网络地址变换对不同扫描攻击的防御优势分析

王 凯[*①②] 陈欣华[③] 陈 熹[②④] 武泽慧[②]
[①](天津大学电气自动化与信息工程学院 天津 300072)
[②](解放军战略支援部队信息工程大学网络空间安全学院 郑州 450000)
[③](郑州幼儿师范高等专科学校计算机系 郑州 450000)
[④](数学工程与先进计算国家重点实验室 无锡 214125)

摘 要：网络地址变换通过动态地改变或映射主机的网络地址，使得攻击者收集到的地址信息变得无效，然而对于扫描到主机即发起攻击的扫描攻击，网络地址变换的防御性能有所下降，很少有研究从理论上分析网络地址变换对不同扫描策略的扫描攻击的防御优势。该文考虑均匀变换和非重复变换两种网络地址变换策略，给出不同扫描策略的扫描攻击在静态地址环境以及网络地址变换环境下的概率模型，概率模型分析了攻击者命中至少一台主机的概率以及攻击者命中主机的数量；通过理论计算两种网络地址变换策略相比于静态地址环境的防御优势。分析结果表明对于可重复扫描攻击，两种网络地址变换策略相比于静态地址环境不具有防御优势；对于非重复扫描攻击，均匀变换仅当主机数量较少时才具有概率优势，非重复变换仅当主机数量占地址空间比例较小时才具有较高的比例优势。

关键词：移动目标防御；网络地址变换；概率模型；防御优势
中图分类号： TP393.08 **文献标识码**： A **文章编号**：1009-5896(2018)04-0794-08
DOI: 10.11999/JEIT170105

On the Defense Advantages of Network Address Shuffling Against Different Scanning Attacks

WANG Kai[①②] CHEN Xinhua[③] CHEN Xi[②④] Wu Zehui[②]
[①](*School of Electrical and Information Engineering*, *Tianjin University*, *Tianjin* 300072, *China*)
[②](*Institute of Cyberspace Security, PLA Strategic Support Force Information Engineering University*, *Zhengzhou* 450000, *China*)
[③](*Department of Computer*, *Zhengzhou Preschool Education College*, *Zhengzhou* 450000, *China*)
[④](*State Key Laboratory of Mathematical Engineering and Advanced Computing*, *Wuxi* 214125, *China*)

Abstract: Network address shuffling invalidates the address information collected by the attacker with dynamically changing or remapping the host's network addresses, however, the defense performance of network address shuffling decreases when against scanning attacks which launch attacks at the same time of discovering targets, and few studies analyze theoretically different defense advantages of network address shuffling against scanning attacks of different scanning strategies. In this paper, two strategies of network address shuffling are considered: uniform shuffling and non-repeat shuffling. It presents probabilistic models of scanning attacks in the static address and network address shuffling environments, which analyzes both the probability of the attacker hitting at least one host and the number of hosts hit by the attacker. Then, the defense advantages of both network address shuffling strategies are theoretically calculated and compared with the static address environment. Analysis results indicate that both shuffling strategies have no defense advantages against repeatable scanning attack compared with the static address environment; uniform shuffling has probability advantage against non-repeat scanning attack only when the hosts number is small, and non-repeat shuffling has significant ratio advantage only when the hosts number accounts for a small proportion in the network space size.

Key words: Moving target defense; Network address shuffling; Probabilistic model; Defense advantages

收稿日期：2017-02-08；改回日期：2018-01-25；网络出版：2018-02-05
*通信作者：王凯 quanjiaokk@163.com
基金项目：国家自然科学基金(61271252)
Foundation Item: The National Natural Science Foundation of China (61271252)

1　引言

网络地址变换[1]通过动态改变主机的网络地址，或者将网络内的主机映射到动态的网络地址，使得攻击者扫描获得的地址信息随着地址变化变得无效。因此，网络地址变换可以有效地阻止攻击者的信息收集，从而可以防止攻击者利用收集的信息发现漏洞或进行漏洞利用开发。

目前研究人员已经提出了多种网络地址变换方法，这些方法的两个重要组成部分包括如何动态改变地址以及地址改变后如何保持主机之间的连接。参与自身防御的应用(Applications that Participate in their Own Defense, APOD)[2]和动态网络地址转换 (Dynamic Network Address Translation, DyNAT)[3]均采用一种网络地址转换(Network Address Translation, NAT)的方式改变地址。在这两种方法中，内部设备对外部网络的 NAT 地址周期性地发生变化。主机间需要通过共享的先验知识，包括动态变换的算法和参数等，维持相互之间的连接。NAT 方式的另一个缺点是难以影响内部网络中的威胁。网络地址空间随机化(Network Address Space Randomization, NASR)[4]提供了一种局域网内的网络地址随机化方法，用于防御目标列表蠕虫。该方法采用动态主机配置协议(Dynamic Host Configuration Protocol, DHCP)更新改变主机地址，并在地址更新后，通过域名系统(Domain Name System, DNS)请求设备的主机名获取新的地址，来重新建立连接，因此该方法无法防御已知目标主机名的攻击者。此外，地址变换受限于局域网的地址空间和主机的地址更新操作，该方法中网络地址变化的频率和不可预测性有限。开放流随机主机突变(OpenFlow Random Host Mutation, OF-RHM)[5]提供了一种软件定义网络(Software Defined Network, SDN)中的地址变换方法，实现了网络地址的透明和快速变化。在该方法中，SDN 控制器为主机动态分配一个随机的虚拟地址，并将其和主机的真实地址进行映射，主机之间通过 DNS 请求获得该虚拟地址进行通信。该方法通过 SDN 控制器改变上述虚拟地址，并通过维护流表使得地址变化不会中断已建立的连接。随机主机突变(Random Host Mutation, RHM)[6,7]在传统网络中实现了上述地址变换方法。此外，目前已有的网络地址变换方法还包括移动目标 IPv6 防御(Moving Target IPv6 Defense, MT6D)[8]、基于主机的 SDN 方法[9]、伪装蜜网[10,11]等。和网络地址变换相关的理论研究包括移动目标防御的统一模型[12,13]，基于网络的移动目标防御的定性分析[14]，移动目标防御技术的比较[15,16]等。在网络地址变换有效性的理论分析方面，Carroll 等人[17]给出了非重复扫描攻击在静态地址环境和完美变换(网络地址变换速率大于扫描速率的均匀变换)环境中的概率模型，模型仅分析了攻击者命中至少一台主机的概率。Crouse 等人[18]在上述模型的基础上增加了蜜罐网络中的概率模型，他们通过定性分析指出仅当主机数量占地址空间比例较小时完美变换才具有防御优势。而本文通过理论分析表明了均匀变换对于攻击者命中至少一台主机的概率的最大优势仅与主机数量成反比，而与地址空间大小无关。文献[6,7]从理论上分析了考虑扫描速率和网络地址变换速率之比时非重复扫描攻击在均匀变换中未命中主机的比例，同样地这些分析也局限于非重复扫描攻击。

然而对于从发现目标到实施攻击间隔较小的网络攻击，网络地址变换的防御性能有所下降。例如在扫描攻击中，攻击者通常在扫描到目标主机的同时即对主机实施网络攻击，如漏洞攻击、分布式拒绝服务(Distributed Denial Of Service, DDOS)攻击等，此时网络地址变换的有效性受限于其隐藏主机网络地址的能力。对于扫描攻击，现有的对网络地址变换的防御优势分析大多是通过实验进行验证的[2−5,8,9]，或者局限于特定的扫描策略和防御优势[6,7,17]，因此缺少网络地址变换对不同扫描策略的扫描攻击的防御优势的理论分析。

本文给出了不同扫描策略的扫描攻击在静态地址环境和不同网络地址变换策略环境中的概率模型，模型分析了攻击者命中至少一台主机的概率以及命中主机的数量；进一步地，通过上述模型从理论上计算了网络地址变换相比于静态地址环境对攻击者命中至少一台主机的概率和命中主机的比例的防御优势，定量分析了主机数量和地址空间大小对不同网络地址变换策略的防御优势的影响。本文考虑两种基本的扫描策略：一种是可重复扫描(repeatable scanning)，即扫描的地址随机产生，可能存在重复，通常由蠕虫及其他恶意软件产生；另一种是非重复扫描(non-repeat scanning)，即扫描的地址不重复，通常由扫描工具，如 Nmap 产生。对于网络地址变换策略，本文除了考虑常见的均匀变换(uniform shuffling)，即防御者周期性地变换主机的网络地址，且对主机重新分配的地址在网络地址空间内均匀分布[4−7,17,18]，还提出了一种变换策略称为非重复变换(non-repeat shuffling)，即防御者在发现对未使用地址的连接请求时，按顺序选择一台主机将主机地址变换为该未使用地址。本文还在理论模型和分析中提供了仿真实验对理论结果进行验

证。理论和实验结果表明对于可重复扫描攻击，两种网络地址变换策略并不具备防御优势；对于非重复扫描攻击者命中至少一台主机的概率，均匀变换的最大优势随主机数量的增加而减小，与地址空间大小无关，而非重复变换的最大优势则随主机数量的增加而减小，随地址空间大小增加而增加；对于非重复扫描攻击者命中主机的比例，均匀变换的最大优势在地址空间足够大时约为常数，而非重复变换的最大优势在地址空间足够大时约为主机数量占地址空间比例的递减函数。

2 扫描攻击的概率模型

在扫描攻击中，扫描者对目标网络的网络地址空间进行扫描，在命中活动主机后即发动进一步的攻击。假设目标网络的地址空间大小为 m，网络中有 $n \le m$ 个主机。令 X_k 表示攻击者在 k 次扫描中命中主机次数的随机变量，Y_k 表示攻击者在 k 次扫描中命中主机数量的随机变量。扫描攻击的概率模型通过以下两个参数进行描述：(1)攻击者在 k 次扫描中命中至少一台主机的概率 $\Pr_{a\text{-}d}(X_k>0)$；(2)攻击者在 k 次扫描中命中主机数量的期望 $E_{a\text{-}d}(Y_k)$。下标 $a \in \{\mathrm{r},\mathrm{n}\}$ 表示攻击者采用的扫描策略，其取值集合中的元素依次表示可重复扫描攻击和非重复扫描攻击；下标 $d \in \{\mathrm{s},\mathrm{u},\mathrm{n}\}$ 表示防御者采用的网络环境，其取值集合中的元素依次表示静态地址环境、均匀变换环境和非重复变换环境。

2.1 可重复扫描攻击

在可重复扫描攻击中，扫描的地址随机产生，所以不论在静态地址环境还是两种网络地址变换策略环境，攻击者每次扫描命中主机的概率都为 n/m。因此可重复扫描攻击相当于放回取球问题，则 X_k 服从二项分布[19]，即

$$\begin{aligned}\Pr_{\text{r-s}}(X_k=x)&=\Pr_{\text{r-u}}(X_k=x)=\Pr_{\text{r-n}}(X_k=x)\\&=C_k^x\left(\frac{n}{m}\right)^x\left(1-\frac{n}{m}\right)^{k-x}\end{aligned}\tag{1}$$

从而可以得到攻击者命中至少一个脆弱主机的概率为

$$\begin{aligned}\Pr_{\text{r-s}}(X_k>0)&=\Pr_{\text{r-u}}(X_k>0)=\Pr_{\text{r-n}}(X_k>0)\\&=1-\Pr_{\text{r-s}}(X_k=0)=1-\left(1-\frac{n}{m}\right)^k\end{aligned}\tag{2}$$

由于可重复扫描攻击者可能重复命中同一台主机，因此 $X_k \ge Y_k$。此时每个主机是否被命中是相互独立的，因此令式(2)中的 n 等于 1 即每个主机在 k 次扫描中被命中的概率，从而可以得到攻击者在 k 次扫描中命中主机数量的期望为

$$\mathrm{E}_{\text{r-s}}(Y_k)=\mathrm{E}_{\text{r-u}}(Y_k)=\mathrm{E}_{\text{r-n}}(Y_k)=n\left(1-\left(1-\frac{1}{m}\right)^k\right)\tag{3}$$

2.2 非重复扫描攻击

在非重复扫描攻击中，攻击者在遍历完地址空间后即停止扫描，即扫描次数 $k \le m$。下面分别给出不同环境下非重复扫描攻击的概率模型。

2.2.1 静态地址环境 在静态地址环境下的非重复扫描攻击中，被命中的主机将不会被再次扫描到，因此静态地址环境下的非重复扫描攻击相当于不放回取球问题，则 X_k 服从超几何分布[19]，即

$$\Pr_{\text{n-s}}(X_k=x)=\frac{C_n^x C_{m-n}^{k-x}}{C_m^k}\tag{4}$$

从而可以得到攻击者在 k 次扫描中命中至少一台主机的概率为

$$\begin{aligned}\Pr_{\text{n-s}}(X_k>0)&=1-\Pr_{\text{n-s}}(X_k=0)\\&=\begin{cases}1-\dfrac{C_{m-n}^k}{C_m^k}, & 0\le k\le m-n\\ 1, & k>m-n\end{cases}\end{aligned}\tag{5}$$

由于被命中的主机将不会被再次扫描到，因此 $X_k=Y_k$，那么可以得到攻击者在 k 次扫描中命中主机数量的期望为

$$\mathrm{E}_{\text{n-s}}(Y_k)=\mathrm{E}_{\text{n-s}}(X_k)=k\frac{n}{m}\tag{6}$$

2.2.2 均匀变换环境 在均匀变换环境中，令 r 表示扫描速率和网络地址变换速率之比。当 $r \le 1$ 时，攻击者任意两次扫描之间网络地址均会发生变换，且变换后的地址在网络地址空间中均匀分布，因此扫描过程相当于可重复扫描攻击，其模型与可重复扫描攻击的概率模型一致。

当 $r>1$ 时，在两次地址变换间隔之间攻击者处于静态地址环境。令 $K=\lfloor k/r \rfloor$，$k_i, i=1,2,\cdots,K+1$ 表示攻击者在第 i 个间隔的扫描次数，$x_i, i=1,2,\cdots,K+1$ 表示攻击者在第 i 个间隔内命中主机的数量，那么可以得到

$$\left.\begin{aligned}k_i&=\begin{cases}\lfloor ir\rfloor-\lfloor(i-1)r\rfloor, & 1\le i\le K\\ k-\lfloor Kr\rfloor, & i=K+1\end{cases}\\ \Pr_{\text{n-u}}(X_k=x)&=\sum_{x=\sum_{i=1}^{K+1}x_i}\left(\prod_{i=1}^{K+1}\Pr_{\text{n-s}}\left(X_{k_i}=x_i\right)\right)\end{aligned}\right\}\tag{7}$$

从而可以得到攻击者在 k 次扫描中命中至少一台主机的概率为

$$\Pr_{\text{n-u}}(X_k>0)=1-\Pr_{\text{n-u}}(X_k=0)=1-\prod_{i=1}^{K+1}\left(\frac{C_{m-n}^{k_i}}{C_m^{k_i}}\right)\tag{8}$$

此时每个主机是否被命中是相互独立的，因此令式(8)中的 n 等于 1 即每个主机在 k 次扫描中被命中的概率，从而可以得到攻击者在 k 次扫描中命中主机数量的期望为

$$\mathrm{E}_{\text{n-u}}\left(Y_k\right)=n\left(1-\prod_{i=1}^{K+1}\left(1-\frac{k_i}{m}\right)\right) \tag{9}$$

特别地，当 $r\geq m$ 时攻击者始终处于静态地址环境，上述模型与静态地址环境下的非重复扫描攻击的概率模型一致。

为了验证模型的正确性，本文采用 Mininet[20] 创建了一个SDN网络用于仿真实验，并利用Python编写的网络操作系统(network Operating System written in Python, POX)[21]在控制器中分别实现了两种网络地址变换策略用于管理上述网络。图 1 显示了在均匀变换环境中，$m=2^8$，$n=\{1,10\}$，$r=\left\{1,50,2^8\right\}$时，非重复扫描攻击者命中至少一台主机的概率和命中主机的数量随着扫描次数增加而变化的理论和实验结果。特别地，其中 $r=1$ 等同于可重复扫描攻击，$r=2^8$ 等同于静态地址环境下的非重复扫描攻击。在实验结果中每个数据点为 100 次结果的均值。从图中可以看出实验结果和理论结果基本一致。

2.2.3 非重复变换环境　在非重复变换环境下的非重复扫描攻击中，每次扫描均受到之前扫描结果的影响，因此难以计算 X_k 的概率分布的完整表达式，这里仅计算攻击者在 k 次扫描中未命中任何主机的概率。在这种情况下，攻击者能够命中的主机数量随失败扫描次数增多而减少，直到失败扫描次数达到 n 时，攻击者将无法命中任何主机，因此可以得到

$$\mathrm{Pr}_{\text{n-n}}\left(X_k=0\right)=\begin{cases}\left(1-\dfrac{n}{m}\right)\left(1-\dfrac{n-1}{m-1}\right)\cdots\\ \quad\left(1-\dfrac{n-k+1}{m-k+1}\right)=\dfrac{(m-n)^k}{A_m^k}, & k\leq n\\ \mathrm{Pr}_{\text{n-n}}\left(X_n=0\right)=\dfrac{(m-n)^n}{A_m^n}, & k>n\end{cases} \tag{10}$$

从而可以得到攻击者命中至少一个脆弱主机的概率为

$$\mathrm{Pr}_{\text{n-n}}\left(X_k>0\right)=1-\mathrm{Pr}_{\text{n-n}}\left(X_k=0\right)=\begin{cases}1-\dfrac{(m-n)^k}{A_m^k}, & k\leq n\\ 1-\dfrac{(m-n)^n}{A_m^n}, & k>n\end{cases} \tag{11}$$

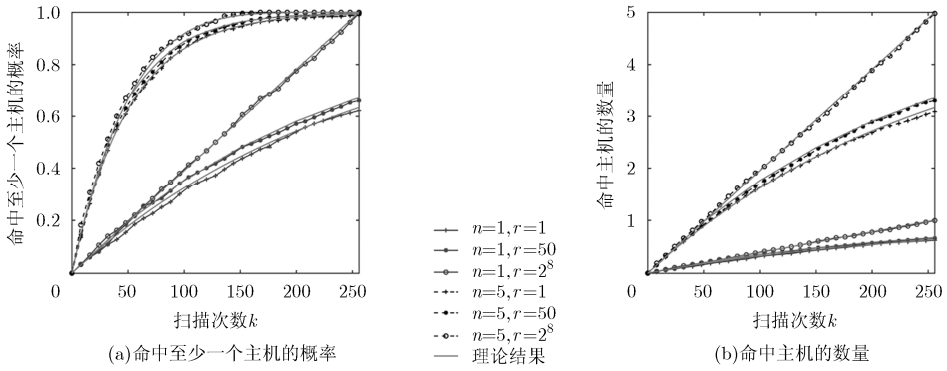
由于每个主机是否被命中不再是相互独立的，因此不能通过计算每个主机在 k 次扫描中被命中的概率来计算 $\mathrm{E}_{\text{n-n}}\left(Y_k\right)$，下面通过均值分析法来计算 $\mathrm{E}_{\text{n-n}}\left(Y_k\right)$。令 U_k 表示第 k 次扫描后主机地址为已扫描地址的平均主机数量，特别地，$U_0=0$，那么攻击者在第 k 次扫描时命中的主机数量平均为 $\mathrm{dE}_k=\dfrac{n-U_{k-1}}{m-k+1}$，失败扫描次数平均为 $1-\mathrm{dE}_k$，即需要发生地址变换的主机数量平均为 $1-\mathrm{dE}_k$。由于在第 $k-1$ 次扫描后已经发生地址变换的主机数量平均为 $k-1-\mathrm{E}_{\text{n-n}}\left(Y_k\right)$，那么根据排队论中的律特法则，第 k 次扫描后未命中主机发生地址变换的数量平均为 $\left(1-\mathrm{dE}_k\right)\dfrac{n-U_{k-1}-\mathrm{dE}_k}{n-\left(k-1-\mathrm{E}_{\text{n-n}}\left(Y_k\right)\right)}$。考虑主机数量为 n，可以得到 $U_k=\max\left(n,U_{k-1}+\mathrm{dE}_k+\left(1-\mathrm{dE}_k\right)\dfrac{n-U_{k-1}-\mathrm{dE}_k}{n-\left(k-1-\mathrm{E}_{\text{n-n}}\left(Y_k\right)\right)}\right)$。综上可以得到攻击者在 k 次扫描中命中主机数量的期望为

$$\mathrm{E}_{\text{n-n}}\left(Y_k\right)=\mathrm{E}_{\text{n-n}}\left(Y_{k-1}\right)+\mathrm{dE}_k \tag{12}$$

其中，

$$\mathrm{dE}_k=\frac{n-U_{k-1}}{m-k+1},$$

$$U_k=\max\left(n,U_{k-1}+\mathrm{dE}_k+\left(1-\mathrm{dE}_k\right)\cdot\frac{n-U_{k-1}-\mathrm{dE}_k}{n-\left(k-1-\mathrm{E}_{\text{n-n}}\left(Y_k\right)\right)}\right)$$



(a)命中至少一个主机的概率　　(b)命中主机的数量

图 1 均匀变换环境中非重复扫描攻击的理论和实验结果

图 2 显示了在非重复变换环境中，$m=2^8$，$n=\{10,50,100,200\}$ 时，非重复扫描攻击者命中至少一台主机的概率和命中主机的数量随着扫描次数增加而变化的理论和实验结果。为了对比，图中还显示了静态地址环境下的非重复扫描攻击的理论结果。在实验结果中每个数据点为 100 次结果的均值。从图中可以看出实验结果和理论结果基本一致。

3 防御优势分析

本节从理论上分析两种网络地址变换策略相比于静态地址环境对可重复扫描攻击和非重复扫描攻击的防御优势，主要考虑以下两个方面的防御优势：(1)对攻击者命中至少一台主机的概率的防御优势，以下简称为概率优势，记为 $\mathrm{PA}_{a\text{-}d}$ (Probability Advantage)；(2)对攻击者命中主机数量的期望占全部主机数量的比例的防御优势，以下简称为比例优势，记为 $\mathrm{RA}_{a\text{-}d}$ (Ratio Advantage)。下标 $a\in\{\mathrm{r},\mathrm{n}\}$ 表示攻击者采用的扫描策略，$d\in\{\mathrm{u},\mathrm{n}\}$ 表示防御者采用的网络地址变换策略。

3.1 对可重复扫描攻击的防御优势

根据 2.1 节的分析，两种网络地址变换策略环境中的可重复扫描攻击的概率模型和静态地址环境中可重复扫描攻击的概率模型一致。由上可得到：

定理 1 对于可重复扫描攻击，均匀变换和非重复变换相比于静态地址环境不具有概率优势和比例优势，即

$$\left.\begin{aligned}\mathrm{PA}_{\text{r-u}}&=\mathrm{PA}_{\text{r-n}}=0\\ \mathrm{RA}_{\text{r-u}}&=\mathrm{RA}_{\text{r-n}}=0\end{aligned}\right\} \tag{13}$$

3.2 对非重复扫描攻击的防御优势

3.2.1 均匀变换 根据 2.2.2 节的分析和图 1 可以得到，对于非重复扫描攻击，均匀变换相比于静态地址环境的概率优势和比例优势均在 $r>1$ 时随着 r 减小而增大，而当 $r\le 1$ 时均匀变换环境中的非重复扫描攻击的概率模型与可重复扫描攻击的概率模型一致，此时均匀变换相比于静态地址环境的概率优势和比例优势最大，因此可以得到

由于 $r\le 1$ 时防御性能最好，因此

$$\left.\begin{aligned}\max_{r,k}\left(\mathrm{PA}_{\text{n-u}}\right)&=\max_{k}\left(\mathrm{Pr}_{\text{n-s}}\left(X_k>0\right)-\mathrm{Pr}_{\text{r-s}}\left(X_k>0\right)\right)\\ \max_{r,k}\left(\mathrm{RA}_{\text{n-u}}\right)&=\max_{k}\left(\mathrm{E}_{\text{n-s}}\left(Y_k\right)-\mathrm{E}_{\text{r-s}}\left(Y_k\right)\right)\Big/n\end{aligned}\right\} \tag{14}$$

进一步地，可以得到(证明略)

$$\max_{r,k}\left(\mathrm{PA}_{\text{n-u}}\right)\le\frac{1}{en} \tag{15}$$

其中，e 为自然底数。

由图 1 可以看出对于非重复扫描攻击，均匀变换相比于静态地址环境的比例优势随扫描次数增加而增加，因此

$$\begin{aligned}\max_{r,k}\left(\mathrm{RA}_{\text{n-u}}\right)&=\left(\mathrm{E}_{\text{n-s}}\left(Y_m\right)-\mathrm{E}_{\text{r-s}}\left(Y_m\right)\right)\Big/n\\ &=1-\left(1-\left(1-\frac{1}{m}\right)^m\right)=\left(1-\frac{1}{m}\right)^m\\ &\approx e^{-1}\,(m\gg 1)\end{aligned} \tag{16}$$

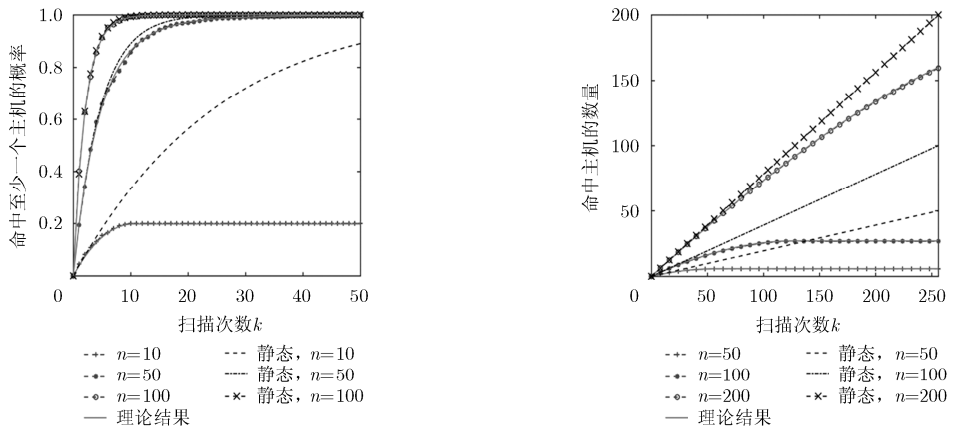
由式(15)，式(16)可以得到

定理 2 对于非重复扫描攻击，均匀变换相比于静态地址环境具有如下的最大概率优势和最大比例优势：

$$\left.\begin{aligned}\max_{r,k}\left(\mathrm{PA}_{\text{n-u}}\right)&\le\frac{1}{en}\\ \max_{r,k}\left(\mathrm{RA}_{\text{n-u}}\right)&=\left(1-\frac{1}{m}\right)^m\approx e^{-1}\,(m\gg 1)\end{aligned}\right\} \tag{17}$$

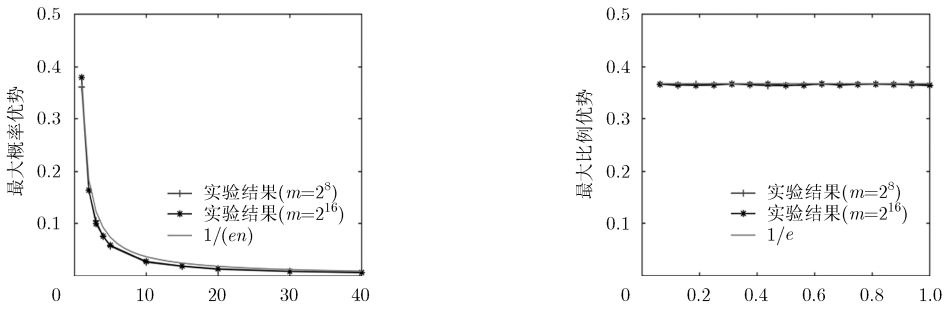
从定理 2 可以看到，对于非重复扫描攻击，均匀变换相比于静态地址环境的最大概率优势与主机数量成反比，与地址空间大小无关；而最大比例优势随地址空间大小增加而增加，与主机数量无关，当地址空间足够大时，最大比例优势约为常数。

图 3 显示了 $m=\left\{2^8,2^{16}\right\}$ 时，均匀变换相比于静



(a)命中至少一个主机的概率　　(b)命中主机的数量

图 2 非重复变换环境中非重复扫描攻击的理论和实验结果



(a)最大概率优势　　(b)最大比例优势

图 3 均匀变换相比于静态地址环境对非重复扫描攻击的最大概率优势和最大比例优势

态地址环境对非重复扫描攻击的最大概率优势和最大比例优势随着主机数量增加而变化的理论和实验结果，其中图 3(b)的横坐标为主机数量与地址空间大小的比值。在实验结果中每个数据点为 100 次结果的均值。

从图中可以看出实验结果和理论结果基本一致。由定理 2 和图 3 可以得到，假设概率优势小于 0.01 时可以忽略不计，则当主机数量大于 $\frac{1}{0.01e}\approx 37$ 时均匀变换相比于静态地址环境不再具有概率优势；均匀变换相比于静态地址环境的最大比例优势约为 $e^{-1}\approx 37\%$ 。

3.2.2 非重复变换　根据 2.2.3 节的分析和图 2 可以得到，对于非重复扫描攻击，非重复变换相比于静态地址环境的概率优势和比例优势均随着扫描次数增加而增加，因此可以得到

$$\left.\begin{aligned}\max_k\left(\mathrm{PA}_{\text{n-n}}\right)&=1-\mathrm{Pr}_{\text{n-n}}\left(X_m>0\right)=\frac{(m-n)^n}{A_m^n}\\ \max_k\left(\mathrm{RA}_{\text{n-n}}\right)&=\left(\mathrm{E}_{\text{n-s}}\left(Y_m\right)-\mathrm{E}_{\text{n-n}}\left(Y_m\right)\right)\Big/n\\ &=1-\mathrm{E}_{\text{n-n}}\left(Y_m\right)\Big/n\end{aligned}\right\}\tag{18}$$

进一步地，通过曲线拟合可以得到

$$\max_k\left(\mathrm{PA}_{\text{n-n}}\right)=\frac{(m-n)^n}{A_m^n}\approx e^{-n^2/2m}\tag{19}$$

由于 2.2.3 节未给出 $\mathrm{E}_{\text{n-n}}\left(Y_k\right)$ 的具体表达式，下面通过考虑另一种网络地址变换策略来计算 $\mathrm{E}_{\text{n-n}}\left(Y_k\right)$ 的上限，以此来分析主机数量和地址空间大小对非重复变换的最大比例优势的影响。在该网络地址变换策略中，防御者仅当失败扫描次数达到 n 时才对所有主机进行地址变换，之后攻击者将无法命中任何主机。令 Z_k 表示该变换环境中攻击者在 k 次扫描中命中主机数量的随机变量，则 $\mathrm{E}_{\text{n-n}}\left(Y_k\right)\le\mathrm{E}\left(Z_k\right)$ 。当 $m-n<n$ 时失败扫描次数无法达到 n ，因此上述变换不会发生，攻击者在扫描完整个地址空间后可以命中所有主机，即 $Z_k\le n$ ；当 $m-n\ge n$ 时，令 N 表示该变换环境中攻击者失败扫描次数达到 n 时的扫描次数的随机变量，那么 $Z_k\le N-n$ ，且 N 服从参数为 $(m,m-n,n)$ 的负超几何分布[19] ，即 $\mathrm{E}(N)=\frac{n(m+1)}{m-n+1}$ ，则 $\mathrm{E}\left(Z_k\right)\le\mathrm{E}(N)-n=\frac{n^2}{m-n+1}$ 。综上可以得到

$$\mathrm{E}_{\text{n-n}}\left(Y_k\right)\le\mathrm{E}\left(Z_k\right)\le\min\left(n,\frac{n^2}{m-n+1}\right)\tag{20}$$

从而可以得到非重复变换相比于静态地址环境的最大比例优势的下限

$$\begin{aligned}\max_k\left(\mathrm{RA}_{\text{n-n}}\right)&\ge\max\left(0,\ \frac{m-2n+1}{m-n+1}\right)\\ &\approx\max\left(0,\ \frac{1-2n/m}{1-n/m}\right)(m\gg1)\end{aligned}\tag{21}$$

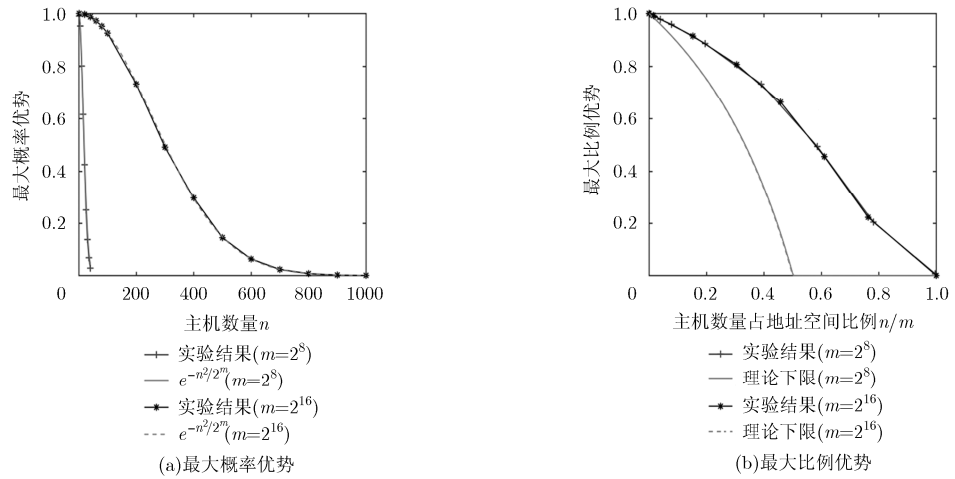
由式(19)，式(21)可以得到

定理 3　对于非重复扫描攻击，非重复变换相比于静态地址环境具有如下的最大概率优势和最大比例优势：

$$\left.\begin{aligned}\max_k\left(\mathrm{PA}_{\text{n-n}}\right)&\approx e^{-n^2/2m}\\ \max_k\left(\mathrm{RA}_{\text{n-n}}\right)&=1-\mathrm{E}_{\text{n-n}}\left(Y_m\right)\Big/n\\ &\ge\max\left(0,\ \frac{m-2n+1}{m-n+1}\right)\\ &\approx\max\left(0,\ \frac{1-2n/m}{1-n/m}\right)(m\gg1)\end{aligned}\right\}\tag{22}$$

从定理 3 可以看到，对于非重复扫描攻击，非重复变换相比于静态地址环境的最大概率优势和最大比例优势均随主机数量增加而减小，随地址空间大小增加而增加；当地址空间足够大时比例优势为主机数量占地址空间比例的递减函数。

图 4 显示了 $m=\left\{2^8,2^{16}\right\}$ 时，非重复变换相比于静态地址环境对非重复扫描攻击的最大概率优势和最大比例优势随着主机数量增加而变化的理论和实验结果，其中图 4(b)的横坐标为主机数量与地址空



(a)最大概率优势 (b)最大比例优势

图 4 非重复变换相比于静态地址环境对非重复扫描攻击的最大概率优势和最大比例优势

间大小的比值。在实验结果中每个数据点为 100 次结果的均值。

从图中可以看出实验结果和理论结果一致。由定理 3 和图 4 可以得到，假设概率优势小于 0.01 时可以忽略不计，则当主机数量大于 $\sqrt{-2m\ln(0.01)} \approx 3\sqrt{m}$ 时非重复变换相比于静态地址环境不再具有概率优势；非重复变换相比于静态地址环境的最大比例优势的理论下限小于实验结果，且理论下限和实验结果均随着主机数量占地址空间比例的增加而减小，与式(21)一致。

4 结束语

本文给出了可重复扫描攻击和非重复扫描攻击在静态地址环境、均匀变换环境以及非重复变换环境下的概率模型。在此基础上，本文从理论上定量分析了两种网络地址变换策略相比于静态地址环境的防御优势。防御优势的理论分析可以更好地指导防御者根据网络中主机数量和地址空间大小以及防御目的的不同选择和应用不同的网络地址变换策略。理论分析表明对于可重复扫描攻击，均匀变换和非重复变换相比于静态地址环境不具有防御优势，因此在部署网络地址变换的网络中，防御者还需要通过一些额外的入侵检测方法如蜜罐增加对可重复扫描攻击行为的探测。对于非重复扫描攻击，均匀变换仅当主机数量较少时才具有概率优势，非重复变换仅当主机数量占地址空间比例较小时才具有较高的比例优势，因此对于旨在减少攻击者命中主机概率以及主机数量较多的网络，防御者应当优先选择非重复变换策略，对于旨在减少攻击者命中主机比例以及主机数量占地址空间比例较大的网络，防御者应当优先选择均匀变换策略。

参 考 文 献

[1] OKHRAVI H, RABE M A, MAYBERRY T J, *et al*. Survey of cyber moving target techniques[R]. Technical Report 1166, Lincoln Laboratory, Massachusetts Institute of Technology, 2013.

[2] ATIGHETCHI M, PAL P, WEBBER F, *et al*. Adaptive use of network–centric mechanisms in cyber-defense[C]. Proceedings of the 6th IEEE International Symposium on Object-Oriented Real-Time Distributed Computing, Hokkaido, Japan, 2003: 183–192. doi: 10.1109/ISORC.2003.1199253.

[3] KEWLEY D, FINK R, LOWRY J, *et al*. Dynamic approaches to thwart adversary intelligence gathering[C]. Proceedings of the DARPA Information Survivability Conference & Exposition II, Los Alamitos, California, 2001: 176–185. doi: 10.1109/DISCEX.2001.932214.

[4] 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. doi: 10.1016/j.comnet.2007.02.006.

[5] JAFARIAN J H, AL-SHAER E, and DUAN Q. Openflow random host mutation: Transparent moving target defense using software defined networking[C]. Proceedings of the First Workshop on Hot Topics in Software Defined Networking, Helsinki, Finland, 2012: 127–132. doi: 10.1145/2342441.2342467.

[6] AL-SHAER E, DUAN Q, and JAFARIAN J H. Random host mutation for moving target defense[C]. Proceedings of the 8th International Conference on Security and Privacy in Communication Networks, Padua, Italy, 2012: 310–327. doi: 10.1007/978-3-642-36883-7_19.

[7] JAFARIAN J H, AL-SHAER E, and DUAN Q. An effective address mutation approach for disrupting reconnaissance

attacks[J]. *IEEE Transactions on Information Forensics and Security*, 2015, 10(12): 2562–2577. doi: 10.1109/TIFS.2015.2467358.

[8] DUNLOP M, GROAT S, URNANSKI W, *et al*. MT6D: A moving target IPv6 defense[C]. Military Communications Conference on Cyber Security and Network Operations, Baltimore, Maryland, 2011: 1321–1326. doi: 10.1109/MILCOM.2011.6127486.

[9] MACFARLAND D C and SHUE C A. The SDN shuffle: Creating a moving-target defense using host-based software-defined networking[C]. ACM CCS Workshop on Moving Target Defense (MTD), Denver, USA, 2015: 37–41. doi: 10.1145/2808475.2808485.

[10] YEGNESWARAN V, ALFELD C, NARFORD B, *et al*. Camouflaging honeynets[C]. Proceedings of IEEE Global Internet Symposium, Anchorage, Alaska, 2007: 49–54. doi: 10.1109/GI.2007.4301430.

[11] URIAS V E, STOUT W, and LOVERRO C. Computer network deception as a moving target defense[C]. IEEE International Carnahan Conference on Security Technology, Taipei, 2015: 1–6. doi: 10.1109/CCST.2015.7389665.

[12] ZHUANG R, DELOADCH S A, and OU X. Towards a theory of moving target defense[C]. Proceedings of First ACM Workshop on Moving Target Defense, Scottsdale, USA, 2014: 31–40. doi: 10.1145/2663474.2663479.

[13] ZHUANG R, BARDAS A G, DELOACH Scott A, *et al*. A theory of cyber attacks: a step towards analyzing MTD systems[C]. ACM CCS Workshop on Moving Target Defense (MTD), Denver, USA, 2015: 11–20. doi: 10.1145/2808475.2808478.

[14] GREEN M, MACFARLAND D C, SMESTAD D R, *et al*. Characterizing network-based moving target defenses[C]. ACM CCS Workshop on Moving Target Defense (MTD), Denver, USA, 2015: 31–35. doi: 10.1145/2808475.2808484.

[15] XU J, GUO P, ZHAO M, *et al*. Comparing different moving target defense techniques[C]. Proceedings of 1st ACM Workshop on Moving Target Defense, Scottsdale, USA, 2014: 97–107. doi: 10.1145/2663474.2663486.

[16] CAI G, WANG B, WANG X, *et al*. An introduction to network address shuffling[C]. 18th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea, 2016: 185–190. doi: 10.1109/ICACT.2016.7423322.

[17] CARROLL T E, CROUSE M, FULP E W, *et al*. Analysis of network address shuffling as a moving target defense[C]. IEEE International Conference on Communications (ICC), Sydney, Australia, 2014: 701–706. doi: 10.1109/ICC.2014.6883401.

[18] CROUSE M, PROSSER B, and FULP E W. Probabilistic performance analysis of moving target and deception reconnaissance defenses[C]. ACM CCS Workshop on Moving Target Defense (MTD), Denver, USA, 2015: 21–29. doi: 10.1145/808475.2808480.

[19] MAHMOUD H M. Pólya Urn Models[M]. London, British, Chapman and Hall, 2008: 124–312.

[20] LANTZ B, HELLER B, and MCKEOWN N. A network in a laptop: Rapid prototyping for software-defined networks[C]. Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks, Monterey, USA, 2010: 1–6. doi: 10.1145/1868447.1868466.

[21] OpenFlow Group at Stanford University. POX Wiki[OL]. https://OpenFlow.stanford.edu/display/ONL/POX+Wiki, 2016.

王　凯：　男，1989 年生，博士，研究方向为信息安全.
陈欣华：　女，1989 年生，讲师，硕士生，研究方向为信息管理.
陈　熹：　男，1988 年生，讲师，硕士，研究方向为信息安全.
武泽慧：　男，1988 年生，讲师，博士，研究方向为网络安全.