

隐马尔可夫模型在 P2P 僵尸网络检测中的应用

万 巍^{1,2}, 李 俊¹

(1 中国科学院 计算机网络信息中心, 北京 100190; 2 中国科学院 研究生院, 北京 100049)

摘 要: 针对 P2P 僵尸网络的特点, 将隐马尔可夫模型应用于 P2P 僵尸网络检测技术中. 首先根据当前僵尸网络的发展状况及存在的问题分析了 P2P 僵尸网络的生命周期和行为特征; 然后对僵尸主机的状态划分采用隐马尔可夫模型对 P2P 僵尸网络进行数学建模, 并提出一种 P2P 僵尸网络的检测方法. 通过实验, 验证了检测方法的可靠性和合理性.

关键词: 僵尸网络; 隐马尔可夫模型; 状态划分

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2012)10-0014-04

Application of Hidden Markov Model in P2P Botnet Detection

WAN Wei^{1,2}, LI Jun¹

(1 Computer Network Information Center of Chinese Academy of Sciences, Beijing 100190, China;

2 Graduate University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract: In accordance with the feature of P2P botnet, the Hidden Markov Model has application in P2P botnet detection. Firstly, according to the situation and problems of the botnet recently, the life cycle and behavior characteristics of the P2P botnet have been analyzed. After that a mathematical model has been built to describe the P2P botnet with the Hidden Markov Model in state division of the bot. Meanwhile, a method of P2P botnet detection has been proposed. Finally, we analyzed and summarized the experimental results, and verified the reliability and rationality of the detection method.

Key words: botnet; Hidden Markov Model; state division

1 引言

僵尸网络是近年来兴起的对互联网安全产生重大安全威胁的一种技术手段. 这些僵尸网络的控制服务器基本都在境外, 严重的威胁到了我国公共互联网环境的安全^[1].

僵尸网络采用一种或多种传播手段, 将大量主机感染僵尸程序, 从而在控制者和被感染主机之间形成一个可以一对多进行控制的网络. 僵尸网络具有一定的分布性, 随着僵尸程序的不断传播, 不断有新的僵尸主机加入到这个网络中来. 控制者利用僵尸网络向僵尸主机下发各种命令以达到攻击的目的. 根据僵尸网络命令与控制的协议的不同, 目前比

较常见的僵尸网络有三种: 基于 IRC 协议的僵尸网络、基于 HTTP 协议的僵尸和基于 P2P 协议的僵尸网络^[2].

2 P2P 型僵尸网络分析

随着 P2P 技术的不但发展, 基于 P2P 协议的僵尸网络也应运而生. 它不同于集中型的 C/S 架构的僵尸网络, 这种僵尸网络没有集中的控制服务器, 每台僵尸主机之间都可以互相接收和传播控制与命令, 因此即使一些僵尸主机被发现或者控制也不会对整个僵尸网络造成太大的影响.

2.1 P2P 型僵尸网络的生命周期

一个典型的 P2P 型僵尸网络的生命周期可以

收稿日期: 2012-03-12; 修回日期: 2012-04-06

基金项目: 中国科学院计算机网络信息中心青年基金项目(CNIC_QN_11003)

划分为以下 5 个阶段:传播阶段、感染阶段、控制阶段、攻击阶段和销毁阶段^[3].

(1) 传播阶段:P2P 型僵尸网络控制者必须拥有一定数量的僵尸主机才能够达到对外攻击的目的,僵尸网络的规模越大,其攻击效果越明显.因此控制者需要制造僵尸程序并传播给受害主机,受害主机一旦感染上僵尸程序后也能够自动对外传播僵尸程序,以达到扩大僵尸网络规模的目的.

(2) 感染阶段:受害主机一旦下载了僵尸程序后会自动执行僵尸程序感染系统,同时受感染的僵尸主机隐藏自身并加入僵尸网络控制与命令通道.

(3) 控制阶段:僵尸主机通过控制与命令通道来获取控制者的指令.对于 P2P 型僵尸网络,获取指令的方法有主动获取和被动接收两种.前者是指僵尸主机定期到某一指定的地点获取指令;后者是控制者将指令发布给某些僵尸主机后,由受控主机按 P2P 的传播方式继续将指令对外传播.

(4) 攻击阶段:僵尸网络控制者利用僵尸网络对某目标网站或主机实施 DDoS 攻击,或者发送大量的垃圾邮件,甚至通过发送含有仿冒 URL 的邮件进行网络钓鱼诈骗等等.

(5) 销毁阶段:有时僵尸网络的控制者为了更好的保护僵尸网络本身而根据僵尸主机的状态主动销毁掉部分僵尸主机.或者僵尸主机通过技术手段被检测出来而人为的销毁.

2.2 P2P 型僵尸网络的特征

P2P 型僵尸网络使用了 P2P 协议,具体表现在它通过 P2P 协议传播僵尸程序扩大僵尸网络规模以及通过 P2P 协议构建僵尸网络控制与命令通信信道^[4].因此 P2P 型僵尸网络的特征除了传统僵尸网络的典型特征以外还同时具有 P2P 网络的许多特征,比如 P2P 僵尸网络中的节点会频繁的加入或者退出以及部分节点的关闭对整个 P2P 僵尸网络不会造成太大的影响.

在 P2P 僵尸网络中,攻击者在某一时刻统一向网络中的僵尸主机发送攻击指令,这使得在同一时刻多台僵尸主机具有相似的网络行为,比如端口扫描、发送垃圾邮件、可执行文件下载、DDoS 攻击等.另外 P2P 僵尸网络还具有在短时间内频繁发送 SYN 包以及 ARP 包请求、周期性的与某些 IP 地址建立连接等 P2P 网络的特征^[5].

3 P2P 僵尸网络数学建模

本文拟研究采用隐马尔可夫模型对 P2P 型僵尸网络进行建模并对其进行检测的方法.

3.1 隐马尔可夫模型

隐马尔可夫模型 (Hidden Markov Models, HMM) 是马尔可夫链的一种,它的状态不能直接观察到,但能通过观测向量序列观察到,每个观测向量都是通过某些概率密度分布表现为各种状态,每一个观测向量是由一个具有相应概率密度分布的状态序列产生^[6]. HMM 是一个双重的随机过程,其中一个有限状态马尔可夫链,它用来描述状态的转移;另一个随机过程用来描述状态与观测值之间的统计对应关系. HMM 可以定义为一个五元组:

$$\lambda = (X, O, A, B, \Pi)$$

$$X = \{S_1, S_2, \dots, S_N\}$$

$$O = \{V_1, V_2, \dots, V_M\}$$

$$A = \{a_{ij} = P(q_{t+1} = S_j | q_t = S_i)\}, i, j \in [1, N]$$

$$B = \{b_j(k) = P(O_t = V_k | q_t = S_j)\},$$

$$j \in [1, N], k \in [1, M]$$

$$\Pi = \{\pi_i = P(q_1 = S_i)\}, i \in [1, N]$$

其中, X 是状态集,一共有 N 个状态,这些状态均满足马尔可夫性质,是马尔可夫模型中隐含表现的状态, q_t 表示在 t 时刻所处的状态, $q_t \in X$; O 表示观察值的集合, M 表示从每一个状态可能输出的不同的观察值的数目; A 是状态转移概率矩阵,表示在当 t 时刻状态为 S_i 的条件下, $t+1$ 时刻跳转为 S_j 的条件概率; B 是观察值的概率分布矩阵,表示在 t 时刻当状态为 S_i 时,观测到的观察值为 V_k 的条件概率; Π 是初始化状态概率分布矩阵,表示初始化时处于状态 S_i 的条件概率. 一般情况下,隐马尔可夫模型可以简化表示为如下的三元组:

$$\lambda = (A, B, \Pi)$$

3.2 建立模型

结合对 P2P 型僵尸网络的生命周期的描述,可以将僵尸主机划分为 4 个状态,其有限状态机如图 1 所示.

僵尸主机有限状态机可以如下描述:

$$M = (Q, \Sigma, \delta, q_0, F)$$

$$Q = \{\text{Normal}, \text{infection}, \text{Active}, \text{Attack}\}$$

$$\Sigma = \{\text{inject}, \text{control}, \text{update}, \text{response}, \text{close}\}$$

$$\delta(\text{Normal}, \text{inject}) = \text{infection}$$

$$\delta(\text{infection}, \text{control}) = \text{Active}$$

$$\delta(\text{Active}, \text{update}) = \text{Active}$$

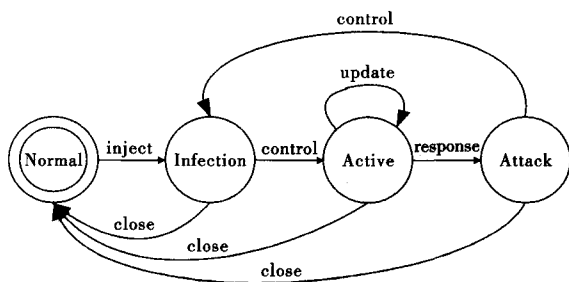


图1 僵尸主机有限状态机

$$\delta(\text{Active}, \text{response}) = \text{Attack}$$

$$\delta(\text{Active}, \text{control}) = \text{infection}$$

$$\delta(\text{infection} | \text{Active} | \text{Attack}, \text{close}) = \text{Normal}$$

$$q_0 = \text{Normal}$$

$$F = \{\text{Attack}\}$$

其中 Q 是有限状态集合; Σ 是有限输入集合, 在任一确定时刻, 有限状态机只能接受一个确定的输入; δ 是状态转移函数; $q_0 \in Q$ 是初始状态; $F \subseteq Q$ 是接受状态。

Normal 态: 表示主机未受僵尸程序感染或者主机上的僵尸程序被关闭或清除时的状态。该状态是主机的正常状态, 可能存在正常的 P2P 行为。

Infection 态: 表示主机被植入僵尸程序时的状态。在该状态下, 主机具有修改注册表、开放特定端口、访问特定 IP 地址、访问特定 URL、扫描特定端口、建立大量的 TCP 连接、发送大量 ARP 请求以及 P2P 行为等异常特征。

Active 态: 表示被感染僵尸程序的主机与其他僵尸主机进行联系和通信的状态。在该状态下, 主机具有周期性的发送更新数据包、周期性访问特定 IP 地址、周期性访问特定 URL、监听特定端口、扫描其他主机漏洞以及 P2P 等异常特征。

Attack 态: 表示僵尸主机接收到控制命令对外发起攻击时的状态, 比如发送垃圾邮件、DDoS 攻击等。

通过分析, P2P 僵尸网络中的僵尸主机的状态变迁也是一个随机的过程, 观察者只能观察到僵尸主机的行为特征或者主机属性, 而僵尸主机的状态并不能直接观察到。另一方面, 僵尸主机的状态变迁过程也符合马尔可夫规则。因此可以利用隐马尔可夫模型对僵尸网络中的僵尸主机的特征行为进行数学建模。

结合隐马尔可夫模型的数学描述和对 P2P 僵尸主机的状态定义, 可以把僵尸主机的 4 个状态看做隐马尔可夫链的状态集 X , 把僵尸主机的行为特

征、网络流量特征、主机属性等看做观察值的集合 O 。在同一个 P2P 僵尸网络中的各僵尸主机应该表现出相似的隐马尔可夫链过程, 因此对 P2P 僵尸主机训练集利用 Baum-Welch 算法迭代寻找使得训练模型似然函数最大化的隐马尔可夫模型参数^[7]。应用聚类算法重复进行这一个过程来对一个给定的僵尸主机构建多个隐马尔可夫模型, 然后将多个隐马尔可夫模型合并为一个最终的混合模型。通过 Viterbi 算法寻找对于一个给定观察值集合 O 和隐马尔可夫模型 λ 最可能的状态序列, 产生最优的模型, 数学表达式可以表示为:

$$\text{class}(O) = \arg\max_c P_{\text{viterbi}}(O, \lambda_c)$$

3.3 检测方法

根据对 P2P 僵尸网络的数学建模, 结合对 P2P 僵尸主机的状态划分, 需要获取检测对象的观察值集合 O , 即主机的基本属性异常特征、网络流量异常特征、网络行为异常特征等。通过比对主机状态转移模型与已训练的 P2P 僵尸网络模型之间的相似度来判断被检测主机是否属于 P2P 僵尸网络。系统结构图如图 2 所示。

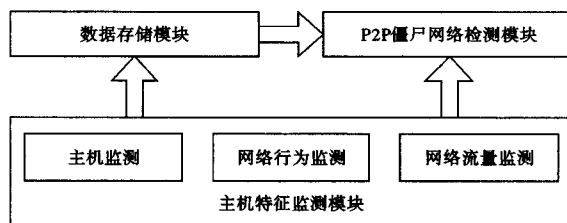


图2 系统结构图

系统主要分为主机特征监测模块、数据存储模块和 P2P 僵尸网络检测模块三大部分。

主机特征监测模块包含主机监测、网络行为监测和网络流量监测三个子模块。主机监测子模块需要部署在监控主机上, 负责记录系统关键文件变化、注册表变化、关键进程变化、端口状态等, 并提取出异常信息作为主机基本属性的异常特征。网络行为监测子模块基于 snort 检测主机产生的异常网络行为, 包括发送垃圾邮件、DDoS 攻击等。网络流量监测子模块基于 netflow 技术对主机的网络流量进行采样, 通过与历史数据比对分析主机的异常流量特征。

数据存储模块存储主机特征监测模块所产生的主机异常特征信息。

P2P 僵尸网络检测模块通过实时获取主机特征监测模块所产生的主机异常特征信息并结合数据存储模块中的历史数据, 通过计算判断该主机是否属

于 P2P 僵尸网络.

4 实验结果

通过对实验环境中的测试主机分别运行 P2P 僵尸程序、其他协议僵尸程序、其他攻击程序、正常 P2P 程序和其他正常程序各 50 种,利用该系统对它们进行检测,结果如表 1 所示.

表 1 P2P 僵尸网络检测结果

检测程序类型	数量	检测结果
P2P 僵尸程序	50	48
其他协议僵尸程序	50	6
其他攻击程序	50	2
正常 P2P 程序	50	4
其他正常程序	50	1

经过计算,利用该方法检测 P2P 僵尸网络的漏报率为 4%,误报率为 6.5%. 经分析,通过增加训练集样本的数量应该能够有效降低系统的漏报率,同时对模型参数的调整可以减少因含有观察特征值的非 P2P 僵尸程序所产生的误报.

5 结束语

本文提出一种 P2P 僵尸网络的检测方法,通过隐马尔可夫模型对 P2P 僵尸网络进行数学建模以检测可疑的僵尸主机. 通过实验评估表明该方法能

够有效的对 P2P 僵尸网络进行检测. 在未来的工作中,将继续研究 P2P 僵尸网络并对模型进行优化,进一步提高检测的效率.

参考文献:

- [1] 国家计算机网络应急技术处理协调中心. 2010 年中国互联网网络安全报告[M]. 北京:电子工业出版社, 2011 年.
- [2] 诸葛建伟, 韩心慧, 周勇林, 等. 僵尸网络研究[J]. 软件学报, 2008, 19(3):702-715.
- [3] Lee WK, Wang C, Dagon D, et al. Botnet detection: countering the largest security threat[J]. New York: Springer-Verlag, 2007, 27(3):25-32.
- [4] 张琛, 王亮, 熊文柱. P2P 僵尸网络的检测技术[J]. 计算机应用, 2010, 30(S1):117-120.
- [5] 周继鹏, 朱良愿. 基于物理网络拓扑的 P2P 系统模型[J]. 微电子学与计算机, 2006, 23(10):65-67.
- [6] 孙永强, 徐昕, 黄遵国. 基于 HMM 的分布式拒绝服务攻击监测方法[J]. 微电子学与计算机, 2006, 23(10):176-186.
- [7] 林果园, 郭山清, 黄皓, 等. 基于动态行为和特征模式的异常检测模型[J]. 计算机学报, 2006, 29(9):1553-1560.

作者简介:

万 巍 男, (1982—), 博士研究生, 工程师. 研究方向为计算机网络安全.

李 俊 男, (1968—), 研究员, 博士生导师.

(上接第 13 页)

- [4] Datta A, Hauswirth M, Aberer K. Updates in highly unreliable, replicated peer-to-peer systems[C]// In Proceedings of the International Conference of Distributed Computing Systems. USA: Rhode Island, 2003.
- [5] Hildrum K, Kubiawicz J, Rao S, et al. Distributed object location in a dynamic network[C]// Proceedings of 14th ACM Symp. on Parallel Algorithms and Architectures (SPAA). Canada: Manitoba, 2002.
- [6] 夏淇. MobiGrid—移动网格的研究[D]. 上海: 上海交通大学, 2006.
- [7] Seung Chul Han, Ye Xia. Optimal leader election

scheme for peer-to-peer applications[C]// Proceedings of the Sixth International Conference on Networking (ICN'07). Sainte-Luce, Martinique, France, 2007: 111-114.

作者简介:

鞠宏军 男, (1973—), 硕士, 副教授. 研究方向为计算机网络及应用.

杜丽娟 女, (1976—), 博士研究生, 副教授. 研究方向为计算机网络及应用.