基于保护流的MANET网MAC层DoS攻击及防御

叶 进 李伶强

(桂林电子科技大学认知无线电与信息处理省部共建教育部重点实验室 桂林 541004)

摘 要 在分析拒绝服务攻击和IEEE802.11协议的基础上,讨论了无线Ad hoc网络可能遭受的拒绝服务攻击类型。针对其中的MAC层拒绝服务攻击中的协同攻击,重点分析了基于保护流的解决方案。基于该方法的基本原理,提出了保护流位置设计的原则和方法。通过仿真分析在加入保护流前后被攻击流的吞吐量和延时,验证了所提出的保护流位置的设计。

关键词 Ad hoc,MAC层,DoS攻击,保护流

中图法分类号 TN915.65 **文献标识码** A

Protecting Flow Based DoS Attack and Defense at the MAC Layer in MANET

YE Jin LI Ling-qiang

(Key Laboratory of Cognitive Radio and Information Processing, Ministry of Education, Guilin University of Electronic Technology, Guilin 541004, China)

Abstract This paper discussed possible DoS attacks induced by IEEE 802.11 in wireless Ad hoc networks. The protecting flow based solutions were emphatically analyzed with respect to CCA DoS attack at MAC layer. This paper proposed the principles of protecting flow design. By placing protecting flows in different positions, we compared the throughput and delay of these flows being attacked. Simulation results show that the design rule of protecting flow is effective and applicable.

Keywords Ad hoc, MAC layer, DoS attack, Protecting flow

1 引言

MANET(Mobile Ad Hoc Network)即移动自组织网络,是由一批具有相同任务或相同兴趣的移动设备形成的暂时网络群体。所有的移动用户节点以无线的多跳路由模式进行通信。它不需要预先布置固定的基础设施,充分体现了无线网络的移动性和灵活性,因而非常适合战场通讯、灾难救助等场合。

拒绝服务(Denial-of-Service,DoS)攻击对当前网络产生越来越大的威胁。从广义上讲,通过任何手段促使正常的使用者无法使用合法服务的攻击都属于拒绝服务攻击。拒绝服务攻击最简单的攻击方式是利用系统的设计漏洞;另外一种攻击方式是过度使用合法服务而消耗被攻击主机的资源,使被攻击主机无法给其他用户提供服务。

IEEE802.11 MAC协议的分布式协调(DCF)工作模式采用带冲突避免的载波侦听多路访问(CSMA/CA)协议,可以作为基于竞争MAC协议的代表。由于该协议的时序、大小、控制和数据包的序列简单,而且公开,因此这个协议在MANET网络中大量采纳。

2 MANET网络中的拒绝服务攻击分析

针对MANET网络的主要攻击目标为网络的物理层、MAC层和网络层等,现有攻击方式的研究以网络层安全机制为主。对物理层和MAC层的拒绝服务攻击往往会对路由层产生很大的影响,通常通过连续的数据注入以获得对目标节点的信道占用。如果多个节点被攻击,会造成整个网络的性能下降。但是目前对MANET中MAC层的DoS的攻击及检测的研究却不多。

对MAC层的攻击大体上可分为:

①单攻击者发动的攻击(SAA,single adversary attack):攻击者入侵到网络中向合法节点发送大量数据,以耗尽合法节点的资源,同时占用节点通信所使用的信道。

②协同攻击(CAA,colluding adversaries attack):利用IEEE802.11协议的不公平性,两个或两个以上的攻击者直接向对方发送大量的数据,以占用附近的信道,致使其他的合法节点不能进行正常的通信。

Gupta[1]仿真并分析了几种SAA的攻击场景,提出了公平的MAC协议,以抵御DoS攻击,但是整体的吞吐量有所降低。Zhou Yihong[2]等人提出使用逐包验证机制来应对SAA攻击,但是会导致传输效率降低、能耗增加。对CAA攻击,Zhou Yihong等人还提出通过加入保护流来保护正常的通信流,但并没有验证其有效性。本文对CAA攻击进行了深入的研究,重点分析了基于保护流的解决方案,提出了保护流位

到稿日期:2010-05-11 返修日期:2010-07-29 本文受国家自然科学基金(60873265),广西青年科学基金(0832084),广西重点实验室主任基金(PF090109)资助。

叶 进(1970—),女,博士,教授,主要研究方向为计算机网络,E-mail:yejin@guet.edu.cn;李伶强 男,硕士生,主要研究方向为计算机网络。

置设计的原则和方法，并通过仿真验证了保护流设置方法。

3 802.11 协议的不公平性及保护流基本原理

802.11 协议的不公平性主要体现在两个方面。

①difs/eifs 时间机制：为了实现多路接入，802.11 协议使用了 3 个不同的时间空隙：短帧间间隔（*sifs*）、DCF 帧间间隔（*difs*）、扩展帧间间隔（*eifs*）。它们之间的关系可以表示为

$$difs = sifs + 2 * SlotTime \tag{1}$$

$$eifs = sifs + \frac{ACK_{framesize}}{BasicRate} + difs \tag{2}$$

sifs 是由物理器件所产生的间隙，而 *difs* 和 *eifs* 则是为了让节点了解信道状态而引入的时隙。很明显 *eifs*>*difs*>*sifs*。因此，如果一个节点只等待 *sifs* 时间后便进行下一个帧的传输，该节点接入信道的概率则会大大提升。

802.11 协议规定，一个节点在进行下一个数据包的传送前需要进行另外 3 个步骤：等待 *difs*/*eifs* 间隙，以确定信道的状态为空闲；开始退避；进行 RTS/CTS 交换。其中，如果一个节点能够正确地解码它所侦听到的最后一个帧，则它需要等待 *difs* 时间间隔，否则它需要等待 *eifs* 时间间隔以确定信道的状态。如果一个节点能够正确解码它所侦听到的最后一帧，则它相对于其它节点会有较高的信道接入权力。

②指数退避机制：为了避免各个节点之间的接入冲突，802.11 协议加入了指数退避机制。但这也同时导致了协议的另一个不公平性，主要体现在当发送端向接收节点发送了 RTS 或者是数据包，而没有收到接收端回复的 CTS 或者 ACK，则发送端将会以指数增大其退避窗口值，然后进行退避。在退避结束后，重新传送 RTS 或者是数据包。这就使得该发送端接入信道的几率大大降低。

基于 802.11 协议中上述的不公平性，Zhou Yihong 等人指出发动 CAA 攻击的最佳位置为网络的边缘。因此本文只分析攻击流在正常通信流的边缘发动攻击的场景。而我们所提出的保护流也正是利用协议中的上述不公平性而对攻击流发动攻击，致使其不能进行正常的通信，以达到保护正常通信流的目的。我们先定义两个性能对比参数 R_t 和 R_d 如下：

$$R_t = \frac{\text{加入保护流后正常流吞吐量}}{\text{加入保护流前正常流吞吐量}} \tag{3}$$

$$R_d = \frac{\text{加入保护流后正常流延时}}{\text{加入保护流前正常流延时}} \tag{4}$$

在本文的仿真中，使用的路由协议为 AODV，攻击流使用 UDP 协议，包的大小为 1k，被攻击流和保护流均使用 TCP 流。被攻击流通信时间为 1s～300s，攻击流攻击时间为 20s～240s，保护流保护时间为 30s～240s。

首先验证保护流的有效性。图 1 给出了一种引入任意保护流位置的拓扑结构。

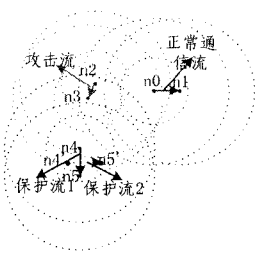


图 1 引入任意保护流的拓扑结构

在图 1 中，n0→n1 是一条正常通信的 TCP 流，攻击流 n2→n3 在其发送端 n0 处发动 DoS 攻击，因此将导致 TCP 流源节点 n0 因 DIFS/EIFS 机制而无法获得信道使用权。n4→n5 和 n4′→n5′为保护流 1 和保护流 2。在这种拓扑中，攻击流位于正常通信流和保护流 1 的发送节点干扰范围内，并处于正常通信流和保护流的接收节点干扰范围外。而保护流 2 的发送端和接收端的干扰范围则只覆盖攻击流的接收节点。分别加入保护流 1 和保护流 2 前后正常 TCP 流的性能对比如表 1 所列。

表 1 加入不同保护流后正常流参数对比

参数 / 保护流	吞吐量比较 R_t	延时比较 R_d	保护效果
保护流 1	0.506	1.102	差
保护流 2	3.671	0.869	良好

从表 1 吞吐量和延时的对比可见，图 1 中的保护流 1 也遭受到了攻击流所发动的攻击，而没达到保护作用。而在加入保护流 2 后正常通信流的吞吐量和延时都有明显的改善。可见对于保护流的位置必须合理地选择。

4 保护流位置的分析

当攻击流对正常通信流发动攻击时，引入的保护流是为了抵抗攻击流的攻击，即保护流应该处于能够对攻击流发动攻击，即使攻击流不能进行正常攻击的位置上。

攻击流对正常通信流发动攻击有两种情况：

①攻击流在正常通信流的发送端。

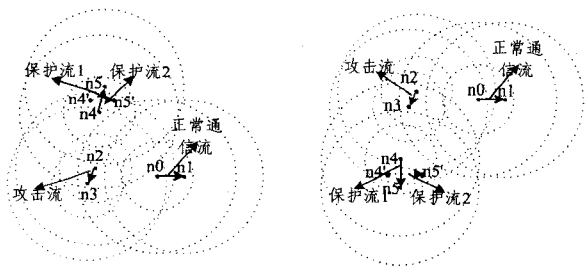
②攻击流在正常通信流的接收端。

本节旨在对以上推论进行验证，从中总结出提高保护流机制的有效性方法。根据以上的分析，我们分两种场景进行研究。

4.1 攻击流在正常通信流的发送端发动攻击

当攻击流在正常通信流的发送端发动攻击时，主要是利用了协议中的 DIFS/EIFS 机制。针对该类型的攻击，可以利用保护流在攻击流的发送端对攻击流发动相同类型的攻击，也可以利用指数退避机制在攻击流的接收端对攻击流发动攻击，以达到保护正常通信流的目的。

攻击流在正常通信流的发送端发动攻击的拓扑结构如图 2 所示。其中拓扑(a)为在攻击流的发送端加入保护流的拓扑结构，拓扑(b)则为在攻击流接收端加入保护流的拓扑结构。

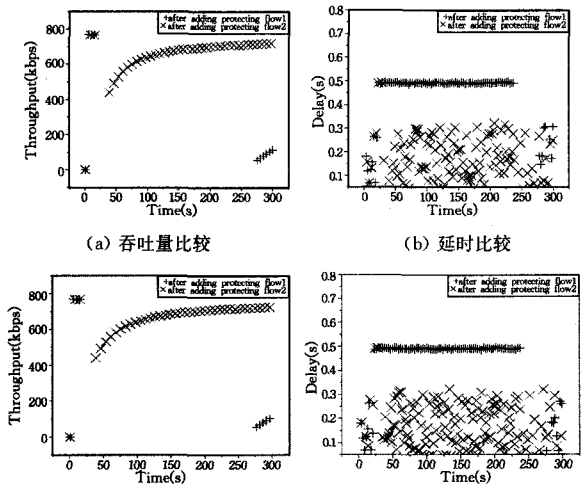


(a)保护流在攻击流的发送端　(b)保护流在攻击流的接收端

图 2 攻击流在正常通信流发送端攻击的拓扑图

在图 2(a)、(b)中，n0→n1 是一条正常通信的 TCP 流，攻击流 n2→n3 在正常通信流发送端 n0 处发动 DoS 攻击，将导致 TCP 流源节点 n0 因 DIFS/EIFS 机制而无法获得信道使用权。n4→n5 和 n4′→n5′为保护流 1 和保护流 2。攻击流位

于正常通信流和保护流 1 发送节点干扰范围内，并处于接收节点干扰范围外。在拓扑(a)中，保护流 2 发送节点和接收节点的干扰范围只覆盖攻击流的发送端；在拓扑(b)中，保护流 2 发送节点和接收节点的干扰范围只覆盖攻击流的接收端。在拓扑(a)、(b)中，加入保护流 1 和保护流 2 后正常 TCP 流的性能对比如图 3 所示。



(a) 吞吐量比较　(b) 延时比较

(c) 吞吐量比较　(d) 延时比较

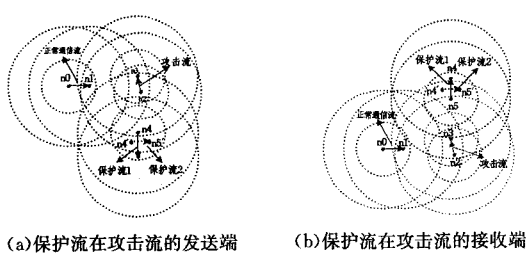
图 3　图 2 中正常流性能对比

在图 3 中，(a)图和(b)图为图 2(a)中在攻击流的发送端加入保护流 1 和保护流 2 后正常通信流的参数对比。(c)图和(d)图为图 2(b)中在攻击流的接收端加入保护流 1 和保护流 2 后正常流的参数对比。在图 2 的拓扑(a)中，加入保护流 1 后，正常通信流的性能对比为 $R_t=0.506, R_d=1.102$。加入保护流 2 后，正常通信流的性能对比为 $R_t=3.671, R_d=0.869$。在图 2 的拓扑(b)中，加入保护流 1 后正常通信流的性能对比为 $R_t=0.506, R_d=1.102$。加入保护流 2 后正常通信流的性能对比为 $R_t=3.673, R_d=0.438$。可见在图 2 的拓扑(a)、(b)中，保护流 2 达到保护效果，而保护流 1 则没有达到保护效果。

4.2　攻击流在正常通信流的接收端发动攻击

当攻击流在正常通信流的接收端发动攻击时，主要是利用了 802.11 协议中的指数退避机制，所以保护流可以利用该机制在攻击流的接收端对攻击流发动攻击，也可以利用 DIFS/EIFS 机制在攻击流的发送端对攻击流发动攻击，以达到保护正常通信流的目的。

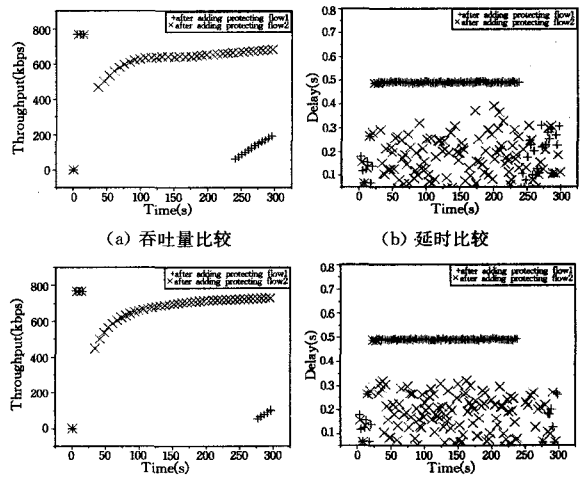
攻击流在正常通信流的接收端发动攻击的拓扑结构如图 4 所示。其中拓扑(a)为在攻击流的发送端加入保护流的拓扑结构，拓扑(b)则为在攻击流的接收端加入保护流的拓扑结构。



(a)保护流在攻击流的发送端　(b)保护流在攻击流的接收端

图 4　攻击流在正常通信流发送攻击的拓扑图

在图 4(a)、(b)中，n0→n1 是一条正常通信的 TCP 流，攻击流 n2→n3 在正常通信流接收端 n1 处发动 DoS 攻击，将导致 TCP 流源节点 n0 因指数退避机制无法获得信道使用权。n4→n5 和 n4′→n5′为保护流 1 和保护流 2。攻击流位于正常通信流接收节点干扰范围内、发送节点干扰范围外，并处于保护流 1 的发送节点干扰范围内、接收节点干扰范围外。在拓扑(a)中，保护流 2 的发送端和接收端的干扰范围只覆盖攻击流的发送端。而在拓扑(b)中，保护流 2 的发送端和接收端的干扰范围只覆盖攻击流的接收端。加入保护流 1 和保护流 2 后正常 TCP 流的性能对比如图 5 所示。



(a) 吞吐量比较　(b) 延时比较

(c) 吞吐量比较　(d) 延时比较

图 5　图 4 中正常流性能对比

在图 5 中，(a)图和(b)图为图 4(a)中在攻击流的发送端加入保护流 1 和保护流 2 后正常通信流的参数对比。(c)图和(d)图为图 4(b)中在攻击流的接收端加入保护流 1 和保护流 2 后正常流的参数对比。在图 4 的拓扑(a)中，加入保护流 1 后正常通信流的性能对比为 $R_t=0.982, R_d=1.003$。加入保护流 2 后正常通信流的性能对比为 $R_t=5.961, R_d=0.8$。在图 4 的拓扑(b)中，加入保护流 1 后正常通信流的性能对比为 $R_t=0.982, R_d=1.003$。加入保护流 2 后正常通信流的性能对比为 $R_t=6.474, R_d=0.425$。可见在图 4 的拓扑(a)、(b)中，保护流 2 达到保护效果，而保护流 1 则没有达到保护效果。以上的分析可归纳为表 2。

表 2　保护流位置及各参数对比

攻击流使用的机制及位置 \ 参数		保护流的位置		吞吐量比较 R_t	延时比较 R_d	保护效果
		保护流发送端	保护流接收端			
DIFS/EIFS 机制	图 3	覆盖	不覆盖	0.506	1.102	差
	(a)	覆盖	覆盖	3.671	0.438	良好
	图 3	覆盖	不覆盖	0.506	1.102	差
	(b)	覆盖	覆盖	3.673	0.869	良好
指数退避机制	图 5	不覆盖	覆盖	0.982	1.003	差
	(a)	覆盖	覆盖	5.961	0.425	良好
	图 5	不覆盖	覆盖	0.982	1.003	差
	(b)	覆盖	覆盖	6.474	0.8	良好

通过以上的分析可以得出结论：当攻击流对正常通信流发动攻击时，无论攻击流利用哪种机制，如果保护流的发送端或接收端的干扰范围可以覆盖到整条攻击流，而另一端的干扰范围却不能覆盖攻击流的任何一个节点，保护流就不会达到预期的保护效果。

结束语　本文分析和仿真了针对 MANET 中 MAC 层的

协同攻击。针对攻击流位置的不同，通过分析在加入保护流前后被攻击流的吞吐量和延时，最终指出保护流的合理位置。通过仿真可以看出，在适当的位置加入保护流可以有效地抵抗攻击流发动的攻击，达到保护正常通信流的效果。

参 考 文 献

[1] Gupta V. Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks[C]// Proceedings of MILCOM. 2002:7-10

[2] Zhou Yihong, Wu Dapeng, Nettles S M. On MAC-layer denial of service attacks in IEEE 802. 11 ad hoc networks: analysis and counter measures[J]. International Journal of Wireless and Mobile Computing, 2006, 1(3/4):268-275

[3] Tran T M C, Scheuermann B, Mauve M. Detecting the Presence of Nodes in MANETs[C]// Proceedings of the ACM MOBICOM. New York, NY, USA, 2007:43-50

[4] Mahajan R, Rodrig M, Wetherall D, et al. Analyzing the MAC Level Behavior of Wireless Networks in the Wild[C]// Proceeding of ACM SIGOCOM. Pisa, Italy, 2006

[5] 任伟，金海. 802. 11 移动 Ad Hoc 网络中针对 MAC 层的分布式拒绝服务攻击[J]. 计算机安全，2005，10:17-20

[6] 任伟，刘腾红，金海. 移动 Ad Hoc 网络中针对拥塞的 RoQ DDoS 攻击及其防御[J]. 计算机研究与发展，2006，43(11):1927-1932

(上接第 86 页)

线变化图。从图 3 可以看出，对于 IPv6 网络利用 IPv6 流标签进行路径控制，采用单程不等长包对的减法带宽测量方法对一条固定路径上的带宽进行测量，其误差可小于 0. 1M。数据表明，该测量结果真实有效。

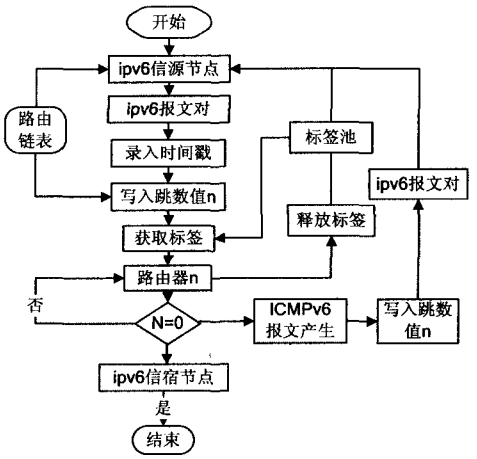


图 2 端到端带宽测量方法实现的流程图

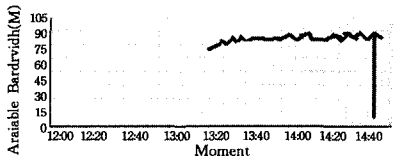


图 3 端到端可用带宽测量结果

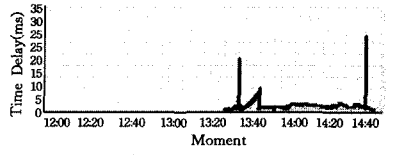


图 4 端到端时延测量结果

从图 3 和图 4 可以看出(由于篇幅有限，这里只列出代表性的一个对比图)，在一定的时间内，一条链路可用带宽值是比较稳定的。但是在 fri 08:00 左右时刻，网络可能有突发流量产生，导致可用带宽值短时间大幅度减少，出现尖刺现象，与此同时，网络延迟大幅度加大。这与实际网络运行是吻合的，说明该时刻，网络传输能力减弱，网络出现了一定的拥塞。此时通过对网络背景流量抓包的分析，发现是网络突发了近 20M 的异常流量，进一步分析得知，该链路的源主机开启了一路接近 20M 的高清视频点播，即时关闭该点播，网络恢复正常，拥塞现象得到改善。

结束语 本文提出了基于 IPv6 协议的单程不等长包对的减法带宽测量方法，结合 IPv6 报头的新字段流标签实现了测量报文序列的路径控制，编程实现了原型系统。特别是利用减法，消除了链路层、时差等因素对可用带宽测量结果精确性的影响。通过可用带宽与时延的实时对比，验证了两者之间的必然关联性，这对网络运行与维护中如何主动降低网络拥塞、重要应用带宽预留和网络性能监测有一定的实际价值。

参 考 文 献

[1] Hung Li-che, Chen Yaw-chung. Parallel table lookup for next generation internet[C]// Proceedings-International Computer Software and Applications Conference. 2008: 52-59. Proceedings-32nd Annual IEEE International Computer Software and Applications Conference. COMPSAC, 2008

[2] 卞静，周保良，张光昭. 可用带宽测量算法 PathPCQ 设计[J]. 中山大学学报：自然科学版，2007，46(3):14-16

[3] 刘敏，李忠诚，石晶，等. IPv6 网络中基于优先级的可用带宽测量方法[J]. 计算机研究与发展，2004，41(8):1361-1367

[4] 张文杰，钱德沛，栾钟治，等. Bing 算法测量网络带宽的研究与实现[J]. 小型微型计算机系统，2004，125(5):833-835

[5] 施金洋，林宇，金跃辉，等. 基于减法模型的端到端瓶颈带宽测量方法[J]. 北京邮电大学学报，2004(z1):10-15

[6] Strauss J, Katabi D, Kaashoek F. A measurement study of available bandwidth estimation tools[A]// Proc ACM InternetMeasurement Conference(IMC) [C]. Miami Beach, Florida, Oct. 2003

[7] Liu Min, Shi Jing-lin, Li Zhong-cheng, et al. A new end-to-end measurement method for estimating available bandwidth[C]// The 8th IEEE International Symposium on Computers and Communications. San Francisco: IEEE Press, 2003:1393-1400

[8] Lai K, Baker M. Measuring link bandwidths using a deterministic model of packet delay[C]// SIGCOMM 2000. Stockholm: ACM Press, 2000

[9] Liu Min, Li Zhong-cheng, Guo Xiao-bing. An end-to-end available bandwidth estimation methodology[J]. Journal of Software, 2006(01)

[10] Saroiu S, Krishna G P, Steven D. Gribble SProbe: a fast technique for measuring bottleneck [J/OL]. http://sprobe ce. Washing ton. Edu/sprobs. Ps, 2007-03-24

[11] Liu Min, Shi Jing-lin, Li Zhong-cheng. A new end-to-end measurement method for estimating available bandwidth[M]. San Francisco: IEEE Press, 2003