doi:10.3969/j.issn.1000-436x.2014.11.004

流量自适应的移动僵尸网络云控机制研究

陈伟，周诗文，殷承宇
（南京邮电大学 计算机学院，江苏 南京 210023）

摘 要：僵尸网络从传统恶意代码进化而来，随着智能手机的计算能力与移动互联网接入技术的快速发展，构建移动僵尸网络已成为一种潜在的威胁。针对移动互联网，提出一种具有流量自适应性的移动僵尸网络云控机制，通过分析用户的流量使用情况，在 3G 和 Wi-Fi 不同网络环境下采取不同的流量使用策略，使用自适应的调度算法执行僵尸指令。仿真实验证明，在确保僵尸网络命令有效执行的情况下，流量自适应调度算法可有效增强移动僵尸网络的隐蔽性和实时性。

关键词：移动僵尸网络；命令与控制；智能手机；调度算法；云控机制
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)11-0032-07

Research on cloud-based traffic adaptive command and control method for mobile botnet

CHEN Wei, ZHOU Shi-wen, YIN Cheng-yu
(School of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210023, China)

Abstract: Botnet is a serious attack evolved from traditional malwares. With the rapid development of computing capability and mobile Internet access technology, building a realistic mobile botnet has become a potential threat. An adaptive traffic control mechanism for cloud-based mobile botnet was proposed. It adopts different traffic consumption strategies according to different 3G or Wi-Fi network environments. Then scheduling algorithms to execute botnet commands was applied. The experimental results show the traffic adaptive algorithm can improve the stealthy and efficiency of mobile botnet while ensure that the botnet commands can be executed effectively.

Key words: mobile botnet; command and control; smart phone; scheduling algorithm; cloud-based control

1 引言

近年来，随着智能手机、平板电脑、移动互联网的大规模普及，移动互联网条件下的僵尸网络开始出现，并逐渐成为国内外研究的热点。移动僵尸网络是指攻击者将僵尸病毒植入到手机终端中，使其成为僵尸手机(Bot)。攻击者再远程控制被感染的僵尸手机群，进一步获取手机上敏感信息或发动攻击。智能手机中往往储存着大量的私人信息并且在网上支付时经常使用，其存储的敏感信息比个人计算机(PC, personal computer)多得多，而智能手机的安全性却远达不到 PC 安全防护的级别，如今智能手机已成为黑客眼中最具吸引力的目标之一，特别是开源的 Android 系统，由于多个手机厂商制定不同的版本带来了版本碎片化的问题，加上第三方市场对应用程序的安全监管水平参差不齐，为恶意软件的创造者提供了越来越多的机会。

2009 年，出现首个针对塞班系统，并且利用基于 HTTP 协议的命令与控制(C&C, command and control)机制的移动恶意代码 SymbOS Yxes，这昭示着手机恶意软件正在向移动僵尸网络发展[1]。Schmidt 等[2]提出了利用 Android 平台手机构建僵尸

收稿日期：2014-07-16；**修回日期**：2014-10-23
基金项目：国家自然科学基金资助项目(61202353, 61272084)；江苏省高校自然科学研究基金资助项目（12KJB520008）；江苏省普通高校研究生科研创新计划基金资助项目(CXLX13_464)
Foundation Items: The National Natural Science Program of China (61202353, 61272084); The Natural Science Foundation of Jiangsu Higher Education Institutions (12KJB520008); Graduate Innovation Foundation of Jiangsu Province (CXLX13_464)

网络的可行性，针对越狱 iPhone 手机的移动僵尸网络 Ikee B 也公众于世[3]。2012 年 12 月，首个安卓僵尸网络 Geinimi 在国内盛行起来。移动僵尸网络与传统僵尸网络基本类似，但也存在着一些区别，主要在于智能手机、平板电脑等移动设备的电量、通信能力都有限，如果僵尸程序消耗的电量或网络流量过大，就会很快引起用户的警觉。

针对移动僵尸网络的特点，设计一种新型移动僵尸网络命令与控制机制方案，能有效地将移动僵尸网络消耗的流量隐藏在用户正常流量中，具有较高的隐蔽性，同时通过对移动僵尸网络命令划分优先级，采用调度算法执行，可有效降低移动僵尸网络命令执行的延时，提高僵尸网络性能。实验证明，提出的流量自适应移动僵尸网络云控机制具有一定的可行性、隐蔽性和实时性。

2　相关工作

基于 PC 的僵尸网络已经成为互联网最为严重的威胁之一，而针对智能手机的移动僵尸网络实施起来并不是那么容易。近年来，针对一些典型的移动僵尸病毒，已经有相关文献介绍了移动僵尸网络命令与控制机制的研究情况。

Cui 等[4]提出一种基于 URL Flux 的移动僵尸网络模型，攻击者将僵尸命令加密绑定至图片上，并将其上传至博客，僵尸手机通过访问博客下载图片，然后解析命令并执行，消除了基于 HTTP 命令与控制信道的单点失效的弊端；Zeng 等[5]提出使用 SMS 短消息作为 C&C 信道，并构建 P2P 结构的僵尸网络，整个僵尸网络内所有命令都通过 SMS 进行通信，有效地降低了命令的延迟度；Wang 等[6]提出了先进的混合式对等僵尸网络；Miller 等[7]提出了在 Android 和 iPhone 以及 Windows Mobile 平台下，如何以注入模糊短信的方式发现手机漏洞并进行攻击和防御，对手机安全的发展有重大意义和影响；Mulliner 等[8]提出了一种基于 SMS-HTTP 混合模式的 C&C 命令与控制信道的移动僵尸网络，其主要思想是把通信分成 HTTP 和 SMS 两部分，将加密签名的文件上传到一个网站，然后通过 SMS 发送僵尸命令相对应的 URL 信息。Singh 等[9]评估了利用电子邮件通信的僵尸网络 C&C 信道的可行性。

如何针对移动僵尸网络的特点，让僵尸命令高效隐蔽地执行所研究的工作并不多。Zhao 等[10]曾提出一种通过 C2DM 服务器传送僵尸命令的方式及详细过程，其利用 Google 的 C2DM 机制构建移动僵尸网络，一旦手机客户端在服务器端有了自身的注册 ID，服务器端便可向客户端实时推送消息指令，包括加密的僵尸程序。如今 C2DM 机制已被更新的 GCM 所取代，Chen 等[11]提出了在 GCM 服务器下，利用图片隐藏等技术实现云控移动僵尸网络，避免了僵尸节点与控制服务器之间直接的网络通信，增强了隐蔽性。由此可见，如何隐蔽实时执行僵尸命令变得越发重要。因此，从移动互联网流量消耗的角度，提出了在智能手机上隐蔽执行僵尸命令的调度算法，以用户每段时间内的流量使用情况为衡量准则，自动适应用户网络流量使用模式，在 3G/Wi-Fi 环境下最大限度地隐蔽执行僵尸指令，同时提高了实时性和隐蔽性。

3　移动僵尸网络命令与控制机制

为了能使僵尸命令可靠执行，使用云控推送服务器来推送僵尸命令，可以避免僵尸主控端与僵尸节点间的直接通信。图 1 描述了移动僵尸网络云控机制的主要流程，僵尸主控端（Botmaster）与云控推送服务器建立连接，僵尸指令则由云控推送服务器发送至僵尸手机（Bot），云控推送服务器可以由提供消息推送的服务器构成，如 Google GCM、airbop、个推、极光等。检测系统无法根据 Bot 收到的僵尸命令判断僵尸主控端的具体位置，加大了检测难度，增强了僵尸网络的隐蔽性。

图 1　移动僵尸网络命令推送

3.1　移动僵尸命令分析

移动僵尸命令可以窃取用户短信，通信录中联系人信息以及手机支付中的网银账号甚至是登录密码，对用户的信息泄露造成很大的威胁和危害。表 1 是目前收集的可能藏匿在手机内部的移动僵尸命令[4]，并对其按照命令的紧急程度及流量消耗情况进行分类，优先级数越小，优先级越高，其中 *Ci* 为每个命令的流量消耗情况预测。

在执行消耗流量的僵尸命令时，需要考虑用户正常的流量消耗情况。当手机处于 Wi-Fi 网络时，

默认此时的网络流量可以无限使用。目前，国内 Wi-Fi 通常是计时收费，用户对 Wi-Fi 流量是不敏感的，很多用户在办公室、住宅等区域使用 Wi-Fi 是免费的，因此在 Wi-Fi 环境下，执行僵尸网络命令，被发现的风险较低，具有较好的隐蔽性。然而当手机使用 3G 上网时，用户对于 3G 流量比较敏感，僵尸命令需谨慎执行，只有确保其流量与用户正常情况下的使用模式相似，才能做到更好的隐蔽性，否则流量消耗过大会引起用户的警觉。

重点设计流量自适应的僵尸命令调度执行算法。首先，对用户流量使用情况进行统计，依据用户消耗的流量确定僵尸命令可用流量的额度，为了保证僵尸命令执行的实时性，根据僵尸网络命令的优先级进行调度执行。在流量自适应的调度算法研究中，有以下几点假设，作为构建隐蔽高效僵尸网络的前提：

1) 假设智能手机有后台应用程序运行，僵尸命令在后台执行时消耗的电量可以忽略不计，通常智能手机都有多个后台进程在运行；

2) 假设僵尸命令是无关付费下载等消耗用户话费的命令，避免了话费开销造成的明显经济损失，本文侧重研究流量消耗类的移动僵尸命令；

3) 假设在 Wi-Fi 网络下，僵尸命令可使用的流量为无穷大，目前国内大部分 Wi-Fi 服务是计时付费，不是计流量付费；

4) 假设在 3G 网络下，网络环境相对稳定，僵尸指令可正常执行；

5) 当用户正常消耗的 3G 流量很大时，默认用户订购的 3G 流量充足，用户对流量消耗的敏感度较低。

3.2 流量自适应的命令控制机制

对于移动僵尸网络，Wi-Fi 网络相比其他通信介质拥有一定的优势。因为 Wi-Fi 背后隐藏着许多不同的开放式网络和 NAT 路由器，利用 Wi-Fi 的僵尸网络可以更容易欺骗检测系统。在 3G 网络下，移动设备必须使用具有非欺骗性的移动 ID 来连接蜂窝网络，并且手机运营商会记录下手机用户的网络流量使用情况，使僵尸命令更容易被发现和追踪，用户发现僵尸程序的可能性也更大。

流量自适应的命令控制机制是指在移动僵尸网络的命令执行过程中，针对每台僵尸手机（Bot），根据僵尸命令的紧急情况以及命令的流量消耗，使其自适应地利用 Bot 端的 3G 和 Wi-Fi 网络，尽可能地将非紧急的以及流量消耗大的攻击命令安排在 Wi-Fi 或用户预留流量充足的情况下执行。根据表 1 列出的僵尸命令优先级和可能消耗的流量 Ci(单位 KB)，移动僵尸命令的执行过程可分为以下几步。

1) 定义变量 Tr 为用户正常上网情况下的一定时间间隔内的流量使用值，单位为 KB。若手机处

表 1 **移动僵尸命令分类**

优先级（从高到低）	命令	流量消耗 Ci/KB	描述
0	Get APP	0	获得手机上已安装的所有 App 名称
	Get Info	0	获得手机短信，联系人，IMEI 号码等信息
1	SMSDoS	0	读取 SMS 信息，对手机联系人进行短信轰炸
	SMS-Spread	0	向联系人发送含有有效 URL 的短信
	GenSMS	0	产生虚假信息，对网络钓鱼很有用
	DenySMS	0	过滤掉运营商发来的提醒警告短信
	Remove	0	远程卸载应用程序
	IP	<1K	获取手机 IP，便于连接发送指令
	Sock	<1K	打开手机 Sock 代理，可发送/接收透传等相关消息
	Call Home	<1K	与一些通信信道保持连接，如 HTTP, E-mail, SMS 等
2	Update	1K~1M	自动更新 Bot 程序
	Position	<1K	秘密报告手机的 GPS 位置，并上传至远程服务器
3	Download	1K~1M	通过推送收到的消息自动后台下载图片或文件（如 GCM、个推等推送服务）
4	DoS	1~100K	通过 QQ、微信、邮箱等方式向联系人发送大量的拒绝服务数据
5	Attacking	1K~10M	SYN Flooding 等淹没攻击

于 Wi-Fi 网络状态下，则设置 *Tr* 为无穷大，此时僵尸命令可以依次执行；若在 3G 网络情况下，则采集用户 *Tr* 的值；若网络不可用，则 *Tr* 为零。

2) 将僵尸命令按照优先级大小排队，优先级高的排在前面先执行，优先级低的排在后面后执行，将排序好的僵尸命令插入就绪队列，指针指向就绪队列第一个进程。当有 *Tr* 到来时，按照先来先服务的调度规则依次执行就绪队列的僵尸命令。

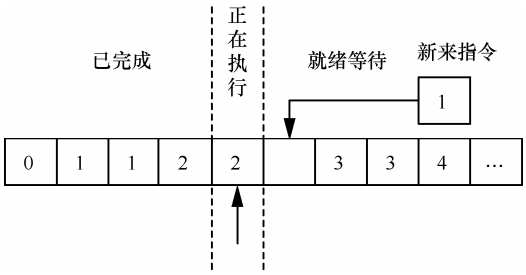
3) 当前时刻采集到的 *Tr* 非负时，赋予其一个网络流量可用系数 α，$\alpha \in [0,1]$，作为僵尸指令的可用流量系数。将 $Tr \times \alpha$ 的流量分配给当前指针指向的命令执行，若当前指令执行完毕所需的流量值大于 $Tr \times \alpha$ 的值，即表示这个时间段内可用的 *Tr* 并不足以使当前僵尸命令完全执行，那么命令调度指针不变，等待下一个时间段到来的 *Tr* 流量值。若当前指令执行完毕后 $Tr \times \alpha$ 还有剩余，则指针依次后移，将执行完的命令状态改为完成态，指针指向就绪队列的下一个命令。

4) 从表 1 中可看出，攻击性越强的僵尸命令对流量的要求越高，其优先级越低。因此，为了保证隐蔽性，可将优先级大于 Spit_Threshold 的命令分片执行。即当指针指到流量要求较高的指令时，将其分片执行，若命令没有一次执行完成，则将其按照优先级大小重新插回队列，等待下一轮 *Tr* 的到来。此算法的伪代码如图 2 所示。

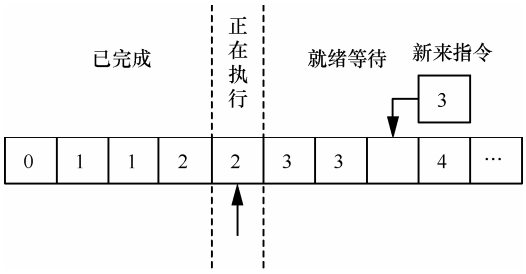
```
1) input Command_list, Tr; // 输入指令列表，当前用户使用流量
2) 将命令按优先级数从小到大排列，先来先服务（FIFS），放入就绪队列等待;
指针指向就绪队列第一个命令;
3) while(Tr>0)   do
{      将 T == Tr×α 的流量分配给指针指向的命令执行;
while(就绪队列!=NULL)   do
                          {if(T –Ci>=0)
                          {将此命令状态改为“Finished”;
                          T == T –Ci;
                          当前命令移出队列;
指针指向下一个命令；}   //执行完的指令出队}
                          else if(优先级数>=Spit_Threshold)
{      出队，分配 T 流量执行，Ci == Ci– T;
按优先级数大小将其重新插入至就绪队列;
                    指针指向下一个命令；}
//spit_Threshold 为分片的阈值，一般设为 4 或 5 级
                                    else
{      指针不变，等待下一个 Tr;
Ci == Ci– T;}
}
}
4) end
```

图 2　流量自适应算法

5) 当在一次执行过程中有新的命令到来时，按照其优先级的高低将其排列到就绪队列。若新来命令的优先级高于当前执行命令的优先级，则将其直接插入当前指针的后面；若新来的命令的优先级低于当前执行命令的优先级时，将其按照顺序插入到就绪队列内。具体过程如图 3 所示。



(a) 优先级高于当前命令



(b) 优先级低于当前命令

图 3　新来僵尸网络命令的入列处理

4　实验分析

对自适应的移动僵尸网络云控推送机制进行实验验证，并从僵尸命令执行的隐蔽性和云控推送机制的实时性这 2 个方面进行性能分析。

4.1　实验环境

首先，运用流量监测软件在 Android 手机上多次收集用户在 24 h 内的流量使用情况，分别按照待机、视频、聊天等网络行为自适应采集用户流量消耗情况。当流量消耗较小时，僵尸命令可用流量也较少，则减小采集频率，等待下一时刻的用户流量；当流量消耗大时，下一时刻的流量不稳定性也越大，则提高采集频率，确保僵尸指令能隐蔽执行。表 2 是实验中根据用户不同网络行为下采集频率的设定。

表 2　　手机不同网络行为下的采集频率

网络行为	采集间隔/min	流量范围/KB
待机	15	≤100
聊天、看网页等	10	100~500
看视频、下载等	5	≥500

为了能更便捷、准确地验证设计算法的可行性，对于表1中所列出的僵尸命令，采取随机生成的方式，将其挂载在手机上，每生成一个僵尸命令，就对其进行相应的处理。具体的命令生成概率如表3所示。

表3 部分僵尸命令生成分布

优先级	僵尸命令	执行频率
0	Get APP、Get Info	泊松分布（λ=15）
1	IP、Sock、Call Home	15 min
2	Update	60 min
	Position	泊松分布（λ=15）
3	Download	泊松分布（λ=15）
4	DoS	60 min
5	Attacking	1次

僵尸命令按照表3中的概率分布随机生成，每来一个命令，按照优先级的大小将其排队入列，等待执行。在Wi-Fi网络情况下，默认僵尸命令可使用的流量为无穷大，此时无需考虑消耗流量问题，就绪队列的僵尸命令可以立即执行；当处于3G网络时，统计各个采集时间段内用户的流量使用情况，并设α=0.8为可用流量系数，按照优先级的高低，采取调度算法，依次执行就绪队列的僵尸命令。

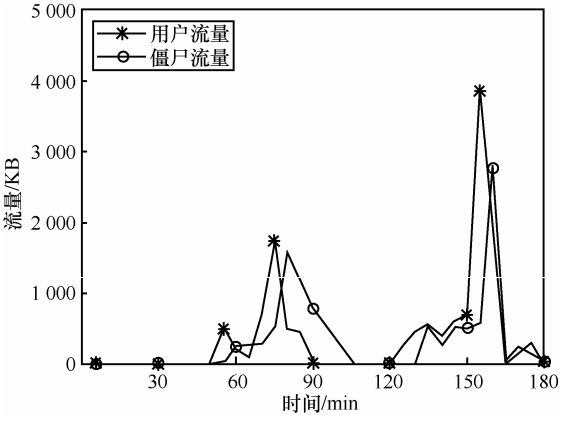
实验对命令的以下几个因素进行统计分析：命令生成时间、延迟时间、命令大小、命令使用流量以及剩余流量。延迟指Bot收到命令至执行完毕的时间间隔；剩余流量指参照用户上一个时间段的流量使用情况，计算出僵尸命令的可用流量与使用流量之差。

为了确保实验的准确性，进行了为期一个月的实验调查，采集了用户在各时间段下的流量使用情况，分别对其进行实验和分析，同时为了增强可靠性，挑选出用户网络使用状况最为活跃的3个小时进行统计分析，得到以下较为精确的性能分析数据。

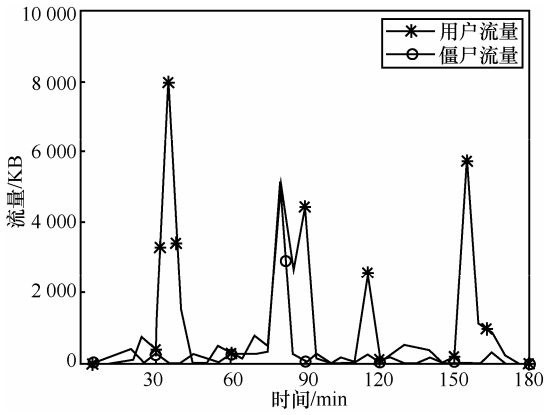
4.2 隐蔽性分析

图4为用户在3G/Wi-Fi网络下正常网络行为的流量分布与僵尸命令使用流量的对比图。由图4(a)可以看出，尽管流量有一定偏移，但在某一时刻流量的消耗差异不大，避免出现异常流量发生，因此在3G网络下实现了较好的隐蔽性。

图4(b)是在Wi-Fi情况下的流量对比图，在Wi-Fi网络下，用户对流量消耗的敏感度较低，调度算法默认流量可以无限使用，此时的僵尸命令可以顺序依次执行，无需考虑用户的流量限制。在已有的僵尸网络检测研究方案中，一般利用手机异常流量进行检测[12]，因此，流量自适应机制可以较好地避开此类检测方法。



(a) 3G网络



(b) Wi-Fi网络

图4 3G/ Wi-Fi连接下的流量对比

图5给出了僵尸流量与用户流量的相似度，这里使用变化点检测的方法[13]，假设用户流量User_traffic满足一定的分布规律，如果僵尸流量Bot_traffic的分布规律与User_traffic相似，利用CUSUM算法得到的累加结果sum应在一定的阈值之内，如果超出阈值则说明分布规律发生变化，Bot_traffic与User_traffic不再相似。计算公式为

$$f(x_i)=\text{Bot\_traffic}(x_i)-\text{User\_traffic}(x_i)$$

$$\text{sum}(x_i)=(\text{sum}(x_{i-1})+f(x_i))^{+}$$

这里阈值设为2000，图5中可以看出，没有使用自适应算法的流量在第50多分钟时超过阈值，出现

变化点，而使用自适应算法的流量始终在阈值范围之内。这说明使用了自适应算法的流量与正常流量的相似度远高于没有使用自适应算法的相似度，能够更好地实现隐蔽性。

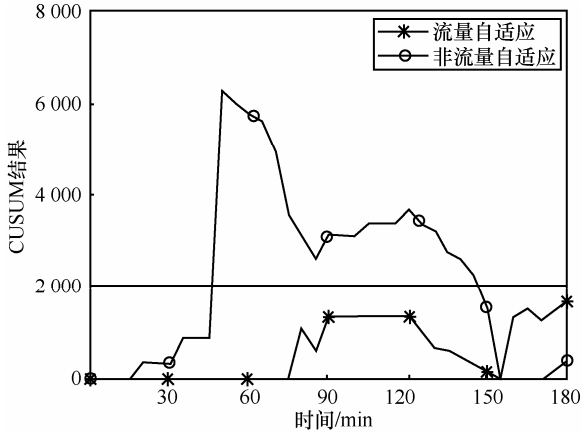


图 5　流量自适应算法与非自适应算法的流量相似度比较

此外，从移动僵尸网络电量消耗的角度考虑其隐蔽性。实验将云控推送机制与短信 SMS[5]和电子邮件[9]机制进行了对比。在移动终端使用 Power-Tutor[14]对每条僵尸命令所需要消耗的电量进行测量和记录。图 6 给出了使用 3 种不同信道推送僵尸命令的电量消耗。从图 6 中可以看出，在僵尸命令只有 1 条时，电子邮件推送消耗的电量是推送的 3 倍，短信也约为推送的 2 倍。随着推送命令的增加，电子邮件与短信机制消耗的电量显著上升，而推送消耗的电量变化不大，相对稳定。因为推送机制使用心跳包维持网络连接，接受新的推送命令时，只需要很少的电量消耗。由此可以看出，采用云控机制推送僵尸命令具有低电量消耗的优势。

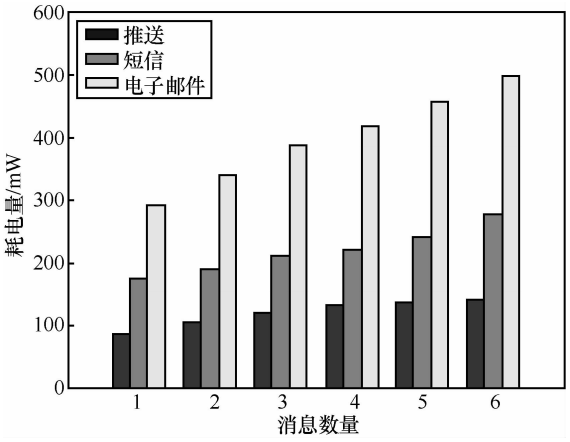
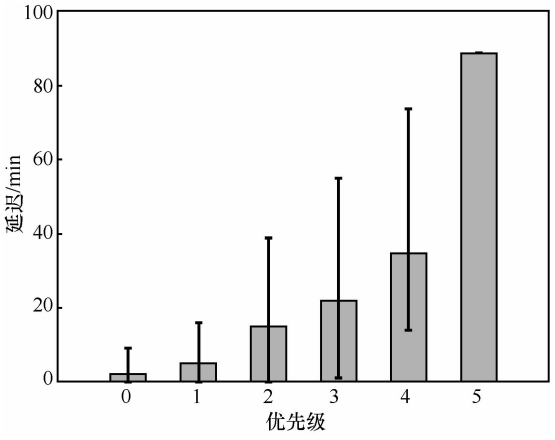


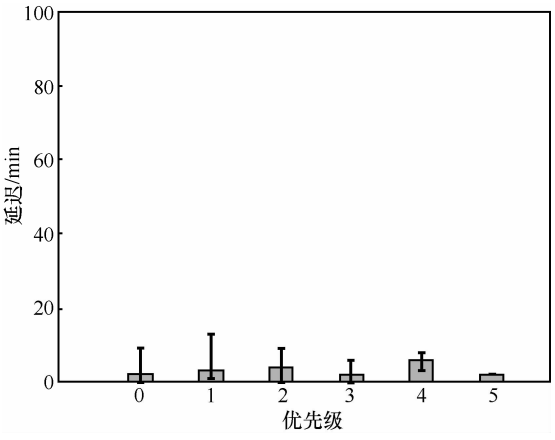
图 6　手机终端的平均电量消耗

4.3　实时性分析

按照优先级分类，图 7(a)展示了 3G 网络下每类僵尸命令的延迟柱状图，显示了每类僵尸命令的平均延迟程度，同时也给出了每类命令的最大延迟与最小延迟。为了避免僵尸攻击命令引起用户注意，针对优先级低的僵尸命令，采取分片执行的方式，因此，其延迟时间明显大于优先级高的僵尸命令。图 7(b)是在 Wi-Fi 网络下的延迟程度，可以看出在 Wi-Fi 情况下，僵尸命令的执行情况明显优于 3G 网络。相对来说，流量自适应调度算法能较好地在隐蔽性和实时性之间进行平衡。



(a) 3G 网络



(b) Wi-Fi 网络

图 7　僵尸网络命令执行的延迟程度

5　结束语

在移动僵尸网络中，构建健壮的僵尸网络命令与控制机制是其核心要素。本文研究了一种在 3G/Wi-Fi 网络环境下具有流量自适应的移动僵尸网络的云控机制，针对不同网络连接情况，设计僵

尸命令调度执行算法，既能满足流量充足时紧急命令立即执行的需求，也能在命令不紧急时，满足隐蔽性的需求，避免造成 3G 流量异常。流量自适应云控机制依赖于推送服务器的可用性，在顽健性上还有待加强。

基于现有的一些检测方案，如基于异常的检测方案[14]以及基于信道挖掘的检测方案[15]都很难检测出云控僵尸网络。为了检测此类僵尸网络，可以用流量监测软件对手机中每个应用程序的流量使用情况进行更细致的分析。另外用户需对手机应用程序进行实时监测，及时发现异常网络行为，用户还应提高防范意识，尽量不要安装非正常渠道的软件。

参考文献：

[1] APVRILLE A. Symbian worm Yxes: towards mobile botnets[J]. Journal in Computer Virology,2012,8(4): 117-131.

[2] SCHMIDT A D, SCHMIDT H G, BATYUK L, *et al*. Smartphone malware evolution revisited: android next target?[A].Proceeding of 4th International Conference on Malicious and Unwanted Software (MALWARE)[C]. Piscataway, NJ, USA, 2009. 1-7.

[3] PORRAS P,SAIDI H, YEGNESWARAN V. An analysis of the iKee B iPhone botnet[A]. Proceedings of the 2nd International ICST Conference on Security and Privacy on Mobile Information and Communications Systems (Mobisec)[C]. Piscataway, NJ, USA, 2010. 141-152

[4] CUI X, FANG B, YIN L, *et al*. Andbot: toward sadvancedmo bilebotnets[A]. Proceedings of the 4th USENIX Conference on Large-Scale Exploits and Emergent Threats[C]. 2011.11.

[5] ZENG Y, SHIN K G, HU X. Design of SMS commanded-and-controlled and P2P-sructured mobile botnets[A]. Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks[C]. New York, NY, USA, 2012. 137-148.

[6] WANG P, SPARKS S, ZOU C C. An advanced hybrid peer-to-peer botnet[J]. IEEE Transactions on Dependable and Secure Computing, 2010, 7(2): 113-127.

[7] MULLINER C, MILLER C. Fuzzing the phone in your phone[EB/OL]. http://www.blackhat.com/presentations/bh-usa-09/MILLER/BHUSA09-Miller-FuzzingPhone-PAPER.

[8] MULLINER C, SEIFERTJ P. Rise of the iBots: owning a telco network[A]. Proceedings of the 5th IEEE International Conference on Malicious and Unwanted Software (Malware)[C]. Nancy, France, 2010.71-80.

[9] SINGH K, SRIVASTAVA A, GIFFIN J, *et al*. Evaluating email's feasibility for botnet command and control[A]. Proceedings of IEEE International Conference on Dependable Systems and Networks (DSN)[C]. Piscataway, NJ,USA, 2008.376-385.

[10] ZHAO S, LEE P P C, LUI J, *et al*. Cloud-based push-styled mobile botnets: a case study of exploiting the cloud to device messaging service[A]. Proceedings of the 28th Annual Computer Security Applications Conference[C]. New York, NY, USA, 2012.119-128.

[11] CHEN W, GONG P, YU L, *et al*. An adaptive push-styled command and control mechanism in mobile botnets[J]. Wuhan University Journal of Natural Sciences, 2013, 18(5): 427-434.

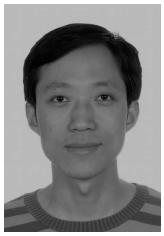
[12] GU G, ZHANG J, LEE W. BotSniffer: detecting botnet command and control channels in network traffic[A]. Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS'08)[C]. San Diego, CA, 2008.

[13] BRODSKY B. Nonparametric Methods in Change-Point Problems[M]. The Netherlands: Kluwer Academic Publishers, 1993.

[14] DONG M, ZHONG L. Self-constructive high-rate system energy modeling for battery-powered mobile systems[A]. Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services[C]. New York, NY, USA, 2011.335-348.

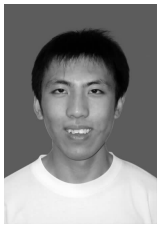
[15] GU G, PERDISCI R, ZHANG J. BotMiner: clustering analysis of network traffic for protocol-and structure-independent botnet detection[A]. Proceedings of USENIX Security[C]. 2008.139-154.

作者简介：



陈伟（1979-），男，江苏淮安人，南京邮电大学副教授，主要研究方向为网络安全、智能移动终端安全。

周诗文（1991-），女，山东济宁人，南京邮电大学硕士生，主要研究方向为移动互联网的安全。



殷承宇（1991-），男，江苏苏州人，南京邮电大学硕士生，主要研究方向为移动互联网的安全。