

基于多智能体社会的僵尸网络协同防御模型

李基初^{1,2}, 唐 俊^{1,2}

(1 同济大学 软件学院, 上海 200092; 2 湖南城建职业技术学院 信息工程系, 湖南 湘潭 411101)

摘 要: 针对现有僵尸网络检测体系结构中协同功能的不足, 给出了一个基于多智能体社会的协同防御模型。模拟多智能体社会中的成员间的协同关系, 设计了侦查、检测与反制三种社会成员角色, 提出了基于协同防御模型的三层协同防御体系。典型案例分析表明本文模型具有较强的可扩展性和可交互性, 可以灵活地部署在各种要保护的网络上, 适应各种应用环境, 具有较好的应用价值。

关键词: 多智能体社会; 僵尸网络; 协同防御模型; 体系结构

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2011)03-0073-04

Study on Collaborative Defence Model of Botnet

LI Ji-chu^{1,2}, TANG Jun^{1,2}

(1 School of Software Engineering, Tongji University, Shanghai 200092, China;

2 Department of Information Engineering, Hunan Urban Construction College, Xiangtan 41110, China)

Abstract: Towards the deficiencies of collaborative functions in existing botnet detection architectures, a collaborative model based on multi-agent social was proposed. Three type roels (track Agent, detection Agent, counterattack Agent) were designed to simulate social roel of multi-agent social, and a botnet collaborative defence architecture on the basis of the proposed model was proposed. The analysis of a representative case indicates that the collaborative model given in this paper has the advantage of good extendibility, interaction, usability.

Key words: multi-agent social; botnet; collaborative defence model; architecture

1 引言

僵尸网络(BotNet), 是互联网上受到黑客集中控制的一群计算机, 往往被黑客用来发起大规模的网络攻击, 如分布式拒绝服务攻击(DDoS)、海量垃圾邮件等, 同时黑客控制的这些计算机所保存的信息也都被黑客随意“取用”。因此, 不论是对网络安全运行还是用户数据安全的保护来说, 僵尸网络都是极具威胁的隐患。然而, 发现一个僵尸网络是非常困难的。根据僵尸网络的命令控制信道是否使用中心服务器可以把僵尸网络分为: 使用基于 IRC 的僵尸网络、基于 Web 的僵尸网络和基于对等网(P2P, peer to peer)的僵尸网络。僵尸网络的命令与控制信道对于僵尸网络非常重要, 只要破解了僵尸网络的命令与控制信道就

可以摧毁整个僵尸网络。目前, 僵尸网络的发现与检测成为了国内外学者研究的热点, 文献[1-3]提出了检测僵尸网络的方法; 但这些检测方法多是针对某一种类型的僵尸网络, 对其他类型的僵尸网络的检测效果可能很差。而多智能体社会具有自主性、分布性、协调性并具有自组织能力、学习能力和推理能力, 在解决实际问题时具有很强的健壮性、可靠性, 并具有较高的求解效率, 已在许多领域得到了成功的应用^[4-6]。基于此, 本文构造了一种基于多智能体社会的僵尸网络协同防御模型。

2 多智能体社会

多智能体社会(multi-agent society, MAS)是由多个可计算的智能体组成的集合^[7]。与单个智能体

收稿日期: 2010-04-16; 修回日期: 2010-07-02

基金项目: 湖南省教育厅资助科研项目(08DX30, 07D018)

相比,MAS有如下特点:(1)每个智能体仅拥有不完全的信息和问题求解能力;(2)不存在全局控制;(3)数据是分散存储和处理的,没有系统级的数据集中处理结构;(4)计算过程是异步、并发或并行的。正如人类群体协作的能力要远远大于个体能力一样,MAS具有比单个智能体更高的智能性和更强的问题求解能力。当前智能体领域的研究也大都集中在MAS身上。

在现实社会当中,人是作为某一种独立体存在其中的,整个社会形成一种以各个独立的人为单位的整体,人与人之间同时存在着相互竞争以及协同合作关系。一般来说,人作为社会中的一个基本单位,总是活动在一定的范围之内,并受到该范围内其它人以及环境对他产生的影响,而这个范围会随着时间的推移发生改变。记社会中的某个人为 a 、 b 和 c ,称其活动的范围为territory,本文给出以下基本概念。

定义 1 设 a 、 b 活动的范围分别记作 $\text{territory}(a)$ 、 $\text{territory}(b)$,若 $\text{territory}(b) \subseteq \text{territory}(a)$,则称 a 认识 b ,记作 $\text{Acq}(a, b)$ 。

定义 2 个体 a 所认识的所有个体构成了个体 a 的局部环境,记作 $LE(a)$ 。

本文认为,局部环境当中的各个个体之间均有可能发生竞争,同时也会发生合作。每次竞争会使强者继续生存,弱者死亡并以一定规则产生一个新的个体来代替死亡个体,新个体会继承原有个体的某些特征;合作可分为成功的和失败的,每次成功的合作均可从对方吸收到某些有利于自己成长的特征,并同时增加两者之间的信任度;而每次失败的合作将会降低两者之间的信任度,下次合作的机会则相对减少。除了合作与竞争之外,个体还可以从其生存环境中得到某些有利于自身发展的特性,同时也会根据个体本身以往所具有的经验来提高自身能量。

基于上述事实,文献[7]引入了一个表示agent之间联系的“熟人关系网模型”,同时对agent之间的信任度关系进行了讨论^[8]。假设一智能体 a 的属性包括: name, address, capability 以及 contact。其中, $\text{name}(a)$ 表示名称; $\text{address}(a)$ 表示联系地址; $\text{capability}(a)$ 用于描述 a 对问题的求解能力; $\text{contact}(a)$ 表示 a 所有熟人通信信息的列表,可表示为 $\text{contact}(a) = \langle l_1, l_2, l_i, \dots, l_m \rangle$, 列表中每一个元素 l_i 称为熟人 i 的联系信息,有 $l_i = \langle \text{name}, \text{address}, \text{trust} \rangle$, 其中 $\text{name}(i)$, $\text{address}(i)$ 和 $\text{trust}(a, i)$ 分别表示熟人 i 的名称,联系地址以及 a 对 i 的信任

度。其中 $\text{trust}(a, i)$ 的取值范围为 $[-1, +1]$,与信任度大的熟人合作,成功的可能性也就越大。

定义 3 个体 a 认为 b 在时刻 t 的信任度为 $\text{trust}(a, b, t)$,规定: $\text{trust}(a, b, t) \in [-1, +1]$;并将初始时刻 $t=0$ 时对 b 的信任度置为0,即 $\text{trust}(a, b, 0) = 0$ 。

agent为了确定熟人的信任度,需从与熟人合作的成功与否来考虑,如果合作成功则给该熟人的信任度增加一个数量值,如果合作失败,则减少一个数量值。为了鼓励agent积极合作,假设在agent社会中,agent遵循“知己难寻,冤家易结”的基本原则确定信任度。设一次失败的合作对agent信任度造成的损失为 γ ,一次成功的合作对agent信任度带来的收益为 δ ,则 $\gamma > \delta$ 。一种简单的信任度确定方法为信任度积累策略,当 a 与 b 合作成功时: $\text{trust}(a, b, t+1) = \text{trust}(a, b, t) + \delta$;当 a 与 b 合作失败时: $\text{trust}(a, b, t+1) = \text{trust}(a, b, t) - \gamma$ 。

3 基于多智能体社会的协同防御模型

基于IRC的僵尸网络和基于Web的僵尸网络采用的是客户服务器模式,即一个僵尸网络由一个控制服务器和多个僵尸客户端组成,对于这两种类型的僵尸网络,防御的重点是检测出控制服务器所在的位置并加以摧毁。而基于对等网(peer to peer, P2P)的僵尸网络采用的是点对点模式,不存在中央控制点,只能采用逐点检测的方法。因此,任何一种检测技术都难以防御所有的僵尸网络,必须采用技术协同作战。协同是确保行为实体共享资源和获取服务、实现复杂问题求解的一种重要技术手段。目前,单位大多是通过一个局域网接入到Internet,对于一个需要保护的单位内网而言,需要建立一个由多个智能体构成的分布式僵尸网络防御系统。分布在不同位置的智能体构成多智能体社会,担任各种社会角色的智能体通过协同能够获取自身所不能获知的信息以及操作自身所不能控制的功能,以便更广泛和更深入地掌控全局情况,综合和精炼所有信息,进而达到更好的检测效果。

僵尸网络协同防御的基本思想:在一个分布式多智能体社会中,根据社会分工为各个智能体指定任务;通过分布网络中多个侦查智能体获取可能存在僵尸网络活动的相关信息,并对这些信息进行汇集处理;然后根据僵尸网络在这些信息中表征出来的内在特性,派遣多种检测智能体去识别并判断出僵尸网络的存在情况,甚至确定攻击者、命令与控制

服务器以及僵尸主机位置;最后反制智能体对检测结果进行处理.结合这个思想,本文提出一个协同模型,在信息收集、特性提取、识别判断上依次进行信息、特性、决策协同,而且协同的级别也是依次升高,如图1所示.

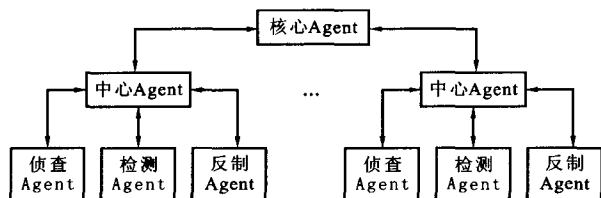


图1 协同防御模型

对该模型说明如下:

(1) 该模型共分为3层:最低层为3种功能的智能体(侦查智能体、检测智能体和反制智能体),每个智能体相当于一个自然人,可以独立地完成特定的功能;中间层为中心智能体,中心智能体相当于一个社区负责人,负责本社区信息的综合管理;最高层是核心智能体,相当于一个城市的最高管理者,主要负责宏观上的调控.

(2) 底层智能体有三种社会分工:侦查、检测和反制.侦查智能体通过各种途径获取因特网上实际存在的僵尸网络命令与控制信道的相关信息,然后模拟成受控的僵尸程序加入僵尸网络中,从而对僵尸网络的内部活动进行观察和跟踪,把收集到的信息及时汇报给中心智能体.检测智能体从中心智能体处获得侦查结果,针对社区僵尸网络内部的工作机制进行有效的检测,确定僵尸网络的破解点.反制智能体则根据检测结果,按照预定的方案清除可能存在的僵尸网络.同一种社会角色的智能体,其实现方式也可能不同,例如有些侦查智能体主要负责跟踪IRC类型的僵尸网络,有些侦查智能体主要负责跟踪P2P类型的僵尸网络.当有新类型僵尸网络出现时,往系统中添加相应的智能体即可,这样就可以有效地实现防御体系功能上的可扩展性.

(3) 中心智能体负责管理本社区智能体的注册、注销、信息汇集处理,并接受核心智能体的宏观调控指令.当本社区添加或删除社区成员时,必须在中心智能体处进行注册或注销工作,以便中心智能体能够掌握本社区成员的确切信息.对收到的多源信息进行融合,并做深度分析检测,同时判断是否需要协同核心智能体,如果需要则根据协同阈值在对应的级别上进行协同.中心智能体是防御体系中的中坚力量,它有5个功能模块:数据融合、关联分析、决策产生、特性提取以及协同服务.中心智能体和底层

智能体在结构上构成一个独立的社区(管理域),这样就保证了整个防御体系具有结构上的可扩展性.当要保护的网路规模扩张时,只需根据需要添加一个或多个社区即可.

(4) 核心智能体

核心智能体为管理员提供一个了解防御系统的可视平台,它能够以直观的形式显示各个社区的工作状态及处理过程中产生的问题;另外,它还为用户提供了一个可操控平台,管理员根据界面显示的决策信息,能够深层次地了解、判断当前僵尸网络活动情况和防御系统工作的状态,进一步做出相应的决策意见,传达给各个中心智能体.

4 模型的实现及部署

图2展示了一个典型的僵尸网络活动环境,包括主干网和区域网.攻击者通过跳板主机直接或间接地向僵尸主机发送控制命令,僵尸主机上的僵尸程序根据接收到的控制命令进行扩散传播、信息窃取、DDoS攻击、发送垃圾邮件等活动.针对这个典型环境,本文的防御系统部署如下:在管理员主机上部署核心智能体;每个管理域(社区)部署一个中心智能体;在蜜罐上部署侦查智能体负责收集捕获社区内的僵尸网络信息,在主要的网络设备(例如路由器)上部署检测智能体,负责收集报文或数据流信息;服务器或者主机上部署的反制智能体负责执行预定清楚僵尸网络的方案.

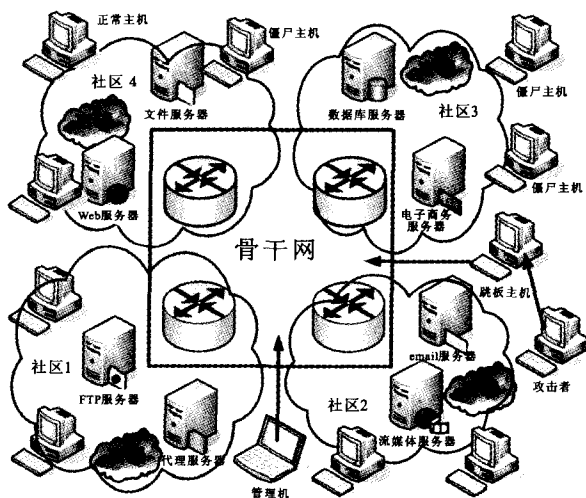


图2 典型的僵尸网络活动环境

为了展示防御体系的工作情况,下面以垃圾邮件发送为例进行说明.图2中,攻击者通过跳板主机命令社区3中僵尸程序帮助查询社区1中僵尸程序使用的域名是否被列入黑名单,如果没有,再操纵这

些僵尸程序向网络中的主机发送垃圾邮件. 社区 3 中的侦查智能体(蜜罐)发现僵尸网络, 检测智能体通过对邮件服务器和受害主机的日志分析, 不仅检测到本社区中的僵尸主机, 中心智能体对信息汇集处理后发给核心智能体(管理机). 然后, 核心智能体向各个中心智能体发送协同检测指令, 各个社区的智能体收到指令后调动本社区的检测智能体结项协同检测, 确定僵尸网络的控制点位置和僵尸主机位置. 最后, 核心智能体发出清除指令, 各个中心智能体收到指令后, 调动本社区的反制智能体清出本社区的僵尸网.

5 结束语

本文针对现有僵尸网络检测体系结构的不足, 提出了一个基于多智能体社会的协同防御模型, 并基于此模型提出一个僵尸网络协同防御体系结构. 该体系结构具有较强的可扩展性和可交互性, 可以灵活地部署在各种要保护的网络上, 适应各种应用环境. 此外, 该协同模型把对僵尸网络的侦查、检测和反制功能融合在一起, 能够对广泛分布的僵尸网络活动做出快速反应.

下一步的研究重点: 实现原型系统, 集成几种典型的检测技术, 并在真实的网络环境中运行, 评估检测结果, 以便对本文提出的协同防御体系结构做出针对性调整; 对于协同, 建立一个合理的关系模型, 并使得其具有局部感知和全局优化的能力, 进而帮助细化协同服务的体系结构.

参考文献:

- [1] Strayer T, Walsh R, Livadas C, et al. Detecting botnets with tight command and control[C]// Proc of the 31st IEEE Conf on Local Computer Networks (LCN' 06). Tampa: IEEE Computer Society Press, 2006: 195-202.
- [2] Livadas C, Walsh B, Lapsley D, et al. Using machine learning techniques to identify botnet traffic[C]// Proceedings 2006 31st IEEE Conference on Local Computer Networks. Tampa, FL: IEEE, 2006: 967-974.
- [3] 应凌云, 冯登国, 苏璞睿. 基于 P2P 的僵尸网络及其防御[J]. 电子学报, 2009, 37(1): 31-37.
- [4] 潘晓英, 焦李成. 项目优化调度的多智能体社会进化算法[J]. 计算机研究与发展, 2008, 45(6): 998-1003.
- [5] 李瑾妹, 刘静, 焦李成, 等. 一种基于多智能体进化的广义图染色算法[J]. 软件学报, 2009, 20(2): 315-326.
- [6] 倪凯. 基于 Agent 的空间数据挖掘研究[J]. 微电子学与计算机, 2007, 24(11): 87-91.
- [7] 赵辉. 基于 MAS 的作战指挥模型的通信技术实现[J]. 微电子学与计算机, 2007, 24(11): 107-109.
- [8] 陈刚, 陆汝钤. 关系网模型: 基于社会合作机制的多 agent 协作组织方法[J]. 计算机研究与发展, 2003, 40(1): 107-114.

作者简介:

李基初 男, (1974-), 硕士研究生, 讲师. 研究方向为人工智能、信息系统安全.

唐俊 男, (1980-), 硕士研究生, 高级工程师, CCF 会员 (E20-0012235M). 研究方向为信息安全、仿生学算法、人工智能等.

(上接第 72 页)

参考文献:

- [1] Tierney J, Rader C M, Gold B. A digital frequency synthesizer[J]. IEEE Trans Audio Electroacoust, 1971 (19): 48-57.
- [2] 李海松, 张奇荣, 权海. DDS 的相位截断及相应的杂散信号分析[J]. 微电子学与计算机, 2006, 23(2): 141-143.
- [3] 马令坤, 张震强, 党宏社. DDS 频率合成器杂散的分析与仿真[J]. 微电子学与计算机, 2007, 24(7): 132-134.
- [4] 蔡剑华, 王先春, 胡惟文. DDS 杂散抑制技术的研究与实现[J]. 微电子学与计算机, 2009, 26(7): 127-133.
- [5] O'Leary, Maloberti P F. A direct-digital synthesizer with improved spectral performance[J]. IEEE Transac-

tions on Communications, 1991, 39: 1046-1048.

- [6] Nicholas H. Samueli T H. An analysis of the output spectrum of direct digital frequency synthesizers in the presence of phase-accumulator truncation[C]// 41st Annual Symposium on Frequency Control. Philadelphia: IEEE, 1987: 495-502.

作者简介:

沈志 男, (1983-), 博士研究生. 研究方向为现代通信信号处理和现代数字信号处理.

王宏远 男, (1946-), 教授, 博士生导师. 研究方向为图像通信、图像信号处理和现代数字信号处理.