doi:10.3969/j.issn.1000-436x.2013.z1.038

非对称路由环境下 SYN flood 攻击防御方法

陶建喜[1,3,4]，周立[2]，周舟[1,4]，杨威[1,4]，刘庆云[1,4]，杨嵘[1,4]

(1. 中国科学院 信息工程研究所，北京 100093；2. 国家计算机网络应急技术处理协调中心，北京 100029；
3. 北京邮电大学 计算机学院，北京 100876；4. 信息内容安全技术国家工程实验室，北京 100093)

摘 要：针对现有网络安全设施无法有效防御非对称路由环境下流量规模较大的 SYN flood 攻击的问题，对 SYN flood 攻击检测技术和 TCP 连接管理策略进行研究，提出了一种轻量级攻击检测和混合连接管理策略相结合的防御方法，利用 SYN 分组比例和目的地址熵进行攻击检测，并根据检测结果对基于 SYN 的连接管理策略和基于数据的连接管理策略进行灵活切换。实验证明该防御方法能有效地减轻 SYN flood 攻击对网络安全设施的影响。

关键词：SYN flood；非对称路由；连接管理；SYN 分组比例；目的地址熵

中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2013)Z1-0285-07

SYN flood attack defense strategy for asymmetric routing

TAO Jian-xi[1,3,4], ZHOU Li[2], ZHOU Zhou[1,4], YANG Wei[1,4], LIU Qing-yun[1,4], YANG Rong[1,4]

(1. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China;
2. National Computer Network Emergency Response Technical Team/Coordination Center, Beijing 100029, China;
3. College of Computer Science and Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China;
4. National Engineering Laboratory for Information Security Technology, Beijing 100093, China)

Abstract: In order to resolve the problem that existing network security facilities can't defend against large-scale SYN flood attack under asymmetric routing environment, attack detection technology and connection management strategy were researched, and a defense architecture combining a light-weight detection method with a hierarchical connection management strategy was presented. The detection method uses SYN packet rate and destination IP address entropy, and the hierarchical connection management strategy consists of a method based on SYN packet and a method based on data packet. The experimental results show that this proposed method can mitigate the influence brought by SYN flood attack.

Key words: SYN flood; asymmetric routing; connection management; SYN packet rate; destination IP address entropy

1 引言

在互联网流量迅猛增长的今天，DDOS 攻击流量的规模和发生频率也随之增长。在被报道的攻击事件中，攻击流量曾经达到 100 Gbit/s[1,2]。据 CNCERT 发布的 2012 年安全态势报告显示，我国境内日均发生流量规模超过 1 Gbit/s 的 DDOS 攻击事件 1 022 起，约为 2011 年的 3 倍，而且攻击流量的规模仍然呈增长趋势。在所有的攻击流量中，SYN flood 攻击流量所占比例最高，这表明 SYN flood 攻击仍是主要攻击方式[3]。在现有的 SYN flood 防御方法中，大部分需要维护连接状态表，但随着攻击规模的增大，连接状态表容易被耗尽。因此，任何带有连接状态表组件的网络设备（或计算机系统）都有可能遭受 SYN flood 攻击，这些设备或系统包括 Web 服务器、状态检测防火墙、入侵检

收稿日期：2013-08-06

基金项目：国家高技术研究发展计划（“863”计划）基金资助项目（2011AA010703）；国家“242”信息安全计划基金资助项目（2012A99）；中国科学院战略性先导科技专项基金资助项目（XDA06030200）；国家自然科学基金资助项目（61303260）

Foundation Items: The National High Technology Research and Development Program of China (863 Program)(2011AA010703); The National Information Security Program of China (242 Program)(2012A99); Strategic Priority Research Program of the Chinese Academy of Sciences(XDA06030200); The National Natural Science Foundation of China (61303260)

测系统、入侵防护系统等网络安全设施。

随着互联网规模的不断扩大，网络结构日益复杂，非对称路由现象越来越普遍。非对称路由是指客户端和服务端在传输数据时，不同方向上的数据流所经过的路径不同[4]。对部署在非对称路由环境下的安全设备来说，它们无法捕获到双向的网络流，而现有的很多网络安全设施的连接状态表都基于完整的 TCP 连接，无法适用于非对称路由环境，这也使得现有的很多防御设施很难有效防御 SYN flood 攻击。

面对日益增大的攻击规模和非对称网络环境给 SYN flood 防御带来的双重挑战，人们必须以新的视角看待 SYN flood 攻击，寻找有效的解决方案。基于此，本文为非对称路由环境下的安全设施提出了一种新的防御方法。该方法结合轻量级攻击检测和混合连接管理策略，对网络流量进行实时检测，并根据检测结果对连接管理策略灵活切换，能有效地减轻 SYN flood 攻击对网络安全设施的影响。

2 相关工作

1994 年，Bill Cheswick 和 Steve Bellovin 首次提出 TCP 协议存在 SYN flooding 缺陷[5]。在过去近 20 年的时间里，很多解决方案被提出来。这些解决方案可以分为 2 类：一类是在正常的 TCP 三次握手过程中加入辅助机制，例如 SYN Cookie、SYN Cache、SYN Proxy、SYN Kill；另一类是根据 TCP 报文中的控制字段进行攻击检测，再对攻击流量进行过滤。

SYN Cookie[6~8]的原理是，TCP 服务器收到 SYN 请求时，并不为 TCB（transmission control block）分配空间，而是根据请求计算一个 Cookie 值，填充在 SYN/ACK 分组的 SEQ 字段返回给客户端。当收到来自客户端的 ACK 分组时，服务器根据 Cookie 值对 ACK 分组的合法性进行检查，只为通过合法性验证的连接请求分配资源，完成连接建立。

SYN Cache[9]用一个超时淘汰的散列表保存半开连接的状态信息，保存状态信息所需要的存储空间要比完整的 TCB 块小很多。当且仅当收到的 ACK 分组的信息在散列表中存在时才分配完整的 TCB 完成连接建立。

SYN Proxy[10]的核心思想是将服务器连接建立的操作移植到代理服务器上，代理服务器对客户端透明，客户端与服务端的三次握手实际上是由代理服务器来完成。

SYN Kill[11]通过主动移除半连接来保证服务器及时响应每一个 SYN 请求。在边界路由器所处的位置对进入子网的 SYN 请求进行监测，发现明显的非法请求（如源 IP 为私有 IP，源端口为保留端口等），直接向目的 IP 发送 RST 分组，结束此连接。对其他的 SYN 请求，直接发送 ACK 分组，然后进行监测，若该连接在一定的时间内未传输数据，则向目的 IP 发送 RST 分组终止连接。

完整的 TCP 数据流都包括连接的建立和终止 2 个过程。在这 2 个过程中，SYN 分组、SYN/ACK 分组、ACK 分组、FIN 分组、RST 分组的数量会存在一定的关系。若 TCP 连接正常建立，SYN 分组和 SYN/ACK 分组的数量具有对称性，即 SYN 分组和 SYN/ACK 分组的数量相等。SYN 分组和 ACK 分组的数量、SYN/ACK 分组和 ACK 分组的数量在连接正常建立时具有对称性。若连接正常地终止，SYN 分组的数量和 FIN 分组加上 RST 分组的数量也具有相同的对称性。当 SYN flood 攻击发生时，上述对称性关系会被破坏。

Wang[12]等人在攻击者所在子网的叶子节点路由上部署的 SYN-Dog 分别对从子网出去的 SYN 分组和进入到子网的 SYN/ACK 分组进行统计，通过 SYN 分组和 SYN/ACK 分组的对称性是否被破坏来进行攻击检测，若对称性被破坏，说明子网内存在攻击源。Takuo[13]等人同样利用 SYN 分组和 SYN/ACK 分组的对称性进行攻击检测，但思路略有不同，它们通过部署在叶子节点路由上的探测程序主动向子网内的主机发送 SYN 请求，统计收到的来自于目标主机的 SYN/ACK 分组的数量来判断该主机是否正在遭受 SYN flood 攻击。

陈[14]等人利用正常 TCP 连接中 SYN 分组和 ACK 分组的对称性对伪造 IP 地址的 SYN flood 攻击进行检测，能有效检测出基于不同 IP 欺骗类型的 SYN flood 攻击。

Sun[15]等人在文中提出了一种更快更准的检测方法—SACK^2，它利用 SYN/ACK 分组和 ACK 分组的对称性来准确检测出 SYN flood 攻击的开始和结束时间。

Wang[16]等人利用一种基于非参数累积和的方法对进入子网的 SYN 分组、FIN 分组和 RST 分组的数量进行统计，通过检查 SYN 分组的数量和 FIN 分组加上 RST 分组数量的对称性来判断是否有攻击发生。

上述 2 类方法能在一定程度上减缓 SYN flood 攻击的影响，在规模较小的攻击中效果比较明显，并且有较高的准确率。但是，它们还是存在一些应用限制。第 1 类防御方法仅仅考虑了对终端系统的防御，而本文所提及的非对称路由环境下的网络安全设施是非终端系统。上述 4 种加入辅助机制的防御方法中，除 SYN Cookie 之外，都需要维护连接状态表，不能承受规模较大的攻击。第 2 类检测方法满足一个前提—检测系统能够捕获到双向的网络流，而本文讨论的网络环境中不存在该前提。另外，攻击者可以通过成对伪造数据分组来逃避检测。以 SYN 分组和 ACK 分组为例，攻击者同时发送数量相同的 SYN 分组和 ACK 分组，这样就能使陈[14]等人所提的方法失效。与上述工作相比，本文所做的贡献主要在于考虑了网络安全设施自身的安全性，提出了一种基于轻量级检测和混合连接管理策略的防御方法，它能动态地调整连接管理的策略，并能很好地适应非对称路由环境，有效地降低了 SYN flood 攻击对网络安全设施带来的影响。

3　防御方法

本文提出的 SYN flood 攻击防御方法及环境如图 1 所示。流量获取模块从底层获取网络流量，并将流量传送给攻击检测模块和连接管理模块。攻击检测模块对流量进行实时检测，并将检测结果输出给连接管理模块，检测结果是系统当前所处的工作状态，包括正常态和被攻击态。正常态表示当前没有攻击存在，被攻击态表示当前存在攻击。连接管理模块有 2 种连接管理策略，分别是基于 SYN 的连接管理策略和基于数据的连接管理策略，根据攻击检测的结果选择策略，并且 2 个策略间能够灵活地切换。连接管理模块将处理好的流传递给上层处理模块进一步处理。本文将对攻击检测模块和 2 个连接管理模块进行详细讨论，其他模块只作为防御方法中的一个组成部分在此提及。

在详细讨论防御方法之前，作者根据 TCP 报文中的头部信息将它们分成如下几类。

1) SP（SYN packet）：SYN 标志位被置为 1 的 TCP 数据分组。

2) AP（ACK packet）：ACK 标志位被置为 1 的 TCP 数据分组。

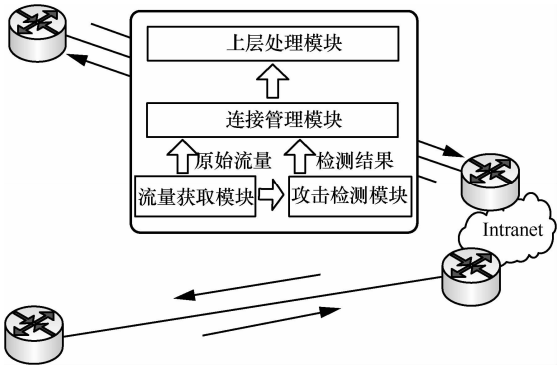


图 1　非对称路由环境下 SYN flood 攻击防御方法

3) DP（data packet）：ACK 标志位被置为 1，且数据域不为空的 TCP 数据分组。

4) RFP（RST or FIN packet）：RST 标识位（或 FIN 标志位）被置为 1 的 TCP 数据分组。

5) 1stDP(first data packet)：连接建立后传送的第一个数据分组。

在本文所讨论的非对称路由环境中，流量获取模块无法获取到完整的三次握手 TCP 报文，但至少能获取到 SYN 分组和 SYN/ACK 分组中的一个，它们都标志着一个 TCP 连接正在建立。因此，本文认为 SYN/ACK 分组都属于 SP。

大量研究表明，网民的正常网络行为产生的流量是相对稳定的，流量的很多统计特性（如数据分组的平均分组长度、各应用层协议数据所占比例等）都在一个有限的范围内平稳地波动，而攻击产生时，会使这些统计特性的波动异常。因此，本文采用基于统计的检测方法。

SYN flood 攻击主要表现为攻击者向目标服务器或网络发送大量的 SYN 请求，使得 SYN 标志位置为 1 的数据分组的比例急剧增加，网络中出现的目的 IP 地址会更加集中。基于上述 2 个特点，本文选取了 SYN 分组比例和目的地址熵作为统计变量。它们的定义如下。

1) SYN 分组比例指 SYN 标志位被置为 1 的 TCP 分组数量与 TCP 分组总数的比值，用 β 表示。

2) 假设目的 IP 地址统计集为：$C_d=\{c_{d_1},c_{d_2},c_{d_3},\cdots,c_{d_m}\}$，$C_{d_i}$ 表示目的地址为 i 的 TCP 连接数，$S_d=-\sum_{i=1}^{m}c_{d_i}$，目的地址熵为[17]

$$Entropy(Dip)=-\sum_{i=1}^{m}\left(\frac{c_{d_i}}{S_{d_i}}\right)\ln\left(\frac{c_{d_i}}{S_{d_i}}\right)$$

完整检测过程的状态转换如图 2 所示。检测周期刚开始的状态为初始态。攻击检测模块在初始态时对 SYN 分组比例和目的地址熵进行统计。用 S_l 表示 SYN 分组比例的下限，S_u 表示 SYN 分组比例的上限，e 表示目的地址熵的阈值。当 $\beta \leqslant S_l$ 时，初始态转化成正常态，表示此刻无攻击。当 $\beta \geqslant S_u$ 时，初始态转化成被攻击态，表示正在遭受攻击。当 β 的值在上下限之间，初始态转化成可疑态，需要用目的 IP 地址熵做进行一步判断。当 $Entropy(Dip) < e$ 时，可疑态转化成被攻击态，当 $Entropy(Dip) \geqslant e$ 时，可疑态转化成正常态。需要指出的是，检测是周期性的工作，而这只是一个检测周期内的状态转换图，β、S_l、S_u、e 可根据实际网络流量环境进行调整。根据攻击检测结果，连接管理模块采用混合连接管理策略，如图 3 所示。(CIT, connection init table)管理半开连接状态信息，(DTT, data transfer table)管理已完成的连接状态信息，(FDC, first data cache)用于缓存连接中前 N 个到达的 DP。除了 DTT 会根据连接正常结束的标识 FIN（或 RST）淘汰连接状态信息外，CIT 和 FDC 仅采用超时淘汰策略。

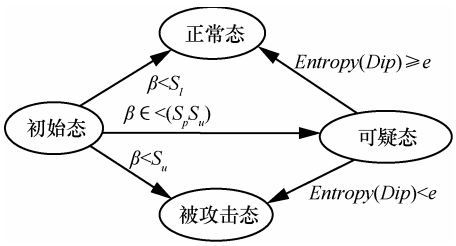


图 2 攻击检测状态转换

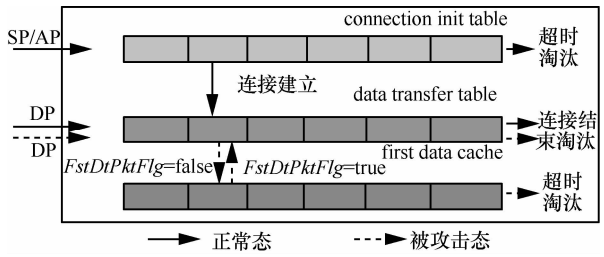


图 3 混合连接管理结构图防御策略

该方法的原理是，根据检测结果将连接管理的工作状态分为正常态和被攻击态，正常态时，按照 TCP 三次握手建立连接、传输数据、终止连接的过程进行连接管理，启用 CIT 和 DTT。被攻击态时，忽略 TCP 三次握手的过程，直接用带数据的 TCP 分组建立连接。但是这种方式可能带来连接建立后传输的第一个数据分组（1stDP）丢失的问题。由于应用层协议的很多特征信息在 1stDP 内，它的丢失可能导致上层处理失败。为了避免这一问题，本方法引入 FDC，将连接的前 N 个数据分组的 SEQ 序号和分组长度信息按 SEQ 序号升序缓存在 FDC 中，如果经过判断后，该序列中不存在“空洞”，则认为 1stDP 已经到达，并用 FstDtPktFlg 标识 1stDP 是否到达。

由于接收方的接收窗口大小有限，发送方在未收到来自接收方对第一个数据分组的确认之前，所发送数据分组的总长度不会超过接收窗口大小。即发送方在未收到来自接收方对第一个数据分组的确认之前，所发送的数据分组个数也有限。假设第 i 个连接的第一个数据分组在第 n_i 个分组到达时，FDC 表中缓存窗口的大小为 W，取 $W = \max\{n_1, n_2, \cdots, n_i, n_{i+1}, \cdots\}$ 时，一定能捕获到 1stDP。虽然无法准确计算 $\max\{n_1, n_2, \cdots, n_i, n_{i+1}, \cdots\}$ 的值，但 n_i 的取值范围有限。一定存在一个足够大的值 N，对于任意的 i，满足 $N \geqslant n_i$，即 $N \geqslant \max\{n_1, n_2, \cdots, n_i, n_{i+1}, \cdots\}$。因此，取 $W = N$，就能解决 1stDP 丢失导致上层处理失败的问题。本文的实验部分会对该方法的有效性以及 N 的取值做进一步验证。

连接管理模块有 2 种策略，基于 SYN 的策略和基于数据分组的策略。根据攻击检测的结果，连接管理模块会选择不同的策略，而且这 2 种策略之间能够自由切换，而且不需要任何过渡操作。从基于 SYN 的策略切换成基于数据分组的策略时，CIT 中已有连接的后续数据分组到来时，会根据数据分组建立新的连接状态实体插入 DTT 表中，而 CIT 中的数据会随时间推移而被 CIT 自身的超时淘汰机制所淘汰。从基于数据分组的策略切换成基于 SYN 的策略时，DTT 表中的信息不变，直接启用 CIT 即可，FDC 中的数据也会随时间推移而被 FDC 自身的超时淘汰机制所淘汰。

基于 SYN 的连接管理策略与 TCP 协议的实现类似，需要对 TCP 协议三次握手、数据传输以及连接终止 3 个过程的数据分组进行处理，连接状态实体的建立是根据三次握手过程中的数据分组完成的。而基于数据分组的连接管理策略不需要处理三次握手过程中的数据分组，其处理过程如图 4 所示，在介绍算法之前，本文先定义如下操作。

1) GetPacketType(Packet)：获取 Packet 的类型，其返回值是一个枚举类型，枚举的值分别是 SP、AP、DP、RFP。

```
输入：Packet
输出：StreamInfo
1) function MANAGEBYDATA(Packet)
2)     PacketType←GetPacketType(Packet)
3)     switch PacketType do
4)       case AP:
5)         if Search(Packet, DTT)=true then
6)           PutInTab(Packet, DTT)
7)           FstDtPktFlg←true
8)         end if
9)       end case
10)      case DP:
11)        if Search(Packet, DTT)=true then
12)          Update(Packet, DTT)
13)        else
14)          PutInTab (Packet, DTT)
15)          FstDtPktFlg←false
16)        end if
17)        if FstDtPktFlg=false then
18)        Cache(Packet)
19)        if CheckHole(Packet)=false then
20)          FstDtPktFlg←true
21)        end if
22)      end if
23)      end case
24)      case RFP:
25)        if Search(Packet, DTT)=true then
26)          MoveOut(Packet, DTT)
27)        end if
28)      end case
29)      case OTHER:
30)        Drop(Packet)
31)      end case
32)    end switch
33)    return StreamInfo
34)  end function
```

图 4　基于数据分组的连接管理算法的处理过程

2) Search(Packet, TAB)：在 TAB 表中搜索和 PKT 具有相同四元组的连接状态实体，若搜索到，返回 TRUE，否则，返回 FALSE。

3) PutInTab(Packet, TAB)：新建一个和 Packet 具有相同四元组的连接状态实体，并插入 TAB 表中。

4) Drop(Packet)：直接丢弃掉 Packet 分组，不做任何处理。

5) Move(Packet, TAB1,TAB2)：从 TAB1 表中将和 Packet 具有相同四元组的连接状态实体转移到 TAB2 表中。

6) MoveOut(Packet, TAB)：从 TAB 表中移除和 Packet 具有相同四元组的连接状态信息实体。

7) Update(Packet, TAB)：更新 TAB 表中和 Packet 具有相同四元组的连接状态信息实体。

8) CheckHole(Packet)：查看 FDC 表中和 Packet 具有相同四元组的窗口中的序列是否存在“空洞”，若存在，返回 TRUE，否则，返回 FALSE。

9) Cache(Packet)：将 Packet 的 SEQ 序号和分组长度信息加入到 FDC 中 Packet 所对应的窗口中，若 FDC 中不存在 Packet 所对应的窗口，先创建。

4　实验

本文从可行性和性能 2 个方面对该防御方法进行了评估。可行性实验主要对 SYN 分组比例和 1stDP 乱序情况进行统计。性能测试是用改进前后的网络安全设备进行对比测试，对比包括在相同流量下的分组丢失率对比和在达到相同分组丢失率的情况下对比改进前后设备的处理流量大小进行对比。需要说明的是，分组丢失是由于攻击流量消耗大量资源，使系统来不及处理而造成的。

4.1　可行性评估

4.1.1　SYN 分组比例统计

SYN 分组比例统计实验主要用于验证前文中所提的 SYN 分组比例在一定的范围内波动这一结论，同时测出 SYN 分组比例的上下限阈值。本文以每秒一次的频率对某运营商网络节点 2013/6/17 9:21~2013/6/18 10:07 近 24 个小时的在线流量进行实时统计，共得到近 86 000 组数据，得到如图 5 所示累计直方图。由图 5 可知，在一天中 80%左右的时间内，SYN 分组比例不超过 5%，有 90%以上的时间，SYN 分组比例在 15%以内。因此，得到的结论是 SYN 分组比例在 5%~15%之间波动。

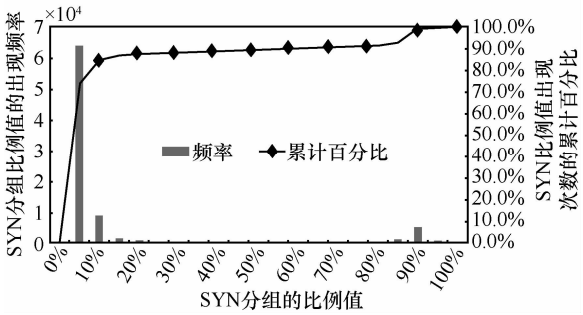


图 5　SYN 分组比例累计直方图

4.1.2　1stDP 乱序情况统计

对 1stDP 乱序情况进行统计主要用于论证使用 FDC 表解决 1stDP 丢失导致上层处理失败问题的可行性，以及其窗口大小 N 的取值。本文对采自某运营商网络节点的 121 GB 数据进行离线统计，得到如表 1 所示的数据。在统计的近 300 万个连接中，头部分组未出现乱序的连接数占总连接的 99.053 28%，头部分组在前 5 个到达的连接占总连接的 99.995 95%。因

此，本文认为 1stDP 在前 6 个数据分组还未到达是小概率事件。因此，本文选择 6 作为 FDC 缓冲窗口的大小，即在被攻击态时，对一个连接的前 6 个数据分组的 SEQ 序号和分组长度信息进行缓存。

表 1 1stDP 乱序情况统计表

1stDP 次序	连接数	百分比	累计百分比
1	2 907 594	99.053 28%	99.053 28%
2	24 700	0.841 46%	99.894 73%
3	1 894	0.064 52%	99.959 26%
4	837	0.028 51%	99.987 77%
5	240	0.008 18%	99.995 95%
6	118	0.004 02%	99.999 97%
>6	1	0.000 03%	100.000 00%

4.2 性能评估

用来性能评估测试的设备分为 2 组，一组采用已有防御方法(与基于 SYN 的连接管理策略类似)，另一组采用本文所提的防御方法。测试的流量是从某运营商网络节点采集，采集流量时该节点正在被攻击，并且该节点处于非对称路由环境中。根据可行性评估中的实验结果，本文所提方法的 4 个参数分别设置如下：SYN 分组比例下限为 5%，SYN 分组比例上限为 15%，目的地址熵的阈值为 4[17]，FDC 的窗口大小为 6。

将采集的流量原速回放，分别导入两台设备，并以每 10 s 一次的频率对设备在处理过程中的分组丢失率进行实时统计。统计结果如图 6 所示。由图可知，防御方法改进后设备的分组丢失率明显比改进前的低。

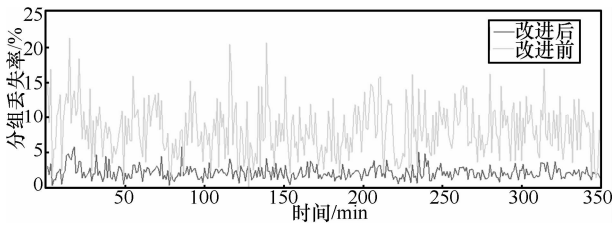


图 6 实时分组丢失率对比连接管理

分别对两台设备注入相同的流量，流量的大小逐渐增大，直到设备的分组丢失率达到万分之一为止，以此来测量设备的处理能力。测试数据如表 2 所示，改进前的设备所处理的业务流量大小为 1.2 Gbit/s 时，其分组丢失率达到万分之一，改进后的设备所处理的业务流量大小为 1.9 Gbit/s 时，才出现万分之一的分组丢失率。由此可见，改进后的设备处理能力比改进前的设备提高了 58.3%。

表 2 万分之一分组丢失率下处理能力对比

改进后	改进前	提升幅度
1.9 Gbit/s	1.2 Gbit/s	58.3%

由两组对比测试的结果可知，本文所提的方法能够有效地过滤 SYN flood 攻击流量，提高网络安全设施的处理能力，减缓 SYN flood 攻击所带来的影响。

5 结束语

针对现有网路安全设施无法有效防御非对称路由环境下的大规模 SYN flood 攻击这一问题，本文对 SYN flood 攻击检测和防御技术进行了研究，提出了一种基于轻量级检测和混合连接管理策略的防御方法，用 SYN 分组比例和目的地址熵进行攻击检测，并根据检测的结果选择合适的连接管理策略。在原有的依靠 SYN 请求来进行连接管理的基础上，作者又提出了一种新的基于数据分组的连接管理策略，策略的核心思想是在攻击发生时，忽略三次握手过程，直接用连接建立后传输的数据分组进行实验。实验流量采自于运营商网络节点，对比了防御方法改进前后的网络安全设备的处理能力和分组丢失率。实验证明，该方法能有效地过滤 SYN flood 攻击流量，减小 SYN flood 攻击对网络安全设施的影响。

未来的研究工作从 2 个方面展开。在用数据分组进行连接管理时，未对第一个数据分组的缓存方案给出理论证明，无法有效地验证第一个数据分组的正确次序，这将是今后的研究工作重点。此外，检测方法还有提升的空间，以便获得更好的防御效果。

参考文献：

[1] Prolexic Quarterly Global DDoS Attack Report Q4 2012[R]. Hollywood: Prolexic Technologies, 2013.

[2] KLEYMAN B. Why Anti-DDoS Products and Services are Critical for Today's Business Environment[R]. Data Center Knowledge (DCK), 2013.

[3] 2012 年我国互联网网络安全态势综述[R]. 北京: 国家互联网应急中心, 2013.
2012 Survey on Internet Security Situation in China[R]. Beijing: National Computer Network Emergency Response Technical Team/Coordination Center, 2013.

[4] What is asymmetric routing[EB/OL]. https://my.stonesoft.c om/support/

document.do?docid=1377, 2013.

[5] EDDY W. TCP SYN flooding attacks and common mitigations [EB/OL]. http://tools.ietf.org/html/rfc4987#section-2.1, 2007.

[6] BERNSTEIN D J. SYN cookies[EB/OL]. http://cr.yp.to/syn-cookies.html.

[7] ZÚQUETE A. Improving the functionality of syn cookies[J]. Advanced Communications and Multimedia Security, 2002, (100):57-77.

[8] HANG B, HU R M, SHI W. An enhanced SYN cookie defence method for TCP DDoS attack[J]. Journal of Networks, 2011, 8(6): 1206-1213.

[9] JONATHAN L. Resisting SYN flood DoS attacks with a SYN cache[A]. Proceedings of the BSD Conference 2002 on BSD Conference[C]. CA, USA, 2002. 89-97.

[10] WU Z, CHEN Z. A three-layer defense mechanism based on web servers against distributed denial of service attacks[A]. Proceedings of the First International Conference on Communications and Networking[C]. Beijing, China, 2006. 1-5.

[11] SCHUBA C L, KRSUL I V, KUHN M G. Analysis of a denial of service attack on TCP[A]. Proceedings of 1997 IEEE Symposium on Security and Privacy[C]. Oakland, CA, USA, 1997. 208-223.

[12] WANG H N, ZHANG D L, SHIN K G. SYN-dog: sniffing SYN flooding sources[A]. Proceedings of the 22′nd International Conference on Distributed Computing Systems (ICDCS'02)[C]. Vienna, Austria, 2002. 421-428.

[13] NAKASHIMA T, OSHIMA S. A detective method for SYN flood attacks[A]. Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC'06)[C]. Washington DC, USA, 2006. 48-51.

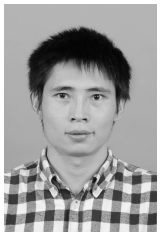
[14] CHEN W, YEUNG D. Defending against TCP SYN flooding attacks under different types of IP spoofing[A]. Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies[C]. Mauritius, 2006. 38-43.

[15] SUN C H, HU C C, TANG Y, *et al*. More accurate and fast SYN flood detection[A]. Proceedings of 18th Internatonal Conference on Computer Communications and Networks[C]. San Francisco, CA, USA, 2009. 1-6.

[16] WANG H N, ZHANG D L, SHIN K G. Detecting SYN flooding attacks[A]. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies[C]. New York, NY, USA, 2002. 1530-1539.

[17] EHRLICH W K, FUTAMURA K, LIU D. An Entropy Based Method to Detect Spoofed Denial of Service (DoS) Attacks[M]. US:Springer US, 2008, 44:101-122.

作者简介：



陶建喜（1988-)，男，湖北石首人，北京邮电大学硕士生，主要研究方向为网络安全。

周立（1980-），女，河南安阳人，博士，国家计算机网络应急技术处理协调中心工程师，主要研究方向为机载网络、网络安全。

周舟（1983-），男，湖南长沙人，博士，中国科学院助理研究员，主要研究方向为网络安全、高性能网络。

杨威（1986-），男，湖南长沙人，硕士，中国科学院助理工程师，主要研究方向为网络安全、信息内容安全。

刘庆云（1980-），男，河北衡水人，硕士，中国科学院高级工程师，主要研究方向为信息安全、网络安全。

杨嵘[通信作者]（1978-），男，山西运城人，硕士，中国科学院工程师，主要研究方向为信息内容安全。E-mail：yangrong@iie.ac.cn。