文章编号:1008-0570(2011)02-0141-02

# 基于 PDNS 的僵尸网络抽象模型研究与实现

*Research and Implement of Large-scale Botnet Abstract Model on PDNS*

(哈尔滨工业大学) 王轩春 张兆心 李 斌 许 政
WANG Xuan-chun ZHANG Zhao-xin LI Bin XU Zheng

**摘要:** 通过分析 PDNS 内部机制和协议添加的基本原理,以及基于 IRC 协议的僵尸网络传播控制模型,提出了基于 PDNS 的僵尸网络抽象模型。在 PDNS 上实现了僵尸网络与蠕虫、分布式拒绝服务攻击三种安全事件的联合运行,从而较好的模拟了大规模僵尸网络的传播、控制和攻击过程。实验结果表明,基于 PDNS 的僵尸网络模型可根据不同的扫描策略对僵尸网络进行真实模拟,从而为网络安全态势预测与分析提供详细的数据支持。

**关键词:** 僵尸网络; IRC 协议; PDNS
**中图分类号:** TP391.9 **文献标识码:** A

**Abstract:** By analyzing the implementation mechanism and principles of protocol adding of PDNS, and the botnet command controlling and communication on IRC protocol, this paper presents an abstract botnet model on PDNS. The botnet, worm and DDoS security events are combined on PDNS with different strategies, and it can simulate the spreading, controlling and attacking procedure of large-scale botnet easily. Experimental results show that the botnet model on PDNS can predict the botnet according to different scanning strategies, and it can provide specific data support for predicting network security trend.

**Key words:** Botnet; IRC protocol; PDNS

技术创新

## 1 引言

僵尸网络(botnet)是指采用一种或多种传播手段,将大量主机感染为僵尸主机(bot),从而在控制者与被控制者之间形成的一个一对多的控制网络。控制者可以利用拥有的网络集群资源发起多种攻击,例如常见的分布式拒绝服务攻击(DDoS)等。对大规模网络安全事件的模拟及对安全态势的预测已是当前安全领域研究的当务之急, 而在目前的研究中并没有涉及到对于僵尸网络的模拟。

PDNS(Parallel and Distributed Network Simulator)作为当前最流行的分布式并行网络模拟软件, 在模拟大规模网络行为方面具有较大优势,故本文以 PDNS 作为模拟平台。首先,分析当前主流的基于 IRC 协议的僵尸网络传播控制模型,提取其中的参数和扫描方式等。然后,在 PDNS 上实现该模型并允许采用多种扫描策略进行感染。另外,僵尸网络经常与蠕虫、DDoS 相结合发起攻击, 故在此平台上也实现了僵尸网络与蠕虫、DDoS 的联合运行模型。实验结果表明:基于 PDNS 的僵尸网络模型可以根据不同的扫描策略对多种僵尸网络进行真实模拟, 从而为网络安全态势预测与分析提供了详细的数据支持。

## 2 基于 IRC 协议的僵尸网络传播控制模型

目前研究的僵尸网络的传播控制模式主要有基于 IRC、HTTP、P2P 协议的三种模式,而根据研究显示,基于 IRC 协议的僵尸网络仍是主流类型。

基于 IRC 协议的僵尸网络传播控制机制主要包括命令控制模块和节点感染模块两部分。文献给出了基于 IRC 协议的僵尸网络传播控制模型,如图 1 所示。文献指出僵尸网络的传播特性是从蠕虫继承而来的,但又与传统蠕虫的自动扩散不同,僵尸网络的传播一般都

有可控性,但鉴于蠕虫的传播扫描机制,可选取较为适用于僵尸网络的传播策略,如基于目标列表、基于本地优先和随机扫描策略等。

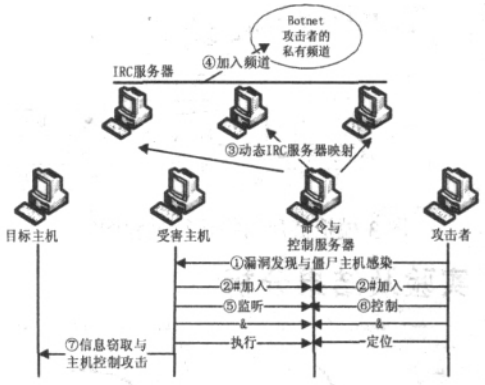


图 1 基于 IRC 协议的僵尸网络传播控制模型

## 3 基于 PDNS 的僵尸网络抽象模型的实现

### 3.1 PDNS 实现机理

PDNS 是在 NS(Network Simulator)的基础上开发的并行/分布式的网络模拟平台, 其体系结构图如图 2 所示。通过图 2 可知,PDNS 使用 libSynk[7]和 RTI 保证了底层的分布式通信,每一个 SIM 上都是由节点集(nodes)和链路集(links)组成的拓扑子图,各 SIM 之间使用远程链路(rlink)来进行连接。每一个 node 是由

王轩春: 硕士研究生

基金项目: 基金申请人: 张兆心; 项目名称: 高性能大规模网络行为模拟系统; 基金颁发部门: 中华人民共和国科学技术部 (2007AA010503)

Classifier、Agent 和 App 三个组件组成，实际上分别对应了 OSI 网络模型中的网络层、传输层和应用层；每一条 link 是由 Queue、Delay 和 TTL 三个组件组成，实际上分别对应着实际链路中的队列、延时和跳步数管理。

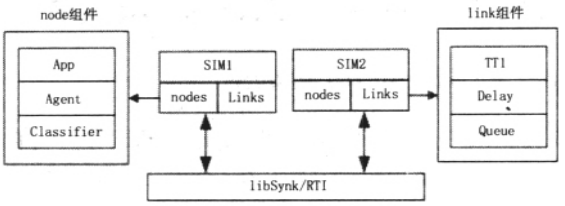


图 2 PDNS 体系结构图

3.2 模型实现

根据图 1，对基于 IRC 协议的僵尸网络在 PDNS 中的实现作了如下的抽象和假设：

(1) 所有频道由 IRC 服务器创建，控制者或者僵尸主机如果被感染需要加入频道；

(2) 主机之间进行包转发时，IP 作为主机标识，不采用昵称(Nick)；

(3) 常见命令控制方式抽象：JOIN、PRIVMSG、PING；

(4) 控制方式使用 IRC 协议的一对多；

根据上述假设，设计的关键主要是对于 IRC 服务器上不同僵尸主机群的维护，在执行的操作中，主要涉及到感染主机添加频道、查询是否该主机已经被感染等操作，因此，设计了一个三层 hash 链表来实现上述操作，时间复杂度在 O(1)即可查询到主机是否被感染。

空间复杂度为 O (n)，n 为在指定的时间内感染的僵尸主机总数。根据假设和数据结构的设计，提出如图 3 所示的按照时间顺序给出的僵尸网络模拟时运行过程图。

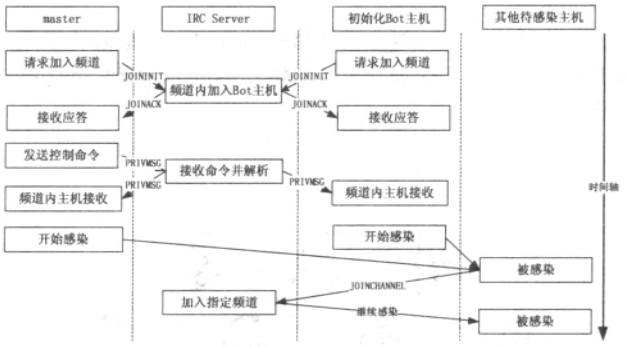


图 3 模拟僵尸网络运行过程图

## 4 实验及结果分析

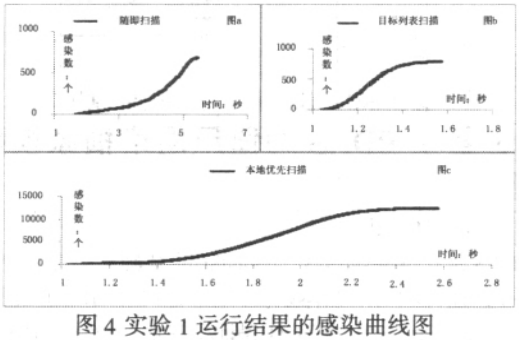


图 4 实验 1 运行结果的感染曲线图

实验环境为两台曙光刀片服务器，2.8GHz 的 CPU，16G 内存，Linux Redhat AS4 操作系统。实验拓扑规模数为 13000。实验 1 共运行了三种不同扫描策略的僵尸网络实例，其中选择初始化的僵尸主机数为 50，模拟时间都为 5 秒。随机扫描的地址范围为 220，目标列表扫描选择的目标为 800 个主机，本地优先扫描概率为 50%。通过图 a~图 c 的三种扫描方式与 “Code-Red Ⅰ”蠕虫[8]的感染曲线相比可知，模拟的趋势大致相似，即初期缓慢增长，中期迅速增长和后期平缓增长的趋势，这说明模拟的结果较为真实。

实验 2 采用了僵尸网络、蠕虫和 DDoS 三种安全事件联合运行的方式：首先，模拟运行僵尸网络 1-5 秒，采用随机扫描策略，指定初始化漏洞主机数为 50，随机扫描范围为 220，并定义控制命令为：在第 5 秒开始采用本地优先的策略执行蠕虫感染，执行本地优先的概率是 50%，执行时间为 3 秒，然后所有被蠕虫感染的主机在第 8 秒开始作为 DDoS 攻击的源，对于某一个目标执行按照恒定速率的攻击，执行时间为 5 秒。图 5 显示了实验 2 的运行结果。

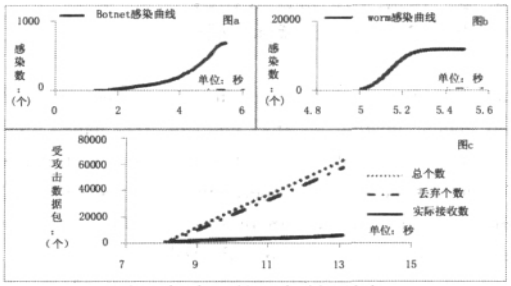


图 5 实验 2 的运行结果图

从图 a 可以看出，从第 1 秒开始，随着时间的增加，感染的僵尸主机数越来越多，按照参数配置，僵尸网络会在第 5 秒时停止感染，此时受感染主机数大约为 800 个，而后如图 b 所示，第 5 秒根据命令开始执行蠕虫感染，并在到 5.5 秒时感染主机数达到 12000，并且在剩下的时间里曲线基本保持平衡。最后如图 c 所示，第 8 秒开始执行对于某一个目标主机的 DDoS 攻击。其中目标主机的承受数据包个数的阈值为 1000，目标节点来链路在第 13 秒共收到 60000 多个包，其中由于目标主机的承受阈值，丢包数量也接近 6 万，实际接收包数维持在 1000。通过实验二进行三者联合运行，可以为网络安全态势预测提供数据支持。

## 5 结论

本文通过分析 PDNS 的内部机制和协议添加的基本原理，以及基于 IRC 协议的僵尸网络传播模型，在 PDNS 上实现了僵尸网络抽象模型并实现了三种安全事件联合运行。实验数据表明，基于 PDNS 的僵尸网络模型可以根据不同的扫描策略进行真实模拟，从而为网络安全态势预测提供了详细的数据支持。

本文作者创新点：提出并实现了基于 PDNS 的僵尸网络抽象模型，较为真实的模拟僵尸网络；与多种安全事件进行联合运行，为网络安全态势提供数据支持。

作者对本文版权全权负责，无抄袭。

参考文献

[1]郑颂武，钱步仁等. IRC 僵尸网络检测方法研究[J]. 微计算机信息. 2010, 4-3:68-69

[2]PDNS -Parallel/Distributed NS. http://www.cc.gatech.edu/ computing/compass/pdns/. 2004

[3]RFC1459. http://irchelp.org/irchelp/text/rfc1459.txt 1993

[4]韩心慧，郭晋鹏，周勇林，诸葛建伟，邹维. 僵尸网络活动调查分析. 通信学报. 2007, 12

(下转第 202 页)

单的协商机制,使得用户可以查看活动空间提供的服务,选择自己感兴趣的服务。

活动参与者第一次访问活动空间时,在同步活动空间数据之前,先通过发现和协商机制获取活动空间提供的活动服务,然后同步活动信息。

客户端调用活动空间 Web 服务的 GetFeatures 方法,服务器返回服务器提供的 Web 服务,在返回数据中,通知客户端服务器服务的特征信息。

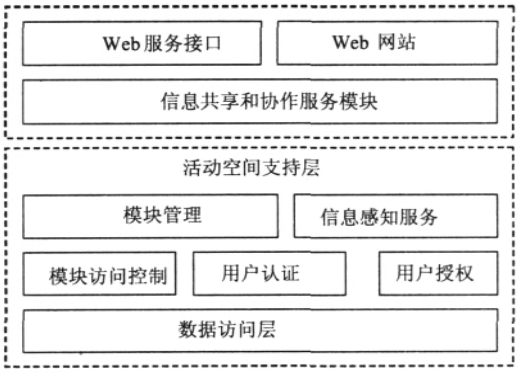


图 5 活动空间的层次结构图

3.3 个人客户端

个人客户端的功能有即时通讯、本地活动管理、联机活动管理、联系人管理、文档管理和工具管理。这些功能结合在一起,提供了对用户活动的管理。

站在用户的视角,活动空间和 ICCS 是透明的,所有活动都是在本地进行和管理的。在整个系统结构中,ICCS 和活动空间服务器是相互独立的,个人客户端把 ICCS 和活动空间服务器联系在一起。所以客户端在以活动为中心的协作平台中起着非常重要的作用。

## 4 结束语

利用计算机进行协作是使用计算机的主题。本文提出了以活动为中心的协作平台模型,实现了一个协作平台的原型系统。该系统还不够全面,需要完善活动模型,增加活动分组功能。还需研究如何管理用户不同活动之间的关系。

本文作者创新点:提出了一种以活动为中心的协作模型,设计与实现了一个协作模型的原型系统。在支持用户协作的同时兼顾了对用户本地的文档和工具的管理。



参考文献

[1]http://www.ccw.com.cn/news2/look/htm2004/20041116_13N50.asp.

[2]史美林.CSCW:计算机支持的协同工作[J]. 通信学报, 1995,16(1):56-57.

[3] http://cscwforum.mmit.stc.sh.cn/Cscwconcept.

[4]Jonathan,Grudin.Computer-supported cooperative work: history and focus.Pages: 19 - 26. 1994.

[5]Jonathan,Grudin. Computer-Supported Cooperative Work and Groupware. 1996.

[6]Workflow Management Coalition Terminology & Glossary (WFMC-TC-1011 Issue 3.0); 1999. David Hollingsworth..

[7]工作流管理联盟工作流标准 2002.7.31

[8]罗海滨,范玉顺,吴澄. 工作流技术综述[J]. 软件学报, 2000,11(7):901-904.

[9]何继江,刘立.基于 B/S 结构的短信息平台架构[J].微计算机信息,2006,22,43.

[10]M. Voorhoeve. Ad-hoc workflow: problems and solutions. 8th International Workshop on Database and Expert Systems Applications. Page: 36.

作者简介:徐长通(1964-),男(汉),河南原阳人,河南师范大学实验师,研究方向:数据库系统

Biography:XU Chang-tong(1964-),male(Han nationality),Yuan Yang,Henan,Experimental division of Henan Normal University, Research field is database system.

(453007 河南 新乡 河南师范大学) 徐长通 李志勇

(Henan Normal University, Henan Xixiang, 453007, China) XU Chang-tong, Li Zhi-yong

通讯地址:(453007 河南省新乡市河南师范大学计算机与信息技术学院) 徐长通

(收稿日期:2010.07.05)(修稿日期:2010.10.05)

(上接第 142 页)

[5] 诸葛建伟, 韩心慧, 周勇林, 叶志远, 邹维. 僵尸网络研究. 软件学报. 2008, 19(3):702-715

[6]Arce I, Levy E. An analysis of the slapper worm. IEEE Security & Privacy, 2003,1(1):82-87

[7]Libsynk.http://www.cc.gatech.edu/fac/kalyan/libsynk.htm. 2005K.

[8]D. Moore, C. Shannon, K. Claffy. Code-Red: A case study on the spread and victims of an Internet worm. The Second Internet Measurement Workshop, 2002:98-106

作者简介:王轩春(1986.01~),男(汉族),山东济宁人,哈尔滨工业大学硕士研究生, 主要研究方向: 网络与信息安全; 张兆心(1979.01~),男(满族),博士,黑龙江哈尔滨人,哈尔滨工业大学副教授,主要研究方向:网络与信息安全; 李斌(1962.10~),男(汉族),黑龙江庆安人,哈尔滨工业大学教授,主要研究方向:网络与信息安全; 许政(1987.01~),女(汉族),山东聊城人,哈尔滨工业大学硕士研究生,主要研究方向:网络与信息安全。

Biography: WANG Xuan-chun(1986.01~), Male (Han nationality). Born in Jining, Shandong Province. Master of Harbin Institute of Technology. Research area: network and information security.

(150001 哈尔滨 哈尔滨工业大学网络与信息安全技术研究中心) 王轩春 张兆心 李斌 许 政

(Network and Information Security Research Center of Harbin Institute of Technology, Harbin 150001, China) WANG Xuan-chun ZHANG Zhao-xin LI Bin XU Zheng

通讯地址:(150001 黑龙江省哈尔滨市南岗区西大直街 92 号哈尔滨工业大学 A16 公寓 608 寝室) 王轩春

(收稿日期:2010.05.28)(修稿日期:2010.08.28)