵御恶意扫描攻击. 然而，以上机制由于仅实施了空间跳变，当攻击者改变扫描频度对目标系统进行跟随扫描时，其跳变的有效性会随之大幅下降. 针对该问题，Jafarian 等人[29]提出了一种时空混合随机跳变(Spatial and Temporal-Random Host Mutation，ST-RHM)机制，它基于 SDN 架构在地址空间跳变的基础上加入时域随机跳变，从而通过时间-空间二维混合跳变以抵御协同扫描. 然而，由于该方法需要对节点空间和时域空间进行双重跳变，随着网络规模和跳变频率的增加，跳变的性能损耗也随之增加，从而具有较大的开销. 此外，尽管以上跳变机制各有优势，但由于它们跳变策略单一、端信息选取盲目，因此防御有效性低.

综上所述，现有网络跳变技术主要存在以下问题：

(1)由于跳变机制缺乏对恶意扫描策略的感知，导致跳变防御策略的选取具有盲目性：随着网络扫描策略愈加多变且具有针对性，“盲目随机”的跳变策略将极大降低防御的效能. 因此，如何面向不同扫描策略有针对地选取跳变策略成为了保证跳变有效的前提.

(2)由于有限跳变空间和固定的跳变周期，导致跳变防御有效性差：由于存在网络跳变中可选攻击面维度和取值范围的有限性，导致跳变不可预测性降低；与此同时，跟随扫描策略可通过变换扫描频率实现端信息跟踪，导致跳变时效性差. 因此，如何提高网络跳变的不可预测性和时效性成为了跳变防御是否有效的关键.

(3)由于跳变实施缺乏约束且部署复杂度高，导致网络跳变防御的可用性和扩展性差：网络跳变的成本主要包括性能消耗和管理成本. 跳变实施增加的网络性能开销是导致跳变可用性差的关键要素. 与此同时，随着网络规模的增加，如何高效部署成为了制约网络跳变实施的关键瓶颈之一. 因此，如何保证跳变机制的可用性和可扩展性成为了跳变防御能否有效实施的保障.

3　威胁模型

假设攻击者的目标是毁瘫网络中的一个服务节

点,其攻击流程如图 1 所示.如图 1 中灰色部分所示,攻击者在实施攻击前主要是发掘目标节点所在子网,并通过扫描目标节点的活跃端口和服务列表识别目标节点的资源脆弱性.因此,网络扫描[4]是各种攻击手段的先导技术和初始阶段,主要分为 3 个阶段:

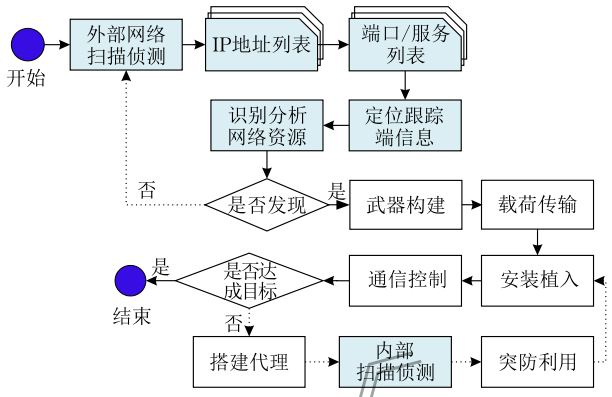

图 1 网络攻击流程图

(1) IP 地址探测阶段.它是网络扫描的第一个阶段,攻击者通过发送 ICMP 回应请求报文在未知网络中探测端节点的可达性和 IP 地址.

(2) Port 探测阶段.端口探测是网络扫描的第二个阶段.当攻击者锁定了活跃的端节点 IP 地址,它会通过 TCP 扫描和 UDP 扫描探测目标节点的开放端口列表.其中,针对 TCP 的扫描主要利用全 TCP 扫描,即通过 TCP 三次握手与目标节点建立完整 TCP 连接以确定端口是否开放;伪造 TCP 报文片段,如伪造的 SYN、FIN、Xmas 和 NULL 位等报文探测目标端口是否开放.对 UDP 的扫描侦测则主要利用 ICMP 报文实施.

(3)资源脆弱性探测.当目标节点的 IP 和开放端口被锁定,攻击者会进一步对端节点的系统指纹、所用协议配置和漏洞等进行探测,从而为接下来设计后门、制定攻击策略和实施攻击做准备.由于主流系统指纹扫描工具,如 SinFP3、Namp 等,是通过 TCP/IP 协议中的协议代码、TCP 选项推断通信双方所用协议和系统指纹的.因此协议代码、TCP 选项是系统指纹最具判别性的特征.

由于网络扫描是通过向选定范围内的节点发送探测报文以获取目标网络中节点信息的侦测手段,因此可用扫描速率(Scanning Rate,r_{scn})和扫描频率(Scanning Frequency,f_{scn})两个属性描述.其中,扫描速率是单位时间内扫描源访问不同目的地址的连接数量,它表征某一时刻攻击者的扫描范围,且扫描宽度=平均扫描速率×时间.扫描频度是扫描源对每个目的地址发出的扫描数量,它表征扫描的频次.攻击者针对网络的结构特点和获得的先验知识,采用不同的扫描策略,以提高扫描的有效性.依据扫描速率和扫描频度可分为盲扫描、半盲扫描、跟随扫描和混合扫描 4 种策略:

(1)盲扫描策略.盲扫描策略是攻击者对全部节点空间内的端信息进行均匀扫描以侦测活跃端节点所采用的策略.由于现有网络架构具有确定、静态的特性,因此,盲扫描策略具有高扫描速率和低扫描频率的特点.攻击者通过采用盲扫描策略可实现无重复的均匀扫描[30],以提高侦测速率.

(2)半盲扫描策略.半盲扫描策略是攻击者对选定范围的节点空间进行重复性非均匀扫描以侦测活跃端节点所采用的策略.由于攻击者已知端节点的分布状况,因此,半盲扫描策略具有较高扫描速率和固定扫描频率的特点.攻击者通过半盲扫描进行重复性的非均匀扫描[14],以提高扫描的成功率.

(3)跟随扫描策略.跟随扫描策略是攻击者对特定节点进行非均匀扫描,并通过压缩端信息空间和改变扫描频率等手段对特定跳变节点空间进行努力跟随以侦测活跃端节点所采用的策略.这是一种针对网络跳变的恶意扫描策略,因此,跟随扫描策略具有低扫描速率和变扫描频率的特点.当防御者实施随机网络跳变时,攻击者依据获得的节点分布和跳变周期规律[31],努力使扫描持续指向特定的端节点.

(4)混合扫描策略.混合扫描策略是攻击者通过综合使用盲扫描、半盲扫描和跟随扫描策略以实现高效侦测活跃节点所采用的策略.攻击者依据获得知识信息的改变动态地调整扫描频率和扫描速率,从而提高扫描的有效性.

4 网络自适应跳变设计

网络跳变通过伪随机地改变通信双方的系统配置和状态,如 IP 地址和端口以及操作系统指纹等信息,实现持续、动态地转移被防护系统的网络攻击面,以诱骗、迷惑和混淆攻击者的探测,从而提高漏洞和后门的利用难度,增加攻击的难度和成本,达到保证目标系统安全的目的.现有的研究主要采用自主式跳变方法[22,29],它依据安全目标进行跳变配置,并通过跳变实施部署下发网络跳变配置信息.由于自主式跳变缺少对攻防环境的感知,因此在跳变策略选取的针对性、跳变策略制定的有效性和跳变实施部署可用性上具有一定的局限性.

针对以上问题，NAS-SAMT 采用网络自适应跳变进行主动防御. 它由网络威胁感知、跳变策略生成和跳变实施部署三部分组成，具体如图 2 所示. 在前期研究的基础上[32]采用基于 Sibson 熵的威胁感知机制，通过假设检验分析恶意扫描策略，以提高跳变策略选取的针对性；在此基础上，设计基于视图距离的跳变策略生成算法，通过选取使得视图距离最大的跳变端节点，并利用跳变周期自拉伸策略从时空二维自适应地转换网络攻击面，以提高跳变的不可预测性和时效性；与此同时，提出基于 SMT 的启发式跳变部署算法，形式化描述 NAS-SAMT 要满足的跳变性能约束，以保证跳变实施的低开销和可扩展性. 从而在保证网络服务质量的前提下最大化防御收益. NAS-SAMT 中涉及的主要符号如表 1 所示.

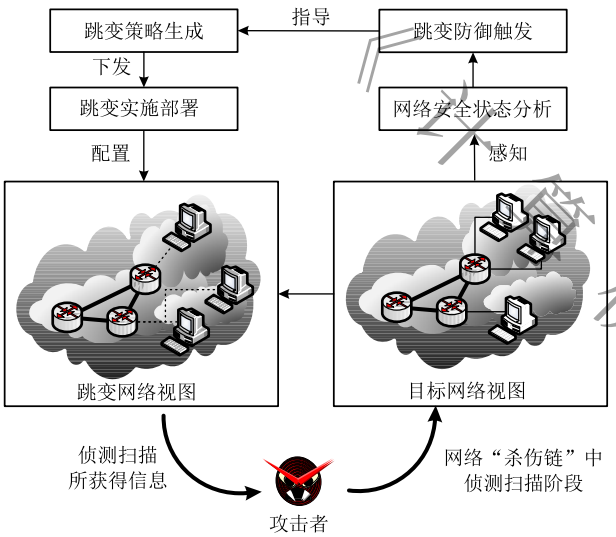

图 2　网络自适应跳变架构

表 1　NAS-SAMT 所用的符号

符号	含义
T_{BHR}	基跳变周期
T_{LTHR}	低频时域跳变周期
T_{HTHR}	高频时域跳变周期
T_{EHP}	端节点信息跳变周期
m_B	基跳变周期对应的跳变空间
m_L	低频时域跳变周期对应的跳变空间
m_H	高频时域跳变周期对应的跳变空间
N_{fail}	请求失败的报文总数量
$P_i^{Src}(\pi)$	请求失败报文中源地址的分布概率
$P_i^{Dst}(\pi)$	请求失败报文中目的地址的分布概率
$\boldsymbol{\varphi}$	网络状态初始分布向量
$\boldsymbol{P}$	网络状态马尔可夫链转换矩阵
$\boldsymbol{B}$	网络延迟观测矩阵
D_{NV}	网络视图 NV 的视图距离
w_i^{EI}	权值
$C(hR_i)$	路由最大承载量
$L_{\max}$	转发路径最大长度
C_{j_1,j_2},B_j^k,b_i^k	布尔变量
δ_i,B_f	设定的阈值

假设有 $H=\{h^1,h^2,\cdots,h^l\}$ 端节点分布在 $\{s^1,s^2,\cdots,s^k\}$ 的子网内需要进行防御，每个子网分配的跳变节点信息空间为 $\{hEI_1,hEI_2,\cdots,hEI_k\}$. 跳变节点信息(hopping Endpoint Information，hEI)由 IP 地址、端口和协议组成，可表示为 $hEI=\{hIP,hPort,hProtocol\}$. 可用跳变节点空间即为所有跳变空间 hEI_A 去除实际的节点信息(Endpoint Information，EI)，即 $EI=\{IP,Port,Protocol\}$ 以及不符合要求的节点信息空间的集合，具体可以表示为：$\{hEI\mid hEI_A\wedge\neg(EI_1\vee\cdots\vee EI_t)\wedge\neg(hEI)\}$. 由于每个端节点跳变的不可预测性与选择的可用跳变节点空间大小成正相关；每个子网在给定时刻只能分配特定地址块，所有端节点无法同时从所有可用跳变节点空间中随机选取. 因此 NAS-SAMT 采用分层跳变的方法分配跳变节点信息空间.

$$N_{hEI}=\sum_{s_x}N_{\mathrm{BHR}}^x,\ N_{\mathrm{BHR}}=\sum_{i\in s_x}N_{\mathrm{LTHR}}^i,$$

$$N_{\mathrm{LTHR}}^i\geq\left\lceil\frac{T_{\mathrm{LTHR}}}{T_{\mathrm{EHP}}^i}\right\rceil n_{\mathrm{HTHR}}\tag{1}$$

$$n_{\mathrm{HTHR}}=f(V^i)\tag{2}$$

如式(1)所示，可用跳变空间 $\{hHI\}$ 在 NAS-SAMT 中依据子网的数量和规模在 T_{BHR} 内被划分为 m_B 个大小不同的基跳变空间块(Base Hopping Range，BHR)；每个 BHR 则在 T_{LTHR} 内依据子网中端节点的个数和重要程度划分为 m_L 个不同的低频时域跳变地址块(Low-frequency Temporal Hopping Range，LTHR)；每个 LTHR 在 T_{HTHR} 内分配给端节点大小为 n_{HTHR} 的高频时域跳变地址块(High-frequency Temporal Hopping Range，HTHR)，端节点依据不同的跳变策略从相应的 HTHR 中选取一个 hEI. 其中 n_{HTHR} 与端节点的重要程度关系如式(2)所示，端节点在一个高频时域跳变周期内分配的端信息空间 n_{HTHR} 随主机节点 i 重要程度 $V^i\in[0,10]$ 的增加而增加；且有 $T_{\mathrm{HTHR}}=T_{\mathrm{EHP}}$，$T_{\mathrm{BHR}}=c\cdot T_{\mathrm{LTHR}}$，$(c\in Z^+)$ 成立.

4.1　基于 Sibson 熵的网络威胁感知

为了提高跳变防御的针对性，NAS-SAMT 通过统计探测报文确定恶意扫描的目标，并利用基于 Sibson 熵的假设检验通过分析不同扫描策略的行为特点感知不同扫描策略，以指导下一步的跳变策略生成.

NAS-SAMT 首先设定一个探测时间窗口 $T_{\mathrm{EHP}}<T_c<T_{\mathrm{LTHR}}$，通过分析探测时间窗口内的扫描频率判断是否存在恶意扫描行为. 因为总存在探测时间窗

口内只有正常用户的探测行为，可以由此获取正常用户的扫描频率区间，具体如式(3)和式(4)所示：

$$f_{\mathrm{scn}}^{S}-\overline{f_{\mathrm{scn}}^{S}}\geq\frac{1}{k}\sum_{i=1}^{k}\max(f_{\mathrm{scn}}^{S_i})-\min(f_{\mathrm{scn}}^{S_i}) \quad (3)$$

$$f_{\mathrm{scn}}^{D}\geq\frac{1}{l}\sum_{i=1}^{l}\max(f_{\mathrm{scn}}^{D_i}) \quad (4)$$

如式(3)所示，NAS-SAMT 通过计算只有正常用户扫描行为条件下，探测的平均扫描频率 $\overline{f_{\mathrm{scn}}^{S}}$ 和扫描频率最大值和最小值的平均标准偏差 $\frac{1}{k}\sum_{i=1}^{k}\max(f_{\mathrm{scn}}^{S_i})-\min(f_{\mathrm{scn}}^{S_i})$，分析 k 个子网内的扫描频率是否超过正常阈值. 若超过阈值，则说明存在异常扫描行为. 在此基础上，利用式(4)判断被恶意扫描的目标节点. 它通过计算只有正常用户扫描行为条件下，目的节点的平均扫描频率 $\frac{1}{l}\sum_{i=1}^{l}\max(f_{\mathrm{scn}}^{D_i})$，判断被保护的 l 端节点中潜在的目标节点.

在判定存在异常扫描行为并确定扫描目标之后，利用 Sibson 熵统计请求失败报文的概率分布以确定扫描策略. 之所以对请求失败的报文进行分析是因为请求成功的报文中同时包含合法用户和攻击者成功扫描的请求报文，且在一个跳变周期内划分的节点空间只有一个为有效值，而剩余的均无效，因此分析的样本数量可有效刻画恶意扫描策略. Sibson 熵是基于信息论计算两个给定概率分布差异度的理论，它针对相对熵非对称的问题进行了改进. 由于 Sibson 熵具有较高的准确性和良好的稳定性[33]，适用于不同网络条件下的异常检测，并取得了较好的效果. 假设第 t 次 T_{EHP} 内请求失败的报文总数量为 N_{fail}，第 i 块划分的节点空间中请求失败的报文数量可表示为 N_{fail}^{i}.

$$P_i^j(\pi)=\pi_k\cdot\Big(\sum_{k=1}^{N_{\mathrm{fail}}}\pi_k\Big)^{-1} \quad (5)$$

$$D_S(P_{t-1}^{Src}(\pi),P_t^{Src}(\pi))=\frac{1}{2}\{D_i[P_{t-1}^{Src}(\pi),\overline{P^{Src}}]+D_i[P_t^{Src}(\pi),\overline{P^{Src}}]\} \quad (6)$$

基于 Sibson 熵的策略感知方法首先计算式(5)计算每个 T_{EHP} 内请求失败报文的源地址概率分布 $P_i^{Src}(\pi)$ 和目的地址的概率分布 $P_i^{Dst}(\pi)$，其中 $j\in\{Src,Dst\}$，$\pi\in\{hEI\}$. 如式(6)所示，通过计算第 i 个跳变端节点在两个相邻 T_{LTHR} 中请求失败报文的源地址概率分布的 Sibson 熵，分析相邻 T_{LTHR} 中扫描各端节点的源地址分布以判断是否存在跟随扫描. 之所以选取相邻的 T_{LTHR} 是因为对于每个端节点，相邻 T_{LTHR} 的 $P_i^{Src}(\pi)$ Sibson 熵相较于相邻 T_{EHP} 的 $P_i^{Src}(\pi)$ Sibson 熵可有效避免由于网络干扰造成的误判，从而准确性更高. 在此基础上，通过与设定的置信区间比较以判断是否为跟随扫描策略. 其中 $D_i(p,q)=\sum_{\pi\in\Pi_i}p(\pi)\cdot\log\frac{p(\pi)}{q(\pi)}$；$\overline{P^{Src}}=\frac{1}{2}[P_{t-1}^{Src}(\pi)+P_t^{Src}(\pi)]$.

$$\frac{N_{\mathrm{fail}}^{i}-N_{\mathrm{fail}}/m_Bm_L}{(m_Bm_L)^2/12}<-\xi \quad (7)$$

$$D_S\Big(P_t^{Dst}(\pi),\frac{N_{\mathrm{fail}}}{m_B'm_L'}\Big)=\frac{1}{2}\left\{D[P_t^{Dst}(\pi),\overline{P_t^{Dst}}]+D\left[\frac{N_{\mathrm{fail}}}{m_B'm_L'},\overline{P_t^{Dst}}\right]\right\} \quad (8)$$

若不存在跟随扫描，则通过分析 T_{EHP} 内扫描的端节点目的地址分布以判断是否存在盲扫描. 式(7)利用肖维勒准则剔除异常的高频跳变地址块 m_H. 因为攻击者如果采用盲扫描策略，那么理想状况下每个划分的节点空间在每个 T_{EHP} 内平均被扫描的次数为 N_{fail}/m_Bm_L. 然而，由于一次 T_{EHP} 内攻击者不一定能够完成对全网地址空间的随机扫描，直接计算请求失败报文中目的地址概率分布与 N_{fail}/m_Bm_L 的 Sibson 熵将偏大. 式(8)则在式(7)的基础上通过计算第 t 个 T_{EHP} 内请求失败报文中目的地址概率分布与修正后平均概率分布的 Sibson 熵. 从而判定攻击者是否采用盲扫描策略. 其中相对熵为 $D(p,q)=\sum_{\pi\in\Pi}p(\pi)\cdot\log\frac{p(\pi)}{q(\pi)}$；$\overline{P_t^{Dst}}=\frac{1}{2}\left(P_t^{Dst}(\pi)+\frac{n_{\mathrm{fail}}}{m_E'm_L'}\right)$，$m_E'm_L'$ 为剔除异常节点空间后剩余的节点空间划分个数.

4.2 基于视图距离的跳变策略生成

如图 3 所示，NAS-SAMT 在攻击面与探测面的基础上，通过定义视图距离生成跳变策略，以保证跳变的有效性.

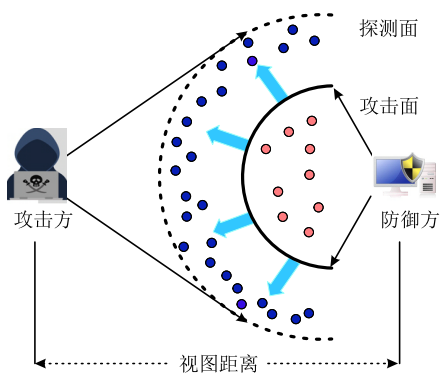

图 3 网络攻击面与网络探测面

定义 1. 攻击面(Attack Surface,AS). 又称为内部攻击面,是在某一时刻 t,防御方为了防止攻击方进入并实现攻击目的所需转移和变换的网络资源集合,它由攻击面维度(Attack Surface Dimension,ASD)以及维度取值(Attack Surface Value,ASV)共同确定,可记为 $AS(t)=\prod ASD_i^t \cdot ASV_i^t$.

定义 2. 探测面(Exploration Surface,ES). 又称为外部攻击面,是在某一时刻 t,攻击方为了能够进入目标系统并实现攻击目的所需探索的网络资源集合,它由探测面维度(Exploration Surface Dimension,ESD)以及维度取值(Exploration Surface Value,ESV)共同决定,即为 $ES(t)=\prod ESD_i^t \cdot ESV_i^t$.

与此同时,攻击面与探测面具有以下两个特性:

(1) $\exists asd_i^t \in AS_{S_1}(t) \bigcap AS_{S_2}(t)$, s. t. $AS_{S_1}(t)\{asv_i^t\} \neq AS_{S_2}(t)\{asv_i^t\}$; $\exists esd_i^t \in ES_{S_1}(t) \bigcap ES_{S_2}(t)$, s. t. $ES_{S_1}(t)\{esv_i^t\} \neq ES_{S_2}(t)\{esv_i^t\}$,即不同的网络系统配置可能存在相同维度的攻击面(探测面),但该维度的攻击面(探测面)的取值不一定相同.

(2) $\forall t_\delta > 0$, $AS_{S_1}(t) \neq AS_{S_2}(t+t_\delta)$; $ES_{S_1}(t) \neq ES_{S_2}(t+t_\delta)$,即在一个网络系统中,系统的攻击面(探测面)及其取值(值域)随着时间发生改变.

因此,在 NAS-SAMT 中攻击面维度与探测面维度相同,即 $ESD=ASD=\{ip,port,protocol\}$. 然而,攻击面取值为 $ASV=\{\{IP\}^t,\{Port\}^t,\{Protocol\}^t\}$;探测面取值为 $ESV=\{\{hIP\}^t,\{hPort\}^t,\{hProtocol\}^t\}$.

定义 3. 网络视图(Network View,NV). 给定网络系统 N,网络视图由三元组 $NV=(H,C,\nu)$ 构成. 其中 $H=\{h^1,h^2,\cdots,h^l\}$ 是网络中可观测的端节点集合;$C \subseteq H \times H$ 是端节点之间的连通关系;$\nu: H \rightarrow EI$ 是端节点到端信息的映射关系.

由于攻击方是通过扫描侦测获得先验知识、构建网络视图;防御方是通过收集配置信息生成网络视图. 因此,攻防双方对网络系统的认知并不相同,攻击面与探测面也可能存在差异. 然而,在 MTD 攻防过程中,攻击方会通过不断扫描侦测、收集信息努力使自己构建的网络视图与防御方相同,并通过压缩探测面发掘网络视图中的攻击面;防御方则通过改变网络属性和配置信息变换网络视图和攻击面,以限制和降低系统脆弱性曝光程度. 攻防双方的视图差异被称之为视图距离,具体定义如下.

定义 4. 视图距离(View Distance,VD). 给定网络视图集合 $\{NV\}$,对于 $\forall NV_i \in \{NV\}$, $VD: NV_i \times NV_j \rightarrow D$.

视图距离满足如下几个特性:

(1) $VD(NV_i,NV_j)=VD(NV_j,NV_i) \geq 0$,即视图距离满足交换律.

(2) $VD(NV_i,NV_j)=0$,即若 NV_i 和 NV_j 相同,则它们的视图距离为 0.

如图 4 所示,NAS-SAMT 在 SDN 的全网视图基础上,依据感知的扫描策略构建 T_{EHP} 跳变周期的网络视图 $NV^{T_{\mathrm{EHP}}}=(H,C,\nu)$. 为了能够提高跳变的有效性,NAS-SAMT 基于图相似性理论确定网络视图距离,并在此基础上选取合理的跳变空间提高跳变的不可预测性;设定适宜的跳变周期保证跳变的时效性,从而实现防御收益的最大化.

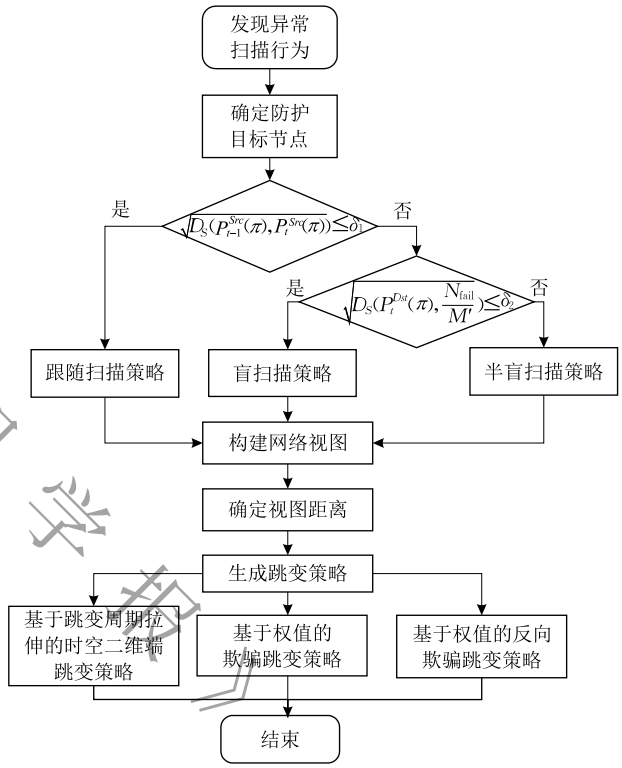

图 4　基于视图距离的跳变策略生成

$$VD(NV^{T_{\mathrm{EHP}}},NV^{T_{\mathrm{EHP}}+1}) = 2\omega_{\mathrm{base}}^{EI}\sum_{i=1}^{l}\frac{V^{ij}(|\nu_i' \bigcap \nu_j|+|C_i' \bigcap C_j|)}{V^i(|\nu_i'|+|C_i'|)+V^j(|\nu_j|+|C_j|)} \quad (9)$$

如式(9)所示,NAS-SAMT 利用图编辑距离理论[34]比对跳变周期 $T_{\mathrm{EHP}}+1$ 与 T_{EHP} 时的网络视图相似性,通过设定需要满足的最小视图距离 $D_{T_{\mathrm{EHP}}}$ 计算端信息权值基线 $\omega_{\mathrm{base}}^{EI}$. 其中 V^i 表示节点 i 的重要程度,V^{ij} 表示 $NV^{T_{\mathrm{EHP}}}$ 和 $NV^{T_{\mathrm{EHP}}+1}$ 中重合节点的重要程度. NAS-SAMT 基于 $\omega_{\mathrm{base}}^{EI}$ 选取可用跳变端信息集合,并生成跳变策略,具体如下:

(1) 当 $\sqrt{D_S(P_{t-1}^{Src}(\pi),P_t^{Src}(\pi))} \leq \delta_1$ 成立时,攻击者采用跟随扫描策略. 由于单一的空间跳变无法使跳变系统与攻击者之间存在一个空间自适应策略

的纳什均衡[16],因此 NAS-SAMT 采取基于跳变周期拉伸的时空二维跳变策略.该策略是在基于权值的欺骗跳变基础上引入跳变周期拉伸方法,其中基于权值的欺骗跳变详见下文;跳变周期拉伸是指跳变周期依据网络环境和攻击者扫描频率进行的动态改变.当攻击者实施跟随攻击时,攻击方会以低扫描速率和变扫描频率努力跟随跳变节点.因此,NAS-SAMT 依据攻击者的扫描频率减小跳变周期 T_{EHP},且随着网络异常状态持续时间的增长加速减小跳变周期,以增加通信的安全;当在连续两次跳变周期内未感知到跟随攻击,则依据网络延迟缓慢增加跳变周期,以提高通信的性能.

$$T_{\mathrm{EHP}}^{t+1}=\max[\alpha T_{\mathrm{EHP}}^{t} d/n_{\mathrm{fail}}^{t}+(1-\alpha)T_{\mathrm{EHP}}^{t},T_{\mathrm{EHP}}^{lb}] \quad (10)$$

跳变周期减小的幅度如式(10)所示,它表示在第 $t+1$ 次的 T_{EHP}^{t+1} 由攻击者的扫描频率和第 t 次的跳变周期共同决定.在 T_{EHP}^{t} 内,n_{fail}^{t} 为 d 个主机节点中恶意扫描失败总数,因此 T_{EHP}^{t} 内的扫描频率为 $T_{\mathrm{EHP}}^{t} d/n_{\mathrm{fail}}^{t}$.其中设定的跳变周期最小值为 $T_{\mathrm{EHP}}^{lb}\geq 2RTT$,以防止由于跳变周期过短而导致的通信中断;$\alpha$ 为平滑系数,有研究实验得到 $\alpha=0.7$[35].

$$T_{\mathrm{EHP}}^{t+1}=\begin{cases}T_{\mathrm{EHP}}^{ub}, & \text{其他}\\ T_{\mathrm{EHP}}^{t}+t_d', & T_{\mathrm{EHP}}^{t}+d_d'\leq T_{\mathrm{EHP}}^{ub}\end{cases} \quad (11)$$

跳变周期增加的幅度如式(11)所示,它表示在第 $t+1$ 次的跳变周期的增加幅度由网络延迟决定.其中设定的跳变周期最大值为 T_{EHP}^{ub},以防止由于跳变周期过长而导致的通信安全下降.NAS-SAMT 采用离散时间隐马尔可夫模型[36]对网络时延进行预测,它用五元组表示:$\lambda\triangleq\{N,M,\boldsymbol{\varphi},\boldsymbol{P},\boldsymbol{B}\}$,其中 $\boldsymbol{\varphi}$ 是网络状态初始分布矢量;$\boldsymbol{P}$ 是网络状态马尔可夫链转移矩阵;$\boldsymbol{B}$ 是从网络状态到网络时延的观测矩阵.定义网络状态空间为 $Q_s=\{1,2,\cdots,N\}$;网络时延 t_d 的量化空间为 $Q_s=\{1,2,\cdots,M\}$.首先经过 $t\cdot k$ 次采样后产生的网络状态序列为 $q_s^{kt}=\{q_1,q_2,\cdots,q_{kt}\}$,且 $q_s^{kt}\in Q_s$.其次,将 $t\cdot k$ 次采样后产生的网络时延序列经过 K-均值聚类量化处理后得到时延量化序列为 $o=\{o_1,o_2,\cdots,o_{kt}\}$.再次,采用不完全数学期望最大化算法计算 $\lambda\triangleq\{N,M,\boldsymbol{\varphi},\boldsymbol{P},\boldsymbol{B}\}$ 的极大似然估计 $\lambda^{*}=\arg\max P(o|\lambda)$;在此基础上利用 Viterbi 算法计算出最优状态序列 $q_s^{kt\prime}=(q_1',q_2',\cdots,q_{kt}')$;最后利用 $q_s^{kt\prime}$ 和概率转移矩阵 $\boldsymbol{P}$ 计算第 $t+1$ 次跳变周期内可能的网络时延 $t_d'=o_{t+1}'$,从而获得跳变周期的增长幅度.

(2) 当 $\sqrt{D_S\left(P_t^{Dst}(\pi),\dfrac{N_{\mathrm{fail}}}{M'}\right)}\leq\delta_2$ 成立时,攻击者采用盲扫描策略,NAS-SAMT 采用基于权值的欺骗跳变策略.当攻击方采用盲扫描策略时,攻击方对全部节点空间内的端信息进行均匀扫描以提高扫描效率.因此,在每个跳变周期内,NAS-SAMT 通过遍历 $NV^{T_{\mathrm{EHP}}}$,依据节点所属的弱连通分量(Weakly Connected Component,WCC)将端节点进行分组,假设与端节点 h^i 存在弱连通关系的节点集合记为 $\{WCC(h^i)\}$,t 时刻对应的 hEI 可表示为 $\{hEI_i|hEI\ \text{of}\ WCC(h^i)\}$.NAS-SAMT 通过选取同组内被扫描的端节点空间,以有效规避恶意扫描.

$$w_i^{EI}=1-\frac{1}{\delta_2}\min(\sqrt{D_S},\delta_2) \quad (12)$$

如式(12)所示,通过计算 T_{EHP} 内分配给每个端节点的 HTHR 中 hEI 的权值 w_i^{EI},并将其与权值基线 w_{base}^{EI} 进行比较,选取 w_i^{EI} 值高的端信息空间作为下一跳变周期的可用跳变端信息.这是因为被扫描过的 hEI 的 Sibson 熵为低于未被扫描过的 hEI,因此被扫描过的 hEI 的权值 w_i^{EI} 更高.当选取的端信息权值 $w_i^{EI}\geq w_{\mathrm{base}}^{EI}$ 时,可有效规避攻击者的恶意扫描.

(3) 当 $\sqrt{D_S(P_{t-1}^{Src}(\pi),P_t^{Src}(\pi))}>\delta_1$ 且 $\sqrt{D_S\left(P_t^{Dst}(\pi),\dfrac{N_{\mathrm{fail}}}{M'}\right)}>\delta_2$ 成立时,攻击者采用半盲扫描策略,NAS-SAMT 采用基于权值的反向欺骗跳变策略实施防御.这是因为攻击方采用半盲扫描策略时,在下一个跳变周期依然会对选定的节点空间进行扫描.因此在每个跳变周期内,NAS-SAMT 依据节点所属的弱连通分量将端节点进行分组,并选取不存在弱连通关系的端信息空间作为下次跳变的端信息.

$$\boldsymbol{ts}_{t+1}^{i}=\alpha\boldsymbol{ts}_{t}^{i}+(1-\alpha)\boldsymbol{ts}_{0}^{i} \quad (13)$$

NAS-SAMT 首先利用式(12)计算 T_{EHP} 内分配给每个端节点的 HTHR 中 hEI 的权值 w_i^{EI},并依据权值 w_i^{EI} 进行降序排列.如式(13)所示,利用转移概率 $\boldsymbol{ts}_t^i$ 确定在 $t+1$ 时需要分别从 $\{\neg WCC(h_i)\}$ 和 $\{WCC(h_i)\}$ 中转移的端信息数量 $\boldsymbol{ts}_t^i|WCC(h^i)|$.并依据排列从 $\{\neg h_i(WCC)\}$ 中选取权值 w_i^{EI} 低于 w_{base}^{EI} 的后 $\boldsymbol{ts}_t^i|\neg WCC(h^i)|$ 个端信息;从 $\{h_i(WCC)\}$ 中选取权值 w_i^{EI} 高于 w_{base}^{EI} 的前 $\boldsymbol{ts}_t^i|WCC(h^i)|$ 个端信息.其中 $\boldsymbol{ts}_t^i$ 基于当前连通性,通过马尔可夫随机游动模型[37]计算获得;$\boldsymbol{ts}_0^i$ 表示初始转移概率,且 $\boldsymbol{ts}_0^i[i]=1$,$\alpha=0.75$.从而通过选取不同组中 w_i^{EI} 值低于 w_{base}^{EI} 的端信息空间作为下一时刻可选跳变空间,以降低攻击者的扫描成功率.

(4) 当攻击者采用混合扫描策略时，NAS-SAMT 在构建网络视图的基础上，依据跟随扫描策略、半盲扫描策略和盲扫描策略的优先级顺序生成相应的跳变策略.

最后，NAS-SAMT 针对恶意扫描的三个阶段，依据式(14)～式(16)对端节点的 IP 地址、端口和协议进行跳变，从而选取下一跳变周期的跳变端信息. 其中 $f(\cdot)$ 是变换函数；地址跳变中的共享密钥 K_{SA}、端口跳变中的共享密钥 K_{SP} 和协议跳变中的共享密钥 K_{SS} 都是共享秘钥 K_s 生成的.

$$hIP=\begin{cases} hIP \oplus 1, & hIP=0,2^k-1 \\ f(K_{SA},IP,EID,t), & \text{其他} \end{cases} \tag{14}$$

$$hPort=\begin{cases} f(K_{SP},Port,SrvID)\oplus 1024, & hPort\in[1,1024] \\ f(K_{SP},Port,SrvID,t), & \text{其他} \end{cases} \tag{15}$$

$$hProtocol=f(K_{SS},Protocol,TCP\ Option) \tag{16}$$

IP 跳变算法如式(14)所示，由于 IP 地址为 0 时不可用：为 2^k-1 时为广播地址，因此当 IP 跳变为该地址时通过“OR”运算生成可用跳变 IP 地址. 其中 EID 表示端节点身份标识信息. 端口跳变算法如式(15)所示，由于 0～1024 为常用端口，因此当 $Port$ 值跳变到常用端口范围内，通过“OR”操作生成可用的跳变端口. 其中 $SrvID$ 表示端节点提供的服务标识. 最后，协议跳变算法如式(16)所示，其中 $Protocol$ 为协议代码；$TCP\ Option$ 是 TCP 选项. 为了防止攻击方通过解析协议推断端节点的操作系统类型和版本. NAS-SAMT 通过修改协议代码值和 TCP 选项以欺骗攻击方. 为了防止由于报文修改导致的包丢弃，进而造成的网络服务质量下降，NAS-SAMT 在修改参数的基础上通过重新排序选项实现误操作选项编码，从而保证选项长度的正确性.

4.3　基于 SMT 的启发式跳变部署

由于求解 SMT 是 NP 问题，且 NAS-SAMT 要在保证跳变端信息满足约束的前提下实现最优跳变. 因此 NAS-SAMT 通过 SMT 形式化描述跳变端信息部署要满足的约束条件，并在此基础上利用启发式算法求解最优跳变端信息空间，从而实现跳变的可扩展性和低开销. 由于 NAS-SAMT 是基于 SDN 架构下实施跳变，需要路由和控制器协同实施，因此从跳变路由、端节点和转发路径三个方面对跳变进行约束. 定义布尔变量 $b_T^v(k)$ 表示路由节点 v 在跳变周期 T_{EHP} 内是否转发第 k 条数据流，若转发则 $b_T^v(k)=1$；否则 $b_T^v(k)=0$. NAS-SAMT 所需满足的约束具体如下.

(1) 容量约束条件. 该约束通过选取能承载累计所需最大流表长度的路由节点，以防止由于数据溢出造成的丢包问题.

$$c_v(k)=C_v(\sigma^{1-\frac{C_v(k)}{C_v}}-1) \tag{17}$$

$$\forall hR_i,\text{若 } C_{\max}^v-\sum_{i=1}^{k}b_T^v(i)\cdot c_v(i)\geq C_{th}^v,\text{则 } b_T^v(i)=1 \tag{18}$$

$$\sum_k\sum_{j_1}\sum_{j_1\neq j_2}B_{j_1}^k\wedge B_{j_2}^k\wedge C_{j_1,j_2}\geq\Phi \tag{19}$$

由于基于边际成本的指数函数可有效量化不同条件下网络资源性能消耗的指标[9]，因此本文采用基于边际成本的指数函数量化路由节点的资源开销. 式(17)表示添加一条新的流表项所需的边际成本函数. 其中，σ 为调整参数，经过理论分析选取 $\sigma=2n$[38]；$1-\frac{C_v(k)}{C_v}$ 表示当第 k 条数据流的转发信息添加到路由节点 v 后流表的利用率. 式(18)说明累计流表增加的边际成本必须在所选路由节点可承载范围 $C_{\max}^v$ 之内，且剩余的流表长度不小于 C_{th}^v 从而不会出现数据溢出等问题. 其中 C_{th}^v 表示路由节点需要保留的最小数据量. 式(19)则通过临近分配原则和路由聚合降低路由更新时所需的负载. 其中 $C_{j_1,j_2}\in\{0,1\}$ 表示地址段 j_1 和 j_2 是否为连续的；$B_j^k=\bigvee\limits_{h^i\in s^k}b_j^i$ 表示子网 s_k 中至少有一个主机节点 h^i 的地址在地址段 j 中；Φ 表示每个划分的地址段所包含的地址空间下限.

(2) 跳变空间选择约束. 该约束通过限制跳变地址空间的重复率，以保证跳变的不可预测性.

$$\sum_{1<j\leq M}b_i^j\geq 1 \tag{20}$$

$$\sum b_i^j\geq\frac{N_{\text{HTHR}}^i-1}{2\delta_3 n_{\text{HTHR}}} \tag{21}$$

$$\forall hEI\in m_H^{T_{\text{EHP}}},\ b_i^j=0 \tag{22}$$

其中式(20)保证了每个端节点都被分配了跳变地址. 因为均匀选取 hEI 可令跳变不可预测性最大，因此为了保证跳变空间的不可预测性，式(21)通过设定重复率阈值 δ_3，使得一次低频跳变内选取某个跳变地址空间的重复率不能超过阈值，$b_i^j=1$ 表示跳变地址 j 分配给了端节点 i. 此外，式(22)要求端节点在相邻 HTHR 选取的 hEI 不能重复，以保证跳变的有效性.

(3) 可达性约束条件. 该约束通过限制转发路径的选取，从而防止转发回路.

$$\text{若 } b_T^k=1,k\in[1,n],\text{则}\sum_{i\in T}b_T^v(i)=\sum_{o\in O}b_T^v(o) \tag{23}$$

$$\text{若 } b_t^k=1,\text{则 } \forall hR_j\in\chi(hR_i),\ \sum b_j^k=2 \tag{24}$$

$$\text{若 } \forall hR_j\in\{hR\mid next\text{-}hop\ \text{of}\ hR_i\},d_k^{j-Dst}\leq d_k^{i-Dst} \tag{25}$$

式(23)表示每条转发路径上所有路由节点的入

度和出度是相同的.式(24)表示路径中的每个转发节点都与其上一跳和下一跳路由节点物理邻接,$\chi(hR_i)$表示去除转发路径的源地址和目的地址后的路由节点集合.然而,将数据流从一个节点转发到其相邻的下一跳节点并不能保证数据的可达.因此,式(25)表示从下一跳路由节点到目标节点的距离不大于现有转发节点到目标路由节点的距离,其中d_k^{i-Dst}表示路由节点i到目标节点的距离.

(4)传输时延约束条件.该约束通过选取传输时延满足约束的转发路径,以防止由于传输时延过大造成的服务性能下降,具体如式(26)所示.

$$\sum b_i^k \leq L_{\max},\ i\in\{Src,hR_1,\cdots,Dst\} \quad (26)$$

由于传输时延与转发路径中路由节点个数成正相关[39],因此式(26)表示每条数据流的转发路径长度不能超过设定的最大值$L_{\max}$.

由于启发式算法(Heuristic Algorithm,HA)是一种能够高效求解近似最优解的方法,NAS-SAMT通过提出启发式跳变部署算法,从而在保证跳变端信息满足约束的同时实现跳变的高效部署,以求解视图距离最大的跳变端信息集合,即$\max(D_{T_{\text{EHP}}})$.具体如下.

算法 1. 启发式跳变实施部署算法.

输入:当前的网络视图NV',最小视图距离$D_{\min}$,符合条件的跳变端信息集合$\{hEI\}$;变量参数i

输出:跳变周期T_{EHP}的视图距离$D_{T_{\text{EHP}}}$,选取的端信息集合$Q(hEI)$

1. 初始化选取的跳变端信息集合$Q(hEI)\leftarrow\varnothing$;
2. 始化视图距离D_{NV}^0和端信息权值基线w_{base}^{EI};
3. 随机产生跳变端信息地址空间;
4. 设定评估次数est_k;
5. WHILE ($i\leftarrow 1$ to est_k)
6. FOR ($i\leftarrow 1$ to est_k)
7. 计算视图距离D'_{NV};
8. IF ($D'_{NV}\geq D_{NV}$)
9. $D_{NV}\leftarrow D'_{NV}$;
10. ELSE $\left(P=\exp\left(\frac{NV'-NV}{D'_{NV}}\right)>ran(0,1)\right)$
11. $D_{NV}\leftarrow D'_{NV}$;
12. END IF
13. $i++$;
14. $Q(hEI)\leftarrow getComb\{hEI\}$;
15. $D_{T_{\text{EHP}}}\leftarrow D_{NV}$;
16. END FOR
17. $D_{NV}\leftarrow\alpha\cdot D_{NV}$;
18. RETURN $Q(hEI)$和$D_{T_{\text{EHP}}}$;

该算法主要由产生新解和接收新解两部分组成.在产生新解的过程中,首先判断是否$D'_{NV}\geq D_{\min}$成立.若成立,则判断在设定的评估次数est_k中是否得到最优解.若没有,则以$D_{NV}\leftarrow\alpha\cdot D_{NV}$的概率降低$D_{NV}$,从而继续寻找最优端信息跳变空间,其中参数设置为$\alpha=0.95$.接收新解则是依据 Metropolis 准则[40],即当$D'_{NV}\geq D_{NV}$时,总是接受该解;当$D'_{NV}<D_{NV}$时,则以概率$\exp\left(\frac{NV'-NV}{D'_{NV}}\right)$接受.因此,该算法的计算复杂度为$O\left(est_k\left\lceil\frac{D_{NV}^0-D_{\min}}{\alpha}\right\rceil\right)$.

5 NAS-SAMT 架构组成与实施

5.1 架构组成

NAS-SAMT整体架构如图 5 所示,它通过跳变

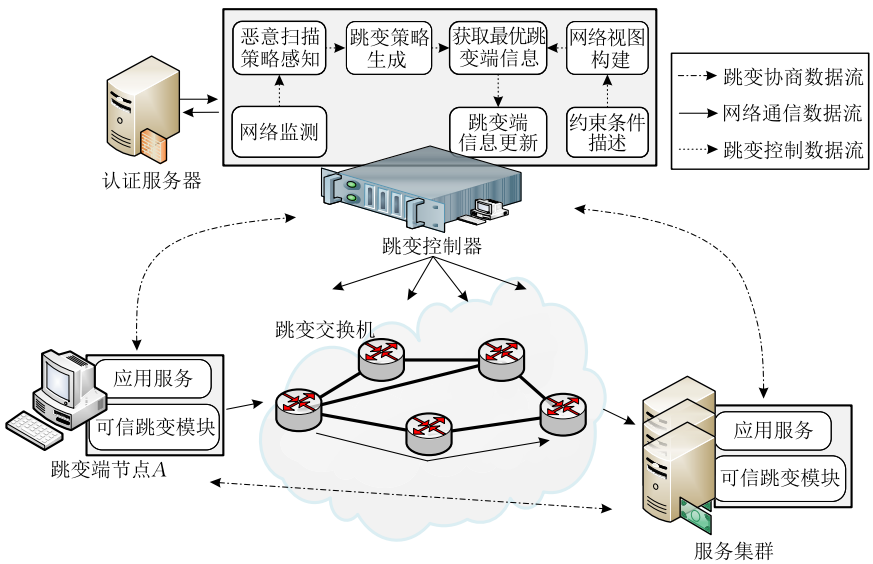

图 5 NAS-SAMT 架构组成

交换机(Hopping Switch，HS)、跳变控制器(Hopping Controller，HC)和可信跳变模块(Trusted Hopping Component，THC)实现网络节点自适应跳变. 其中 HC 将{*hEI*}依据子网的数量和规模划分 BHR；每个 HS 将获得的 BHR 依据端节点的数量和重要程度划分为 LTHR；THC 则依据跳变策略，利用端节点与 HS 的共享参数选取 *hEI*.

HC 主要由恶意扫描策略感知、跳变决策和部署实施三部分组成. 其中恶意扫描策略感知的作用是依据 HS 上报的非法连接请求，利用基于 Sibson 熵的假设检验分析恶意扫描策略；跳变决策则是依据分析的恶意扫描策略选择不同的跳变策略加以应对；跳变节点空间 SMT 求解器则利用跳变约束和全局视图求解符合要求的节点空间，并在此基础上构建网络视图. 最后，HC 将跳变策略和 LTHR 下发给 HS.

THC 主要用于与其他通信节点进行跳变通信. 由于网络层与传输层的身份分离[41]，THC 通过虚拟映射实现 *EI* 到 *hEI* 的转换，使得通信双方的传输协议栈是通过识别 *EI* 来鉴别一个会话的，而网络传输通过 *hEI* 进行转发，从而使得网络层 *EI* 到 *hEI* 的无缝跳变，该模块可利用基于通用虚拟网卡内核驱动 TAP[42]实现. 其主要过程如下：

(1) 连接拦截. 它通过创建 *EI* 与 *hEI* 的映射用 *hEI* 替换 *EI*，使得通信双方的传输协议栈识别由 *hEI* 标识的会话连接，从而实现端节点 *EI* 与网络会话 *hEI* 相分离，以保证端信息的跳变对端节点是透明的. 对于基于 TCP 协议的会话，在 INET 套接字层利用 *inet_sendmsg*()和 *inet_recvmsg*()函数拦截从应用层到传输层连接建立时的系统调用函数，包括 socket，accept，connect，close 等，并保存与 *EI* 相关的会话参数. 对于基于 UDP 协议的会话，在 INET 套接字层利用 *inet_sendmsg*()和 *inet_recvmsg*()函数截取 getsockname 和 getpeername 系统调用，并保存于 EI 相关的会话参数.

(2) 端信息变换. 在连接拦截基础上，THC 中的端信息转换模块通过截取网络层中的转发分组将分组的头部信息进行转换. 如果是流入的分组，则将 *EI* 转换为 *hEI*；若是流出的分组，则将 *hEI* 转换为 *EI*. 由于 Iptables 可以实现数据包过滤、网络地址转换和其他的数据包处理. THC 主要利用 Iptables 中的 NAT 表实施端信息跳变；利用 Mangle 表阻止针对 *EI* 或过期 *hEI* 的连接. 对于流入的数据包，THC 在 Pre_routing 链上执行目的地址转换、在 Input 链上执行源地址转换；对于流出的数据包，THC 在 Output 链上执行源地址转换、在 Post_routing 链上执行目的地址转换.

(3) 连接迁移与同步. 在前两步的基础上，待迁移的连接被暂停并在另一个进程中恢复. 当待迁移的连接被挂起时，THC 中的迁移模块保存 *EI* 和 *hEI* 映射信息，并利用式(10)与通信节点的 THC 实现跳变端信息的通告. 当连接恢复时，迁移模块更新 *hEI* 信息并与通告通信节点的 THC. 此外，流表更新规则将上报给 HC. THC 中的迁移输出进程和迁移输入进程基于共享密钥进行迁移协商，迁移输出进程通过挂起、保存、销毁等操作对原有映射进行处理；迁移输入进程则通过创建、恢复等操作建立新的映射.

HS 的主要作用是依据流表对通信数据流进行修改和转发，对于不能匹配流表的数据包以及 ARP、ICMP、DNS、DHCP 等协议的数据包则转发到 HC 中处理；检测、过滤和收集非法连接请求，并定期上报给 HC；以及与跳变端节点的 THC 同步跳变端信息.

为了保证跳变同步过程中跳变的有效性，NAS-SAMT 首次获取 *hEI* 时同时获取两个跳变地址，其中一个暂时保留作为下次跳变的切换 *hEI*. 在节点当前 *hEI* 即将失效时将下一跳变周期的 *hEI* 通告给与之通信的节点，从而做好切换准备. 跳变切换后的新会话必须使用新的 *hEI* 以保证通信的安全. 与此同时，由于跳变更新时网络中依然有持续进行的会话，因此为了降低由于切换造成的负载，设置地址转换生存期(Change Time To Live，CTTL). 在 CTTL 内，原有 *hEI* 依然可用于接收网络传输的原有会话；当 CTTL 到期后，原有 *hEI* 将无效.

5.2　NAS-SAMT 通信与更新

SDN 环境下 NAS-SAMT 工作流程如图 6 所示，其具体步骤如下：

(1) 进行相关配置. 在被保护的客户端配置受保护的服务集群列表，在被保护的服务器节点配置合法用户的 ID 信息. 被保护节点进行初始化，THC 组件读取配置信息并建立空会话列表.

(2) 进行信息请求与签名. 客户端 *A* 发送会话请求报文 $K_{Ec}(ID_A, req, K_s)$，利用客户端的私钥 K_{Ec} 对客户端身份信息 ID_A，请求信息 *req* 和共享密钥 K_s 进行签名.

(3) 身份验证. THC 组件截获请求，将请求报文中的 HOST 字段与受保护服务器集群列表进行比

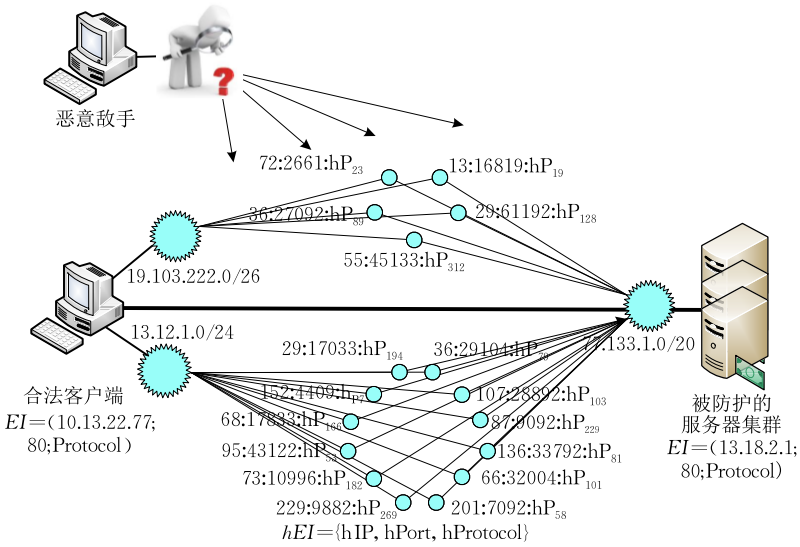

图 6 NAS-SAMT 实施实例

对.若要访问的服务器不在被保护列表中,则采用标准的访问机制;若要访问的服务器属于被保护之列,则将身份信息发送至客户端 A 所属的 HS 进行验证.

(4)通过验证.客户端 A 所属 HS 收到验证报文后利用客户端公钥 K_{D_C} 进行签名验证,并验证身份信息 ID_A,验证通过后向 HC 请求服务器映射的 hEI.

(5)进行签名.HC 通过查询服务器端所属 HS 获取 EI 映射的 hEI,发送 $K_{E_{HC}}(ID_{HC}, hEI')$ 给客户端 A 所属 HS,利用 HC 公钥 $K_{E_{HC}}$ 对 RC 身份信息 ID_{HC} 和跳变端 hEI 进行签名.

(6)映射和跳变.HS 收到 HC 返回的数据包,利用 HS 的私钥 $K_{E_{HS}}$ 发送 $K_{E_{HS}}(ID_{HS}, hHI', Stgy)$ 给客户端 A,其中包括服务器映射的 hEI 和跳变策略 $Stgy$.

(7)信息修改.客户端 A 的 THC 依据跳变策略选取跳变端信息,并对请求数据包端信息进行修改 $(\{IP(A), Port(A)\}, \{hIP(B), hPort(B), Protocol\} \rightarrow \{hIP(A), hPort(A)\}, \{hIP(B), hPort(B)\}, hProtocol)$.

(8)若服务器跳变的 hEI 已在 HS 转发流表中,网络路由节点依据流表规则进行转发;若服务器跳变的 hEI 不在 HS 转发流表中,网络路由节点将转发数据包上报给 HC.

(9)HC 对流表规则进行更新,并依据“逆序添加,顺序删除”的顺序部署到转发路径上的路由节点.

(10)服务器所属 HS 收到请求报文后将其转发给被保护的服务器集群.

(11)若被保护的服务器集群 hEI 发生跳变,由于跳变前的 hEI 在 CTTL 内依然可用,服务器集群的 THC 拦截收到的数据包,并将服务器的 hEI 映射到 EI,并交由上层应用依据请求内容处理响应.

(12)服务器集群的 THC 向正在通信的端节点 THC 发送跳变更新报文;在更新后拦截响应数据包,依据跳变策略修改数据包的端信息 $(\{hIP(A), hPort(A)\}, \{hIP(B), hPort(B), hProtocol\} \rightarrow \{hIP(A), hPort(A)\}, \{hIP'(B), hPort'(B)\}, hProtocol')$.

(13)转发.网络跳变路由节点依据流表规则进行转发.

(14)转发.客户端 A 所属 HS 收到响应报文后将其转发给被保护的客户端 A.

(15)过程结束.客户端 A 的 THC 拦截响应数据包,并将服务器的 hEI 映射到 EI,并交由上层应用处理响应.一次通信过程结束.

由于 NAS-SAMT 通过虚拟映射动态变换节点地址,因此网络跳变对上层应用是透明的,不会导致现有会话的中断.与此同时,NAS-SAMT 中的 THC 组件是基于可信平台模块[43](Trusted Platform Module,TPM)构建的,通过启动可信链,接管原有系统 Boot 部分,以保证端信息跳变实施的可信性和完整性,从而防止端信息被泄露和篡改.

此外,由于跳变过程中易出现流表更新不一致导致的数据流不可达的问题.针对该问题 NAS-SAMT 采用逆序添加,顺序删除的更新方法,具体算法如下所示.所谓“逆序添加”是指跳变控制器按照从目的节点到源节点的逆序方向对跳变路径上的路由节点安装流表信息;“顺序删除”则是指跳变控制器按照从源节点到目的节点的顺序方向删除旧的流表规则.6.2 节中定理 1 证明了该方法可在流表更新过程中,保证转发数据的可达性.

算法 2.　NAS-SAMT 流表更新算法.

输入：选取的端信息集合 $Q(hEI)$，跳变周期 T_{EHP}

输出：更新路由顺序 $hR=\{r_1\rightarrow r_2\rightarrow\cdots\rightarrow r_n\}$

1. 对转发路由进行分类；
2. IF ($hR\in\{hR\in hR_{\mathrm{new}}\wedge hR\notin hR_{\mathrm{old}}\}$)；
3.　逆序添加流表项；
4. ELSE IF ($hR\in\{hR\in hR_{\mathrm{new}}\wedge hR\in hR_{\mathrm{old}}\}$)
5.　逆序添加流表项；
6.　顺序删除原有流表项；
7. ELSE IF ($hR\in\{hR\notin hR_{\mathrm{new}}\wedge hR\in hR_{\mathrm{old}}\}$)
8.　顺序删除原有流表项；
9. END IF

其中，$hR\notin hR_{\mathrm{new}}\wedge hR\notin hR_{\mathrm{old}}$ 表示跳变路由既不属于本次跳变周期内的转发路由集合，也不属于下一周期内的转发路由集合. $\{hR\in hR_{\mathrm{new}}\wedge hR\notin hR_{\mathrm{old}}\}$ 表示即跳变路由只属于下一跳变周期内的转发路由集合. $\{hR\in hR_{\mathrm{new}}\wedge hR\in hR_{\mathrm{old}}\}$ 表示跳变路由既属于本次跳变周期内的转发路由集合，又属于下一周期内的转发路由集合. $\{hR\notin hR_{\mathrm{new}}\wedge hR\in hR_{\mathrm{old}}\}$ 表示跳变路由只属于本次跳变周期内的转发路由集合.

6　理论分析

6.1　安全性分析

(1) 跳变空间

若跳变端信息空间中 IP 地址池、端口地址池和协议池的数量分别为 N_{IP}、N_{PORT} 和 N_{PROTOCOL}. 那么跳变端信息空间数量为 $|S_{hEI}|=N_{\mathrm{PROTOCOL}}N_{\mathrm{PORT}}^2N_{\mathrm{IP}}(N_{\mathrm{IP}}-1)$，其中除去了 $IP_{Src}=P_{Dst}$ 的情况. 当网络中存在 n_{hEI} 个连接要进行网络跳变，则需要的端信息空间大小为 $2n_{hEI}$，跳变后剩余的端信息空间为 $|S_{hEI}|-2n_{hEI}$. 由跳变空间选择约束可知，若每次跳变有 $\alpha|S_{hEI}|$ 端信息被分配，$\alpha\in[0,1)$，则跳变后未被使用的端数量为 $(1-\alpha)|S_{hHI}|$. 因此，由 $(1-\alpha)|S_{hEI}|\leq|S_{hEI}|-2n_{hEI}$ 可得 $n_{hEI}\leq\frac{1}{2}\alpha|S_{hEI}|$. 当 $N_{\mathrm{IP}}=2^{16}$，$N_{\mathrm{PORT}}=2^{16}$，$\alpha=0.75$ 时，NAS-SAMT 可同时支持 6.46×10^{18} 个会话同时跳变. 由于实际配置的内网中网络端节点数量不会超过 65 535 个，每个节点最大并行会话数量为 5×10^5. 因此，当内网所有端节点同时跳变时，每个会话的跳变空间为 1.97×10^8. 与此同时，由于 NAS-SAMT 采用了协议跳变，其跳变空间为 $N_{\mathrm{PROTOCOL}}=2^{328}$. 当攻击方以 10^{20} 个/秒的速率进行猜测，也需要 3.17×10^{15} 年才能成功. 所以 NAS-SAMT 具有足够大的跳变空间.

(2) 抵御恶意扫描攻击能力

由 2.3 节分析可知，RHM[19] 和 ST-RHM[29] 是基于 SDN 的网络跳变中具有代表性的方法. 其中 RHM 采用随机网络跳变；ST-RHM 采用时间-空间混合随机跳变. 本文通过对比不同扫描策略在静态网络、RHM、ST-RHM 和 NAS-SAMT 网络中的扫描成功率，分析说明部署 NAS-SAMT 网络的安全性. 假设网络中有 n_l 个目标节点，节点空间为 m，扫描宽度为 w，频度为 $1/T_{\mathrm{SCN}}$，则扫描的地址数量为 $n_s=w\cdot t/T_{\mathrm{SCN}}$，$n_s\leq m$；扫描频度和跳变频率比为 $r=T_{\mathrm{EHP}}/T_{\mathrm{SCN}}$.

抵御盲扫描的能力：由于盲扫描是非重复的均匀扫描，在静态网络中 $T_{\mathrm{EHP}}=\infty$，攻击者成功扫描到 x 个地址的概率服从超几何分布，可表示为 $P_{\mathrm{b}}(x)=(C_{n_l}^{x}\cdot C_{m-n_l}^{n_s-x})/C_m^{n_s}$. 因此，攻击者成功实施盲扫描的概率为 $P_{\mathrm{b}}^{\mathrm{static}}(x>0)=1-C_m^{n_s}-n_i/C_m^{n_s}$. 在 RHM、ST-RHM 和 NAS-SAMT 网络中，一次跳变后攻击者成功扫描到 x 个目标节点的概率服从伯努利分布，可表示为 $P_{\mathrm{b}}(x)=C_{n_l}^{x}[n_l/(n_l+m)]^x[1-n_l/(n_l+m)]^{n_s-x}$. 因此，攻击者实施盲扫描策略的成功率为 $P_{\mathrm{b}}(x>0)=1-[1-rwn_l/(mn_l+mrw)]^{n_s}$. 特别地，当 $r=1$ 扫描的概率为 $P_{\mathrm{b}}(x>0)=1-[1-wn_l/(mn_l+mw)]^{n_s}$. 比较可知，RHM、ST-RHM 和 NAS-SAMT 相较于静态网络可有效降低攻击者成功扫描的概率，与文献[44]的结论相一致.

抵御半盲扫描的能力：由于半盲扫描会重复扫描与其物理邻接的节点地址空间，不妨假设攻击者在一次跳变周期内可重复扫描 α 次，要扫描的节点空间为 ϕm，$\phi\in(0,1)$，其中包含的目标节点个数为 n_l'. 在静态网络中，攻击者成功实施半盲扫描的概率为 $P_{\mathrm{hb}}^{\mathrm{static}}(x>0)=1-aC_{\phi m-n_l'}^{n_s/a}/\phi C_{\phi m}^{n_s/a}$. 由于 RHM 网络中只采用了随机跳变的方法，因此攻击者扫描成功率为 $P_{\mathrm{hb}}^{\mathrm{RHM}}(x>0)=1-a[1-wrn_l'/(\phi mn_l'+\phi mwr)^{n_s}]$. 在 ST-RHM 网络中，由于跳变周期和所选端信息都是随机改变的，因此攻击者扫描成功率为 $P_{\mathrm{hb}}^{\mathrm{ST\text{-}RHM}}(x>0)=1-ar[1-wrn_l'/(\phi mn_l'+\phi mwr)^{n_s}]$. 在 NAS-SAMT 网络中，由于每个跳变周期内都采用基于权值的反向欺骗跳变策略，会令 $n_\gamma=\boldsymbol{ts}_t^i|WCC(h^i)|$ 个 hEI 在下一个跳变周期内失效，一次跳变后攻击者成功扫描 x 个目标节点的概

率为 $P_{hb}(x)=C_{n_j'}^{x}[(n_l'-n_\gamma)/(n_l'+\phi m)]^x[1-(n_l'-n_\gamma)/(n_l'+\phi m)]^{n_s-x}$. 因此,攻击者经过 a 次半盲扫描后成功率为 $P_{hb}(x>0)=1-ar[1-(wrn_l'-\phi mn_\gamma)/(\phi mn_l'+\phi mwr)]^{n_s}$. 由此可知,NAS-SAMT 和 ST-RHM 相较于 RHM 可有效降低攻击者实施半盲扫描的成功率.

抵御跟随扫描的能力:当攻击者实施跟随扫描时有 $r\geq 1$,因此不妨设一次跳变周期内攻击者可重复扫描 a 次,目标节点个数为 n_l'. 在静态网络中,攻击者成功实施跟扫描的概率为 $P_{fu}^{static}(x>0)=1-aC_{\phi m-n_l'}^{n_s/a}/\phi C_{\phi m}^{n_s/a}$. 攻击者在 RHM 网络中采用跟随扫描策略的成功率为 $P_{fu}^{RHM}(x>0)=1-[1-an_l'(n_l'-\phi ma)]^{n_s}$,分析结果与文献[16]相符合. 攻击者在 ST-RHM 网络中实施跟随扫描的成功率为 $P_{fu}^{ST\text{-}RHM}(x>0)=1-[1-(an_l'-n_\gamma)/(n_l'+\phi ma)]^{n_s}$. 由于 NAS-SAMT 采用了跳变周期拉伸策略,当感知到跟随扫描时 NAS-SAMT 将提高跳变频率,最终使得 $r\leq 1$. 因此,攻击者的成功率为 $P_{fu}(x>0)=1-[1-(rn_l'-n_\gamma)/(n_l'+\phi m)]^{n_s}$. 分析可知,相较于 ST-RHM 采用时域随机跳变的策略,NAS-SAMT 的跳变周期拉伸策略可大幅降低攻击者的扫描成功率.

6.2 性能分析

(1)流表更新一致性

为了防止跳变过程中存在流表更新不一致导致的数据流不可达的问题,NAS-SAMT 采用逆序添加,顺序删除的更新方法,定理 1 证明了该方法的正确性.

定理 1. NAS-SAMT 的更新方法保证了流表更新的一致性.

证明. 假设从源节点 S 到目的节点 D 的传输路径中经过路由为 $hR=\{r_1\rightarrow r_2\rightarrow\cdots\rightarrow r_n\}$. 在第 t 个跳变周期时路由 s 的流策略为 $f_t^{r_i}:pkt(X)\rightarrow Y_t$,它表示对数据包 $pkt(X)$依据策略 Y_t处理. 因此,数据流经过多个路由时可表示为 $F_t=f_t^n(\cdots f_t^2(f_t^1(pkt(X))))$. 若数据包成功传输完毕,有 $F(pkt(X))=F_t(pkt(X))$;否则上报给跳变控制器,跳变控制器依据当前策略进行转发,即有 $F(pkt(X))=Y_i$. NAS-SAMT 中的跳变路由可分为 4 类:

① 若 $\{r_1,r_2,\cdots,r_n\}\subset\{hR\notin hR_{new}\wedge hR\notin hR_{old}\}$, $F(pkt(X))=F_t(pkt(X))$成立.

② 若 $\{r_1,r_2,\cdots,r_n\}\subset\{hR\in hR_{new}\wedge hR\notin hR_{old}\}$,路由节点要更新流表策略,则有 $f_t\rightarrow f_{t+1}$. 数据包 $pkt(X)$会被上报给跳变控制器,控制器依据策略 f_{t+1}转发数据包,即 $f_t^1(pkt(X))=Y_{t+1}$. 与此同时,由于 NAS-SAMT 采用逆序添加的方法,因此 $\exists i\in[1,n]$, s. t. $f_t\rightarrow f_{t+1}$,则有 $F(pkt(X))=F_{t+1}(pkt(X))$成立.

③ 若 $\{r_1,r_2,\cdots,r_n\}\subset\{hR\in hR_{new}\wedge hR\in hR_{old}\}$,路由节点要更新流表策略,则有 $f_t\rightarrow f_{t+1}$. 数据包在初始路由节点时,由于 NAS-SAMT 采用顺序删除的方法,则路由节点 r_1 中的流策略 f_t被删除,$pkt(X)$被上报给跳变控制器,控制器依据策略 f_{t+1}转发数据包,即 $f_t^1(pkt(X))=Y_{t+1}$. 若数据包 $pkt(X)$已经在传输路径上,由于 NAS-SAMT 采用逆序添加的方法,因此 $\exists i\in[1,n]$, s. t. $f_t\rightarrow f_{t+1}$,最终有 $F(pkt(X))=F_{t+1}(pkt(X))$成立.

④ 若 $\{r_1,r_2,\cdots,r_n\}\subset\{hR\notin hR_{new}\wedge hR\in hR_{old}\}$,路由节点要更新流表策略,则有 $f_t\rightarrow f_{t+1}$. 数据包在初始路由节点时,由于 NAS-SAMT 采用顺序删除的方法,则路由节点 r_1 中的流策略 f_t被删除,$pkt(X)$被上报给跳变控制器,控制器依据策略 f_{t+1}转发数据包,即 $f_t^1(pkt(X))=Y_{t+1}$. 如果数据包 $pkt(X)$在传输路径上,则依据原有策略进行转发,即 $F(pkt(X))=F_t(pkt(X))$成立. 证毕.

综上所述,NAS-SAMT 的流表更新方法可使得 $F(pkt(X))=F_{t+1}(pkt(X))$或者 $F(pkt(X))=F_t(pkt(X))$成立,即在流表更新时能够成功完成传输. 所以,逆序添加、顺序删除的更新方式保证了网络跳变中流表更新的一致性.

(2)跳变成本

静态网络、RHM、ST-RHM 和 NAS-SAMT 网络的跳变成本如表 2 所示,它主要包括跳变算法计算复杂度、平均时延和流表长度.

表 2 跳变成本

跳变方式	算法复杂度	平均时延	流表大小量级
静态网络	$O(1)$	t_{tran}	n_{hEI}
RHM	$O(S_{hEI})$	$t_{tran}+t_{proc}$	$1+n_{hEI}$
ST-RHM	$O(S_{hEI}n_{hEI})$	$t_{tran}+t_{proc}$	$1+n_{hEI}$
NAS-SAMT	$O(S_{hEI}n_{hEI}/r)$	$t_{tran}+t_{proc}$	$1+n_{hEI}/n_a$

对于算法复杂度:当一个子网内会话数量为 n_{hEI},可跳变的节点空间为 $|S_{hEI}|$,由于静态网络不存在跳变,可令其算法复杂度为 $O(1)$. 由于 RHM 仅采用随机空间跳变,其算法复杂度为 $O(S_{hEI})$. 由于 ST-RHM 采用时间-空间混合随机跳变,其算法复

杂度为 $O(S_{hEI}n_{hEI})$. 由于 NAS-SAMT 依据扫描策略动态改变跳变策略，其算法复杂度为 $O(S_{hEI}n_{hEI}/r)$.

对于平均时延：网络时延主要由节点处理转发时延和传输时延组成. 由于 RHM、ST-RHM 和 NAS-SAMT 改变了端节点信息，因此转发时延会由于端信息跳变而增加；然而，网络跳变并不影响数据传输，因此传输时延与静态网络的相同.

对于流表大小量级：在静态网络中，流表大小量级为 $|S_{hEI}|$. 在 RHM 和 ST-RHM 网络中，因为每次跳变时从所有可用的节点空间中随机选取，因此 RHM 和 ST-RHM 在 T_{EHP} 内所需更新的流表大小量级为 $1+n_{hEI}$. 在 NAS-SAMT 网络中，当一个子网内可进行聚合的地址大小为 n_a. 由于 NAS-SAMT 利用容量约束，其在 T_{LTHR} 内所需更新的流表大小量级为 $1+n_{hEI}/n_a$，其中 n_{hEI}/n_a 表示聚合后 NAS-SAMT 在 T_{LTHR} 内跳变所需的流表大小. 因此，NAS-SAMT 通过容量约束可有效降低流表大小.

7　实验分析

为了验证 NAS-SAMT 的可行性和有效性，利用 Mininet[45] 构建仿真网络拓扑，采用 Erdos-Renyi 模型生成随机网络拓扑. 采用支持 OpenFlow[46] 协议的 OpenVSwitch(OVS)为 HS，OpenDaylight[47] 作为 HC. 通过 OpenDaylight 和 OVS 部署 NAS-SAMT 系统实施跳变，同时利用 MATHSAT5 作为 SMT 求解器. 实验网络中源节点和目的节点的配置如表 3 所示.

表 3　实验环境配置

节点	操作系统	配置	V
Web Server	CentOS 7	16 Core 2.8 GHz，64 GB 内存	5
FTP Server	CentOS 7	16 Core 2.8 GHz，64 GB 内存	3
Clients	Ubuntu 14.04	8 Core 2.2 GHz，8 GB 内存	2

NAS-SAMT 设置跳变节点地址空间由一个 B 类 IP 地址池和大小为 2^{16} 的端口池组成，令 $\sigma=5$，$\delta_1=0.05$，$\delta_2=0.075$，$\delta_3=0.05$，$\gamma=0.4$，$\lambda=0.02$，$L_{max}=32$，$T_{LTHR}=200$ s. 实验分别从 NAS-SAMT 对不同策略扫描攻击的防御能力、跳变实施性能开销等方面进行验证与分析.

7.1　恶意扫描攻防分析

(1) 网络跳变空间

对于网络中每个跳变端节点，若最大并行会话数量为 5×10^5，在时间 T 内改变跳变周期 T_{EHP}，所需的端信息数量如图 7 所示. 与此同时，为了实现跳变不可预测性的设计目标，NAS-SAMT 设计了如式(14)～式(16)所示的跳变算法. 为了验证 NAS-SAMT 生成跳变端信息的不可预测性，本文统计了 20000 组跳变端信息的利用率. 如图 8 中的虚线所示，跳变端信息的平均利用率约为 0.32%.

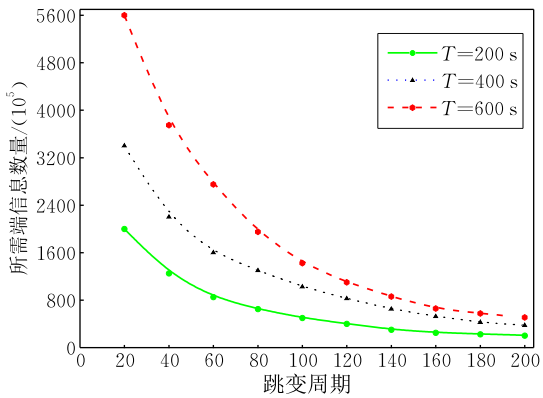

图 7　不同跳变周期下 NAS-SAMT 所需跳变端信息

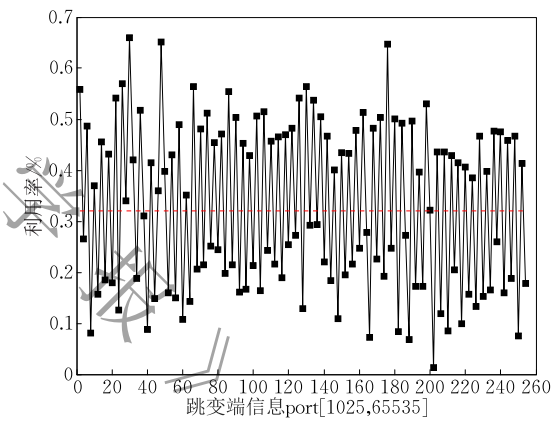

图 8　跳变端信息利用率

(2) 恶意扫描攻防分析

为了证明 NAS-SAMT 跳变的有效性，利用 Nmap 扫描器对 10.168.1.0/24 子网进行 SYN 扫描. 该子网内由实际 IP 地址为 10.168.1.117 的 IP 跳变节点、IP 为 10.168.1.124 的端口跳变节点、IP 为 10.168.1.138 的协议跳变节点和 IP 为 10.168.1.153 的静态节点组成，4 个节点都只开启了 TCP(port 21)和 UDP(port 34287)端口，结果如表 4(a)～(c)所示.

表 4(a)　Nmap 扫描 IP 地址结果

扫描命令	10.168.1.0/24
nmap 10.168.1.0	10.168.1.12 is up 21 ms latency 10.168.1.124 is up 19 ms latency 10.168.1.138 is up 20 ms latency 10.168.1.153 is up 19 ms latency

在表 4(a)中,扫描命令是对 10.168.1.0/24 网络进行远程扫描,这是最常用的网络扫描方式.由于 10.168.1.117 节点进行了网络跳变,Nmap 扫描 IP 地址后并未检测到该地址.

表 4(b) Nmap 扫描端口结果

扫描命令	nmap -sS -sO 10.168.1.117/153
10.168.1.117	Not available
10.168.1.124	10.168.1.124 is up 25 ms latency 21 -tcp -closed; 111 -tcp -open 34287 -upd -closed; 33259 -upd -open scanned in 19.26 second
10.168.1.138	10.168.1.138 is up 19 ms latency 21 -tcp -open; 34287 -upd -open
10.168.1.153	10.168.1.153 is up 21 ms latency 21 -tcp -open; 34287 -upd -open scanned in 14.26 second

在表 4(b)中,该命令是对实际 IP 地址为 10.168.1.117/124/153 的端节点进行端口扫描.由于 10.168.1.117 节点实施了 IP 地址跳变,因此没有端口扫描信息.10.168.1.124 由于只进行了端口跳变,虽然 Nmap 经过较长时间的扫描,但是反馈的端口扫描结果依然不是实际开启的端口号.由于 10.168.1.138 只进行了指纹跳变;10.168.1.153 是静态节点,因此 Nmap 正确获得了节点开启的所有端口.

表 4(c) Nmap 扫描系统指纹结果

扫描命令	nmap -O -osscan-guess 10.168.1.117/153
10.168.1.117	Not available
10.168.1.124	10.168.1.124 is up 22 ms latency OS match: Linux 2.6.3-3.6 (100%)
10.168.1.138	10.168.1.138 is up 35 ms latency OS match: Fedora 18-23 (94%) Linux 2.6.x-3.6.x (94%) AT&T 3G MircroCell WAP (94%) FreeBSD 7.0-9.0 (94%)
10.168.1.153	10.168.1.153 is up 20 ms latency OS match: Linux 2.6.32-3.6 (100%)

在表 4(c)中,该命令是对系统指纹进行扫描.由于 Nmap 会通过发送一系列报文后分析反馈数据包的 TCP 选项支持和排序等,以分析并匹配已有数据库的系统指纹.由于 10.168.1.117 节点实施了 IP 地址跳变,因此没有系统指纹扫描信息.10.168.1.138 只进行了端口跳变;10.168.1.153 是静态节点,因此 Nmap 以很高的正确率获得了节点的指纹系统.10.168.1.138 节点通过协议跳变,因此即使 Nmap 经过较长时间的扫描,但是反馈的系统指纹结果置信度很低.所以,NAS-SAMT 通过端信息跳变可以有效规避恶意扫描.

在此基础上,针对现有恶意扫描策略,分别在盲扫描、半盲扫描、跟随扫描和混合扫描 4 种情况下比较静态网络、RHM、ST-RHM 和 NAS-SAMT 网络中攻击者扫描的节点空间数量与扫描成功率间的关系.

抵御盲扫描能力:如图 9 所示,在静态网络中,当攻击者采用平均扫描策略进行盲扫描,耗时 334 s 即可达到 100%的扫描成功率;在 RHM 和 ST-RHM 网络中,由于被保护的服务器集群采用随机网络跳变动态改变端信息,攻击者即使经过长时间扫描,扫描的成功率也不超过 10%.此外,由于 NAS-SAMT 采用了基于网络视图距离的跳变端信息选取方法,因此恶意扫描的成功率低于 4.7%.

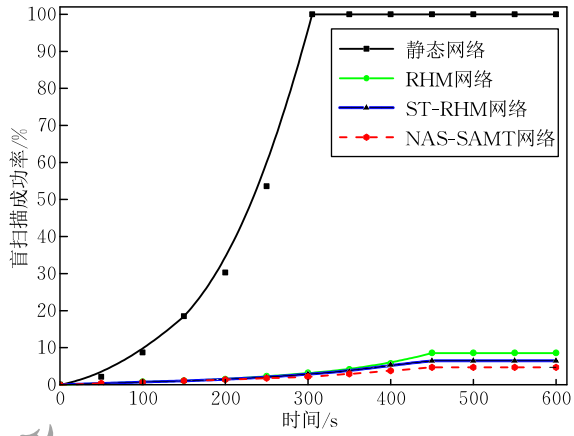

图 9 盲扫描的成功率

抵御半盲扫描攻击:如图 10 所示,在静态网络中,由于攻击者对所扫描的目标网络具有一定的先验知识,通过对特定范围内节点空间进行重复性非均匀扫描,攻击者耗时 256 s 后即可达到 100%的成功率,相较于盲扫描策略减少了 30.46%的扫描时间.在 RHM 网络中,由于 RHM 只采用随机跳变策略,因此当攻击者具有端节点分布状况的一定知识后,扫描成功率可提高到 18.8%.在 NAS-SAMT

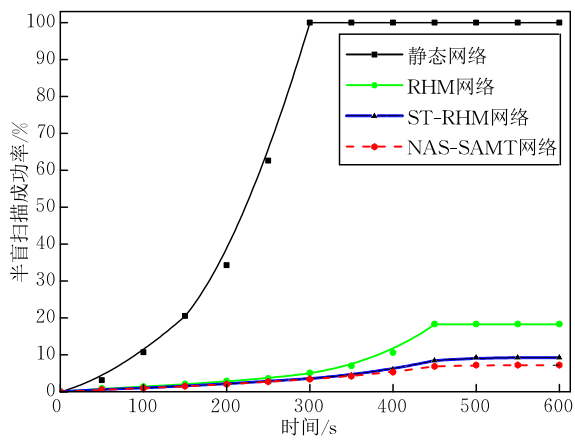

图 10 半盲扫描的成功率

和 ST-RHM 网络中，由于 NAS-SAMT 使用基于权值的反向欺骗跳变策略同时利用网络视图距离选取，因此可以抵御 92.7%以上的半盲扫描；ST-RHM 由于采用时间-空间混合随机跳变的方法，因此也可以有效抵御半盲扫描.

抵御跟随扫描能力：如图 11 所示，由于跟随扫描主要是针对 NMTD 网络实施的扫描策略，因此在静态网络中，攻击者的扫描成功率与半盲扫描结果一样，这与 4.1 节中理论分析的结果一致. 在 RHM 网络中，由于 RHM 仅在端信息空间维度进行跳变，而每个被保护节点的跳变周期是固定的. 因此攻击者可以通过改变扫描频度的方法实现对跳变节点的跟随，在 378 s 即可达到 89%以上的扫描成功率. 在 ST-RHM 网络中，虽然 ST-RHM 引入了时间跳变，但是该方法仅随机改变跳变周期，攻击者可以通过提高扫描频度的方法增加跟随跳变节点的成功率，因此攻击者在 ST-RHM 中的扫描成功率可达到 45.7%. 在 NAS-SAMT 网络中，由于 NAS-SAMT 针对跟随扫描采用跳变周期拉伸，并在采用基于权值的欺骗跳变策略同时全球使得网络视图距离最大的跳变端信息集合，因此可依据扫描的频度和范围实现端信息选取空间和时间的自适应改变，从而提高了网络视图的视在不确定性. NAS-SAMT 可以成功抵御 91.1%以上的跟随扫描.

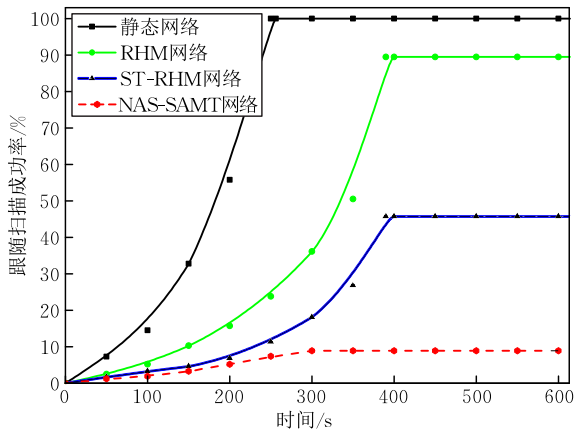

图 11　跟随扫描的成功率

抵御混合扫描能力：在实际条件下[30]攻击者往往通过盲扫描对扫描的节点空间进行过滤筛选，在此基础上通过半盲扫描或跟随扫描对特定的节点空间范围进行重复扫描. 因此攻击者常采用盲扫描与半盲扫描或跟随扫描相混合的攻击策略实施恶意扫描以增加侦测成功率. 混合扫描结果如图 12 所示，在静态网络中，扫描成功率随着攻击者从盲扫描策略转向半盲扫描而出现增长率升高的情况. 相较于单一地采用盲扫描策略，混合扫描策略减少了 23.24%的扫描时间. 在 RHM 网络中，攻击者通过将盲扫描策略改变为半盲扫描或跟随扫描，可有效实现对跳变节点的跟随，进而大幅提升了扫描成功率. 在 ST-RHM 网络中，当攻击者采用跟随扫描策略时，扫描成功率可以达到 41.2%以上. 在 NAS-SAMT 网络中，由于 NAS-SAMT 依据攻击者所采用的扫描策略选取跳变策略，并依据网络视图距离选取不可预测性最大的端信息集合. 因此，即使攻击者采用混合扫描策略，NAS-SAMT 依然可以抵御 92.1%以上的恶意扫描. 它相较于 ST-RHM 可有效降低约 33.1%的恶意扫描；相较于 RHM 可有效降低约 80.1%的恶意扫描.

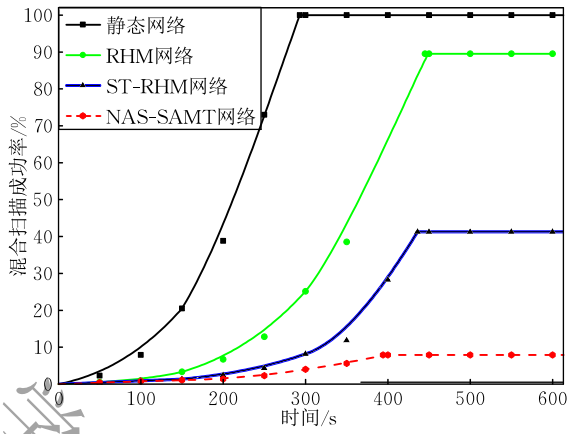

图 12　混合扫描的成功率

综上可知，NAS-SAMT 具有充足的跳变容量和良好的不可预测性；跳变策略的自适应性实现了在不同扫描策略下跳变防御收益的最大化，有效保证了目标网络的安全.

7.2　性能分析

由于 NAS-SAMT 跳变的性能开销主要由算法复杂度、转发时延、流表开销和流表不一致更新导致的包丢失概率 4 部分组成，本节对 NAS-SAMT 中 SMT 的计算开销、跳变引起的处理转发时延、转发流表大小和丢包概率 4 部分进行实验.

(1) NAS-SAMT 计算开销. 由于 NAS-SAMT 的算法开销主要是由求解符合要求的跳变端信息集合产生的. 本文设计了启发式跳变部署算法，并采用 MATHSAT5 求解器对跳变过程中的 SMT 约束进行求解. 结果如表 5 所示，其中 UNSAT 表示 SMT 求解器无法求出符合条件的解；FAIL 表示 SMT 求解器无法对输入的条件进行求解，以上问题可通过减弱限制条件获得满足条件的解集合. 分析可得，SMT 求解器的运行时间随网络中跳变节点的数量、

跳变节点空间和流表大小的改变而变化.且相较于网络节点和节点空间,流表大小的改变对 SMT 求解时间影响更大. NAS-SAMT 通过采用启发式算法实现了对 SMT 求解效率的优化.

表 5 SMT 求解时间

节点数量	节点空间	流表上限	时间/s
100	200	100	4.17
100	300	100	5.06
100	400	100	5.92
300	400	100	UNSAT
300	400	120	FAIL
300	500	160	109.1
300	500	200	97.88

(2) NAS-SAMT 处理转发时延.由于 NAS-SAMT 是采用跳变端节点 THC、HS 和 HC 协同实施的,因此处理转发时延主要由 THC 模块和 HC 两部分组成.因此,通过计算相同数据流经过 THC 的时间差获得 THC 处理时延;利用网络环回时间计算 HC 的处理时延.经过 2000 次实验,结果如表 6 所示.端节点 THC 模块的平均处理时延为 2.12 ms;HC 的平均处理时延为 10.89 ms,NAS-SAMT 一次网络跳变的平均处理转发时延为 15.85 ms,相较于静态网络,总时延平均增加了 10.98%[48].

表 6 NAS-SAMT 转发处理时延

处理节点	平均时延/ms	标准差
THC	2.12	0.47
HC	10.89	0.98
---	15.85	0.63

(3) NAS-SAMT 流表开销.由于 NAS-SAMT 跳变时转发路由的复杂与流表更新的大小成正比,因此通过对流表更新的大小进行实验以分析 NAS-SAMT 跳变产生的路由负载.

由图 13 可知,由于 RHM 和 ST-RHM 并未采用容量约束,当网络规模增加到 800 个节点时,RHM 和 ST-RHM 的转发路由负载增加至 1000 以上.此外,由于 ST-RHM 中跳变周期随机改变,选择的跳变周期越小,对转发路由负载越大. NAS-SAMT 中的路由容量约束则可降低 69.24%的流表数量,且随着网络规模的增加,其约束效果越明显.

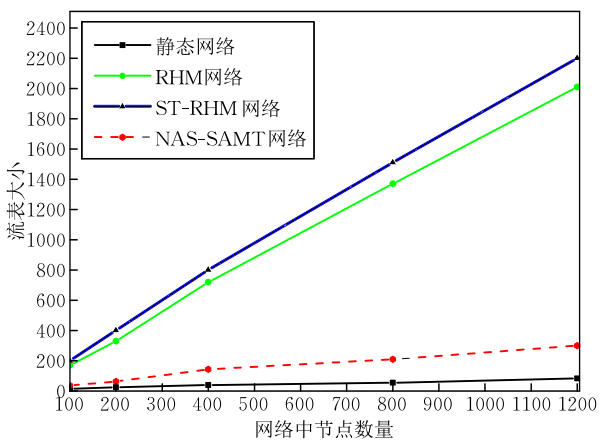

图 13 流表大小实验

(4) 不同跳变周期下的丢包概率.由于网络跳变过程中,端信息迁移导致的流表更新不一致易造成网络中包丢失概率的增加.不同跳变方法的丢包概率如图 14 所示,由于 NAS-SAMT 采用逆序添加,顺序删除的流表更新策略,因此相较于 RHM 和 ST-RHM 降低了 64.13%.因此,NAS-SAMT 使用的流表更新策略有效保证了传输数据的可达性.

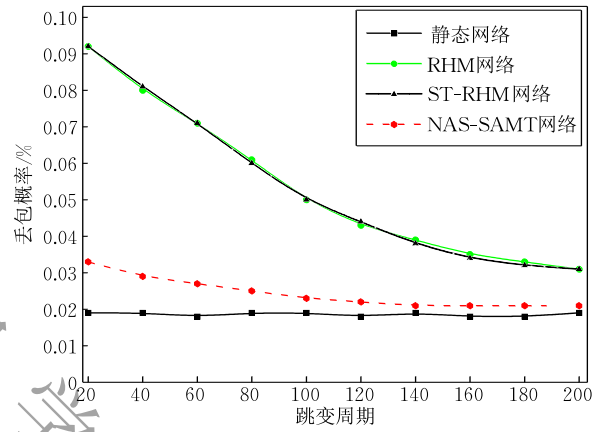

图 14 不同周期下的丢包概率

通过分析可知,NAS-SAMT 的处理转发平均时延为 20 ms,在合理范围内. NAS-SAMT 通过采用基于 SMT 的启发式跳变部署,有效降低了路由节点的负载,并提高了部署效率;通过使用逆序添加,顺序删除的流表更新策略有效防止了流表更新不一致导致的传输数据不可达.从而实现了跳变实施的低开销和跳变部署的可扩展性,保证了跳变实施的可用性和可扩展性.

8 结束语

本文提出了一种基于网络攻击面自适应转换的移动目标防御技术.针对跳变策略盲目随机的问题,采用了基于 Sibson 熵的威胁感知机制,通过判断扫描攻击策略选取跳变策略.在此基础上,设计了基于视图距离的跳变端信息生成算法,通过选取使得视图距离最大的跳变端节点,从而提高跳变的不可预测性;与此同时,采用跳变周期自拉伸策略以保证跳变的时效性,进而从时间和空间两个维度实现了网

络攻击面的自适应转换，最大化了跳变的防御收益.针对跳变实施缺乏约束和部署复杂度高的问题，提出了基于可满足性模理论的启发式部署算法，通过形式化描述跳变实施要满足的约束限制跳变实施的开销，并设计启发式算法实现跳变机制的高效部署，从而保证了跳变的可用性和可扩展性.理论分析通过比较 NAS-SAMT 与静态网络、RHM 和 ST-RHM 抵御不同恶意扫描的能力和跳变实施的成本，证明了 NAS-SAMT 在保证跳变低开销的同时有效抵御了不同策略的扫描攻击.仿真实验结果表明，NAS-SAMT 在混合策略下可抵御 92.1%以上的恶意扫描，比 ST-RHM 提高了 33.1%；比 RHM 提高了 80.1%.与此同时，相较于 RHM 和 ST-RHM，NAS-SAMT 通过采用路由容量约束可平均降低 69.24%的流表数量；通过启发式跳变部署提高了 SMT 求解效率；通过采用“逆序添加，顺序删除”的流表更新策略，降低了 64.13%的包丢失.因此，NAS-SAMT 在保证网络服务质量的同时，有效实现了跳变防御收益的最大化.

参 考 文 献

[1] Okhravi H, Streilein W W, Bauer K S. Moving target techniques: Leveraging uncertainty for cyber defense. Lincoln Laboratory Journal, 2016, 22(1): 100-109

[2] China Internet Network Information Centre. Chinese Internet Security Report in 2015. Beijing, 2016, 6(in Chinese)
(中国互联网络信息中心. 2015 年中国互联网网络安全报告. 北京，2016 年 6 月)

[3] Sun K, Jajodia S. Protecting enterprise networks through attack surface expansion//Proceedings of the 2014 Workshop on Cyber Security Analytics, Intelligence and Automation. Scottsdale, USA, 2014: 29-32

[4] Bou-Harb E, Debbabi M, Assi C. Cyber scanning: A comprehensive survey. IEEE Communications Surveys & Tutorials, 2014, 16(3): 1496-1519

[5] Zhuang R, DeLoach S A, Ou X. Towards a theory of moving target defense//Proceedings of the 1st ACM Workshop on Moving Target Defense. Scottsdale, USA, 2014: 31-40

[6] Lei C, Ma D, Zhang H, et al. Moving target network defense effectiveness evaluation based on change-point detection. Mathematical Problems in Engineering, 2016: 126-140

[7] Cimatti A, Griggio A, Schaafsma B J, et al. The MathSAT5 SMT solver//Proceedings of the International Conference on Tools and Algorithms for the Construction and Analysis of Systems. Rome, Italy, 2013: 93-107

[8] Kirkpatrick K. Software-defined networking. Communications of the ACM, 2013, 56(9): 16-19

[9] Lazaris A, Tahara D, Huang X, et al. Tango: Simplifying SDN control with automatic switch property inference, abstraction, and optimization//Proceedings of the 10th ACM International on Conference on Emerging Networking Experiments and Technologies. Sydney, Australia, 2014: 199-212

[10] Lei C, Ma D H, Zhang H Q. Optimal strategy selection for moving target defense based on Markov game. IEEE Access, 2017, 5: 156-169

[11] Kewley D, Fink R, Lowry J, et al. Dynamic approaches to thwart adversary intelligence gathering//Proceedings of the DARPA Information Survivability Conference & Exposition II(DISCEX'01). Washington, USA, 2001, 1: 176-185

[12] Fink R A, Brannigan M A, Evans S A, et al. Method and apparatus for providing adaptive self-synchronized dynamic address translation: U.S. Patent 7,043,633. 2006-5-9

[13] Antonatos S, Akritidis P, Markatos E P, et al. Defending against hitlist worms using network address space randomization. Computer Networks, 2007, 51(12): 3471-3490

[14] Badishi G, Herzberg A, Keidar I. Keeping denial-of-service attackers in the dark. IEEE Transactions on Dependable and Secure Computing, 2007, 4(3): 191-204

[15] Dunlop M, Groat S, Urbanski W, et al. MT6D: A moving target IPv6 defense//Proceedings of the Military Communications Conference (Milcom 2011). Baltimore, USA, 2011: 1321-1326

[16] Lin Kai, Jia Chun-Fu, Shi Le-Yi. Improvement of distributed timestamp synchronization. Journal on Communications, 2012, 33(10): 110-116(in Chinese)
(林楷，贾春福，石乐义. 分布式时间戳同步技术的改进. 通信学报，2012，33(10)：110-116)

[17] Wang H, Jia Q, Fleck D, et al. A moving target DDoS defense mechanism. Computer Communications, 2014, 46: 10-21

[18] Sun J, Sun K. DESIR: Decoy-enhanced seamless IP randomization//Proceedings of the 35th Annual IEEE International Conference on Computer Communications. San Francisco, USA, 2016: 1-9

[19] Al-Shaer E, Duan Q, Jafarian J H. Random host mutation for moving target defense//Proceedings of the 8th International Conference on Security and Privacy in Communication Networks. Padua, Italy, 2013, 106: 310

[20] Hari K, Dohi T. Dependability modeling and analysis of random port hopping//Proceedings of the 9th International Conference on Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC). Fukuoka, Japan, 2012: 586-593

[21] Malathi P. Mitigating distributed denial of service attacks in multiparty applications in the presence of clock drifts//Proceedings of the 4th International Conference on Computing, Communications and Networking Technologies (ICCCNT). Tiruchengode, India, 2013: 1-6

[22] Yackoski J, Bullen H, Yu X, et al. Applying self-shielding dynamics to the network architecture. Moving Target Defense II. New York, USA: Springer, 2013: 97-115

[23] Jafarian J H, Al-Shaer E, Duan Q. Openflow random host mutation: Transparent moving target defense using software defined networking//Proceedings of the 1st Workshop on Hot Topics in Software Defined Networks. Chicago, USA, 2012: 127-132

[24] MacFarland D C, Shue C A. The SDN shuffle: Creating a moving-target defense using host-based software-defined networking//Proceedings of the 2nd ACM Workshop on Moving Target Defense. Denver, USA, 2015: 37-41

[25] Wei Q, Wu Z, Ren K, et al. An OpenFlow user-switch remapping approach for DDoS defense. KSII Transactions on Internet & Information Systems, 2016, 10(9): 4529-4548

[26] Debroy S, Calyam P, Nguyen M, et al. Frequency-minimal moving target defense using software-defined networking// Proceedings of the 2016 International Conference on Computing, Networking and Communications (ICNC). Hawaii, USA, 2016: 1-6

[27] Ma D, Lei C, Wang L, et al. A self-adaptive hopping approach of moving target defense to thwart scanning attacks// Proceedings of the 18th International Conference of Information and Communications Security (ICICS 2016). Singapore, 2016, 9977: 39

[28] Wang L, Wu D. Moving target defense against network reconnaissance with software defined networking//Proceedings of the International Conference on Information Security. Honolulu, USA, 2016: 203-217

[29] Jafarian J H H, Al-Shaer E, Duan Q. Spatio-temporal address mutation for proactive cyber agility against sophisticated attackers//Proceedings of the 11th ACM Workshop on Moving Target Defense. Scottsdale, USA, 2014: 69-78

[30] Wang Y, Wen S, Xiang Y, et al. Modeling the propagation of worms in networks: A survey. Communications Surveys & Tutorials, 2014, 16(2): 942-960

[31] Hobson T, Okhravi H, Bigelow D, et al. On the challenges of effective movement//Proceedings of the 1st ACM Workshop on Moving Target Defense. Scottsdale, USA, 2014: 41-50

[32] Lei C, Zhang H, Ma D, et al. Network moving target defense technique based on self-adaptive end-point hopping. Arabian Journal for Science and Engineering, 2017: 1-14

[33] Elhadef M. A multimetric approach for discriminating distributed denial of service attacks from flash crowds. Advanced Multimedia and Ubiquitous Engineering. Berlin Heidelberg, Germany: Springer, 2016: 17-23

[34] Yang Y, Yu J X, Gao H, et al. Mining most frequently changing component in evolving graphs. World Wide Web, 2014, 17(3): 351-376

[35] Gleich D F. PageRank beyond the Web. SIAM Review, 2015, 57(3): 321-363

[36] Cong S, Ge Y, Chen Q, et al. DTHMM based delay modeling and prediction for networked control systems. Journal of Systems Engineering and Electronics, 2010, 21(6): 1014-1024

[37] Page L, Brin S, Motwani R, et al. The PageRank citation ranking: Bringing order to the web. Technical Report 1999-66, Stanford Digital Library Technologies Project, Stanford InfoLab, USA, 1999

[38] Huang M, Liang W, Xu Z, et al. Dynamic routing for network throughput maximization in software-defined networks// Proceedings of the IEEE INFOCOM the 35th Annual IEEE International Conference on Computer Communications. San Francisco, USA, 2016: 978-986

[39] Peng B, Kemp A H, Boussakta S. QoS routing with bandwidth and hop-count consideration: A performance perspective. Journal of Communications, 2006, 1(2): 1-11

[40] Metropolis N, Rosenbluth A W, Rosenbluth M N, et al. Equation of state calculations by fast computing machines. The Journal of Chemical Physics, 1953, 21(6): 1087-1092

[41] Crosby S, Carvalho M, Kidwell D. A layered approach to understanding network dependencies on moving target defense mechanisms//Proceedings of the 8th Annual Cyber Security and Information Intelligence Research Workshop. Oak Ridge, USA, 2013: 36

[42] Narayanan R, Lin G, Syed A A, et al. A framework to rapidly test SDN use-cases and accelerate middlebox applications// Proceedings of the 38th Conference of Local Computer Networks (LCN 2013). Sydney, Australia, 2013: 763-770

[43] Das S, Zhang W, Liu Y. Reconfigurable dynamic trusted platform module for control flow checking//Proceedings of the 2014 IEEE Computer Society Annual Symposium on VLSI. Florida, USA, 2014: 166-171

[44] Carroll T E, Crouse M, Fulp E W, et al. Analysis of network address shuffling as a moving target defense//Proceedings of the IEEE International Conference of Communications (ICC). Sydney, Australia. 2014: 701-706

[45] Kaur K, Singh J, Ghumman N S. Mininet as software defined networking testing platform//Proceedings of the International Conference on Communication, Computing & Systems (ICCCS. 2014). Chennai, India, 2014

[46] Kim H, Feamster N. Improving network management with software defined networking. IEEE Communications Magazine, 2013, 51(2): 114-119

[47] Medved J, Varga R, Tkacik A, et al. Opendaylight: Towards a model-driven sdn controller architecture//Proceedings of the 15th International Symposium on World of Wireless, Mobile and Multimedia Networks. Budapest, Hungary, 2014: 1-6

[48] Lin Chuan, Zhao Hai, Bi Yuan-Guo, et al. Research on network delay of Internet. Journal on Communications, 2015, 36(3): 19-2015069(in Chinese)
(林川, 赵海, 毕远国等. 互联网网络时延特征研究. 通信学报, 2015, 36(3): 19-2015069)

LEI Cheng, born in 1989, Ph. D. candidate. His main research interests include network security, moving target defense and net-flow exchange security.

MA Duo-He, born in 1982, Ph. D., assistant professor. His main research interests include network security, moving target defense and cloud security.

ZHANG Hong-Qi, born in 1962, Ph. D., professor, Ph. D. supervisor. His main research interests include network security and classification protection.

YANG Ying-Jie, born in 1971, Ph. D., associate professor. His main research interests include data mining, situation awareness and security management.

WANG Li-Ming, born in 1978, Ph. D., associate professor. His main research interests include trusted computing and cloud computing security.

Background

Network mutation plays an important role in moving target defense research. It can resist malicious scanning. However, existing network mutation techniques are hard to maximize the mutation defense benefit on the basis of ensuring the network service quality. To cope with the problem above, a novel technique named moving target defense technique based on network attack surface self-adaptive mutation is proposed. Aimed at the poor effectiveness of mutation mechanism in the course of defense, self-adaptive endpoint mutation mechanism is designed. It consists of network threat awareness mechanism based on Sibson entropy and mutation strategy algorithm based on network view distance. Aimed at the low availability caused by limited network resource and high mutation overhead, heuristic mutation deployment algorithm based on SMT is designed. Heuristic algorithm is adopted so as to solve approximate optimal solution efficiently. After that, theoretical analysis and simulation experiments show that compared with existing typical endpoint mutation mechanisms, Random Host Mutation and Spatial and Temporal Random Host Mutation, the proposed method can disrupt more than 92.1% of different types of scanning strategies in network attacks. Besides, the flow table size of NAS-SAMT decreases 69.24%, and the packet drop rate also decreases 64.13%. Consequently, NAS-SAMT can achieve the maximum mutation defense benefit on the basis of low performance overhead.

Our project mainly focuses on defense strategy selection, endpoint mutation, forwarding path migration, multi-elements collaborative mutation, and effectiveness assessment. This project is supported by the National Basic Research Program of 973 Program of China (2011CB311801), the National High Technology Research and Development Program of China (2015AA016106), and the Zhengzhou Science and Technology Talents (131PLKRC644). This paper figures out how to maximize mutation benefit. It is a further step in endpoint self-adaptive mutation by introducing cyber deception concept through network view distance. Besides, it optimizes the mutation deployment based on SMT by designing heuristic algorithm.