基于公平MAC协议的RTS注入攻击的防御方法

叶 进 王正飞 聂东举 张向利
(广西无线宽带通信与信号处理重点实验室 桂林 541004)
(桂林电子科技大学信息与通信学院 桂林 541004)

摘 要 针对WLAN环境下对AP的RTS注入攻击方式,引入虚拟队列管理机制,提出了基于公平MAC协议的解决方案。与已有的方案相比,该方案只需要在AP上部署,算法简单有效,具有良好的工程可行性。仿真结果表明,该方法能够有效抵御RTS攻击且对MAC层其它形式的DoS攻击也具有普遍意义上的防御性。

关键词 MAC协议,无线网络,RTS攻击,802.11
中图法分类号 TN929.5 **文献标识码** A

Fair MAC Protocol Based RTS Injection Attack and Defense

YE Jin WANG Zheng-fei NIE Dong-ju ZHANG Xiang-li
(Guangxi Key Laboratory of Wirelese Wideband Communication & Signal Processing, Guilin 541004 China)[1]
(School of Information and Communication, Guilin University of Electronic Technology, Guilin 541004, China)[2]

Abstract This paper focused on RTS injection attacks to access point in WLAN. A solution based on fair MAC protocol was proposed, which utilizes virtual queue management. Compared with the existed schemes, our solution is of simplicity and feasibility to be deployed at AP. Simulation results show that our solution can defense against RTS attacks effectively. The proposed fair MAC protocol can also help to defense against other types of DoS attacks.

Keywords MAC protocol, Wireless network, RTS attack, 802.11

1 引言

随着无线局域网(Wireless Local Area Network, WLAN)的广泛应用,其安全性也越来越受到重视。DoS(Denial of Service)攻击又称拒绝服务攻击,是一类破坏网络服务的攻击行为,其目的是使被攻击的主机或者网络无法及时接收和处理外界的请求而导致网络吞吐量急剧下降。RTS(Request To Send)攻击泛指利用IEEE802.11中的RTS/CTS(Clear To Send)机制漏洞而发起的以恶意占用信道为目的的攻击。RTS攻击可以采取多种方式,既可针对AP(Access Point),也可针对移动节点;既可单独利用RTS来实现,也可利用RTS/CTS来实现[1]。显然,RTS攻击也属于DoS攻击的范畴。本文中所指的RTS攻击是在WLAN环境下的针对AP的RTS注入攻击方式。

MAC(Media Access Control)层的DoS攻击主要表现为:攻击者通过伪造特定类型的控制帧侵入网络,消耗合法节点的资源(包括能量和服务能力)或恶意占用有限的信道资源[2]。以RTS攻击为例,攻击者入侵网络后不断发送伪造的RTS帧至某合法节点,从而造成该节点信号覆盖范围内的其他节点无法访问信道,导致大面积的拒绝服务攻击,而该节点也会因为不停地回复CTS包而快速消耗电量。无线节点的能量是有限的,如果节点一直回应虚假的请求,那么该节点的能量就会很快耗尽。

目前,针对MAC层的RTS攻击,可以采用加密的方法来防御。文献[3]提出使用逐包验证机制来抵抗单节点入侵攻击。其原理为:先假定密钥已经通过安全的信道发送到每个合法节点中,验证过程则集中于RTS和CTS控制帧的交换过程中。如果一个节点通过拒绝回复CTS控制帧的方式来拒绝转发数据包,或者是该节点所发送的RTS控制帧含有错误的信息,则该节点被定为攻击节点。文献[4]提出按需逐跳源认证协议,该协议是专门针对不稳定的无线网所设计的,可以以较高的概率过滤垃圾数据,而且可以确保合法节点的数据安全转发。其他的方法有:文献[5]中提出的使用RTS有效性验证的方法,即在接收到一个RTS控制帧后,开始退避RTS_DEFFER_TIME,若退避结束信道仍然空闲,并没有数据包的传输,则丢弃该RTS控制帧;若有数据传输,则按原退避时间进行退避。文献[6]提出在AP处使用CTSR算法来抵抗RTS攻击,即在AP收到一个RTS控制帧后对其回复CTS并侦听信道是否空闲,若源节点有数据包传送过来则不采取任何措施;若侦听到信道空闲,AP便广播一个NAV

本文受国家自然科学基金项目(61163060),国家科技支撑计划项目(2012BAH18F03),广西区重点基金资助项目(2011GXSFD01802),广西科技开发项目(桂科攻12118017-2C),桂林市科技开发资助项目(20120104-13),广西区研究生创新基金(YCSZ2012069)资助。

叶 进(1970-),女,博士,教授,主要研究方向为网络协议优化,E-mail:yejin@guet.edu.cn;王正飞(1989-),男,硕士生,主要研究方向为网络安全;聂东举(1988-),男,硕士生,主要研究方向为计算机网络;张向利(1968-),女,博士,教授,主要研究方向为物联网技术、网络化监控系统、计算机应用。

(Network Allocation Vector)位置0的CTS控制帧,其他的节点收到该CTS控制帧后,便会将自身的NAV置0,这样所有节点便重新开始竞争信道。

但是上述几种方法也有自身的局限性。如文献[3]提出的逐包验证机制要求各个节点在每次RTS和CTS控制帧的交换过程中都要进行加密和解密,这显然会影响MAC层数据帧的收发速度,并可能引起拥塞。文献[4]提出的按需逐跳源认证协议则只能在使用DSR(Dynamic Source Routing)路由协议的链路中使用,但目前多以AODV(Ad hoc On-Demand Distance Vector Routing)路由协议为主。文献[5]中所提出的防御方案则需要对合法节点所使用的协议进行修改,并且只对RTS半连接攻击起作用。文献[6]提出的机制在广播NAV位置0的CTS帧后显然会在节点间引起新一轮的信道争用。总之,端到端的认证能在一定程度上防御针对MAC层的单节点攻击,却对协同攻击无能为力。

因此本文提出公平MAC协议的防御方法,旨在通过动态调节各节点的接入次数使各节点获得公平使用信道的权力,从而遏制因MAC层RTS攻击而产生的网络拥塞。在我们先前的工作中,已经对MAC层DoS攻击中的保护流位置做了详尽的分析,并提出了基于保护流的防御方法[7]。本文主要研究在AP上部署公平MAC协议,使得各个接入节点能够公平地享用信道,从而达到防御WLAN中MAC层RTS攻击的目的。

2 IEEE 802.11的不公平性问题

IEEE 802.11协议为无线网络的物理层和MAC层提供了接入标准,它在MAC层定义了两种工作方式:分布式协调功能(Distributed Coordination Function,DCF)和点协调功能(Point Coordination Function,PCF)。IEEE 802.11标准规定,所有的实现都必须有DCF功能,而PCF只作为可选模式,因此,我们将IEEE 802.11 DCF作为研究WLAN MAC层机制的基础。IEEE802.11MAC协议的不公平性主要体现在以下两个方面[8]。

(1)由帧优先级机制引起的不公平性。为了实现多路接入,IEEE 802.11DCF中使用了3个不同的时间空隙:短帧间间隔(Short InterFrame Space,SIFS)、分布式协调功能帧间间隔(Distributed Coordination Function IFS,DIFS)、扩展帧间间隔(Extended IFS,EIFS)。它们之间的关系如下:

$$DIFS=SIFS+2*SlotTime \tag{1}$$

$$EIFS=SIFS+\frac{ACK_{framesize}}{BasicRate}+DIFS \tag{2}$$

在式(1)和式(2)中,SIFS是最短的帧间间隔,用来分开属于一次对话的各帧。DIFS是在DCF工作模式下要发送数据前所必须等待的时间。EIFS则是节点在接收到损坏帧后需要等待的时间。由式(1)和式(2)可知EIFS>DIFS>SIFS,因此,若一个节点只等待SIFS时间间隔后就进行下一个帧的传输,便会大幅提高该节点接入信道的概率,同时抑制其他节点的接入需求。

(2)由二进制指数退避(Binary Exponential Backoff,BEB)机制引起的不公平性。为了避免各个节点之间在接入AP时争用信道,802.11协议引入了BEB机制,即当发送端向接收端发送了RTS帧或数据帧后却没能收到接收端回复的CTS帧或ACK时,发送端将会以指数级增大其退避窗口值,并在退避结束后重传刚才发送的帧。这将使该发送端再次接入信道的概率大幅降低。

目前,国内外针对IEEE 802.11MAC协议公平性的研究主要集中在对CSMA/CA机制的改进上,并且提出了许多改进的方案,主要有基于信道感知型和非信道感知型[9]。

基于信道感知型的改进方案的基本思想是:节点通过感知到的信道信息计算出当前的网络信息(空闲时隙数、竞争节点数、信道状态等),并据此来动态调整自身的行为(调整争用窗口大小、传输速率)。文献[10]分析了功率约束的方法,以提高RTS/CTS机制的有效性。文献[11]提出FMAC/CSR协议解决节点接入AP的公平性问题。这类改进方案存在两个难点:一是如何计算出相应的网络信息;二是如何调整节点的行为。

非信道感知型改进方案主要是利用802.11协议栈自身的反馈信息(TCP拥塞控制等)来调整节点自身的行为。比如,利用AIMD(Additive Increase Multiplicative Decrease)[12,13]、PISD(Proportional Increase Synchronized multiplicative)[9]等。

上述两类方法能够在一定程度上解决无攻击情况下MAC协议的公平性问题,但是算法复杂,不利于在节点或AP上部署。

3 基于公平MAC协议的RTS攻击防御解决方案

在正常的网络通信活动中拥塞是不可避免的。对于这种由网络自身资源(带宽、路由器性能等)有限而引起的拥塞,人们已经找到了一些相应的拥塞控制机制,如慢开始、快重传、随机早期检测、显示拥塞通告等[14]。但是,如果拥塞是因MAC层的RTS攻击而造成的,那么上述的拥塞控制机制就显得无能为力,而且IEEE 802.11本身的不公平性将使得这种攻击很快达到抢占信道、拒绝服务的目的。当WLAN受到RTS攻击时,其AP会收到大量来自攻击者的RTS帧。而IEEE 802.11协议中的退避机制规定当前发包失败的节点其退避窗口要翻倍,而当前发包成功的节点其退避窗口回到最小值。这就造成了攻击者更容易持续占用信道,加剧了攻击的效果。

本文提出的RTS攻击防御的公平MAC协议的基本思想是:通过在AP上部署公平MAC协议,动态地调节网络中各节点的接入次数,使各个节点享有公平使用信道的权力。为了进一步描述该算法,我们定义了一个ADT(Abstract Data Type),如下所示:

ADT FMA_VQ\\FMA:Fair MAC Algorithm,VQ:Virtual Queue

{Object:struct VQ={address,threshold,num,j},string rec

(把虚拟队列看成操作对象,其地址、门限值、RTS帧数目、连续翻转次数作为元素)

\\ address:节点的源地址

\\ threshold:该节点的门限值

\\ num:收到来自该节点RTS包的数目

\\ j:该节点门限值增加的次数

\\ rec:记录上一次收到RTS包中的源地址

Relation:

$R_1=\{N_i \rightarrow addr, i\in 1,\cdots,n \mid \langle addr, rec\rangle, \langle addr, threshold, num\rangle, \langle addr, threshold, j\rangle\}$

Operation:

Find_VQ(VQ. address, record)

操作结果:在缓存中查找虚拟队列,并记录下此次查找到的地址,返回结果。

Add_VQ(VQ. address)

操作结果:增加相应的虚拟队列。

If_num(VQ. address, VQ. threshold, VQ. num)

操作结果:判断虚拟队列中的 RTS 帧计数器的值是否大于该队列当前门限值。

Reply_CTS(VQ. address)

操作结果:向节点回复 CTS 帧。

If_Doubled(VQ. address, record)

操作结果:判断此次接收 RTS 帧地址是否与前次相同

Update_threshold(VQ. address, VQ. threshold, j)

操作结果:生成新的队列门限值。

If_J(j)

操作结果:判断 j 值是否大于 3。

Rest_Threshold(VQ. address, VQ. threshold)

操作结果:初始化该虚拟队列的门限值

Clearall()

操作结果:清空缓存中的所有虚拟队列信息。

}

每个接入 AP 的节点都分配一个虚拟队列 VQ,FMA_VQ 中的 addr 不仅表示节点的源地址,还代表一个虚拟队列。

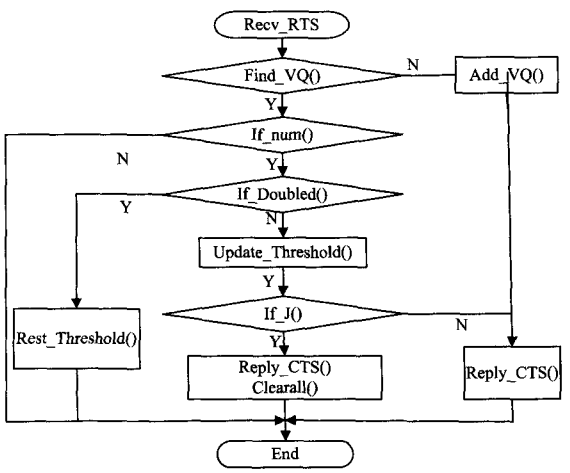

图 1 公平 MAC 协议工作流程

图 1 为我们提出的公平 MAC 协议工作流程。首先查看该流程有以下 4 个关键点:

(1)在 AP 上部署公平 MAC 协议。当节点 N_i 向接入点 AP 发送 RTS 控制帧预约信道时,AP 虚拟队列是否有节点 N_i 的 VQ_i,若有,则将其 RTS 控制帧计数器 $VQ.num$ 的值加 1;若无,则在 MAC 层记录下 N_i 的地址并建立对应的虚拟队列 VQ_i。以此类推,在 AP 的 MAC 层为每个向 AP 发送 RTS 控制帧的节点建立对应的虚拟队列,并初始化缓存阈值为 1,即 $Thres_{min}=1$。

(2)AP 对虚拟队列 $VQ_1\cdots VQ_n$ 采用 AQM(Active Queue Management)的方式进行管理。当 AP 缓存中的队列数大于 1 时,激活公平 MAC 算法。即:当 VQ_i 中的 RTS 控制帧计数器 $VQ.num$ 达到或超过其对应的缓存阈值 $VQ.threshold$ 时,AP 对节点 N_i 回复 CTS 控制帧,允许节点 N_i 接入信道,同时清空 VQ_i($VQ.num$ 和 $VQ.threshold$ 清零);若 VQ_i 中的 $VQ.num$ 未达到其对应的阈值 $VQ.threshold$,则不进行任何操作。

(3)当节点 N_i 连续 2 次接入 AP 时(即图 1 中的 If_Doubled()判断当前收到的 RTS 帧的源地址是否与上次收到的相同,若相同则为连续 2 次接入 AP),VQ_i 的缓存阈值变化如式(3)所示:

$$Thres[N_i]=2^{VQ_i.j}\times Thres_{min}\quad VQ_i.j\in[0,3] \tag{3}$$

式中,$VQ_i.j$ 为对应节点 N_i 连续 2 次接入 AP 的次数,$Thres_{min}$ 为各节点的初始缓存阈值,$Thres[N_i]$ 为调整后 VQ_i 的缓存阈值。其中"连续"是指紧接着第一次接入后的第二次接入,而对于某节点非连续的多次接入,其队列缓存阈值是不会变化的。这实际上起到的作用是:对节点连续占用信道的行为进行提前预防。

(4)若在节点 N_i 接入期间还有其它节点同时接入 AP,则将 VQ_i 的缓存阈值恢复为初始阈值;若在节点 N_i 接入期间没有其他节点接入,则当 VQ_i 的缓存阈值连续翻倍超过 3 次(说明节点 N_i 至少连续接入了 6 次)后,AP 将清空其 MAC 层缓存中所有的地址存储列表及其对应的虚拟队列。

4 仿真实验

我们使用 NS2 仿真平台对提出的公平 MAC 协议进行仿真。在仿真实验中,启动 RTS/CTS 机制并采用大尺寸 UDP(User Datagram Protocol)流模拟对正常通信的 TCP(Transmission Control Protocol)流进行干扰和攻击(每个 UDP 包都需要通过 RTS/CTS 握手来发送),其中,"干扰"是指 UDP 流和正常通信的 TCP 流同时正常地接入 AP 的情况,"攻击"是指 UDP 流恶意地、连续地接入 AP 占用其信道的情况。

4.1 单节点攻击实验

实验的拓扑结构如图 2 所示。其中正常通信 TCP 流的时间设为 300s,UDP 流使用指数流量产生器,采用不同的发包时间模拟干扰 UDP 流和恶意攻击 UDP 流,干扰流 burst_time_设置为 200ms,idle_time_设置为 300ms,恶意流 burst_time_设置为 500ms,idle_time_设置为 1ms。干扰流和攻击流的区别在于发包速的度不同,idle_time 越小则发包速度越大,而发包速度越大则攻击强度越大。进一步地,对两种 UDP 流(记为 UDP1 和 UDP2)分别采用连续发包和脉冲发包两种方式,连续发包时间为:20~300s,脉冲发包时间为:20~100s,170~240s,速率设置为 1Mb/s。路由协议采用 AODV 协议。

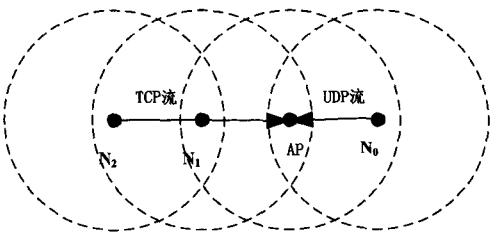

图 2 单节点攻击仿真实验拓扑结构

在图 2 中,N_2 到 AP 为一条正常通信的 TCP 流,N_0 到 AP 为一条干扰 UDP 流。对 AP 使用公平 MAC 协议前后,

TCP 流的吞吐量变化情况分别如图 3、图 4 所示。

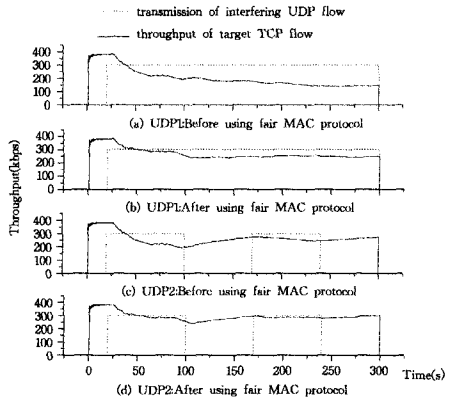

图 3　干扰 UDP 流下正常通信 TCP 流的性能

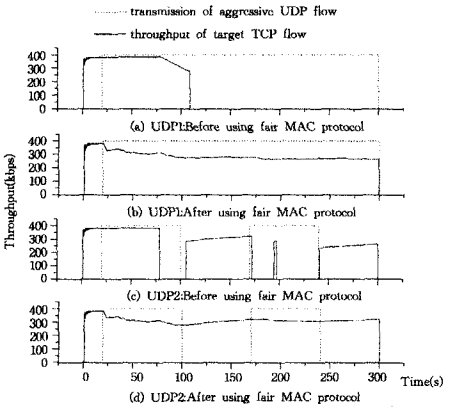

图 4　攻击 UDP 流下正常通信 TCP 流的性能

在图 3 中，虚线处于高位表示干扰 UDP 流通信时间。可以看出，在没有干扰流存在时，正常 TCP 流的平均吞吐量达到 350kbps。20s 后干扰流开始接入，在连续发包方式的 UDP1 干扰流的影响下，正常 TCP 流的吞吐量下降了接近 50%，如图 3(a)所示。启动公平 MAC 协议后，正常通信 TCP 流的吞吐量明显上升，并没有受到干扰流太大的影响，平均吞吐量达 320kbps，如图 3(b)所示。脉冲发包方式的 UDP2 干扰流开始接入后，脉冲发包周期内，正常 TCP 流的吞吐量呈持续下降趋势，脉冲发包周期之后，正常 TCP 流的吞吐量开始上升至正常水平，如图 3(c)所示。启动公平 MAC 协议之后，UDP2 干扰流的脉冲发包周期并没有对正常 TCP 流造成影响，如图 3(d)所示。

从图 4 可以看出，20s 后攻击流开始接入，在连续发包方式的 UDP1 攻击流的影响下，正常通信 TCP 流的吞吐量在 100s 后持续下降，并很快下降至 0，造成拒绝服务攻击，如图 4(a)所示。启动公平 MAC 协议后，正常 TCP 流的吞吐量虽然下降到 300kbps，但是能正常通信，呈现很强的鲁棒性，如图 4(b)所示。当 UDP2 攻击流采用脉冲发包时，正常通信 TCP 流在 75s 和 170s 左右被 UDP2 攻击流所覆盖，造成断流，攻击结束之后才开始恢复，如图 4(c)所示。在启动公平 MAC 协议后，UDP2 攻击周期期间，正常 TCP 流的的吞吐量并没有下降太多，更没有断流，如图 4(d)所示。

4.2　多节点攻击实验

实验的拓扑如图 5 所示，为简单起见，我们只部署了 2 个攻击节点(N_3 和 N_4)。其中节点 N_3 在 20s 时开始连续攻击，节点 N_4 在 40s 时开始连续攻击，其他配置同 4.1 节。

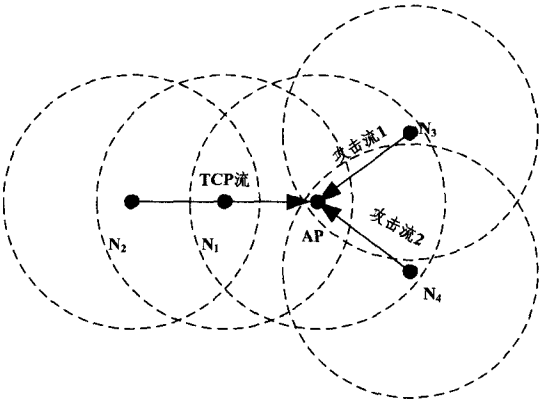

图 5　多节点攻击仿真实验拓扑结构

从图 6 中可以看出，20s 后，节点 N_3 开始攻击 AP，N_1 与 AP 通信的 TCP 的吞吐量立即下降到 0，造成拒绝服务攻击，如图 6(a)所示。启动公平 MAC 协议后，正常通信 TCP 流的吞吐量在加入攻击 UDP 流后虽然有些下降，但很快就能回升，仍能进行正常的通信，如图 6(b)所示。

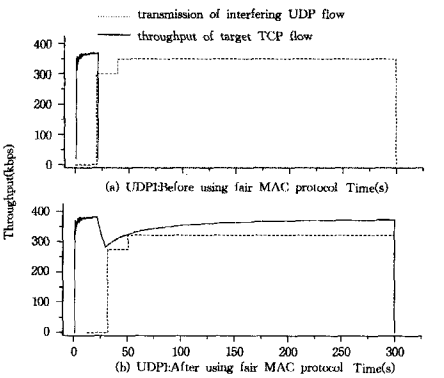

图 6　多条攻击 UDP 流下正常通信 TCP 流的吞吐量变化

4.3　实验分析

为了进一步描述使用公平协议前后正常通信 TCP 流的性能，我们定义参数 R_{thr}，它反映了在 AP 处使用公平 MAC 协议后网络平均吞吐量的提升程度。

$$R_{thr}=\frac{\text{使用公平协议后正常 TCP 流的平均吞吐量}}{\text{使用公平协议前正常 TCP 流的平均吞吐量}} \quad (4)$$

从表 1 的数据可以看出，在使用公平 MAC 协议后，即使 WLAN 遭受 DoS 攻击，正常 TCP 流的吞吐量都有比较明显的提升，尤其在多节点攻击的情况下更加明显。

表 1　性能对比总表

实验场景			图示	R_{thr}
单节点攻击	正常干扰 UDP 流	连续加入	图 4(b/a)	1.717
		脉冲加入	图 4(d/c)	1.103
	恶意攻击 UDP 流	连续加入	图 5(b/a)	2.577
		脉冲加入	图 5(d/c)	1.210
多节点攻击			图 6(b/a)	13.709

结束语　本文所提出的在 WLAN 环境下的基于公平 MAC 协议的 RTS 攻击防御方案最大的特点就是只需要在 AP 上部署，算法简单，具有良好的可行性，并且对 MAC 层的 DoS 攻击具有普遍意义上的防御性。我们的工作为在 AP 上实现该防御机制提供了理论支持，下一步将着手从工程实现的角度研究该防御机制在 AP 上的部署问题。此外，对于其他形式的 RTS 攻击(如针对移动节点的攻击、RTS-CTS 联合攻击)及其防御办法也将是我们今后研究的重点。

参 考 文 献

[1] 曹春杰,杨红娃,王巍.针对IEEE 802.11 CSMA/CA的RTS-CTS攻击[J].通信对抗,2009,4(4):32-35

[2] Gupta V, Krishnamurthy S, Faloutsos M. Denial of service attacks at the MAC layer in wireless Ad Hoc networks[A]// MILCOME[C]. 2002,2:1118-1123

[3] Zhou Y, Wu D, 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

[4] Gu Q, Liu P, Chu C H. Defense against packet injection attacks in unreliable Ad Hoc networks[A]// IEEE Global Telecommunications Conference[C]. 2005,3

[5] Ray S, Starobinski D. On false blocking in RTS/CTS based multihop wireless networks[J]. IEEE Transactions on Vehicular Technology, 2007, 56(2): 849-862

[6] Acharya, Thuente M D. Intelligent jamming attacks, counterattacks and(counter)2 attacks in 802.11b Wireless Networks[A]// OPNETWORK-2005 Conference[C]. 2005

[7] 叶进,李伶强.基于保护流的MANET网MAC层DoS攻击及防御[J].计算机科学,2011,38(4):118-121

[8] Karamad E, Ashtiani F. A modified 802.11-based MAC scheme to assure fair access for vehicle-to-roadside communications[J]. Computer Communications, 2008, 1: 2898-2906

[9] Jian Y, Zhang M, Chen SG. Achieving MAC layer fairness in CSMA/CA networks[J]. IEEE/ACM Transactions on Nnetworking, 2011, 19(5): 1472-1484

[10] Xu Kai-xin, Gerla M, Bae S. How effective is the IEEE 802.11RTS/CTS handshake in Ad Hoc networks[A]// IEEE GLOBECOM[C]. 2002, 1: 72-76

[11] Li Z F, Gupta A K, Nandi S. FMAC/CSR: a fair MAC protocol for wireless Ad-hoc networks[OL]. http://www.ntu.edu.sg/home5/pg03802331/papers/fmaccsr%20final.pdf

[12] Heusse M, Rousseau F, Guillier R, et al. Idle sense: An optimal access method for high throughput and fairness in rate diverse wireless LANs[J]. ACM SIGCOMM, 2005, 35(4): 121-132

[13] Grunenberger Y, Heusse M, Rousseau F, et al. Experience with an implementation of the idle sense wireless access method[A]// ACM CoNEXT[C]. 2007,24

[14] Tanenbaum A S. Computer netwokrs[M]. Beijing: Prentice-Hall International, Inc., 1997

(上接第355页)

表3 一些常用常数的连分数的精确度分析

	精度要求	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}	10^{-8}
π	最佳逼近	3	$\frac{22}{7}$	$\frac{22}{7}$	$\frac{333}{106}$	$\frac{333}{106}$	$\frac{355}{113}$	$\frac{355}{113}$	$\frac{355}{113}$
e	精度要求	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}	10^{-8}
	最佳逼近	3	$\frac{11}{4}$	$\frac{19}{7}$	$\frac{106}{39}$	$\frac{193}{71}$	$\frac{1264}{465}$	$\frac{2721}{1001}$	$\frac{2721}{1001}$
$\sqrt{2}$	精度要求	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}	10^{-8}
	最佳逼近	1	$\frac{7}{5}$	$\frac{17}{12}$	$\frac{41}{29}$	$\frac{239}{169}$	$\frac{577}{408}$	$\frac{1393}{985}$	$\frac{3363}{2378}$
$\sqrt{3}$	精度要求	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}	10^{-8}
	最佳逼近	2	$\frac{7}{4}$	$\frac{26}{15}$	$\frac{71}{41}$	$\frac{265}{153}$	$\frac{989}{571}$	$\frac{3691}{2131}$	$\frac{5042}{2911}$
普朗克常数	精度要求	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}	10^{-8}
	最佳逼近	$\frac{13}{2}$	$\frac{20}{3}$	$\frac{53}{8}$	$\frac{762}{115}$	$\frac{762}{115}$	$\frac{3101}{468}$	—	—
基本电荷	精度要求	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}	10^{-8}
	最佳逼近	$\frac{3}{2}$	$\frac{5}{3}$	$\frac{8}{5}$	$\frac{141}{88}$	$\frac{149}{93}$	$\frac{598}{367}$	—	—
万有引力常数	精度要求	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}	10^{-8}
	最佳逼近	7	$\frac{367}{55}$	$\frac{367}{55}$	$\frac{367}{55}$	$\frac{754}{113}$	$\frac{1875}{281}$	—	—

注:表3中的无理数都是通过保留小数点后50位来进行分析的,其中物理领域中的万有引力常数 $G=6.67259\times10^{-11}\,N\cdot m^2/kg^2$,重力加速度 $g=9.80665 m/s^2$,普朗克常数 $h=6.6260755\times10^{-34}J\cdot S$,基本电荷 $e=1.60217733\times10^{-19}C$,在分析中,只考虑小数部分。因篇幅问题,表中只分析每个实数的前几个渐进分数的精确度。

结束语 本文通过对小数有理化的整体研究与分析,给出了一些常用的数学、物理与工程计算常数的连分数表示和各个渐进连分数的误差,这样就可以根据计算精度的要求确定最佳渐进分数。我们将进一步研究如何在这些渐进分数表示的基础上设计一种分数的整数化表示的最终实现实数的整数化表示。

参 考 文 献

[1] Gianantonio P D. Real Number Computability and Domain Theory[J]. Information and computation, 1996(127): 11-25

[2] Wiedmer E. Computing with infinite objects, Theoret[J]. Comput. Sci., 1980(10): 133-155

[3] Wu Zheng-peng, Wang Da-yuan, Qiu Ro-bin, et al. Dynamic Simulation for Hotel Service Industry Based on Continued Fraction[C]// ICSSI. 2010

[4] http://www.nsfc.gov.cn/nsfc/cen/xmzn/2013xmzn/01/01sl/001.html

[5] http://www.nsfc.gov.cn/nsfc/cen/xmzn/2012xmzn/01/06xx/001.html, 2012

[6] http://www.nsfc.gov.cn/nsfc/cen/xmzn/2011xmzn/01/06xx/001.html, 2011

[7] http://www.nsfc.gov.cn/nsfc/cen/xmzn/2010xmzn/01/06xx/001.html, 2010

[8] http://www.nsfc.gov.cn/nsfc/cen/xmzn/2009xmzn/01/06xx/001.html, 2009

[9] http://www.nsfc.gov.cn/nsfc/cen/xmzn/2008xmzn/01ms/06xx/001.html, 2008

[10] Rosen K H. 初等数论及其应用(第5版)[M]. 夏鸿刚,译. 北京:机械工业出版社,2009

[11] Strassen V. The computational complexity of continued fractions [C]// Proceeding SYMSAC '81 Proceedings of the fourth ACM symposium on Symbolic and algebraic computation. NY: ACM Press, 1981: 51-67

[12] 王丹华,杨海文,刘咏梅. 初等数论[M]. 北京:北京航天航空大学出版社,2008

[13] 潘承洞,潘承彪. 简明数论[M]. 北京:北京大学出版社,2005

[14] Silverman J H. 数论概论(第3版)[M]. 孙智伟,吴克俭,卢青林,等译. 北京:机械工业出版社,2008

[15] 何光. 实数的连分数展开及程序设计[J]. 重庆文理学院学报,2012,1(31)

[16] Vuillemin J. Exact Real Computer Arithmetic with Continued fractions[J]. IEEE Transaction on computers, 1990, 39(8): 1087-1105