第34卷 第14期 计 算 机 工 程 2008年7月
Vol.34 No.14 Computer Engineering July 2008
·博士论文· 文章编号：1000—3428(2008)14—0023—03 文献标识码：A 中图分类号：TP393.08

IPv6中的DoS/DDoS攻击流量突发检测算法

杨新宇[1]，李 磊[1]，张国栋[2]
(1. 西安交通大学计算机科学与技术系，西安 710049；2. 上海浦东发展银行总行产品开发部，上海 200233)

摘 要：IPv6下的安全体系结构IPSec对IPv6网络的安全起到了一定的作用，但是它对某些特殊攻击的防范，例如泛洪DoS/DDoS攻击，却无能为力。该文通过对IPv6中泛洪DoS/DDoS攻击发生时的流量特征的分析，对基于网络流量突发变化的DoS/DDoS攻击检测算法在IPv6下的应用进行研究，分别用Matlab和NS-2对算法进行有效性和可行性验证。结果表明，突发流量检测算法在IPv6环境中运行良好。
关键词：IPv6协议；DoS/DDoS攻击；流量突发检测

DoS/DDoS Traffic Burst Detecting Algorithm in IPv6

YANG Xin-yu[1], LI Lei[1], ZHANG Guo-dong[2]
(1. Dept. of Computer Science & Technology, Xi'an Jiaotong University, Xi'an 710049;
2. Innovation & Promotion Dept., Shanghai Pudong Development Bank, Shanghai 200233)

【Abstract】The IPv6 security architecture, IPSec, plays a positive role in the protection of IPv6 networks. To some special attacks, especially DDoS attacks, IPSec appears relatively weak. By analyzing the flow characteristics when IPv6 flooding DoS/DDoS attack occurred, it studies the flooding DoS/DDoS detecting algorithm based on traffic burst used in IPv6. Experiments in Matlab and NS-2 show the detection algorithm can be very good in IPv6 environment for application.
【Key words】 IPv6 protocol; DoS/DDoS attack; traffic burst detecting

1 概述

随着互联网的发展，IPv6[1]必然取代IPv4 而成为下一代互联网协议。相应地，IPv6网络的安全问题也成为下一代互联网研究的关键问题。

拒绝服务攻击(Denial of Service, DoS)和分布式拒绝服务攻击(Distributed Denial of Service, DDoS)以其易实施、破坏力强和难以追踪的特点成为互联网的主要威胁。它的主要目标是在一定时间内彻底使被攻击的网络丧失正常服务功能[2]。DoS/DDoS攻击在IPv6网络中依然存在，IPv6中的DoS/DDoS攻击主要有与邻居发现协议[3-4]有关的DoS/DDoS攻击和泛洪DoS/DDoS攻击。IPSec[5]可以较好地对与邻居发现协议有关的DoS/DDoS攻击进行防御，但是对于泛洪DoS/DDoS攻击却无能为力[6]。因此，需要对泛洪DoS/DDoS攻击进行检测，以便在攻击发生的时候进行防御。

本文针对IPSec不能对IPv6下的泛洪DoS/DDoS攻击完全进行很好的防御，甚至会加大攻击的影响这一问题，根据泛洪DoS/DDoS攻击发生时的流量特征对基于网络流量突发变化的DoS/DDoS攻击检测算法在IPv6下的应用进行研究。

2 IPv6中的DoS/DDoS攻击

2.1 IPv6中与邻居发现有关的DoS/DDoS攻击

IPv6中的邻居发现协议引入了新的DoS/DDoS攻击，通过实验对这些新引入的DoS/DDoS攻击的有效性进行验证[6]，主要有如下几种：

(1)邻居请求/通告欺骗。攻击主机发送一个伪造的邻居请求，其中伪造攻击主机的链路层地址，将这个地址设置为其他合法主机的地址或者一个不存在的地址，这样被攻击主机就会发送相应的邻居通告消息到那个伪造的链路层地址上。

(2)邻居不可达检测。恶意节点发送假的邻居通告响应邻居不可达检测过程中的邻居请求消息，使发送请求的节点误以为它请求的节点可达。

(3)地址重复检测。在主机通过无状态地址自动配置获得地址进入网络的这类网络中，攻击节点可以通过响应欲进入网络的主机的每个重复地址检测来发动拒绝攻击。

(4)“杀死”缺省路由器。这种攻击中，攻击者“杀死”缺省路由器，使得链路上的节点认为所有节点都是本地的(如果发送方节点的缺省路由器列表为空，就假设目的节点在本地)。

(5)欺骗性重定向消息。重定向消息的作用是把给定目的地的数据包发送到链路上任意的链路层地址。

2.2 IPSec与DoS/DDoS攻击

IPSec是IPv6的一个必要组成部分，为IPv6提供了一定的安全保护。在配置了IPSec的IPv6网络中，当进行数据传输的时候，两台进行通信的主机就会对它们通信的数据进行加密和认证。这个时候网络的安全性能有了较大的提高，单纯通过伪造数据包的DoS/DDoS攻击就达不到攻击的效果。为了在IPv6网络中可以安全地访问，IPSec对每一个数据报都要进行加密、解密和认证等工作，但是这样就使得网络性能受到了损失。IPSec在进行这些工作的同时也需要耗费大量的系统资源，那么主机的网络处理能力也就相应降低了。当攻击主机使用伪造数据报的泛洪DoS/DDoS攻击对配置了IPSec的被攻击主机进行攻击的时候，被攻击主机可以对伪

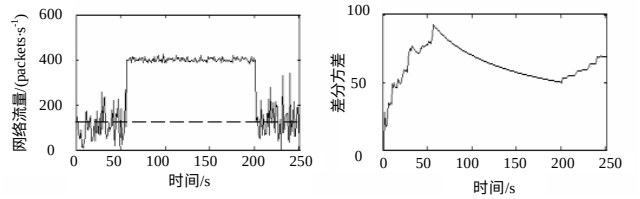
基金项目：国家自然科学基金资助项目(60403028)；陕西省自然科学基金资助项目(2004F43)
作者简介：杨新宇(1973－)，男，教授、博士，主研方向：计算机网络安全；李 磊，硕士研究生；张国栋，工程师、硕士
收稿日期：2007-08-03 **E-mail：**yxyphd@mail.xjtu.edu.cn

造数据报所造成的攻击，比如重复地址检测等攻击进行防御。但是因为伪造数据报的数量太多，被攻击主机就会花费大量的时间和资源来处理这些无用的数据，这样不但对泛洪攻击无能为力，甚至还会因为对伪造数据报进行检验而耗费大量的资源，加大了攻击对主机的影响。所以即使配置了 IPSec 协议，还是不能对 DoS/DDoS 攻击完全进行防御。所以本文对基于网络流量突发检测的 DoS/DDoS 攻击检测算法在 IPv6 中的应用进行了研究。

3 DoS/DDoS 攻击检测算法在 IPv6 中的应用

3.1 IPv6 下泛洪 DoS/DDoS 攻击发生时的流量特点

实验室用一台 IPv6 下的 FTP 服务器作为被攻击主机，用于观察泛洪 DoS/DDoS 攻击发生时的流量特征。图 1(a)为其网络流量测量数据，测量长度为 250 s。在第 57 s 对服务器进行 IPv6 下泛洪 DoS/DDoS 攻击，在当主机受到此类拒绝服务攻击时，到达主机的流量表现出与正常流量不同的统计特征。正常情况下，流量的上下波动比较大，且流量均值小于被攻击主机的饱和状态；当受到泛洪 DoS/DDoS 攻击时，流量发生突增，然后在一段时间内趋于平稳。结合统计量来描述，就是攻击时的流量测量值远大于平常的流量的整体平均值，并且流量的方差在流量突发后的局部范围内呈现减少的趋势。图 1(a)中，实线和虚线分别代表实际流量和平均流量。可以看出在攻击过程中，实际流量远高于平均流量，而正常情况下实际流量在平均流量周围波动。图 1(b)是数据的差分方差，可以看出它在攻击过程中的减小趋势。



(a)IPv6 下的攻击流量　　(b)流量差分方差

图 1　IPv6 下 Dos/DDoS 攻击发生时的流量特点

3.2 基于网络流量突发检测的 DoS/DDoS 攻击检测算法

文献[7]通过研究和实验提出一种基于网络流量突发变化的 DoS/DDoS 攻击的检测算法。该算法在 IPv4 下对泛洪 DoS/DDoS 攻击有着较好的检测效果，但在 IPv6 中的应用还需要进一步试验。通过对 IPv6 下的泛洪 DoS/DDoS 攻击发生时的流量特征进行分析，用所采集的流量数据对检测算法在 IPv6 中的应用进行实验和研究。

3.2.1 统计量的计算

假设在 t 时刻，原始流量为 $C(t)$，整体均值(所有 $i \le t$ 时刻 $C(i)$的均值)为 $c\_mean(t)$，流量的差分值为 $z(t)$，差分方差(所有 $i \le t$ 时刻 $z(i)$的方差)为 $d\_var(t)$，$z(t)$的均值可认为是 0，记为 $d\_mean(t)$。对统计量的计算如下：

$$(1)\ c\_mean(t)=\frac{1}{t}((t-1)\times c\_mean(t-1)+C(t))$$

$$(2)\ z(t)=C(t)-C(t-1)\quad \text{其中}(t>1)$$

$$(3)\ d\_var(t)=\frac{1}{t-1}\sum_{i=2}^{t}(z(i)-d\_mean(t))^2=$$

$$\frac{1}{t-1}\sum_{i=2}^{t}z(i)^2=$$

$$\frac{1}{t-1}(\sum_{i=2}^{t-1}z(i)^2+z(t)^2)=$$

$$\frac{1}{t-1}((t-2)\times d\_var(t-1)+z(t)^2)$$

(4)为了衡量 t 时刻流量的大小，定义函数 $\mu(t)$

$$\mu(t)=\begin{cases}0 & C(t)<lt\times c\_mean(t)\\ \dfrac{C(t)}{(ht-lt)\times c\_mean(t)}-\dfrac{lt}{ht-lt} & C(t)\in[lt\times c\_mean(t),ht\times c\_mean(t)]\\ 1 & C(t)>ht\times c\_mean(t)\end{cases}$$

其中，$lt \times c_mean(t)$表示认为流量“大”的下限，即当流量小于平均流量的 1/lt 时，流量不大，即流量隶属于“大”的程度为 0。区间[$lt \times c\_mean(t)$, $ht \times c\_mean(t)$]的意义是当流量 $C(t)$属于这个区间时认为流量“大”的程度由函数 $\mu(t)=\dfrac{C(t)}{(ht-lt)\times c\_mean(t)}-\dfrac{lt}{ht-lt}$ 来定义。$ht \times c_mean(t)$表示能够忍受的流量的上限，当流量超过平均流量的 ht 倍时，流量很大，即流量隶属于“大”的程度为 1。在应用中，参数 lt 和 ht 应该根据实际网络情况定义，例如根据长期的网络流量采集数据规定。

3.2.2 攻击的判定

根据 $\mu(t)$的定义，认为当 $\mu(t) = 0$ 时没有攻击发生，如果 t 时刻 $\mu(t) > 0$，可能是攻击的开始，此时启动攻击判定过程，以确认攻击的发生。

算法流程如图 2 所示。

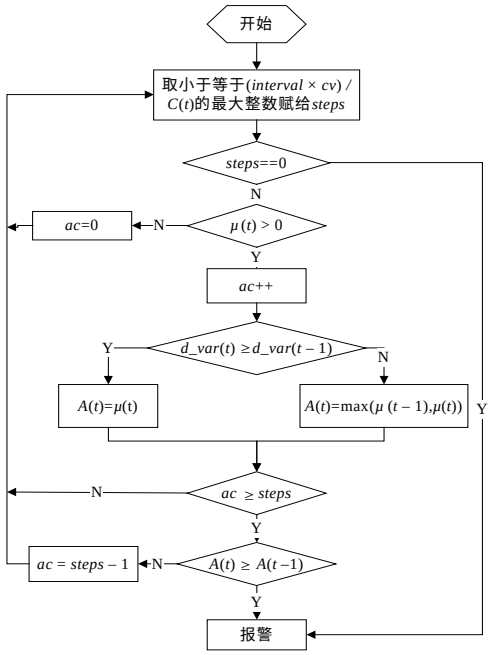


图 2　攻击判定的流程

算法描述如下，其中有 2 个预定义的变量：$interval$ 表示检测周期；cv(代表主机能承受的流量上限。对检测周期中的每个时间片 t，$A(t)$代表该时间片的攻击强度。令 $steps$ 为小于($cv \times interval$) / $C(t)$的最大整数。参数 ac 和 $steps$ 配合决定何时报警。判定过程启动后，ac 按下面的规则计算：如果攻击强度隶属于“大”ac 自增 1，否则设置为 0 如果($A(t) < A(t\text{-}1)$), ac 置为 $steps$-1，若 ac 的值达到或超过 $steps$ 则报警。

$interval \times cv$ 表示单位时间的处理能力，$steps$ 表示主机可以允许当前的流量强度持续多少时间周期，因此，把小于等于($interval \times cv$)/$C(t)$的最大整数赋值给 $steps$，如果发生大流量的脉冲攻击或闪电拥塞，$C(t)$会极大(超过 $interval \times cv$)，这导致 $steps$ 等于 0，将立即报警。当 $\mu(t)$>0，流量隶属于“大”，说明发生了流量突增，可能是攻击的开始，ac 增加 1。如果 t 时刻差分方差相对 t–1 时刻变大或不变，说明流量波动程度没有降低，有两种可能引起流量波动：流量增大，此时 $\mu(t) \ge$

$\mu(t-1)$，攻击可能性增大，$\mu(t)$取 μ 值较大者即 $\mu(t)$；流量减小，此时 $\mu(t) < \mu(t-1)$，攻击可能性减小，$\mu(t)$取 μ 值较小者，也为 $\mu(t)$；如果差分方差变小，说明流量趋于平稳，攻击可能性增大，因此 $A(t)$取 μ 值较大者。如果流量不隶属于“大”，将 ac 赋值为 0，程序进入下一个检测周期。当 $ac \geq steps$ 和 $A(t) \geq A(t-1)$同时发生，说明攻击可能性在 $steps$ 个周期内持续增加或者至少保持不变，而且这种可能仍有增加趋势，所以发出报警；如果 $ac \geq steps$ 但是 $A(t) < A(t-1)$，说明尽管攻击可能性已经增加或维持了一段时间，它在 t 时刻有所下降，因此，程序继续观察，等待进一步确认。

3.3 实验结果和讨论

通过对采集的数据进行分析，可以看出在 IPv6 下的泛洪 DoS/DDoS 攻击发生时候的流量特征与在 IPv4 下攻击发生时的流量特征十分相似，因此，可以把检测算法应用在 IPv6 中。在 Matlab 下对算法在 IPv6 下的应用进行了验证。

在实验中，笔者以 1 s为一个检测周期，参数cv = 1 200, lt = 2.5, ht = 3.5，这是通过实验选择的检测效果比较好的值。检测结果如下：起始时刻为 57 s；检测到的时刻为 59 s；检测延迟为 2 s。

从检测结果中可以看出，在 57 s 时，发生了泛洪 DoS/DDoS 攻击，检测算法在 2 s 的延迟后发现了攻击，从算法中可以看出延迟是肯定存在的，但是延迟的时间是可以接受的。所以检测算法可以较好地在 IPv6 环境中检测出攻击。

3.4 IPv6 中的应用

由于 IPSec 无法防御泛洪 DoS/DDoS 攻击，所以需要在 IPv6 下引入基于网络流量突发检测的 DoS/DDoS 攻击检测算法，主要用于对泛洪 DoS/DDoS 攻击的快速发现和报警。因为在检测的时候所使用的数据是实时的数据，所以在检测攻击的时候会有一定的延迟，但是在 IPv6 网络中因为 IPSec 的存在，网络安全受到一定的保护，此时网络的性能也就有所损失，在这种情况下，延迟也就不会表现得明显。在应用的时候可以根据当时的网络情况对参数进行不断的选择设置，缩短检测周期、选择合适的参数、提高检测的速度和准确率。

4 IPv6 中检测算法的仿真实验

4.1 实验设计

本实验在 NS-2 模拟仿真工具中进行。实验拓扑如图 3 所示。在 IPv6 网络中，节点 0 是被攻击主机节点，节点 1 是正常节点，节点 2~节点 5 节点分别是在不同时刻运用即插即入特性接入到网络中的攻击主机节点，这 4 个节点分别在不同的时刻发动 UDP-Flooding 攻击，节点 0 绑定攻击检测代理(detect_agent)对攻击进行检测。

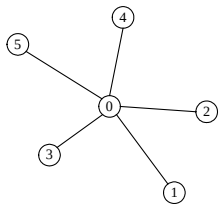


图 3 NS-2 仿真实验拓扑

具体实验步骤为：

(1)0.5 s 时，正常主机节点 1 通过 CBR 流量发生器发送数据包到节点 0。

(2)2 s 时，攻击主机节点 2 发动泛洪 DoS 攻击，流量由一个突然的加大并持续 3 s。

(3)之后其他几个攻击主节点依次发动泛洪 DoS 攻击，每个攻击均持续一段时间，这样不但是对 IPv6 网络中即插即用性质的实现，同时也是对发生不同攻击时的检测性能进行比较。

(4)16 s 时，仿真结束。

在实验中最主要的就是攻击检测代理，这是对流量突发检测算法的实现，完成了对 IPv6 下泛洪 DoS/DDoS 攻击的检测。核心代码如下：

```
/*判断攻击*/
ugti = ugt(flow_now_, flow_u_now);
if (flow_now_>0)
//计算主机可以允许当前的流量强度持续多少时间周期
     accumulate_steps=
     (int)floor(accumulate_volume*interval_/flow_now_);
else
    accumulate_steps = INFINITY;
if ( ugti>0 ) {//ugti 为隶属度
    a_count=a_count+1;
    if ( var_now > var_former )
       Ai=ugti;
    else
    Ai=MAX(ugti_1, ugti);}
else {a_count=0;
if (alarm_== TRUE)
     alarm_= FALSE;}
if (a_count>=accumulate_steps){
if (Ai>=Ai_1){
            //流量持续增加或保持不变，攻击有可能发生
if (alarm_==FALSE){alarm_=TRUE;
    cout << local_time <<" attack detected!" << endl;}
else a_count=accumulate_steps-1;
//攻击可能发生，但是流量有所降低，需要进一步观察}}
```

4.2 实验结果

通过进行多组实验，选择其中最有代表性的一组对实验结果进行讨论。表 2 显示了不同突发程度(实验中用攻击强度来反映)下的检测结果。设定节点正常连接时的速率为 20 packet/s，攻击的强度变化如表 1 所示。检测参数是：cv = 400, lt = 2.5, ht = 3.5。

表 1 实验检测效果

每个节点的攻击强度/(packet·s^{-1})	攻击开始的时间/s	检测到攻击的时间/s	延迟/s
200	2	2.2	0.2
160	5.5	5.7	0.2
100	9	9.3	0.3
60	12.5	12.8	0.3

从表 1 中还可以看出，检测算法对不同突发强度的敏感程度，攻击速率越高，算法响应越快。

5 结束语

本文阐述了在 IPv6 下引入基于流量的泛洪 DoS/DDoS 攻击检测的必要性。并根据 IPv6 下泛洪 DoS/DDoS 攻击发生时的流量特征，对基于网络流量突发检测的 DoS/DDoS 攻击检测算法在 IPv6 中的应用进行了研究。通过对检测算法在 IPv6 环境中性能和可行性的实验，可以发现，检测算法在 IPv6 环境中有很好的应用，对攻击强度比较大、持续时间比较长的攻击有较好的检测效果。 (下转第 34 页)