基于主动网的SYN攻击防御

肖 原* 王 晟 李乐民

(电子科技大学 宽带光纤传输与通信系统技术国家重点实验室 成都 610054)

【摘要】针对目前传统网防御TCP同步泛滥攻击的服务器主机、路由器过滤、防火墙方法的局限性，利用主动网的动态特性，提出一种基于主动网的同步泛滥防御机制，并通过仿真实验将它与传统网环境下的防火墙防御进行了性能比较和分析，结果表明主动网技术为同步泛滥攻击提供了良好的防御性能。

关 键 词 同步泛滥攻击; 防御; 防火墙; 主动网

中图分类号 TN915.01 文献标识码 A

Active Network Based SYN-FLOOD Defense

Xiao Yuan Wang Sheng Li Lemin

(State Key Laboratory of Broadband Optical Fiber Transmission and Communication Networks, UEST of China Chengdu 610054)

Abstract This paper outlines the limitation of some currently schemes of defending SYN-Flood in traditional networks, and presents an active network based SYN-Flood defense mechanism, which takes advantage of the active network' s dynamic environment. In additon, we analyze the performance of our scheme via simulation experiments and compare it with the firewall based mechanism . The experiments show that active network based mechanism provides better capability for SYN-Flood defending.

Key words SYN-Flood attack; defense; firewall; active network

同步泛滥(SYN-Flood)是最常用的分布式拒绝服务(distributed denial of service)攻击方法，它利用了TCP/IP协议实现上的一个缺陷，通过向网络服务所在端口发送大量伪造的TCP连接请求，使被攻击方资源耗尽而拒绝服务。目前，很多操作系统、防火墙、路由器的设计都加入了SYN-Flood的防御机制，但在传统网络的环境下防御SYN-Flood攻击较困难。

主动网是一种可编程的分组交换网络,它的本质特征是动态特性[1]：新的或修改的网络服务能够利用网络设施动态地在网络中传播和分布，这与现有的互联网不同。在主动网中，主动节点为可执行的定制程序提供运行平台。通过主动网提供的通用开放的网络可编程接口，应用程序可直接向节点插入定制的程序或通过在报文分组中包含可执行的程序代码段来配置或扩展网络的核心功能，通过每跳执行的方式来配置并优化它们的任务，提供某种定制的网络服务。主动节点收到数据后进行计算，再将数据传送到下一节点。

主动网的概念为防御SYN-Flood攻击提供了一种新的思路，本文提出了一种基于主动网的SYN-Flood攻击防御的解决方案并通过仿真实验进行了性能分析。

1 目前SYN-Flood攻击的主要防御机制及其局限性

SYN-Flood攻击是由于大量的非法连接请求占满服务器的连接缓存队列，使合法用户的正常连接请求无法进入而被服务器拒绝，达到了攻击者的攻击目的。通常分布式SYN-Flood攻击较难防御，因为它不是利用系统的弱点，而是针对连接在网络的主机，是由于大量的流量造成。目前有很多DDoS工具，使用源地址

2002年12月23日收稿

* 女 30岁 硕士 主要从事主动网技术方面的研究

伪装、反射及其他的技术隐藏真正的攻击源[2~4]，征用不知情的分布于网络各处的合法用户作为攻击代理，所以从源头阻止攻击面临许多困难。

从防御考虑，目前主要有三类SYN-Flood防御机制[5, 6]。

1) 针对服务器主机的方法。增加连接缓冲队列长度和缩短连接请求占用缓冲队列的超时时间。该方式最简单，被很多操作系统采用，但防御性能也最弱。在分布式攻击中，攻击者可以容易的达到服务器的服务极限，达到攻击目的。

2) 针对路由器过滤的方法。由于DDoS攻击，包括SYN-Flood，都使用地址伪装技术，所以在路由器上使用规则过滤掉被认为地址伪装的包，会有效的遏制攻击流量。它针对所有类型的DDoS攻击，RFC 2267建议在全球范围的互连网上使用向内过滤的机制。该方式完全依赖于规则的定义，如果攻击者所伪造的地址是本子网的合法地址，它就不适用了。此外在路由器上使用访问控制列表会带来额外的负荷，特别是已经满载的骨干路由器会受到明显的威胁。

3) 针对防火墙的方法。在SYN请求连接到真正的服务器之前，使用基于防火墙的网关来测试其合法性。它是一种被普遍采用的专门针对SYN-Flood攻击的防御机制，例如Cisco的路由器就提供了这样的功能[7]，其原理如图1所示。它也是目前在系统遭受攻击时能最大限度的保证合法连接被接受的方式，因此成为推荐使用的SYN-Flood防御机制。但由于防火墙的介入，合法用户的连接建立时延会增加，当系统访问量较大时，防火墙自身的负荷会较高。

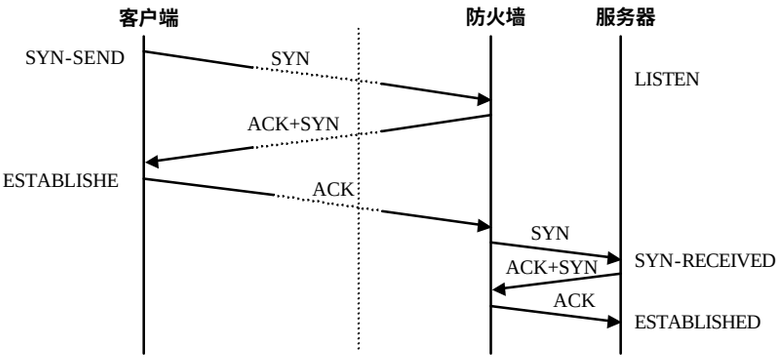

图1　基于防火墙的SYN-Flood防御机制

SYN-Flood攻击防御机制在不断的发展，由于传统网络环境本身的非动态性，其防御机制依赖于网络管理员的专业技术，如防火墙机制。如果在服务器运行期间一直提供，会对合法用户的连接过程造成额外的延时；当被攻击时启动，使系统在攻击发生时不能快速建立防御机制，需要专业管理员及时发现进行人工配置，主动网的动态特性能够弥补传统网的不足。

考虑主动网在防御DDoS攻击方面的优势，如文献[8]提出一种基于主动网的内向过滤机制，它利用主动网仅在攻击发生时启动的动态特性，降低了路由器的日常负荷。文献[9]提出了使用主动网防御DDoS攻击的网络体系结构，介绍了主动网在这种环境下的灵活性。文献[10]利用数台主机构建了一个类似真实网络的环境，使用主动网技术实现了攻击下过滤机制的动态分配和启动，证实了利用主动网技术在传统网中防御DDoS攻击的可行性。基于上述研究可以得出结论：主动网可能不能直接改善现有的防御技术，但利用主动网的动态特性，可以重新组织现有技术并提供较传统防御更开放的方式来提高防御的效率。

2　基于主动网的SYN-Flood攻击防御机制

由于SYN-Flood攻击防御机制的局限性和主动网技术的可行性，利用主动网技术来改善SYN-Flood攻击防御机制的优点：

1) 可扩展性：网络攻击技术不断发展，新的防御软件不断出现并且需要被分派到网络中，主动网能使这一过程更快速并更简单的自动进行。

2) 高效性：当攻击发生时，能充分利用主动网技术的潜在能力使主机受到攻击时快速反应，自动启动防御代码快速的在网络中传播并驻留在最有效果且最有效率的位置来对抗SYN-Flood攻击。

2.1　防御机制描述

主动网防御机制原理如图2所示，它是对防火墙防御的一种扩展。防火墙防御的优点是攻击者始终见不到真正的服务器，承受攻击流量的是防火墙。在大量攻击流量下，传统的防火墙防御难以做到对SYN-Flood

攻击免疫，如Cisco的设计是在进入攻击防御模式时，立刻将连接缓存队列的超时时限降为一半；如果进入的连接请求超出了可维持的半连接数，会接受新的连接而丢弃最早的一个连接请求，但是，合法连接仍可能被丢弃，利用主动网技术能改善这种状况。

首先，在服务器运行期间要运行一个攻击检测例程以监视本机是否受到攻击，一旦检测到攻击发生就启动防御机制。该机制包括两种分离的服务例程，一种为前端例程，用于拦截所有目的为受害者的SYN请求报文，以服务器的身份测试该请求的合法性，会驻留在离攻击源最近的主动节点(图2中的主动节点*A*)。另一种为后端例程，用于拦截测试合格后的连接请求报文，代表客户端与服务器建立连接，驻留在服务器的第一跳主动节点(图2中的主动节点*B*)。就样将防火墙防御中的功能进行了分离，为TCP连接的建立过程构建通过整个链路的防火墙，提高了防御效率。

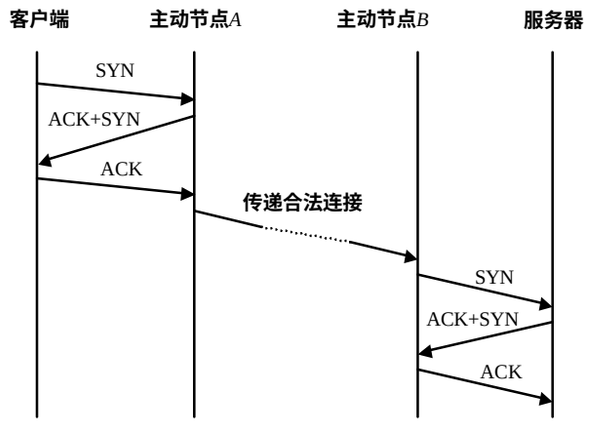

图2 基于主动网的SYN-Flood攻击防御机制原理

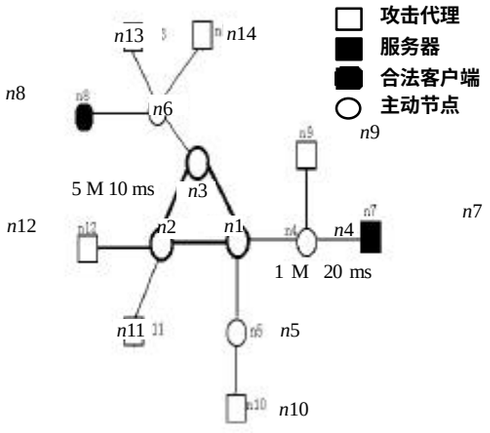

图3 仿真网络拓扑模型

当服务器检测到攻击发生，立刻利用主动网的代码分配协议启动防御代码的传送，向有SYN请求到达的所有本地接口送出。服务器要启动传送两种防御例程：后端例程只用传一跳后驻留在该节点；前端例程将依次向前推进，并分散到所有离分布在全网的攻击源点最近的主动节点。为了在代码传递期间能够进行反击，在前端例程的传送过程中，它在经过的每一跳节点复制代码并构建前端，其优点是当攻击期间有新的攻击源启动时，会在它到达的第一个主动节点被阻截，并适应新的攻击状况从这里启动代码的进一步分派。由于前端例程只拦截针对受害者的SYN请求，所以它的构建不会影响其他的数据报文传送。

非法的连接请求会被前端例程拦截测试后丢弃，而合法用户的SYN请求经过测试后，利用传统的网络传输服务，以一种特殊标记的报文传递到后端例程。当后端例程收到测试合格的连接请求后，继续完成与服务器的连接过程。如果服务器没有响应后端例程的SYN请求，则经过超时时限，后端例程向客户端发RST报文以复位该连接，由于后端例程位于服务器的第一跳，该超时时限容易确定。当后端例程和服务器的三次连接完成后，服务器端和客户端才建立了连接，可以进行数据传送，主动节点由于只拦截特定的报文不会影响该连接的数据传送过程。

由于分布式攻击的特点，其分派的前端例程也是分布式的，攻击的负荷被分布式的前端例程分担了，提高了合法请求的执行效率，使非法请求在第一时间被控制，减轻了网络的负荷。

2.2 仿真与性能分析

为了验证SYN-Flood攻击防御设想，使用网络仿真工具(network simulation, NS)建立一种简化的网络模型，拓扑结构如图3所示，同时进行了仿真实验。

对于仿真模型的构建有两点需要说明：

1) 该防御机制不限制所有的节点都是主动节点，非主动节点(传统路由器)在该机制中没有特殊作用，只提供传统的传送服务，所以仿真拓扑中没有构建非主动节点。

2) 在仿真实验中没有实现真正的代码传送，在NS下提供真正意义上的代码传送也是不实际的。所以服务例程已先作为仿真模块驻留在节点中，代码分配的实现是通过服务器发送特定包来激活模块完成的。

防火墙防御在现有的SYN-Flood攻击防御中占有重要的地位，是一种最常用的 SYN-Flood攻击防御机制，下面用防火墙防御与本文的防御机制进行性能比较。

使用防火墙防御时在$n4$上构建如图1所示的防火墙。

在实验中，合法客户端($n8$)每秒发出2.5个连接请求(2.5 pkt/s)。仿真时，在1 s时刻所有的攻击源($n9$～$n14$)同时发动攻击，每个攻击源攻击速率为6 pkt/s；在180 s时，防御机制启动；在300 s时攻击速率增为每个源70 pkt/s。

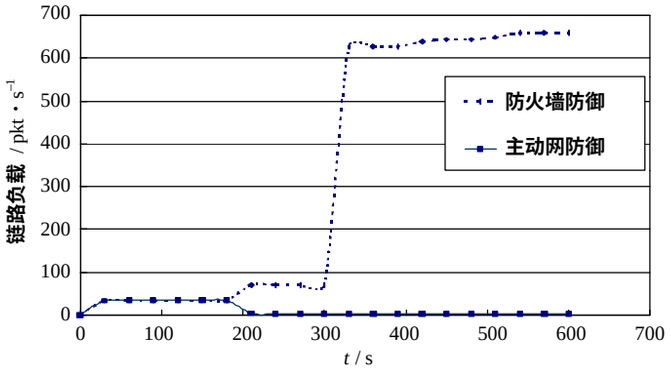

图4　防火墙防御和主动网防御的链路负荷比较

图4所示为当攻击源的攻击速率变化时，在不同的防御机制下，$n1$—$n4$链路的网络负荷变化。从图中可以看出当主动防御启动后，立刻降低了链路负荷，当攻击流量激增后，仍能有效地遏止链路负荷的增加。而在防火墙防御机制下，链路流量甚至略有增加，因为它要为所有的合法和非法的连接请求发ACK+SYN报文。在攻击速率激增后，防火墙防御对链路的负荷无能为力，负荷会随着攻击速率的激增而激增。

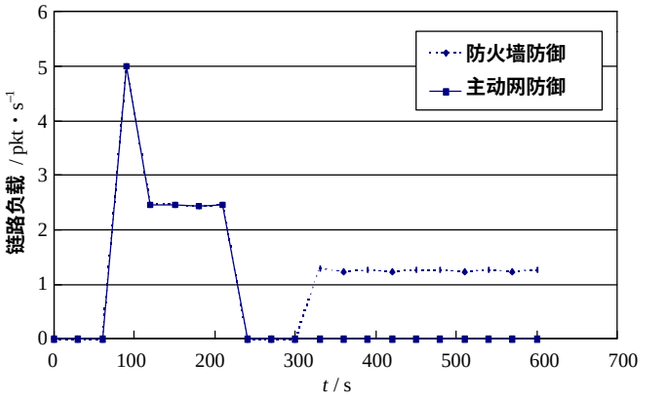

图5　合法请求在防火墙防御和主动网防御中未建立连接的丢包率比较

图5显示了由于攻击流量的影响，在不同的防御机制下合法连接请求被拒绝的可能性。图中可以看出在防御机制启动前，由$n8$每秒发出的2.5个合法连接请求都被拒绝了(图中的突起是由于攻击流量突然出现不仅使连接请求被丢掉，还丢掉了攻击前已完成两次握手的连接被丢失共同造成的)。当防火墙启动后，由于它对请求缓存队列的保护，使所有合法连接请求都被接受并完成了连接。当攻击流量增加，合法请求会因为网络瓶颈处的拥塞(如图4中的$n1$)而造成一定的丢失。在主动网防御中，这种情况却不会发生，随着攻击流量的增加，合法连接请求仍旧会被接收并完成连接。

主动节点附加的防御机制会对合法用户的TCP连接造成一定的时延，但比较图1、2可见，在主动网防御中，前端例程和后端例程之间传递连接信息的方式会减少连接的三次握手过程在链路间的往返流量和时间消耗，所以通过这种方式可以使主动节点所附加的时延有所降低；另外防火墙防御时所遭受的攻击负荷被分布式的前端例程分担了，也会在一定程度上降低合法连接的时延。在本文的仿真模型中，使用防火墙防御，合法连接的连接建立耗时367.2 ms，主动网防御可以降到228 ms。

3 结 论

本文提出一种基于主动网的SYN-Flood攻击防御机制，并对它进行了仿真实验，将其与目前的基于防火墙的防御机制进行了性能分析和比较，结果表明，基于主动网的防御机制提供了良好的SYN-Flood攻击的防御性能，也证明主动网为目前的网络攻击检测和对策提供了一种可用的、更为灵活的手段。

参 考 文 献

[1] Jonathan M S, Sincoskie W D, Wetherall D, *et al.* A survey of active networks research[J]. IEEE Communications Magazine, 1997, 35: 80-86

[2] Dittrich D. The DoS project's trinoo distributed denial of service attack tool[EB/OL]. http://staff.washington.edu/dittrich/misc/trinoo.analysis, 2002-03-05

[3] Dittrich D. The stacheldraht distributed denial of service attack tool[EB/OL]. http://staff.washington.edu/dittrich/misc/stacheldraht.analysis, 2002-05-17

[4] Dittrich D. The Tribe flood network distributed denial of service attack tool[EB/OL]. http://staff.washington.edu/dittrich/misc/stacheldraht.analysis, 2002-08-23

[5] Andrian P. Denial of service and distributed denial of service attacks[J]. Modern Problems of Radio Engineering,Telecommunications, and Computer Science (TCSET)' 2002 , 2002, 18-23: 303-304

[6] Pars M. Defending against a denial-of-service attack on TCP[EB/OL]. http://www.raid-symposium.org/raid99/PAPERS/ParsMutaf.pdf, 2002-04-12

[7] Cisco. Configuring TCP Intercept (Preventing Denial-of-Service Attacks)[Z]. Cisco IOS Security Configuration Guide

[8] Krsul I, Kuhn M, Spafford G, *et al.* Analysis of a denial of service attack on TCP[C]. IEEE Computer Society Symposium on Research in Security and Privacy, 1997

[9] Gitae K. Active edge-tagging(ACT): an intruder identification &isolation scheme in active network[C]. Sixth IEEE Symposium on Computers and Communications (ISCC'01), 2001

[10] Stamatis K. Dealing with denial-of service attacks in agent-enabled active and programmable infrastructures[C]. 25th Annual International Computer Software and Applications Conference (COMPSAC'01), 2001

[11] Diahardari K, Salupari R, Cholter W L, *et al.* Active network based DDoS defense[R]. NAI Labs Technical Report #01-035, 2002

编 辑 漆 蓉