具有异构感染率的僵尸网络建模与分析

牛伟纳[1,2] 张小松[1,2] 杨国武[1] 卓中流[1] 卢嘉中[1]
(电子科技大学计算机科学与工程学院 成都 611731)[1]
(电子科技大学网络空间安全研究中心 成都 611731)[2]

摘 要 僵尸网络作为共性攻击平台,采用目前先进的匿名网络和恶意代码技术为APT攻击提供了大量有效资源。为了有效控制僵尸网络的大规模爆发,需研究其构建规律。考虑到在传播过程中僵尸网络的不同区域具有不同的感染率,结合疾病传播模型,提出了一种具有异构感染率的僵尸网络传播模型。首先,通过对僵尸网络稳态特征的分析,使用平均场方法从动力学角度研究了其传播特性;然后,在BA网络中通过模拟实验来分析异构感染率如何影响僵尸网络的传播阈值。实验结果表明,该模型更符合真实情况,且僵尸程序传播阈值和异构感染率的关系与节点数量无关。

关键词 僵尸网络,动力学,异构感染率,疾病传播模型,平均场方法
中图法分类号 TP309.5 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.07.022

Modeling and Analysis of Botnet with Heterogeneous Infection Rate

NIU Wei-na[1,2] ZHANG Xiao-song[1,2] YANG Guo-wu[1] ZHUO Zhong-liu[1] LU Jia-zhong[1]
(School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China)[1]
(Center for Cyber Security, University of Electronic Science and Technology of China, Chengdu 611731, China)[2]

Abstract Botnet, as a common attack platform, uses the current advanced anonymous network and malicious code technology to provide a lot of effective resources for APT attacks. In order to effectively control the large-scale outbreak of botnet, it is necessary to study its construction rules. This work proposed a botnet propagation model with heterogeneous infection rate based on disease model due to nodes with different infection rates in different regions. Through analyzing the characteristics of botnet in the steady-state, the mean-field approach is used to study its propagation characteristics from the dynamic point of view. Then, how the heterogenous infection rate affects the botnet propagation threshold in BA network is explored. The experimental results show that the proposed model is more realistic, and the relationship between threshold and heterogeneous infection rate has nothing to do with the number of nodes.

Keywords Botnet, Dynamics, Heterogeneous infection rates, Disease propagation models, Mean-field approach

诞生于1993年的僵尸网络(Botnet)[1],最早在IRC聊天网络中被发现,该类僵尸程序主要通过Bot工具(命名为Eggdrop)实现清除空闲用户、防止聊天室灌水等功能。融合了传统的恶意软件(如计算机病毒、蠕虫和木马等技术)的僵尸网络已成为因特网上的最大威胁之一,因为它们能够为攻击者提供一种发起大规模攻击的平台,可以实现多种恶意攻击活动,如分布式拒绝服务攻击(DDoS)、垃圾邮件、网络钓鱼、信息窃取、点击欺诈等[2]。僵尸网络具有隐秘性、受控性、群体性、协作性以及攻击性等特点,因此网络监管部门和终端用户都难以检测和规避僵尸网络。

对僵尸网络的构建过程进行建模分析可以有效控制僵尸程序的大面积蔓延。已有的僵尸网络建模方法都是采用疾病传播模型来分析僵尸程序扩张过程,但是模型中所有节点的感染率都是相同的[3],并且使用规则网络或随机网络进行模拟分析。而在真实情况中,网络结构是无标度的,且不同区域设备的感染率也具有差异性。为了解决这一问题,本文提出了一种基于异构感染率的僵尸网络建模方法。首先,详细分析了僵尸网络的工作原理;然后,使用改进的SIR模型来构建僵尸网络的扩张过程,并使用平均场理论对其进行理论分析;接着,通过模拟实验对比分析了在不同参数设置下其对网络形成的影响,揭示异构感染率对僵尸网络传播阈值的作用。

1 相关工作

僵尸网络的研究主要集中在僵尸程序的检测上,Reza

到稿日期:2017-05-22 返修日期:2017-08-06 本文受国家自然科学基金面上项目(61572115),四川省重大基础研究课题(2016JY0007)资助。
牛伟纳(1990-),女,博士生,主要研究方向为网络攻击建模与检测,E-mail:niuweina1@126.com;张小松(1968-),男,博士,教授,主要研究方向为网络安全、数据安全,E-mail:johnsonzxs@uestc.edu.cn(通信作者);杨国武(1966-),男,博士,教授,主要研究方向为模型检测、机器学习;卓中流(1990-),男,博士生,主要研究方向为网络攻击检测;卢嘉中(1988-),男,博士生,主要研究方向为网络攻击检测。

Sharifnya 等[4]提出了针对利用 Domain-flux 技术的僵尸网络的解决方案 DFBotKiller。Gu 等[5]提出的 BotHunter 系统利用 Snort 入侵检测系统实现基于特征码的恶意行为检测。GU 等[6]又提出了 BotMiner 解决方案，根据处于相同僵尸网络中的僵尸主机 C&C 通信行为与恶意攻击行为具有相似性的特点来识别僵尸网络流量。Singh 等[7]提出一种使用随机森林算法来识别 P2P 僵尸网络的框架。Tegeler 等[8]开发出了一个完全基于纯网络层包头信息的僵尸网络检测方法并将该方法实现为 BotFinder 系统。Kong 等[9]提出了一种使用图聚类的数据包处理方法来检测僵尸网络。

在僵尸网络建模方面，较为经典的描述僵尸网络传播的模型有：SEM 模型、SIR 模型、双因素模型、基于时区的模型、AD-SIR 模型、控制模型。随后，相关研究人员又在这些模型的基础上对传染率等参数做出一些改变。国内的研究主要是对不同的网络拓扑结构中的僵尸网络进行深入研究，以及对在线率、感染率等进行改变。国外研究已经将网络结构离散化，并结合先前的模型研究出了新的模型(用矩阵构建模型)。2012 年，钱权等[10]详细分析了两种典型的结构化 P2P 协议(即 Chord 和 Kademlia 的工作原理，结合双因子免疫机制、主机在线率等因素，建模分析结构化 P2P 僵尸网络的传播规律)。根据网络流量阻塞这一 Internet 中的常态现像，欧阳晨星等[11]在 2013 年提出了一种基于无尺度网络结构的僵尸网络传播模型，该模型重点考虑了真实 Internet 中节点的增长性和择优连接性。同年，曹晓丽等[12]提出了基于加权网络的僵尸网络传播模型。2013 年，成淑萍等[13]基于简单病毒传播模型深入分析了僵尸程序的传播特性，考虑了僵尸程序在传播过程中存在的网络流量阻塞、提前免疫主机和感染后免疫主机等因素，提出了一个新的僵尸网络传播模型。2015 年，Sricharan 等[14]提出了基于不同的网络通道存在不同风险性的随机模型，并且在内存随机化的基础上验证了该模型安全防御的效果。2016 年，Ren 等[15]提出了基于 P2P 网络的带时滞的 SEIR 僵尸网络传播模型，考虑了网络中被僵尸网络病毒感染的节点在感染病毒后到启动防御修复措施之间的时间延迟。

2 僵尸网络构建过程模型化

2.1 僵尸网络的构建过程与建模

初始构建过程是攻击者将僵尸程序放入网络中进行传播的过程。在初始构建过程中，所创建的僵尸网络节点不断增加，其网络结构也根据新节点的加入而发生改变。僵尸网络在构建过程中所形成的网络结构与其僵尸程序所用的协议、控制算法等相关。

僵尸网络的初始构建过程是为了发展新的节点加入，本身的僵尸网络形态还没有形成，在该阶段，该僵尸网络的主要行为是加入新的节点和构建网络结构，因此该阶段的僵尸网络行为特征主要包括：端口扫描行为、漏洞扫描利用行为、僵尸网络程序更新行为等。以全分布式僵尸网络构建过程为例，其初始构建过程的网络形态以及行为如图 1 所示。

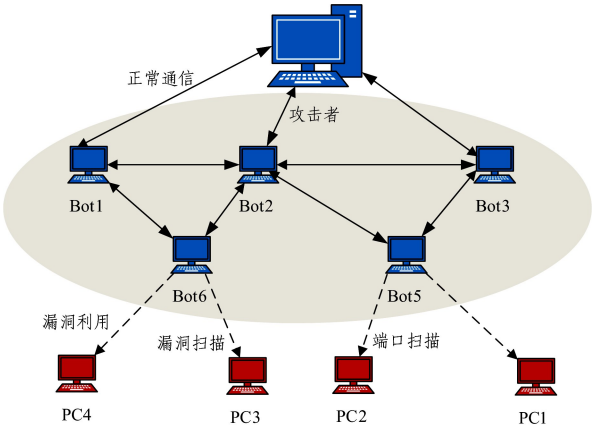

图 1 全分布式的僵尸网络初始构建形态

Fig. 1 Initial building form of fully distributed botnet

全分布式僵尸网络的初始构建过程是通过已加入僵尸网络的节点(如图 1 中的 Bot1，Bot2，Bot3，Bot5，Bot6)向周围节点进行扫描攻击来发展新的节点，如图 1 中的 Bot5；通过端口扫描来寻找与其相连且存在脆弱性的 PC1 和 PC2；也可以是攻击者通过自身的攻击模块向周围节点进行扫描攻击，以引入新的节点，如图 1 中的 Bot6；利用漏洞来攻击 PC3 和 PC4。最后让新发展的节点下载僵尸网络程序并将其加入到僵尸网络中。不同结构类型的僵尸网络在传播过程中体现的性质是相似的，某个区域内加入僵尸网络的主机有以下 3 种途径：

1)僵尸主机从整个 Internet 中随机寻找与其相连且存在脆弱性的设备，并对其进行渗透攻击；

2)攻击者寻找存在脆弱性的设备，并对其进行攻击；

3)处于感染状态的节点从其他区域流动进来。

因为具有不同度的节点的传播情况是不同的，本文将具有相同度的节点集群视为一个区域，且区域间的节点存在相互流动的现象，被感染的主机中的僵尸程序被清除后并不影响再次感染。为了进一步刻画僵尸网络构建过程的动力学，引入 SIR(Susceptible-Infected-Recovered)模型[16]。在任一时刻，网络中任一节点处于这 3 种状态中的一种，具体转化如图 2 所示。其中，S 为易感染状态，表示网络中的节点可以被僵尸程序感染；I 为感染状态，表示网络中的节点已经成功执行僵尸程序并将其加入到僵尸网络中；R 为恢复状态，表示网络中的被感染节点已经采用某种防治措施成功清除掉僵尸程序。

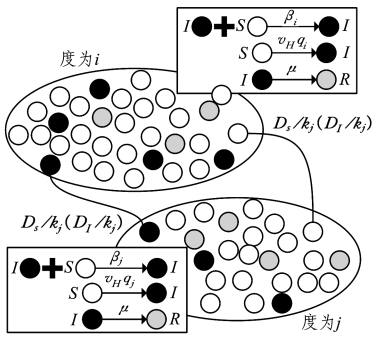

图 2 节点状态变化图

Fig. 2 Changing chart of node status

僵尸网络传播模型为：

$$I+S\xrightarrow{\beta_i}2I,S\xrightarrow{\upsilon_H q_i}I,I\xrightarrow{\mu}R \tag{1}$$

其中，β_i 表示度为 i 的设备被传播感染的被感染率，$\upsilon_H q_i$ 表示度为 i 的设备被攻击感染的被感染率，μ 分别表示节点从感染状态到恢复状态的变化率，D_S/k_i，D_I/k_i 分别表示度为 i 的处于易感染状态的设备和处于感染状态的设备移动到其他区域的概率。

2.2　理论分析

度为 k 的节点在时刻 t 处于状态 I 和状态 S 的节点的平均数量分别为：

$$\rho_{S,k}=\frac{1}{\upsilon_k}\sum_{j|k_j=k}S_j(t),\rho_{I,k}=\frac{1}{\upsilon_k}\sum_{j|k_j=k}I_j(t) \tag{2}$$

假设节点的传播感染率为：$\beta_k=\dfrac{k^\alpha\beta}{\langle k^\alpha\rangle}$，其中 $\langle k^\alpha\rangle=\sum_k k^\alpha P(k)$。节点的攻击感染率不仅与当前处于感染状态的节点数量有关，还与节点的度分布有关，因此假设度为 k 的节点的攻击感染率为 $\upsilon_H q_k=\gamma_k\rho_{I,k}$，其中 $\rho_{I,k}$ 表示度为 k 的区域中处于 I 状态的节点数量，$\gamma_k=\dfrac{k^\alpha\gamma}{\langle k^\alpha\rangle}$。因此，感染率分别为：

$$\beta_k=\frac{k^\alpha\beta}{\langle k^\alpha\rangle},\upsilon_H q_k=\frac{k^\alpha\gamma}{\langle k^\alpha\rangle}\rho_{I,k} \tag{3}$$

使用平均场分析方法来表示状态 I 和状态 S 节点的变化率：

$$\frac{\partial\rho_{I,k(t)}}{\partial t}=[-u\rho_{I,k(t)}+\upsilon_H q_k\rho_{S,k(t)}+\beta_k\Gamma_{k(t)}]-D_I[(1-u)\rho_{I,k(t)}+\upsilon_H q_k\rho_{S,k(t)}+\beta_k\Gamma_{k(t)}]+k\sum_{k'}P\left(\frac{k'}{k}\right)\frac{D_I}{k'}[(1-u)\rho_{I,k'(t)}+\upsilon_H q_{k'}\rho_{S,k'(t)}+\beta_{k'}\Gamma_{k'(t)}] \tag{4}$$

$$\frac{\partial\rho_{S,k(t)}}{\partial t}=[u\rho_{I,k(t)}-\upsilon_H q_k\rho_{S,k(t)}-\beta_k\Gamma_{k(t)}]-D_S[\rho_{S,k(t)}+u\rho_{I,k(t)}-\upsilon_H q_k\rho_{S,k(t)}-\beta_k\Gamma_{k(t)}]+k\sum_{k'}P\left(\frac{k'}{k}\right)\frac{D_I}{k'}[\rho_{S,k'(t)}+u\rho_{I,k'(t)}-\upsilon_H q_{k'}\rho_{S,k'(t)}-\beta_{k'}\Gamma_{k'(t)}] \tag{5}$$

由于

$$\Gamma_{k(t)}=\rho_{S,k(t)}\rho_{I,k(t)} \tag{6}$$

且处于稳态时，不同状态的节点数量不再发生变化，因此令式(4)和式(5)等于 0，得到：

$$\rho_{I,k(t)}=(1-D_I)[(1-u)\rho_{I,k}+\upsilon_H q_k\rho_{s,k(t)}+\beta_k\Gamma_k+\frac{D_I k(1-\mu)}{\langle k\rangle}\rho_I+\theta] \tag{7}$$

$$\rho_{S,k(t)}=(1-D_S)[\rho_{S,k}+\mu\rho_{I,k}-\upsilon_H q_k\rho_{S,k}-\beta_k\Gamma_k+\frac{D_S k}{\langle k\rangle}(\rho_S+\mu_{\rho I}-\theta)] \tag{8}$$

其中，

$$\theta=(1-D_S)[\rho_{S,k}+\mu\rho_{I,k}-\upsilon_H q_k\rho_{S,k}-\beta_k\Gamma_k+\frac{D_S k}{\langle k\rangle}(\rho_S+\mu\rho_I-\theta)] \tag{9}$$

$$\rho=\frac{N}{V}=\rho_I+\rho_S \tag{10}$$

使式(7)除以 $P(k)$，得到：

$$\rho_I=\frac{\Theta}{\mu} \tag{11}$$

将式(11)代入式(7)和式(8)得：

$$\rho_{I,k(t)}=(1-D_I)[(1-u)\rho_{I,k}+\upsilon_H q_k\rho_{S,k}+\beta_k\Gamma_k]+\frac{D_I k}{\langle k\rangle}\rho_I \tag{12}$$

$$\rho_{S,k(t)}=(1-D_S)[\rho_{S,k}+\mu\rho_{I,k}+\upsilon_H q_k\rho_{S,k}]+\frac{D_S k}{\langle k\rangle}\rho_S \tag{13}$$

这里，假设处于状态 I 和状态 S 的节点都会发生节点移动 $D_S=D_I=1$，则：

$$\rho_{I,k}=\frac{k}{\langle k\rangle}\rho_I,\rho_{S,k}=\frac{k}{\langle k\rangle}\rho_S \tag{14}$$

从式(9)和式(11)可得：

$$\rho_I=\frac{1}{\mu}\sum_k P(k)(\gamma_k+\beta_k)\rho_{I,k}\cdot\rho_{S,k} \tag{15}$$

将式(2)和式(14)代入式(15)，可得：

$$\rho_S=\frac{\mu\langle k\rangle^2\langle k^\alpha\rangle}{(\beta+\gamma)\langle k^{(2+\alpha)}\rangle} \tag{16}$$

则：

$$\rho_I=\rho-\rho_I=\rho-\frac{\mu\langle k\rangle^2\langle k^\alpha\rangle}{(\beta+\gamma)\langle k^{(2+\alpha)}\rangle} \tag{17}$$

则僵尸程序传播的阈值为：

$$\rho_C=\frac{\mu\langle k\rangle^2\langle k^\alpha\rangle}{(\beta+\gamma)\langle k^{(2+\alpha)}\rangle} \tag{18}$$

由于稳定状态时，僵尸网络中不同状态的节点数量不再发生变化，因此僵尸程序的传播阈值不再受处于感染状态的节点数量的影响。

由式(18)可知，僵尸程序的传播阈值在 $\alpha=0$ 时为 $\rho_C=\dfrac{\mu\langle k\rangle^2}{(\beta+\gamma)\langle k^2\rangle}$；当 $\alpha>0$ 时，ρ_C 与 α 值负相关；当 $\alpha<0$ 时，ρ_C 与 $|\alpha|$ 值正相关。

3　实验分析

采用 Matlab 对僵尸程序的传播进行模拟仿真，为了更真实地表示实际情况，采用 BA 网络来模拟网络环境。

1)假设区域数量为 2，每个区域内的节点数量是：$N(S)=490$，$N(I)=10$，$N(R)=0$，区域 1 内节点的平均度 $\langle k\rangle=1.996$，且度为 k 的处于易感染状态或者感染状态节点的流入/流出概率为 $1/k$。僵尸网络传播模型在区域 1 内的仿真实验结果如图 3 所示。

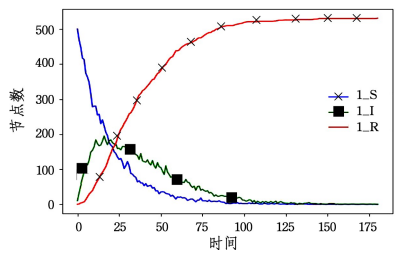

图 3　新的僵尸网络传播模型

Fig. 3　New Botnet propagation model

图 3 表明，与已有的僵尸网络建模方法相比，新模型考虑了不同区域的节点移动，传播模型中易感染节点的数量和感染节点的数量的变化应更具有波动性。此外，后者还在易感染节点的状态变化时引入节点度这一因素，相比于已有的建模方法，僵尸网络达到稳态需要更长的时间周期，因此新的僵尸网络模型中不同状态节点的数量变化情况更符合真实的复杂网络。

2)设置参数值：节点数量 $N=1000$，节点的平均度$\langle k\rangle=3.033$，感染节点变成恢复状态的概率 $\mu=0.05$，$\beta=\gamma=0.05$。得到的僵尸程序传播阈值与异构感染率 α 的关系如图 4 所示。

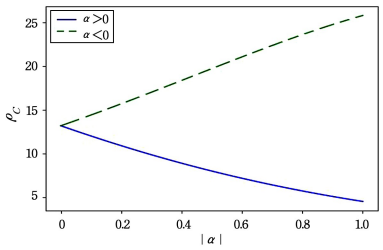

图 4 $N=1000$ 时传播阈值与 α 的关系图

Fig. 4 Relationship between propagate threshold and α when $N=1000$

图 4 表明，当 $\alpha>0$ 时，具有较大 α 值的区域僵尸程序的传播速度较慢，而真实环境中经济比较发达的区域，其安全性的重要程度比较高，则该区域内的设备具有更小的节点流动率，僵尸程序在这一区域的传播速度就较慢。因此可以通过增加设备的安全性，如增强密码复杂度和安装杀毒软件，来抑制僵尸程序的传播。当 $\alpha<0$ 时，$|\alpha|$ 值越大的区域僵尸程序的传播速度越快，即流动性大的区域僵尸程序的传播速度较快，这与真实环境中经济比较发达的区域设备的普及程度更高及流动量更大有关。因此，可以通过增加设备的安全性，如增强设备安全性及减少网络设备的流动性，来抑制僵尸程序的传播。

3)设置参数值：感染节点变成恢复状态 $\mu=0.05$，$\beta=\gamma=0.05$。不同节点数量和平均度下，传播阈值与异构感染率的关系如表 1 所列。

表 1 实验结果

Table 1 Experimental results

节点数量	平均度	节点度分布	阈值与$\lvert\alpha\rvert$的关系	
			$\alpha>0$	$\alpha<0$
2000	3.0530	$P(k)=0.45*(k^{-1.42})$	负相关	正相关
3000	2.9400	$P(k)=0.46*(k^{-1.48})$	负相关	正相关
4000	2.9775	$P(k)=0.46*(k^{-1.45})$	负相关	正相关
5000	2.9432	$P(k)=0.47*(k^{-1.49})$	负相关	正相关
6000	2.9818	$P(k)=0.46*(k^{-1.48})$	负相关	正相关
7000	2.8994	$P(k)=0.47*(k^{-1.51})$	负相关	正相关
8000	2.9432	$P(k)=0.47*(k^{-1.49})$	负相关	正相关

表 1 是仿真实验结果，从中可以看出，僵尸程序传播阈值和 α 之间的关系与节点数量以及节点的度分布无关。网络中节点数量的增加和减少对传播阈值和异构感染率之间的关系并不造成影响。

结束语 攻击型网络是继恶意代码之后的新型网络战武器，其危害不仅仅是被控制终端资源被恶意控制与使用，还可拓展至国家网络基础设施安全、互联网安全与稳定等方面，其原由是僵尸网络综合了恶意代码攻击、大规模网络控制、网络隐藏与并发攻击等多种先进的网络安全技术，涉及的计算机领域包括操作系统、固件安全、网络协议、Web 应用、社交网络等，属于典型的共性攻击技术。

本文针对僵尸网络的共性攻击特征进行分析，形式化描述僵尸网络的扩张过程并对其进行分析，为识别未知僵尸网络以及僵尸网络变种提供基础支撑。通过异构感染成功率来表征不同区域内设备和其他设备的攻击成功率，进而描述具有不同感染成功率的目标节点；使用 SIR 模型来进行形式化表示，最后通过模拟实验对比分析，发现僵尸程序传播阈值与参数 α 具有相关性；且本文建立的模型也比较符合真实情况，同时增加设备安全性和减少联网设备数量可以进一步遏制僵尸网络的传播。

参 考 文 献

[1] EASON G, NOBLE B, SNEDDON I N. On certain integrals of Eggdrop: Open source IRC bot [EB/OL]. http://www.eggheads.org.

[2] KIRUBAVATHI G, ANITHA R. Botnets: A study and analysis [M]//Computational Intelligence, Cyber Security and Computational Models. Springer India, 2014: 203-214.

[3] WANG Y, WEN S, XIANG Y, et al. Modeling the propagation of worms in networks: A survey [J]. IEEE Communications Surveys & Tutorials, 2014, 16(2): 942-960.

[4] SHARIFNYA R, ABADI M. DFBotkiller: domain-flux botnet detection based on the history of activities and failures in DNS traffic[J]. Digital Inestigation, 2015, 12: 15-26.

[5] GU G, PORRAS P A, YEGNESWARAN V, et al. Bothunter: Detecting malware infection through ids-driven dialog correcation[C]// USENIX Security Symposium. 2007: 1-16.

[6] GU G, PERDISCI R, ZHANG J, et al. BotMiner: Clustering Analysis of Network Traffic for Protocol-and Structure-Independent Botnet Detection[J]. USENIX Security Symposium, 2008, 5(2): 139-154.

[7] SINGH K, GUNTUKU S C, THAKUR A, et al. Big data analytics framework for peer-to-peer botnet detection using random forests [J]. Information Sciences, 2014, 278(19): 488-497.

[8] TEGELER F, FU X, VIGNA G, et al. Botfinder: Finding bots in network traffic without deep packet inspection[C]// 8th Iinternational Conference on Emerging Networking Experiments and Technologies. ACM, 2012: 349-360.

[9] KONG X, CHEN Y, TIAN H, et al. A Novel Botnet Detection Method Based on Preprocessing Data Packet by Graph Structure Clustering[C]// 2016 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). IEEE, 2016: 42-45.

(下转第 153 页)

性，使加密存储后的信息特性发生了变化。使用本文方法对用户的信息进行加密存储测试。由图 3 和图 4 可以清晰地看出，未进行加密存储的信息具有明显的排列规律，而利用本文方法对加密信息进行存储，信息序列被打乱，表示为混沌的随机状态，ASCII 值的分布较为均匀，掩盖了原始的信息，有效地抵制了攻击，提高了信息多重加密存储的安全性。

结束语　为解决大数据分析中用户信息的加密存储技术存在的安全性较差的问题，提出了基于超带宽的用户信息加密存储方法。实验表明，利用该方法能有效地降低信息加密存储的复杂性，提高信息的安全性。下一步，将提高各信息节点在存储时的性能，降低信息加密存储使用的强度，增强本文方法的使用价值。

参 考 文 献

[1] SONG K，WU H J. Cloud storage based on privacy protection and efficient micro-encryption scheme[J]. Application of Electronic Technique，2016，42(7)：111-113. (in Chinese)
宋可，吴宏建. 云存储中基于隐私保护的高效的微型加密方案[J]. 电子技术应用，2016，42(7)：111-113.

[2] LEI L，CAI Q W，JING J W，et al. Enforcing Access Controls on Encrypted Cloud Storage with Policy Hiding[J]. Journal of Software，2016，27(6)：1432-1450. (in Chinese)
雷蕾，蔡权伟，荆继武，等. 支持策略隐藏的加密云存储访问控制机制[J]. 软件学报，2016，27(6)：1432-1450.

[3] LI J，LI J F，FANG F. Research of File Encryption Storage and Deletion Mechanism in Cloud Storage[J]. Journal of Chinese Computer Systems，2015，36(4)：836-839. (in Chinese)
李杰，李景峰，房方. 云存储中文件加密存储和删除方法研究[J]. 小型微型计算机系统，2015，36(4)：836-839.

[4] PAN Q H. A Double Thread Complementary Information Encryption Algorithm Based on Random Amplitude Modulation [J]. Bulletin of Science and Technology，2015，31(12)：144-146. (in Chinese)
潘期辉. 采用随机码幅度调制的双线程互补信息加密算法[J]. 科技通报，2015，31(12)：144-146.

[5] WANG S，LU Y，CHEN L Y. Research of mixed encryption algorithm in cloud storage[J]. Electronic Design Engineering，2016，24(23)：54-57. (in Chinese)
王双，卢昱，陈立云. 云存储中的混合加密算法研究[J]. 电子设计工程，2016，24(23)：54-57.

[6] CHENG X X，HAN X Z，CHEN X J，et al. An Optimization Encryption Algorithm for Cloud Storage and Its Simulation[J]. Computer Simulation，2016，33(4)：356-359. (in Chinese)
程肖肖，韩宪忠，陈雪蛟，等. 一种用于云存储的优化加密算法的研究与仿真[J]. 计算机仿真，2016，33(4)：356-359.

[7] LU Y，WANG S，CHEN L Y. Research of Mixed Encryption Algorithm Based on Cloud Storage[J]. Computer Measurement & Control，2016，24(3)：129-132. (in Chinese)
卢昱，王双，陈立云. 基于云存储的混合加密算法研究[J]. 计算机测量与控制，2016，24(3)：129-132.

[8] HANG T X，DING J Y. A Cloud-storage Privilege Revoking Optimizing Mechanism Based on Dynamic Re-encryption[J]. Science Technology and Engineering，2015，15(20)：108-115. (in Chinese)
韩同欣，丁建元. 基于动态重加密的云计算存储平台权限撤销优化机制[J]. 科学技术与工程，2015，15(20)：108-115.

[9] DU Z H，ZHU W Y. Implementation of secure data retrieval schema in cloud storage by using ABE technology[J]. Application Research of Computers，2016，33(3)：860-865. (in Chinese)
杜朝晖，朱文耀. 云存储中利用属性基加密技术的安全数据检索方案[J]. 计算机应用研究，2016，33(3)：860-865.

[10] QIU S W，LI Y Y. Reliable data delivery with low delay in energy harvesting wireless sensor network[J]. Journal of Computer Applications，2015，35(2)：345-350. (in Chinese)
邱树伟，李琰琰. 能量捕获无线传感器网络中低时延的可靠数据传递[J]. 计算机应用，2015，35(2)：345-350.

[11] HU X D，CAI D Q. Design and research of secure encryption clustering algorithm for wireless sensor networks[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition)，2009，21(3)：421-424. (in Chinese)
胡向东，蔡东强. 无线传感器网络安全加密成簇算法的设计及研究[J]. 重庆邮电大学学报(自然科学版)，2009，21(3)：421-424.

(上接第 138 页)

[10] QIAN Q，XIAO C J，ZHANG R. Propagation modeling for P2P botnet in structured P2P network [J]. Journal of Software，2012，23(12)：3161-3174. (in Chinese)
钱权，萧超杰，张瑞. 结构化对等网络中 P2P 僵尸网络传播模型[J]. 软件学报，2012，23(12)：3161-3174.

[11] OUYANG C X，TAN L. New propagation model of Botnet on scale-free network [J]. Computer Engineering and Applications，2013，49(9)：110-114. (in Chinese)
欧阳晨星，谭良. 无尺度网络下的僵尸网络传播模型研究[J]. 计算机工程与应用，2013，49(9)：110-114.

[12] CAO X L，NIU Z L. Study on propagation model of botnet based on weighted networks [J]. Computer Applications and Software，2012，30(7)：180-184. (in Chinese)
曹晓丽，牛志玲. 基于加权网络的僵尸网络传播模型研究[J]. 计算机应用与软件，2013，30(7)：180-184.

[13] CHENG S P，TAN L，HUANG B，et al. Botnet propagation modeling and analysis [J]. Computer Engineering and Applications，2013，49(1)：107-111. (in Chinese)
成淑萍，谭良，黄彪，等. 僵尸网络传播模型分析[J]. 计算机工程与应用，2013，49(1)：107-111.

[14] SRICHARAN K G，KISORE N R. Mathematical model to study propagation of computer worm in a network[C]// 2015 IEEE International Advance Computing Conference (IACC). IEEE，2015：772-777.

[15] REN W，SONG L P，FENG L P. A novel mathematical model on Peer-to-Peer botnet [J]. Journal of Measurement Science and Instrumentation，2014，5(4)：62-67.

[16] BUONO C，VAZQUEZ F，MACRI P A，et al. Slow epidemic extinction in populations with heterogeneous infection rates [J]. Physical Review E，2013，88(2)：022813.