基于 LLMNR 协议与证据理论的本地网络 C&C 信息分享机制

郭晓军[①②③] 程 光*[①③] 胡一非[①③] 戴 冕[①③]
[①](东南大学计算机科学与工程学院 南京 210096)
[②](西藏民族大学信息工程学院 咸阳 712082)
[③](东南大学计算机网络和信息集成教育部重点实验室 南京 210096)

摘 要：僵尸主机(Bot)安全隐蔽地获取控制命令信息是保证僵尸网络能够正常工作的前提。该文针对本地网络同类型 Bot 隐蔽地获取控制命令信息问题，提出一种基于 LLMNR 协议与证据理论的命令控制信息分享机制，首先定义了开机时间比和 CPU 利用率两个评价 Bot 性能的指标。其次本地网络中多个同类 Bot 间利用 LLMNR Query 包通告各自两个指标值，并利用 D-S 证据理论选举出僵尸主机临时代表 BTL(Bot Temporary Leader)。接着仅允许 BTL 与命令控制服务器进行通信并获取命令控制信息。最后，BTL 通过 LLMNR Query 包将命令控制信息分发给其它 Bot。实验结果表明，该机制能使多个同类 Bot 完成命令控制信息的共享，选举算法能根据 Bot 评价指标实时有效选举出 BTL，在网络流量较大时仍呈现较强的鲁棒性，且选举过程产生流量也具有较好隐蔽性。

关键词：网络安全；僵尸网络；命令控制；D-S 证据理论；LLMNR 协议
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1009-5896(2017)03-0525-07
DOI: 10.11999/JEIT160410

C&C Information Sharing Scheme in Local Network Based on LLMNR Protocol and Evidential Theory

GUO Xiaojun[①②③] CHENG Guang[①③] HU Yifei[①③] Dai Mian[①③]
[①](*School of Computer Science and Engineering*, *Southeast University*, *Nanjing* 210096, *China*)
[②](*School of Information Engineering*, *Xizang Minzu University*, *Xianyang* 712082, *China*)
[③](*Key Laboratory of Computer Network and Information Integration Ministry of Education*, *Southeast University*, *Nanjing* 210096, *China*)

Abstract: The bot must obtain the Command and Control (C&C) information covertly and securely, which is a necessary precondition to ensure botnet work correctly and normally. For the problem that how to covertly get and share C&C information between the same type bots in local network, a C&C Information Sharing scheme based on Link-Local Multicast Name Resolution (LLMNR) protocol and Evidential (CCISLE) theory is proposed. Firstly, for measuring bot performance, two metrics are defined: running time ratio and CPU utilization rate. Secondly, the same type bots will inform their own two metrics to each other via LLMNR query packets and utilize D-S evidential theory to vote BTL (Bot Temporary Leader). Then only BTL can be proved to communicate with C&C servers and C&C information can be obtained. Lastly, BTL will share the C&C information with other bots through LLMNR query packets. The experimental results show that CCISLE can help the same type bots achieve sharing C&C information successfully. The voting algorithm based on D-S evidential theory is able to elect BTL effectively with two proposed metrics and still present better robustness when in heavy network traffic. Moreover, the traffic produced during BTL voting process also has good covertness.

Key words: Network security; Botnet; Command and control; D-S evidential theory; Link-Local Multicast Name Resolution (LLMNR) protocal

1 引言

近年来，由僵尸网络(Botnet)[1]引发的网络安全事件层出不穷，危及我国公共互联网安全运行，对国家信息安全造成严重危害。僵尸网络是一个高度受控平台，其核心思想都是借助专用恶意代码感染智能手机、平板、计算机等设备，使其变为受控节点(Bot)，攻击者通过命令与控制(Command and Control Server, C&C)服务器向 Bot 主动推送命令控制信息(Push 模式)，或者 Bot 主动从 C&C 服务器上获取命令控制信息(Pull 模式)，来对这些 Bot 进行管理。在 Bot 得到命令控制信息后，可根据相应指令对指定目标实施信息窃取，DDoS 攻击、垃圾邮件轰炸、会话劫持等恶意行为[2−4]。

可见，攻击者与 Bot 之间能安全传送命令控制信息是保证 Botnet 正常工作的基本要素。从目前已

收稿日期：2016-04-25；改回日期：2016-09-09；网络出版：2016-11-14
*通信作者：程光 gcheng@njnet.edu.cn
基金项目：国家 863 计划项目(2015AA015603)，江苏省未来网络创新研究院未来网络前瞻性研究项目(BY2013095-5-03)，江苏省“六大人才高峰”高层次人才项目(2011-DZ024)，江苏省普通高校研究生科研创新计划资助项目(KYLX_0141)
Foundation Items: The National 863 Program of China (2015AA 015603), Jiangsu Future Net-works Innovation Institute: Prospective Research Project on Future Networks (BY2013095-5-03), Six Talent Peaks of High Level Talents Project of Jiangsu Province (2011-DZ024), The Scientific Research Innovation Projects for General University Graduate of Jiangsu Province (KYLX_0141)

有公开文献来看，多数 Bot 获取命令控制信息仍采用先通过某种途径获得 C&C 服务器 IP 地址或域名，并与 C&C 服务器通信，然后再以 Push 模式或 Pull 模式从 C&C 服务器获取命令控制信息[5−12]。由于该方式是让 Bot 直接从 C&C 服务器处获取命令控制信息，当位于同一局域网的多个主机感染相同恶意代码而成为同类 Bot 后(例如，同实验室多人打开本实验室 QQ 群共享中含有恶意代码的文件，某部门的多位人员通过公司域名下邮箱收到相同的附件中携带伪装恶意代码的邮件等)，这些同类 Bot 必须各自独立重复执行该方式才能获取命令控制信息。在此情况下，网络监管者根据这些同类 Bot 所产生网络流量的行为相似性来识别和追踪 C&C 服务器[13−20]，同时也容易导致局域网中 Bot 位置的暴露和检测，进而破坏 Botnet 正常运作过程，使其威胁性和危险性大大降低，甚至失去实用价值。

针对上述问题，僵尸网络控制者会利用各种技术手段尽量模糊化或随机化 Bot 产生的流量特征而避逃避检测和追踪，以让僵尸网络在隐蔽性增强的同时更加高效地工作，其中借用现有网络协议秘密地进行命令控制信息收发就是一种常用方法，而且多个本地网络同类型 Bot 间还可利用组播性质的协议来收发命令控制信息，以避免网络流量行为相似性检测，提高传输效率。因此，本文提出一种基于 LLMNR(Link-Local Multicast Name Resolution)协议[21]的本地网络同类 Bot 间命令控制信息分享机制，首先定义了开机时间比和 CPU 利用率两个评价 Bot 性能指标，其次本地网络中多个同类 Bot 利用 LLMNR Query 包将各自两个指标值通告给其它 Bot，并借用 D-S 证据理论[22]选举出 Bot 临时代表 BTL(Bot Temporary Leader)，接着仅被选为 BTL 的 Bot 与 C&C 服务器通信并从 C&C 服务器获取命令控制信息，最后，BTL 再次通过 LLMNR Query 包将所获取的命令控制信息分发给其它 Bot，并进行了相关实验测试。

本文第 1 节介绍安全隐蔽地获取 C&C 信息对于僵尸网络中 Bot 的重要性和关键性；第 2 节针对本地网络多个同类 Bot 间安全隐蔽地获得 C&C 信息问题，提出基于 LLMNR 协议和 D-S 证据理论 C&C 信息分享机制 CCISLE(C&C Information Sharing scheme based on LLMNR protocol and Evidential theory)，并给出该机制相关细节；第 3 节对 CCISLE 机制的关键部分 —— BTL 选举算法的有效性、鲁棒性及隐蔽性等进行评估；第 4 节讨论了 CCISLE 机制的局限性；最后给出结论，并指出后续的研究方向。

2 CCISLE 分享机制

CCISLE 分享机制可分为 BTL 选举、BTL 的获取 C&C 信息及 C&C 信息分发 3 个阶段，如图 1 所示。

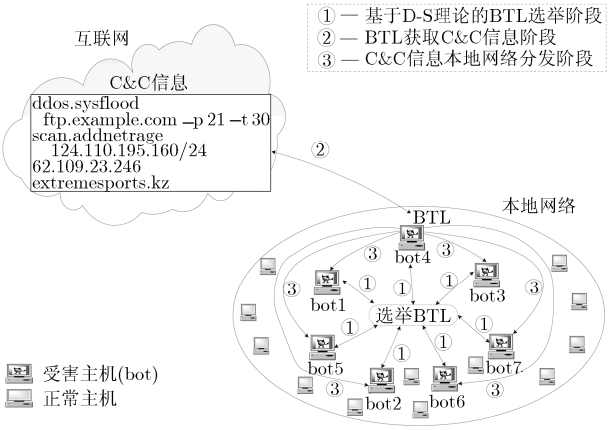

图 1 CCISLE机制过程

在 BTL 选举阶段，每个 Bot 将自己的评价指标数值通过 LLMNR 协议告知其它 Bot，再利用 D-S 证据理论融合这些评价指标数值以选举最优 Bot 作为 BTL；然后 BTL 查找 C&C 服务器地址并与之取得通信，并利用 PULL 或 PUSH 模式以较为隐蔽的方式从 C&C 服务器获取最新命令控制信息；最后，BTL 再次利用 LLMNR 协议将所获取的命令控制信息分发给本地网络的其它 Bot。

2.1 基于 D-S 证据理论的 BTL 选举过程

BTL 是本地网络多个同类 Bot 的代表，负责从 Internet 上获取 C&C 信息，并分发给其他同类 Bot。由于各 Bot 所在受害主机的开机时间、软硬件资源配置等方面存在差异，因此需要择优选出较好的 Bot 作为 BTL。

2.1.1 评价指标 本文选择 Bot 开机时间比与 CPU 使用率作为该 Bot 能否成为 BTL 的评价指标。在 Bot 开机时间比相同的情况下，CPU 使用率越小，说明该 Bot 可使用的硬件资源越充足，所以应优先选择 CPU 使用率小的 Bot 作为 BTL；在 CPU 使用率相同的情况下，Bot 开机时间比越大，说明该 Bot 正常工作时间越稳定，所以应优先选择 Bot 开机时间比越大的 Bot 作为 BTL。

(1)Bot 开机时间比： 在 BTL 选举中，Bot 开机时间越长，表示该 Bot 所在的受害主机能正常持续运行的时间越长，处于活跃状态，越有利于该 Bot 成为 BTL。此处用 Bot 开机时间比 $g(j)$ 来衡量第 j 个 Bot 的开机时间，定义为

$$g(j)=t(j)/\Omega \tag{1}$$

其中，$t(j)$ 表示 Bot j 的累积开机时间，Ω 为观察的时间窗口长度。

(2)CPU 利用率：　在 BTL 选举中，Bot 所在受害主机 CPU 利用率小，表示能被该 Bot 所利用的主要硬件资源越多，Bot 代码执行时给受害主机所造成负担较轻，不易引起受害主机用户的觉察，增加了 Bot 的隐蔽性，有助于该 Bot 成为 BTL。CPU 利用率定义为在观察时间长度为 Ω 内的 CPU 利用率平均值，记为 $h(j)$。

2.1.2 融合评判　为消除两种评价指标下选择 BTL 结果的不一致性，本文借用 D-S 证据理论合成规则将两种指标的结果进行融合判决，以选举出合适的 BTL。选择过程如图 2 所示。

设辨别框架 $\Theta=\{\theta_1,\theta_2,\theta_3\}$，$\theta_1$ 为 BTL 集合，θ_2 模糊 Bot 集合，θ_3 为普通 Bot 集合，且满足 $\theta_1\cap\theta_2=\varnothing$，$\theta_2\cap\theta_3=\varnothing$，$\theta_1\cap\theta_3=\varnothing$。然后对 Bot 开机时间比 $g(j)$ 与 CPU 使用率 $h(j)$ 分别建立隶属度函数，隶属度函数衡量了当前 Bot 属于 θ_1，θ_2 或 θ_3 的可能性大小，在归一化后即可得到信度分配函数 BPAF(Basic Probability Assignment Function)，只要将 Bot 的两个特征值代入 BPAF 即可求得支持该 Bot 属于各集合的基本信度。图 2 给出了基于 D-S 证据理论的 BTL 选举方法，其中 $m_1(\theta_i)$，$m_2(\theta_i)$，$(i=1,2,3)$ 分别为两个指标对命题 θ_i 的基本信度，$m(\theta_i)$ 为经过 D-S 证据理论合成法则得到的综合基本信度。

对于 Bot 开机时间比 $g(j)$，本文选用广义钟型隶属函数作为指标 $g(j)$ 下度量 Bot j 属于 $\theta_1,\theta_2,\theta_3$ 的程度。设 T_1,T_2,T_3 分别表示集合 θ_1，θ_2 及 θ_3 的隶属度函数，则

$$T_1\big(g(j)\big)=\frac{1}{1+\left|\dfrac{g(j)-\beta_1}{\alpha_1}\right|^{2\gamma_1}} \tag{2}$$

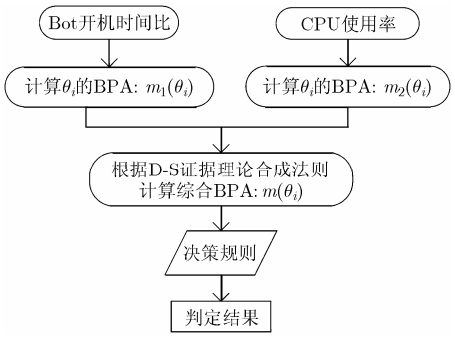

图 2 基于D-S证据理论的BTL选举过程

$$T_2\big(g(j)\big)=\frac{1}{1+\left|\dfrac{g(j)-\beta_2}{\alpha_2}\right|^{2\gamma_2}} \tag{3}$$

$$T_3\big(g(j)\big)=\frac{1}{1+\left|\dfrac{g(j)-\beta_3}{\alpha_3}\right|^{2\gamma_3}} \tag{4}$$

其中，$\alpha_1,\beta_1,\gamma_1,\alpha_2,\beta_2,\gamma_2,\alpha_3,\beta_3,\gamma_3$ 为常数，可以调整函数 T_1，T_2，T_3 对应的曲线形状。$T_1(g(j))$，$T_2(g(j))$，$T_3(g(j))$ 衡量 Bot j 属于相应类别可能性大小。对 $T_1(g(j)),T_2(g(j)),T_3(g(j))$ 归一化操作后，可得到对应的 BPAF 值：$m_1(\theta_1),m_1(\theta_2)$ 及 $m_1(\theta_3)$，如式(5)所示。

$$m_1\big(\theta_i\big)=\frac{T_i\big(g(j)\big)}{\sum_{i=1}^{3}T_i\big(g(j)\big)} \tag{5}$$

对于 CPU 利用率 $h(j)$，本文选择 Sigmoid 型函数和 Gauss 型隶属函数作为 $h(j)$ 下度量 Bot j 属于集合 $\theta_1,\theta_2,\theta_3$ 的程度。设 S_1,S_2,S_3 分别表示集合 θ_1,θ_2 及 θ_3 的隶属度函数，则

$$S_1\big(h(j)\big)=\frac{1}{1+\mathrm{e}^{-\mu_1(h(j)-\phi_1)}} \tag{6}$$

$$S_2\big(h(j)\big)=\mathrm{e}^{\frac{-(h(j)-\phi_2)^2}{2\mu_2^2}} \tag{7}$$

$$S_3\big(h(j)\big)=\frac{1}{1+\mathrm{e}^{-\mu_3(h(j)-\phi_3)}} \tag{8}$$

其中，e 为自然对数的底，通过设置常数 μ_1,μ_2,μ_3，$\varphi_1,\varphi_2,\varphi_3$ 来调整函数 S_1,S_2,S_3 对应的曲线。在对 $S_1(h(j)),S_2(h(j)),S_3(h(j))$ 归一化处理后，类似式(5)，可计算出 CPU 利用率的 BPAF 值：$m_2(\theta_1)$，$m_2(\theta_2)$ 及 $m_2(\theta_3)$。

由于两个指标 $g(j),h(j)$ 不存在相关性，因此可以假设在此两个评价指标下产生的结果是相互独立的。为消除两种评价指标下选择 BTL 结果的不一致性，利用式(9)的 Dempster 证据合成规则可以得到两指标融合后对于各类别的 BPAF 值。其中 $1-R$ 为归一化常数。当各证据间冲突不大时，使用 Dempster 合成规则融合时可得到较好效果。

$$m(\theta)=m_1(\theta)\oplus m_2(\theta)=\frac{\sum_{X\cap Y=\theta}m_1(X)m_2(Y)}{1-R} \tag{9}$$

$$R=\sum_{X\cap Y=\varnothing}m_1(X)m_2(Y) \tag{10}$$

至此，得到 Bot j 在两个评价指标下的综合信度评价结果：$m(\theta_1),m(\theta_2)$ 和 $m(\theta_3)$ 分别表示对 Bot j 成为 BTL，模糊 Bot 及普通 Bot 的综合支持信度。本文此处根据 3 个值的最大者来确定 Bot j 所属的类别。

2.1.3 选举过程步骤 基于 D-S 证据理论的 BTL 选举过程分为如下 3 个步骤：

(1)各 Bot 利用 LLMNR 协议的 Query 包在本地网内通告自己的开机时间比 $g(j)$ 与 CPU 使用率 $h(j)$ 两个指标值，其他 Bot 收到该 Query 包后记录下两个指标及源 IP 地址。

本文将两个指标以“btlvote+指标 1+指标 2”的格式放置在 LLMNR Query 包的 Name 字段中。例如 Name 字段为“btlvote8623”时，“btlvote”为关键字，表示该 Query 包的作用是选举 BTL，“86”与“23”分别表示该 Bot 的 $g(j)$ 与 $h(j)$ 指标值。由于 LLMNR 协议采用组播工作方式，这能够保证本地网络内的 Bot 都能收到其它 Bot 发出的 Query 包。

(2)各 Bot 根据收到所有 Bot 的两个指标值，利用 2.1.2 节中 D-S 证据理论计算出 BTL 集合 θ_1。

(3)采用集合 θ_1 中 IP 地址最大者对应的 Bot 作为 BTL。由于 BTL 集合 θ_1 中元素的个数可能大于 1，因此本文选择 θ_1 中 IP 地址最大者的 Bot 作为 BTL。

当 BTL 失效时，重新进行 BTL 选举过程。

2.2 BTL 获取 C&C 信息

BTL 在被选举出之后，需要通过一定的方式从 Internet 上获取 C&C 信息。为提高 BTL 获取 C&C 信息过程的隐蔽性，本文此处借鉴文献[23,24]中思想，通过含有隐藏信息的博文内容来获取 C&C 信息。攻击者借用信息隐藏手段事先将要发布的 C&C 信息隐藏于某个知名博客博文内容的 HTML 代码中，然后 BTL 利用嵌入在恶意代码中的博客地址构造算法产生出含有 C&C 信息的博客链接，最后 BTL 通过该链接访问该博客，并恢复出隐藏于该博客博文 HTML 代码中的 C&C 信息，从而 BTL 完成获取 C&C 信息的过程。

2.3 基于 LLMNR 协议的 C&C 信息分发

当 BTL 获得 C&C 信息时，组成形成 C&C 信息列表，列表中的每项控制命令信息都是独立的，如图 1 中“C&C 信息”部分所示。BTL 在分发控制命令信息时，以“ccinfoXXSSF +命令控制信息内容”格式嵌入在 LLMNR Query 包的 Name 字段中(类似 2.1.3 节中 BTL 选举时的 Query 包格式)。其中，ccinfo 为关键字，表示 C&C 信息，XXSSF 为标识位，其含义如表 1 所示。

由于有些控制命令信息比较长，可能包含多个参数，为防止命令信息内容在 Name 字段中过长而引发检测，可将较长的控制命令信息其拆分成多个段，并添加 XXSSF 标识后，分别嵌入在不同 LLMNR Query 包的 Name 字段中进行传输，当 Bot 接收到这些 Query 包后可通过 XXSSF 标识恢复出该控制命令信息。例如，对于命令控制信息“**ddos. sysflood** ftp.example.com -p 21 –t 30”，可将其拆分为： 01000ddos.sysflood, 01010ftpexample.com, 01020p21 和 01031t30，并分别作为 LLMNR Query 包的 Name 字段发送。

表 1 分发标识位含义

位名称	含义
XX	控制命令信息编号
SS	控制命令信息的分段编号
F	控制命令信息分段结束标志，F=0 表示未结束，F =1 表示结束。

3 实验与分析

本文将实验室所在局域网作为图 1 所示的本地网络环境。主要程序代码通过 Python 来实现，并借用 Scapy 工具[25]来实现 LLMNR Query 包的构造与解析功能。由于选举 BTL 是本文所提机制的核心部分所在，因此，本实验主要针对基于 D-S 证据理论的 BTL 选举过程进行了测试。根据多次实验测试的结果，式(2)~式(4)中参数较为合理的值为 $\alpha_1=0.2$，$\beta_1=1.0$，$\gamma_1=1.5$，$\alpha_2=0.1$，$\beta_2=0.5$，$\gamma_2=1.5$，$\alpha_3=0.2$，$\beta_3=0.0$，$\gamma_3=1.5$，式(6)~式(8)中参数较为合理的值为 $\mu_1=0.2$，$\varphi_1=0.0$，$\mu_2=0.1$，$\varphi_2=0.5$，$\mu_3=20.0$，$\varphi_3=0.7$。观察时间窗口长度 $\Omega=24$ h。实验室计算机的软硬件配置均为 AMD A10-5800K 3.8 GHz (CPU), 4 GB(内存)，250 GB (硬盘)，RTL8168/8111/8112 Gigabit Ethernet(网卡)，操作系统为 Ubuntu 14.04(64 位)。

3.1 BTL 选举有效性

为测试基于 D-S 证据理论 BTL 选举算法的有效性，本文此处测试了不同 Bot 总数(BotNum)下，在使用本文中 D-S 证据理论方法选举 BTL 后，BTL 集合 θ_1，模糊 Bot 集合 θ_2 和普通 Bot 集合 θ_3 所包含 Bot 数量占全部 Bot 数量的比例，如图 3 所示。可以看出，对不同 Bot 总数执行 BTL 选举过程后，普通 Bot 集合 θ_3 所包含的 Bot 数量最多，所占比例均超过 65%，相比之下 BTL 集合 θ_1 与模糊 Bot 集合 θ_2 所占比例较小，这样比例情况较为合理。随着 Bot 总数的增加，属于 BTL 集合 θ_1 的 Bot 数量比例大约在 10%~15%，基本可以保证有充足数量的 Bot 作为 BTL。

3.2 BTL 选举时效性与鲁棒性

本文主要从含有 BTL 选举关键字“btlvote”的 LLMNR Query 包发送速率与背景流量影响两个角度对 BTL 选举算法的时效性与鲁棒性进行了实验。图 4 展示出了在不同 Bot 数量下，含有“btlvote” LLMNR Query 包发送速率与选举算法选出 BTL 所花费时间的关系。从图 4 中来看，不同 Bot 数量下，

BTL 选举时间会随着含有“btlvote”LLMNR Query 包的发送速率的增加而迅速下降，且呈现平稳趋势。当含有“btlvote”LLMNR Query 包发送速率为 0~400 pps(packet per second)时，BTL 选举时间会随着含有“btlvote”LLMNR Query 包发送速率的增大而急剧减小。这主要是由于含有“btlvote”LLMNR Query 包发送速率小，各 Bot 需要较长时间才能从网络中捕获并过滤出该类型的 LLMNR Query 包，占据了大部分的 BTL 选举时间开销。而当大于 400 pps 时，Bot 能快速发送含有“btlvote”LLMNR Query 包，再加上 LLMNR 协议采用组播工作方式，使得各 Bot 能在极短时间内从网络中捕获和过滤其它 Bot 发送含有“btlvote”LLMNR Query 包，极大降低了因捕获该类型包而耗费的时间，而此时通过 D-S 证据理论计算 BTL 过程则成为时间开销的主要因素，且每增加 10 个 Bot，时间开销大约增加 0.1 s。

另外，本文在不同本地网络背景流量下 BTL 选举算法的鲁棒性进行了测试，结果如图 5 所示，含有“btlvote”LLMNR Query 包发送速率为 500 pps。局域网背景流量采用工具 iPerf[26]生成。从图 5 可看出，在 Bot 数量 BotNum 保持不变情况下，网络背景流量 bg 的增大对选举 BTL 时间的影响并不明显。这主要是由于一方面 Scapy 工具借助实验主机上的千兆网卡能以极高的效率捕获局域网背景流量，并能按照设定的过滤规则，结合主机千兆网卡充足的硬件资源优势，高效过滤出含有“btlvote”标识的 LLMNR Query 包；另一方面 BTL 选举算法基于 D-S 证据理论，计算过程时间复杂度较低，在得到各 Bot 的开机时间比与 CPU 利用率两个指标后，能以较快的速度计算出 BTL。此外，图 5 也说明随着局域网内 Bot 数量的增加，选举出 BTL 所花费时间也在以近似线性的方式增加，这也印证了图 4 中所展示的实验结果。

3.3 BTL 选举过程安全性

BTL 选举过程安全性主要体现在 BTL 选举过程所产生流量的隐蔽性上。隐蔽性此处是指含有“btlvote”LLMNR Query 包在所有本地网络的 LLMNR Query 包中出现的随机程度，可反映出 BTL 选举算法抗检测能力的强弱。本文此处采用含有“btlvote” LLMNR Query 包的自信息 $I(p)$ 来描述。自信息可用于表示某个事件出现的概率与其不确定性(即随机性)的关系，若该事件出现概率较大，则其自信息较大，随机性较小，反之就大，其计算公式如式(11)所示。

$$I(p)=\lg(1/p)=-\lg p \tag{11}$$

$$p=N_b/N_a \tag{12}$$

其中，p 表示在嗅探持续时间 T 内含有“btlvote”LLMNR Query 包出现的概率，此处定义为含有“btlvote”LLMNR Query 包的数量 N_b 与所有 LLMNR Query 包的数量 N_a 之比。图 6 给出了在多个嗅探持续时间内，不同 Bot 数量下对 $I(p)$ 的测试结果。

可以看到，Bot 数量保持不变情况下，随着嗅探持续时间 T 增长，自信息 $I(p)$ 呈现出逐步增大趋势，即含有“btlvote”LLMNR Query 包在本地网络 LLMNR Query 流量中的随机性不断增加。主要原因是随着 T 增长，本地网络所有 LLMNR Query 包总数的增加量要远大于含有“btlvote”LLMNR Query 包总数的增加量，尤其是当正常用户进行查找网络邻居等操作时，需要解析多个主机名字，会产生大量的正常 LLMNR Query 包。而含有“btlvote”LLMNR Query 包仅在 BTL 选举时产生一次，出现时间也极短，大大降低了其在本地网络流量暴露的可能性。此外还可看到，由于 Bot 数量的增加必然引起含有“btlvote”LLMNR Query 包总数的增加，提高了此类型包在本地网络 LLMNR Query 流量中出现的概率，从而导致出现其 $I(p)$ 会随 Bot 数量的增加而明显增大的现象，例如当 Bot 数量分别为 10, 30 和 50 时，在 $T=240$ s 情况下，所对应的 $I(p)$ 分别为 7.3, 5.5 和 4.5。

另外，由于当前多数本地网络采用百兆以上以太网技术，各种网络应用和网络管理任务(如 HTTP, QICQ, TCP, STP 等)所产生的网络流量，无论持续时间还是数据包数量方面也远大于 BTL 选举过程产生的 LLMNR Query 流量。这些大量持

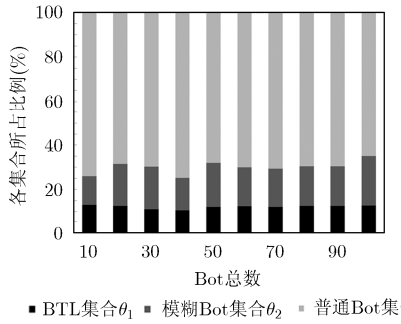

图 3　BTL选举算法产生的各集合Bot数量比例关系

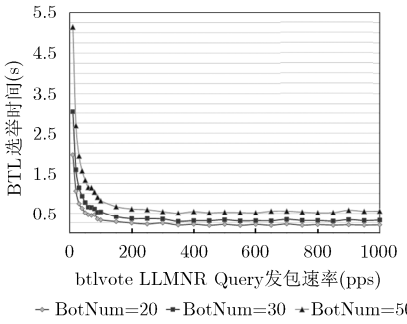

图 4　btlvote LLMNR Query包速率对BTL选举时间影响

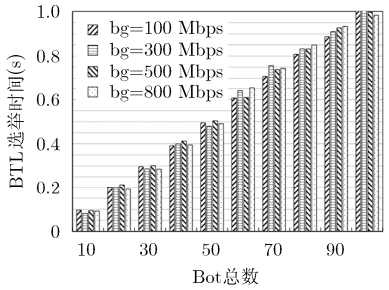

图 5 本地网络背景流量对 BTL 选举时间影响

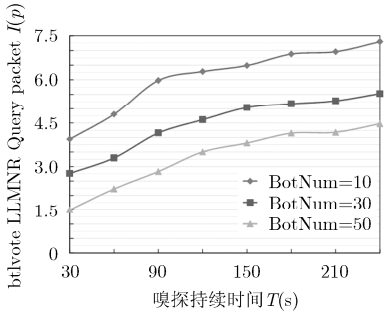

图 6 自信息 $I(p)$与嗅探持续时间 T 的关系

续数据包的产生进一步降低了 BTL 选举过程的 LLMNR Query 流量在本地网络流量中所占的比例，极大增加了从本地网络流量中观测含有“btlvote” LLMNR Query 包的难度，在很大程度上起到了掩护“btlvote” LLMNR Query 包的作用，从而进一步提高了 BTL 选举过程 LLMNR Query 流量的隐蔽性。

4 局限性讨论

本文针对本地网络内同类 Bot 间共享 C&C 信息机制进行了初步探究，但还存在以下局限性与不足：

(1)本文所提机制的存在性。截止本文完成时，虽然通过公开文献未见到类似机制的报道，但从本文分析与模拟实验可以看出，攻击者是完全可以通过现有的局域网网络协议与技术方法来实现该机制的。因此，本文认为 CCISLE 完全可能成为一种新的 C&C 信息获取途径。

(2)BTL 选举和 C&C 信息分发过程所使用的 LLMNR Query 包中 Name 字段内容(如“btlvote ####”)仍为明文，存在容易遭到入侵和渗透的问题。若专门针对 LLMNR 流量进行抓取和分析，则含有“btlvote####” 的 LLMNR Query 包容易引起怀疑，从而可能暴露出 BTL 选举过程。由于本文是对 CCISLE 机制的初步研究，为简单起见，故而采用了明文方式。下一步将研究如何采用隐蔽的方法(如加密等)传输 Name 字段内容，避免直接使用明文，以提高安全性。

(3)未给出针对本文所提机制的检测方法。由于本文所提机制在 BTL 选举及 C&C 信息过程中，LLMNR Query 包的 Name 字段含有明文形式的关键字(如“btlvote”,“ccinfo”)，相应的检测方法也比较简单，如可使用 DPI(Deep Packet Inspection)方法[27]对本地网络 LLMNR Query 流量进行检测。下一步本文将在解决问题(2)的基础上，再深入研究针对隐蔽性提高后的 Name 字段的检测方法。

5 结束语

为避免检测和追踪，Bot 需要安全隐蔽地获取控制命令信息，本文提出一种基于 LLMNR 协议与证据理论的本地网络同类型 Bot 间命令控制信息分享机制 CCISLE，其核心思想是各 Bot 首先通过本地网络常用的 LLMNR 协议通告各自的两个 Bot 性能评价指标，并应用证据理算法论选出 BTL, BTL 使用较为隐蔽的方式从 C&C Server 处获取命令控制信息，最后 BTL 再通过 LLMNR 协议将获取的命令控制信息分发给其它 Bot。实验结果也表明该机制能有效选举出 BTL，完成与本地网络内多个同类 Bot 的命令控制信息共享。但也存在一些不足，下一步研究工作将在进一步提高 CCISLE 的安全性与隐蔽性，考虑针对 CCISLE 的检测方法等方面展开。

参 考 文 献

[1] 王天佐, 王怀民, 刘波, 等. 僵尸网络中的关键问题[J]. 计算机学报, 2012, 35(6): 1192–1208. doi: 10.3724/SP.J.1016.2012.01192.
WANG Tianzuo, WANG Huaimin, LIU Bo, *et al*. Some critical problems of Botnets[J]. *Chinese Journal of Computers*, 2012, 35(6): 1192–1208. doi: 10.3724/SP.J.1016.2012.01192.

[2] CHEN P, DESMET L, and HUYGENS C. A study on advanced persistent threats[C]. Proceedings of the 15th IFIP TC 6/TC 11 International Conference on Communications and Multimedia Security, Aveiro, Portugal, 2014: 63–72. doi: 10.1007/978-3-662-44885-4_5.

[3] JUELS A and TING F Y. Sherlock Holmes and the case of the advanced persistent threat[C]. Proceedings of the 5th USENIX Conference on Large-Scale Exploits and Emergent Threats, San Jose, CA, USA, 2012: 2–6.

[4] RAFAEL A R G, GABRIEL M F, and PEDRO G T. Survey and taxonomy of botnet research through life-cycle[J]. *ACM Computing Surveys*, 2013, 45(4): 1–33. doi: 10.1145/2501654.2501659.

[5] GU G F, ZHANG J, and LEE W. BotSniffer: detecting botnet command and control channels in network traffic[C]. Proceedings of the 15th Annual Network and Distributed System Security Symposium, San Diego, CA, USA, 2008: 10–22.

[6] STONE-GROSS B, COVA M, CAVALLARO L, *et al*. Your botnet is my botnet: Analysis of a botnet takeover[C].

Proceedings of the 16th ACM Conference on Computer and Communications Security, Hyatt Regency Chicago, IL, USA, 2009: 635–647. doi: 10.1145/1653662.1653738.

[7] PORRAS P, SAIDI H, and YEGNESWARAN V. An analysis of the iKee.B iphone botnet[C]. Proceedings of the 2nd International ICST Conference on Security and Privacy in Mobile Information and Communication Systems, Catania, Sicily, Italy, 2010: 141–152. doi: 10.1007/978-3-642-17502-2_12.

[8] CHO C Y, CABALLERO J, GRIER C, *et al*. Insights from the inside: A view of botnet management from infiltration[C]. Proceedings of the USENIX Workshop on Large-Scale Exploits and Emergent Threats, San Jose, CA, USA, 2010: 120–132.

[9] BILGE L, BALZAROTTI D, ROBERTSON W, *et al*. Disclosure: detecting botnet command and control servers through large-scale netflow analysis[C]. Proceedings of the 28th Annual Computer Security Applications Conference, Orlando, FL, USA, 2012: 129–138. doi: 10.1145/2420950.2420969.

[10] ANDRIESSE D, ROSSOW C, STONE-GROSS B, *et al*. Highly resilient peer-to-peer botnets are here: an analysis of Gameover Zeus[C]. Proceedings of the 8th International Conference on Malicious and Unwanted Software: The Americas, Fajardo, Portugal, 2013: 116–123. doi: 10.1109/MALWARE.2013.6703693.

[11] RAHIMIAN A, ZIARATI R, PREDA S, *et al*. On the reverse engineering of the citadel botnet[C]. Proceedings of the 6th International Symposium Foundations and Practice of Security, La Rochelle, France, 2014: 408–425. doi: 10.1007/978-3-319-05302-8_25.

[12] GAÑÁN C, CETIN O, and VAN E M. An empirical analysis of ZeuS C&C lifetime[C]. Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, Singapore, 2015: 97–108. doi: 10.1145/2714576.2714579.

[13] CHOI H, LEE H, LEE H, *et al*. Botnet detection by monitoring group activities in DNS traffic[C]. Proceedings of the 7th IEEE International Conference on Computer and Information Technology, Aizu-Wakamatsu, Fukushima, Japan, 2007: 715–720. doi: 10.1109/CIT.2007.90.

[14] STRAYER W T, LAPSELY D, WALSH R, *et al*. Botnet Detection Based on Network Behavior[M]. New York, USA, Springer Science Business Media, 2008: 1–24. doi: 10.1007/978-0-387-68768-1_1.

[15] SAAD S, TRAORE I, GHORBANI A, *et al*. Detecting P2P botnets through network behavior analysis and machine learning[C]. Proceedings of the 9th Annual International Conference on Privacy, Security and Trust, Montreal, Quebec, Canada, 2011: 174–180. doi: 10.1109/PST.2011.5971980.

[16] ZHAO D, TRAORE I, SAYED B, *et al*. Botnet detection based on traffic behavior analysis and flow intervals[J]. *Computers & Security*, 2013, 39(4): 2–16. doi: 10.1016/j.cose.2013.04.007.

[17] DIETRICH C J, ROSSOW C, and POHLMANN N. CoCoSpot: clustering and recognizing botnet command and control channels using traffic analysis[J]. *Computer Networks*, 2013, 57(2): 475–486. doi: 10.1016/j.comnet.2012.06.019.

[18] JIANG H and SHAO X. Detecting P2P botnets by discovering flow dependency in C&C traffic[J]. *Peer-to-Peer Networking and Applications*, 2014, 7(4): 320–331. doi: 10.1007/s12083-012-0150-x.

[19] BILGE L, SEN S, BALZAROTTI D, *et al*. EXPOSURE: a passive DNS analysis service to detect and report malicious domains[J]. *ACM Transactions on Information and System Security*, 2014, 16(4): 289–296. doi: 10.1145/2584679.

[20] CHANG W, MOHAISEN A, WANG A, *et al*. Measuring botnets in the wild: Some new trends[C]. Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, Singapore, 2015: 645–650. doi: 10.1145/2714576.2714637.

[21] LEVON E, BERNARD A, and DAVE T. Link-Local Multicast Name Resolution (LLMNR)[OL]. https://tools.ietf.org /html/rfc4795. 2015.

[22] CAVALCANTE A P A, BOUDY J, ISTRATE D, *et al*. A dynamic evidential network for fall detection[J]. *IEEE Journal of Biomedical and Health Informatics*, 2014, 18(4): 1103–1113. doi: 10.1109/JBHI.2013.2283055.

[23] Guo X J, Cheng G, Pan W B, *et al*. A novel search engine-based method for discovering command and control server[C]. Proceedings of the 15th International Conference On Algorithms and Architectures for Parallel Processing. Zhangjiajie, China, 2015: 311–322. doi: 10.1007/978-3-319-27137-8_24.

[24] YIN T, ZHANG Y, and LI S. DR-SNBot: a social network-based botnet with Strong Destroy-Resistance[C]. Proceedings of the 9th IEEE International Conference on Networking, Architecture, and Storage, Tianjin, China, 2014: 191–199. doi: 10.1109/NAS.2014.37.

[25] PHILIPPE B. Scapy[OL]. http://www.secdev.org/projects/scapy/, 2015.NLANR/DAST. iPerf[OL]. https://iperf.fr/, 2015.

[26] NAJAM M, YOUNIS U, and RASOOL R. Speculative parallel pattern matching using stride-k DFA for deep packet inspection[J]. *Journal of Network and Computer Applications*, 2015, 54: 78–87. doi: 10.1016/j.jnca.2015.04.013.

郭晓军：　男，1983 年生，博士生，研究领域为网络安全、网络测量及网络管理.

程　光：　男，1973 年生，教授、博士生导师，主要研究领域为网络安全、网络测量与行为学及未来网络安全.

胡一非：　男，1989 年生，硕士生，研究领域为网络安全、机器学习.

戴　冕：　男，1988 年生，博士生，研究领域为云计算、网络安全.