第26卷 第3期
2011年6月

郑州轻工业学院学报(自然科学版)
JOURNAL OF ZHENGZHOU UNIVERSITY OF LIGHT INDUSTRY(Natural Science)

Vol.26 No.3
Jun. 2011

文章编号:1004-1478(2011)03-0111-05

分布式DoS攻击检测系统的改进研究

马洁[1]， 任平安[1,2]， 马建峰[2]

(1.陕西师范大学 计算机科学学院，陕西 西安 710062；
2.西安电子科技大学 计算机科学学院，陕西 西安 710071)

摘要:为了对抗分布式DoS攻击,提出了一个改进的分布式DoS攻击检测系统:采用贝叶斯方法,根据第一次连接的状态,计算后验概率,据此对系统检测攻能进行改进;采用被动响应的方式,改进系统响应功能,对检测到的入侵行为,进行实时响应.仿真实验表明,该改进措施减少了误报率和漏报率,提高了系统的实时响应性.

关键词:拒绝服务攻击;攻击检测;信息响应;网络安全

中图分类号:TP393.08　　**文献标志码**:A

Improvement research of distributed DoS attack detection system

MA Jie[1], REN Ping-an[1,2], MA Jian-feng[2]

(1. *College of Comp. Sci., Shaanxi Normal Univ., Xi'an* 710062, *China*;
2. *College of Comp. Sci., Xidian Univ., Xi'an* 710071, *China*)

Abstract: An improved distributed denial of service (DDoS) attack detection system was proposed for defending DDoS attack. The system detection was improved using bayesian methods to compute posterior probability and according to the state of the first connection was used. In order to improve system response function, the passive response is used against the intrusions by the real-time response. The result of simulation indicated that the improved system has reduced the rate of false positives and omission, and improved the real-time responsiveness.

Key words: denial of service attacks; attack detection; information response; network security

0 引言

网络的高速发展在丰富我们的生活和学习工作的同时,也给一些别有用心的人以可乘之机,各种病毒、网络攻击层出不穷.拒绝服务攻击DoS(denial of service)以其部署简单、危害巨大、难以防范、难以追踪而成为网络安全头号威胁,其用心就是耗尽系统的带宽,危害程度不亚于黑客盗窃系统关键数据.常见DoS攻击手段有Ping of death, Tear Drop, SYN Flood, Script Flood, Proxy Flood等[1].然而,常用的拒绝服务攻击检测软件,在一定的情况下会出现难以预防和追踪的现象,鉴于此,基于分布式情况,研究了一个分布式DoS攻击检测系统的改进方案.

1 DoS攻击检测系统的体系结构

本文研究的分布式DoS攻击检测系统结构模型是从系统的总体设计上进行考虑的,是对整个系统的高度抽象.本系统按照功能划分为4个部分,即

收稿日期:2011-03-15
基金项目:国家自然科学基金项目(60872041)
作者简介:马洁(1983—),女,新疆维吾尔自治区阜康市人,陕西师范大学硕士研究生,主要研究方向为网络安全.

数据采集模块、协议解码模块、检测分析模块和系统相应模块,系统体系结构如图 1 所示.

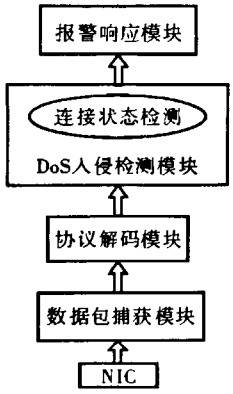

图 1 系统体系结构图

其中,数据采集模块主要是对无线网络内的数据包进行捕获、监听,根据过滤要求进行数据包过滤;协议解码模块对捕获模块捕获并过滤后的原始数据包按照协议结构进行解码,以便于检测分析模块进行入侵分析;检测分析模块对预处理后的数据,通过检测算法对网络流量特征和网络连接状态进行分析和检测,以判断是否有入侵行为;当有入侵行为发生时,调用检测算法检测是否发生了分布式 DoS 攻击;而响应模块则是对确认的入侵行为采取相应的响应.

2 分布式 DoS 攻击检测系统检测功能的改进设计

2.1 存在的问题

通常情况下,分布式 DoS 攻击检测系统只是简单地采用统计某个时间段中的失败 FCC 比率作为分布式 DoS 检测的判据,故误报率和漏报率较大[2].首先,正常主机有可能因为某些原因去访问不可达主机,从而会导致误报;其次,如果检测算法中的失败 FCC 比率为分布式 DoS 开发者获知,则有可能其在分布式 DoS 扫描过程中,插入足够数量的正常连接数据包来逃避检测,导致漏报.

2.2 检测功能的改进思想

本文进行的改进是:采用贝叶斯方法,即利用贝叶斯定理求得后验概率、据此进行决策的方法.通过贝叶斯方法根据第一次连接的状态计算出某主机的后验概率,比较该值与设定阈值之间的关系,来判断该连接的源地址为正常主机还是分布式 DoS 攻击.根据网络数据采集模块捕获的网络数据,在开始建立连接、连接建立、连接拒绝 3 个时刻考察每一个连接.分布式 DoS 检测模块的结构图如图 2 所示.

用贝叶斯公式计算条件概率 $Prob(W|F)$ 和 $Prob(W|S)$,如下式所示:

$$P(\omega_i|x)=\frac{p(x|\omega_i)p(\omega_i)}{p(x)}$$

贝叶斯公式表明了在事件 ω_i 的发生概率为 $p(\omega_i)$ 的前提下,如果事件 x 在事件 ω_i 发生的条件下的条件概率为 $p(x|\omega_i)$,则事件 ω_i 在 x 发生的条件下的条件概率为

$$Prob(W|F)=\frac{Prob(W)\times Prob(F|W)}{Prob(W)\times Prob(F|W)+Prob(B)\times Prob(F|B)}$$

$$Prob(W|S)=\frac{Prob(W)\times Prob(S|W)}{Prob(W)\times Prob(S|W)+Prob(B)\times Prob(S|B)}$$

其中,W 表示主机感染分布式 DoS;B 表示主机未感染 DoS;F 表示该次 FCC 为失败连接;S 表示该次 FCC 为成功连接;$Prob(W)$ 为主机感染分布式 DoS 的概率,初值取 0.5;$Prob(B)=1-Prob(W)$ 为主机未感染分布式 DoS 的概率;$Prob(F|W)$ 为感染分布式 DoS 的主机出现失败 FCC 的概率;$Prob(F|B)$ 为正常主机出现失败 FCC 的概率;$Prob(S|W)=1-Prob(F|W)$ 为感染分布式 DoS 的主机出现成功

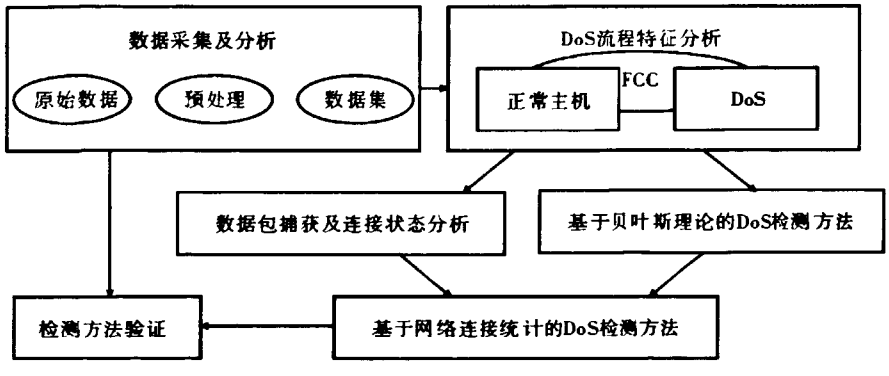

图 2 DoS 检测模块的结构图

FCC 的概率;$Prob(S|B) = 1 - Prob(F|B)$ 为正常主机出现成功 FCC 的概率.

2.3 检测功能的算法描述

具体检测算法如下:

1)初始化主机使分布式 DoS 的概率 $Prob(W) = 0.5$;

2)考察某个连接,其源地址 Orig,目标地址 Dest,检查该源地址是否已经在分布式 DoS 列表中,若在,则放弃对该连接的考察;

3)检查该目标地址 Dest 是否在该 Orig 的第一次连接地址列表 PCDL 中:若在,则放弃对该连接进一步的处理;否则,该连接是一个第一次连接 FCC,且该 Dest 被加入 PCDL 中;

4)FCC 至少属于下面的一种情况,认为是失败的,否则,认为该连接是成功的:Orig 状态为发送 SYN 包,Dest 状态为初始状态;Orig 状态为发送 SYN 包或者 SYN + ACK 包,Dest 状态为 RESET;Orig 状态为 RESET,Dest 状态为初始状态或者半连接状态,并且 Dest 发送字节数和为 0;

5)如果该 FCC 为失败连接,计算 $Prob(W|F)$;

6)若计算出的 $Prob(W|F) > \alpha$,则该主机是 DoS,产生报警,并且将该主机加入 DoS 列表中;如果 $Prob(W|F)$ 在 α 和 β 之间,则 $Prob(W) = Prob(W|F)$;如果该 FCC 为成功连接,则计算 $Prob(W|S)$;

7)若计算出的 $Prob(W|S) < \beta$,则该主机被认为是正常主机,且其 $Prob(W)$ 被重新设置为 0.5;若 $Prob(W|S)$ 在 α 和 β 之间,则 $Prob(W) = Prob(W|S)$;转到步骤 2).

3 分布式 DoS 攻击检测系统响应功能的改进设计

3.1 存在的问题

通常情况下,分布式 DoS 攻击检测系统的响应都是采用主动响应方式,系统自动地或以用户设置的方式来阻断攻击过程或以其他方式影响攻击过程. 它能够阻止正在进行的攻击,使得攻击者不能够继续访问[3]. 但主动响应方式的分布式 DoS 系统在检测到攻击时会对攻击者进行反击,这种响应存在一定风险,有可能影响网络上的无辜用户.

3.2 响应功能的改进设计

本系统采用被动响应的方式,被动响应根据危险程度高低的次序提交用户. 本文研究的分布式 DoS 攻击检测系统中的响应功能模块对检测到的入侵行为,进行实时的响应. 当发现有入侵行为时,调用报警程序完成报警任务,并且写入日志记录下相关信息,如图 3 所示.

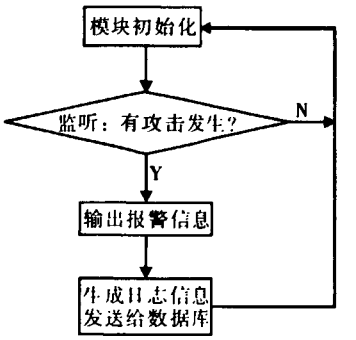

图 3　响应模块的工作流程

在系统工作时,分布式 DoS 攻击检测系统的网络接口应该只响应这样的 2 种数据包:一个是数据包的目标 MAC 地址和本地网络接口相匹配;另一个是数据包的目标 MAC 地址具有"广播地址". 其他数据包将被网络接口抛弃,同样,在网络层将判断该数据包的目标 IP 地址是否为本机所绑定的 IP 地址,如果不是,也将被丢弃. 只有符合自己 IP 地址的数据包,才交给传输层进行处理. 在传输层中,将判断该包对应的 TCP 或者 UDP 目标端口是否在本机已经打开,如果是,则向相应的应用层提交包中的数据,否则也抛弃这些包.

因此,要响应到流经的所有的数据包,必须绕过系统正常的处理机制,直接访问网络的链路层. 首先将网卡工作模式置于混杂(Promiscuous)模式,当网络接口处于这种"混杂"方式时,该网络接口具备"广播地址"的作用,它将提醒操作系统处理流经该物理媒体的每一个数据包. 操作系统将直接访问数据链路层,响应相关数据,并由应用程序而非上层如网络层、传输层协议对数据进行过滤处理. 这样,就可以响应流经网卡的所有数据链路层的数据.

4 分布式 DoS 攻击检测系统的实验分析

4.1 系统的实验环境

本文利用 OPNET 平台将局域网分为节点模型和进程模型 2 个部分:节点模型描述各类通信节点的内部功能模块,如发送和接收;进程模型用于确定节点对数据的处理方式和处理过程,如信息流的生成、存储、排队和传输[4].

1)节点模型.为分析各通信节点MAC层的接入和传输,简化对MAC层之上的各OSI通信层的建模,用1个源模块(Source)和1个接收模块(Sink)模拟高层的通信.MAC层和物理层的LAN模型由lan_mac process(MAC进程),transmitter(发射机),receiver(接收机)和channel streams(信道流)构成[5].网络中各节点的模型结构相同,如图4所示.

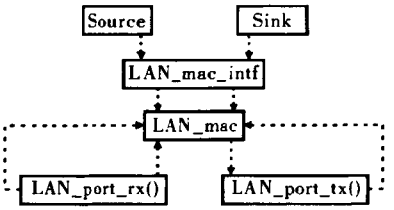

图4 MAC节点模型

2)进程模型.进程模型用于具体实现节点模型中各个模块的功能.利用OPNET仿真内核提供的核心函数族packet package,interrupt package,queue package等,实现数据包的创建、分发、接收和销毁,数据包字段设置,队列和列表的创建,信息包的插入、换位、取出和删除,中断的创建等功能.进程实现采用C++编程.

4.2 系统的仿真过程

建立如图5所示的DoS仿真实验拓扑结构.

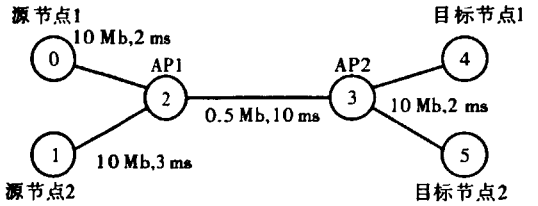

图5 仿真拓扑图

图5中的源端节点分别产生FTP和CBR(Constant Bytes)数据流,经由中间节点到达终端.2个AP之间为瓶颈链路,假设拓扑结构中瓶颈链路的带宽和延迟为0.5 Mb/s和10 ms,其他链路带宽设为10 Mb/s,传输延迟分别为3 ms和2 ms.在仿真实验中,将普通的数据包长度设置为500 B.

```
#设置CBR流(按照一个确定的速率产生数据,分组的长度为一常数值)
proc new-cbr{src dst pktSize rate fid startTime{stopTime -1}}{
global ns
set udp[ $ns create-connection UDP $src Null $dst $fid]
set cbr[ $udp attach-app traffic/CBR]
.....}
return $cbr}
#设置源端发送的数据流
new-cbr $node_(s0) $node_(d0)500 0.12 Mb 1 0.1
```

在源节点1和目标节点1之间产生1个数据流标签为1,数据包长度为500 B,发送速率为0.12 Mb/s的CBR数据流,并且在0.1 s的时候开始发送.

```
new - tcp $node_(s0) $node_(d0)500 10 2 1.2
```

在源节点1和目标节点2之间产生1个数据流标签为2,数据包长度为500 B,发送窗口大小为10的FTP数据流,并且在1.2 s的时候开始发送.

```
#bad traffic,设置DoS攻击数据流
set cbr_[new-cbr $node_(s0) $node_(d1)500 0.1 Mb 5 0.0
```

从仿真一开始就在源节点2和目标节点2之间产生1个数据流标签为5的CBR流作为攻击数据流.

```
new-cbr $node_(s0) $node_(d1)500 0.05 Mb 5 14.0 38.0
new-cbr $node_(s0) $node_(d1)500 0.05 Mb 5 15.0 37.0
.....
```

在IP网络中,拥塞控制一般是通过路由器的队列管理来进行的,网络完全依靠末端主机来对拥塞做出反应,并且它希望数据流在丢包后减小它们的速度(称之为反应流).问题是,恶意的数据流在发生丢包后并不降低它们的发送速率,充满了路由器的缓冲区,剥夺了其他的数据流的带宽(称之为无反应流).给予这一网络行为,在OPNET中模拟DoS攻击,就是在发生拥塞的情况下,不断地增加源端发送的数据包,即从13 s开始,不断地增加源节点2和目标节点2之间数据流标签为5的CBR流,以此作为仿真的攻击数据源.

4.3 系统的测试结果

实验中的攻击类型选取SYN flood,攻击数据利用Synflooder工具产生,以根据需要产生不同攻击速率和不同时间长度的攻击数据,实现对模拟的DoS攻击进行检测[6].检测性能指标如表1所示.

通过分析表1中的数据,可以得出该检测算法对于攻击速率比较高(30次/s)的DoS攻击检测较为准确.由于实际网络中发生DoS攻击时,攻击速率远远高于30次/s,因此该算法对于现实中的DoS攻击是有效的;同时,检测算法能够在20 s(2个时间片段)内检测出DoS攻击,具有较好的实时性.

实验中采用以下2个参数来描述系统的性能:

表1　SYN 洪泛攻击检测性能

ID	攻击速率 /(次·s^{-1})	持续时间 /s	检测时间 /s	检测率 /%
1	5	20	0	0
2	10	32	0	0
3	15	31	0	0
4	30	30	6	85.7
5	100	30	10	93.5
6	500	22	14	95.1
7	3 000	23	8	97.0

误报率 FPR(false positive rate) =
正常连接误报为异常连接的数目/正常连接总数目
检测率 DR(detection rate) =
已检测出来的异常连接的数目/异常连接总数目

记录结果如图6所示.

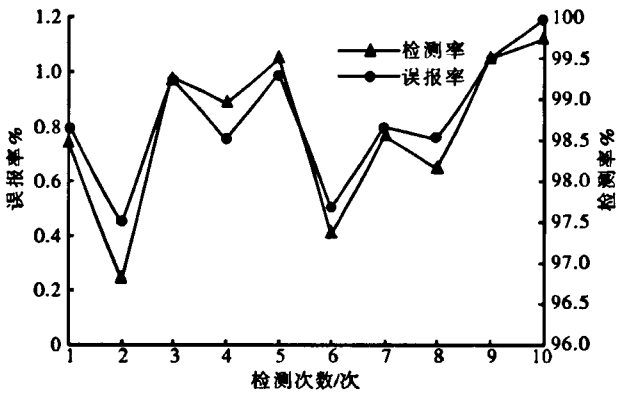

图6　误报率、检测率与检测次数关系图

从图6中可以看到误报率控制在2%以下时，检测率可达95%以上，与其他的检测算法相比性能有很大的提高.

5　结语

分布式 DoS 攻击危害巨大，为了对抗分布式 DoS 攻击，本文提出了一个改进的分布式 Dos 攻击检测系统，该分布式 DoS 攻击检测可以有效提高攻击检测的实时性与准确率.

1)通过贝叶斯方法根据第一次连接的状态计算出某主机的后验概率，比较该值与设定阈值之间关系，据此进行决策，从而减少分布式 DoS 攻击检测系统的误报率和漏报率.

2)采用被动响应的方式，根据分布式 DoS 攻击的危险程度高低次序提交用户，从而避免反击响应造成的网络风险.

参考文献：

[1] 刘滨，位绍文. 我国入侵检测系统(IDS)研究综述[C]//全国计算机安全学术交流会论文集(第24卷)，合肥：中国科学技术大学出版社，2009：213-216.

[2] 陈伟，何炎祥，彭文灵. 一种轻量级的拒绝服务攻击检测方法[J]. 计算机学报，2006(8)：78.

[3] 李一兵，黄旭. 一种改进的 DDoS 攻击综合防御系统[J]. 计算机应用研究，2009(6)：174.

[4] Li Xiangyang, Ye Nong. A supervised clustering algorithm for computer intrusion detection[J]. Knowledge and Infor Syst, 2005, 8(4): 44.

[5] 高能，冯登国，向继. 一种基于数据挖掘的拒绝服务攻击检测技术[J]. 计算机学报，2006(6)：77.

[6] Demirkol I, Alagoz F, Delic H, et al. Wireless sensor networks for intrusion detection: packet traffic modeling[J]. IEEE Com Letters, 2006, 10(1): 22.