无线VoIP系统MAC层RoQ攻击仿真研究

李鹏勇
山西阳城广播电视局　阳城　048100

摘　要　随着无线VoIP技术的不断发展，其安全问题倍受关注。通过介绍无线VoIP系统MAC层的RoQ攻击原理，用网络仿真工具NS2模拟了RoQ攻击。实验结果表明，RoQ攻击大量占用无线信道资源，使语音数据包丢失以及网络延迟明显增大，进而导致无线VoIP用户无法使用语音服务。

关键词　无线VoIP；RoQ攻击；IEEE802.11；MAC

引言

VoIP(Voice over IP)，也称为IP电话或网络电话。它将语音信号编码压缩后，打包成IP封包的形式，利用IP网络传送语音信号。VoIP与传统电话相比，语音质量基本相同但资费低廉。近年来无线接入Internet技术如雨后春笋般迅猛发展，使得无线局域网(WLAN)在人们生活中得到普及，这为无线VoIP技术的产生奠定了的基础。无线VoIP结合VoIP资费低廉和无线局域网移动灵活方便的特点，使其在通信领域逐渐崭露头角。

在无线VoIP得到广泛应用的同时，其安全问题倍受人们的关注。RoQ攻击、DoS攻击、语音窃听、垃圾语音邮件、中间人攻击、服务窃取等都对无线VoIP系统产生严重的威胁。因此，对无线VoIP的安全问题进行研究具有重要的现实意义。如何检测与防御各类攻击成为目前无线VoIP研究的热点之一。

本文将对无线VoIP的RoQ攻击进行研究。所谓RoQ攻击，即降低质量攻击，是攻击者通过某种方法消耗系统有限的资源，从而使系统向合法用户提供的服务质量大大降低。RoQ攻击与DoS攻击较为相似。两者在攻击原理上具有相同的地方，都是通过某种方式来消耗系统有限的资源。不同之处在于它们的攻击效果。DoS攻击会耗尽系统资源，以致于系统不能向合法用户提供服务；而RoQ攻击则严重消耗但不耗尽系统资源，使得系统提供给合法用户的服务质量大大降低，最终致使用户不能享受到一定的服务质量而主动放弃服务。DoS攻击通过发送大量数据包来耗尽系统资源，攻击速率较高，很容易被监控软件发现并过滤。而RoQ攻击的平均攻击速率比DoS低，能避开一般监控软件的检测，具有隐蔽性强的特点。综上所述，RoQ攻击具有低速率攻击、隐蔽性强、攻击方法简单而效果显著等特点，对实时性网络业务影响较大。

在无线环境下，信号通过无线电波传输，在信号所覆盖的范围内，任何用户都可以接触到数据。这使得无线网络的安全变得相对比较薄弱，像RoQ之类的攻击更容易实施。

本文将研究基于IEEE802.11协议的无线VoIP系统MAC层的RoQ攻击，分析攻击原理，并利用NS2网络仿真工具对攻击进行模拟，详细讨论其对无线VoIP系统产生的影响。

1　MAC层基本原理[1]

近年来，无线局域网得到了迅速发展，其中IEEE802.11是目前最主流的无线局域网协议。IEEE802.11的MAC层分为上下两层来控制访问信道。上层是中心协调机制(Point Coordination Function，PCF)，为可选机制；下层是分布式协调机制(Distributed Coordination Function，DCF)。

PCF基于集中控制的接入算法，通过接入控制点(一般为AP)控制用户的轮询。通过使用PCF模式，整个过程被分为竞争周期(Contention Period，CP)和非竞争周期(Contention Free Period，CFP)的相互重复

交替。每个站点在CP阶段采用DCF机制竞争接入无线信道，而在CFP阶段，采用PCF机制，通过AP轮询发送数据，站点之间不会产生冲突。因此，PCF机制有利于传输实时业务数据，但是在实际应用中，PCF模式的效果不尽如人意。文献[2]指出，在实时业务较少且竞争信道的非实时业务不多时，采用PCF模式可以使网络性能达到较好的水平。但是随着实时与非实时网络负载的增加，它们的传输性能却变得很差，导致综合网络性能严重下降，不能满足网络负载的传输要求。此外，IEEE802.11标准规定PCF为可选模式，大多数无线网络产品并不支持它，因此，在配置无线局域网时，往往会选择DCF模式接入Internet。

DCF机制通过使用载波监听/冲突避免(CSMA/CA)机制，使各个终端通过竞争来获取信道。该机制通过物理层的载波监听功能或MAC层的虚拟载波监听(Virtual Carrier Sense)机制完成信道状态的检测。当信道由忙变闲时，各终端必须等待一个DIFS(Distributed InterFrame Space)的帧间间隔时间，并执行相应的退避算法，计算随机退避时间以便再次接入无线信道。CSMA/CA的退避算法，见图1。

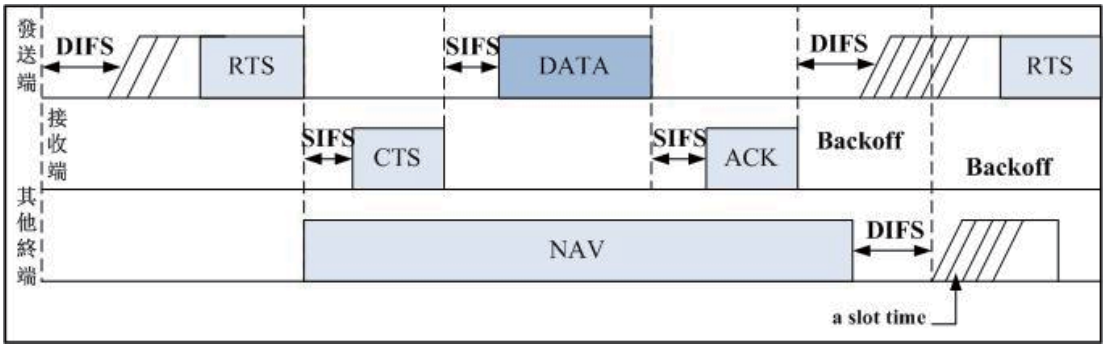

图1 CSMA/CD退避算法示意图

各终端在[0，CW]区间内随机选择一个数，CW表示竞争窗口(Contention Window)的大小，且CW∈N(N为自然数集合)。通过上面所选择的随机数来计算退避时间Tbackoff = Random(0,CW)* slot time。Slot time为协议时隙，是IEEE802.11标准定义的一个固定时间。当检测到信道处于空闲状态的时间超过DIFS时，终端将启动退避计时器。当退避计时器倒数为零并且信道仍为空闲时，就开始通过传输RTS(Request To Send)和CTS(Clear To Send)数据包来保留信道。发送端首先发送RTS包到接收端，接收端则发送CTS包给发送端作为响应。RTS和CTS数据包都包含占用信道所需的时间值，其他的终端会根据该值来调整自己的网络分配向量NAV(Network Allocation Vector)值，该值表示避免信道冲突的时间。随后，发送端发送DATA数据包，当正确接收后，接收端发送ACK包作为响应。此时发送端的CW值将重置为CWMin(Minimum Contention Window)。如果发送端没有收到CTS或ACK包，则其CW值将会加倍，直至达到预设的CWMax(Maximum Contention Window)值[3]。

2 无线VoIP系统MAC层RoQ攻击

在众多的攻击策略中，DoS和RoQ攻击是无线VoIP系统最大的安全威胁。

文献[4]提出了基于SIP协议的DoS攻击模型，讨论有线VoIP终端和SIP服务器的DoS攻击。对VoIP终端的DoS攻击采用了伪造SIP协议中的CANCEL和BYE信令来中止合法用户的正常会话。对SIP服务器的DoS攻击采用发送大量伪造错误数据包来消耗服务器资源，致使VoIP终端无法正常注册而不能进行会话。

文献[5]详细列举了针对VoIP系统的DoS攻击类型。例如请求泛洪(Request Flooding)、错误请求和信息

(Malformed Requests and Messages)、QoS滥用(QoS Abuse)、虚假信息(Spoofed Messages)。通过上述这些攻击都可使VoIP系统陷入瘫痪状态。文献[5]还列举了针对网络服务的DoS攻击，这些攻击同样能使VoIP系统陷入瘫痪状态。

这两篇文章分别从固定网络、SIP协议及VoIP系统等多方面较全面地介绍了各种针对VoIP系统的DoS攻击。但是随着无线VoIP的出现，专门针对无线VoIP系统的新型RoQ及DoS攻击也不断发生。本文将讨论一种针对无线VoIP系统MAC层的RoQ攻击。该攻击通过修改IEEE802.11标准的MAC层参数，较长时间地占用无线信道，致使合法无线VoIP用户在竞争无线信道时处于劣势，语音质量严重下降，甚至无法实现通信。

2.1 无线VoIP中MAC层RoQ攻击原理

IEEE802.11MAC层采用了CSMA/CA机制有效避免节点接入无线信道时的冲突，并通过合理竞争，使各节点能够高效地使用信道，但是这种机制也存在安全隐患。RoQ攻击通过修改MAC层参数，可以达到降低服务质量的攻击目的，其攻击方式主要以脉冲式为主[6]。

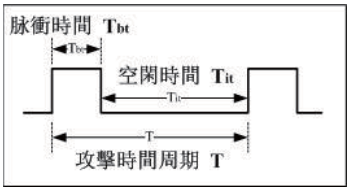

图2 RoQ脉冲攻击方式

图2描述了脉冲攻击方式，其中T为攻击时间周期，即两次连续攻击脉冲之间的时间间隔。T=Tbt+Tit，Tbt为脉冲时间，也称忙时，此时攻击者发动高速率攻击，攻击速率为R；Tit为空闲时间，简称闲时，此时攻击者不发送任何数据包，因此，攻击节点瞬时攻击速率r可以用数学表达式表示为：

$$\text{瞬时攻击速率 } r=\begin{cases} R & \text{忙时} \\ 0 & \text{闲时} \end{cases} \text{速}$$

即使攻击速率R较高，但由于RoQ攻击采用脉冲方式，整个周期的平均攻击速率R_{avg}并不很高。通过公式$R_{avg}=(L*R)/T$可知，RoQ的平均攻击速率R_{avg}仅为攻击速率R的L/T(T>L)倍。正由于其平均攻击速率不高，不易被一般的检测软件所发现，所以该类攻击对系统产生较大的安全威胁。

2.2 针对MAC层RoQ攻击类型

无线VoIP的MAC层可能受到的RoQ攻击有下面几种[7]：

1）RTS Pulsing攻击。IEEE802.11为了解决站点隐藏以及报文碰撞的问题，采用了RTS/CTS报文控制机制。节点通过发送RTS和CTS数据包来保留信道。该攻击则利用了此机制，周期性地向目标节点发送大量的RTS数据包，从而周期性地占用信道，致使无线信道利用率下降，严重影响语音通话质量。

2）NAV Spoofing攻击。与RTS Pulsing攻击类似，NAV Spoofing攻击也通过发送大量的RTS数据包到目标节点。不同的是，NAV Spoofing攻击修改了自己的NAV值，通过发送较大NAV值的RTS数据包来长时间占用信道。该攻击严重浪费了信道资源，使得其他合法节点无法及时接入信道而增大了网络延时。

3）SIFS Spoofing攻击。攻击者通过修改MAC层相关通信模块程序，将短帧间隔SIFS(Short Inter Frame Space)值设置得更小，使得攻击节点可以优先接入无线信道，造成了不公平使用信道的现象，最终影响大量无线VoIP用户的正常使用。

4）CW Spoofing攻击。该攻击利用了CSMA/CA退避机制，修改并使用较小的CWMin值，使攻击节点优先占用无线信道，致使其他合法无线VoIP节点在竞争信道中处于劣势，从而导致通话质量严重下降。

上述几类RoQ攻击，其本质都是通过修改IEEE802.11的MAC层参数，实现优先并长时间占用无线信道，致使合法用户得到的服务质量大大降低。本文仅以CW Spoofing攻击为例，使用NS2进行模拟，重点分析其对无线VoIP系统所产生的影响。

3 模拟与分析

本文采用NS2[8]对攻击进行模拟。NS2受到DARPA支持，并由USI/ISI、Xerox PARC、LBNL和UC Berkeley等美国大学和实验室合作开发，是基于离散事

件驱动的网络模拟工具。

NS2能够仿真多种网络类型的性能，并支持多种协议。如传输层的TCP、UDP协议；应用层的FTP、Telnet协议；还支持Protail、RED等路由队列管理机制，以及动态路由、静态路由等多种路由算法。NS2主要是基于Unix平台，通过使用TCL语言来编辑模拟场景的脚本。其源代码全部公开，为用户提供了开放的接口，也使得NS2更容易配置和扩展。

为了获得与实际网络环境相似的模拟实验场景，我们的模拟符合如下几点要求：

1）能够模拟具有Internet特征的负载流量；

2）能够模拟具有无线VoIP通信过程的数据流量；

3）能够实现网络拥塞的随机性。

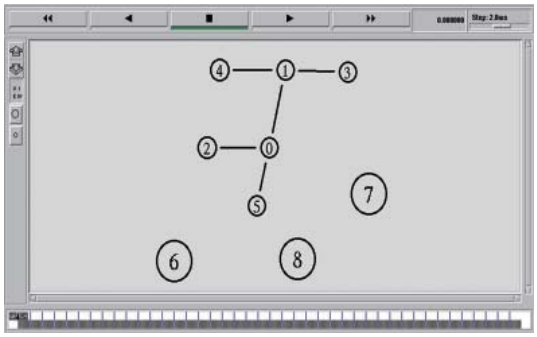

图3　模拟实验拓扑结构图

根据上面的要求，我们设计的实验场景如图3所示。节点0、1、2、3、4、5为有线网络通信节点。其中0、1为路由节点，连接0、1节点的链路为瓶颈链路；2、3为网络背景流量产生节点；4为有线VoIP用户；5为无线AP，为无线用户提供接入Internet的服务。6为合法无线VoIP用户；7使用无线网络访问Internet。8为发起攻击的节点。

实验场景的参数设置如下：信号传输方式为TwoRayGround；接口管理采用PriQueue；天线模式选择OmniAntenna；接入点AP的无线路由协议采用DSDV；MAC层协议采用IEEE802.11b，其数据传输速率为11Mb/s，详细的MAC层参数设置，见表1。

3.1　网络背景流量模型[9]

Internet流量中，不仅有语音等实时业务数据包，还有WWW等非实时业务数据包。为了使模拟实验的效果与实际网络环境的效果相似，我们需要在模拟环境中构造出与实际网络背景流量相似的数据流量模型。

表1　无线VoIP系统MAC层详细参数设置表

参数名	数值	参数名	数值
dataRate_	11Mb	Slot Time	0.000010s
basicRate_	2Mb	SIFS	0.000020s
CWMin_	31	DIFS	0.000050s
CWMax	1023	PF	2

下面简单介绍WWW流量的特性。用户从打开网页到关闭网页，经历如下三个过程：发送请求、接收数据、发送响应。研究表明[9-10]，用户发送请求的间隔符合指数分布，接收到的数据包大小呈现重尾分布，致使WWW数据流具有自相似的特性。在数学上，最简单的重尾分布就是Pareto分布。我们采用NS2自带的Pareto分布来描述WWW业务的数据包大小。详细的参数设置，见表2。

表2　WWW业务详细参数设置

参数	函数表达	数值
数据包大小	Pareto分布	10kb
数据包发送速率	常数	1Mb/s
用户请求间隔	指数分布	1

3.2　无线VoIP业务流量模型[10]

无线VoIP用户的整个通话过程可以分为两个过程，一个是通话过程，一个是静音过程。我们可以用0/1分布函数来描述。在通话期间，无线VoIP的数据流量为恒定速率流量，其速率为Rvoice。而在静音过程没有数据流产生。在模拟实验中，我们采用了ITU-T的语音编码压缩标准G.729。

语音信号经过编码压缩后，成为20个字节的语音数据包，再加上RTP、UDP及IP包头后，其大小达到60个字节，然后以24kb/s的速率在Internet上进行数据的传输。

无线VoIP的呼叫间隔和呼叫持续过程符合指数分布。模拟实验中，我们使用NS2自带的具有指数分布特性的流量发生器EXPOO_Traffic模拟呼叫间隔与持续过程。一般情况下，平均语音活动时间为1.67s，而平均语音静音时间为2.5s。具体的参数设置，见表3。

表3　无线VoIP业务详细参数设置

参数	函数表达	数值
语音平均活动时间	指数分布	1.67s
语音平均空闲时间	指数分布	2.5s
传输速率	常数	24kb/s
数据包大小	常数	480bit

3.3　模拟RoQ攻击流量

RoQ攻击采用脉冲攻击方式。在模拟过程中，设置其攻击周期T为500ms，其中脉冲时间Tbt为100ms，空闲时间Tit为400ms，忙闲比为1：4。攻击速率R在不同的攻击环境下取不同的数值。

模拟开始30s后，攻击节点向随机目标节点发送大小为1000bit的UDP数据包。

4　模拟结果分析

4.1　衡量标准[10]

衡量无线VoIP语音质量的标准有以下两方面：

4.1.1　语音数据包单向传输延迟

根据ITU－T的G.114[11]对VoIP推荐的传输延迟标准，传输延迟小于150ms为人们所能接受的范围，详细划分，见表4。

表4　语音延迟等级

好	较好	一般	可以忍受	不能忍受
<=50ms	50～70ms	70～90ms	90～150ms	>150ms

在模拟实验中，我们在节点4测量无线VoIP节点6产生的语音数据包单向传输延迟。

4.1.2　语音数据包的丢包率

无线VoIP的语音数据包以UDP形式在IP网络中传输。UDP是一个不可靠的传输协议，当丢包发生后，发送端不会再重发丢失的数据，在无线VoIP中表现为通话断续。数据包丢失将影响通话效果。一般认为，丢包率小于3%为可以忍受的范围。丢包率大于3%则严重影响通话质量，属于人们不能忍受的范围。

4.2　模拟结果及分析

通过实验模拟，我们可以看到，在没有受到攻击的情况下，语音数据包延迟，如图4所示。其平均延迟为64.07ms，最大延迟为88ms，整体通信效果良好。图5描述了在正常情况下AP节点接收到数据包的情况。横坐标表示时间，纵坐标表示1秒钟内到达AP点的数据包个数。

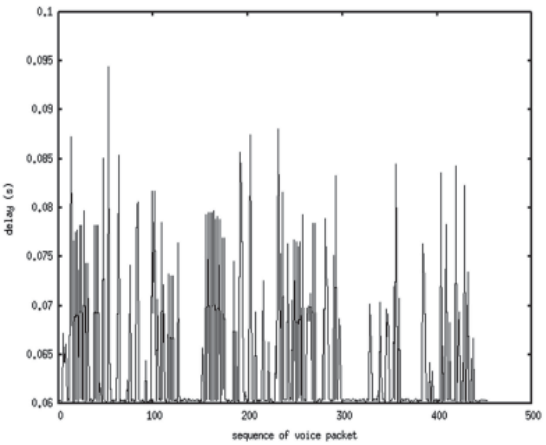

图4　正常情况下的无线VoIP语音延迟

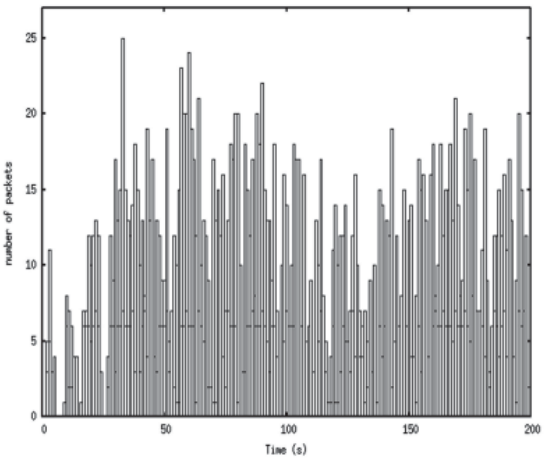

图5　正常情况下AP节点接收数据包的直方图

当无线VoIP系统遭受到RoQ攻击时，语音数据包延迟增加、丢包率加大，通话质量有所下降。攻击节点从第30秒开始发送大量的数据包进行攻击，语音数据包的延迟情况，如图6所示。虚线左边的时间段为正常情况，虚线右边为受到CW Spoofing攻击后的情况。

从图6可以看出，受到CW Spoofing攻击(CWMin=15，R=1Mb/s)后，语音数据包延迟显著增加，其平均延迟增加至72.61ms，最大延迟达到218.66ms。AP点接收到的数据包情况，如图7所示。显然受到攻击后，AP节点接收到的数据包数目增多，大量的攻击数据包占用了无线信道资源。

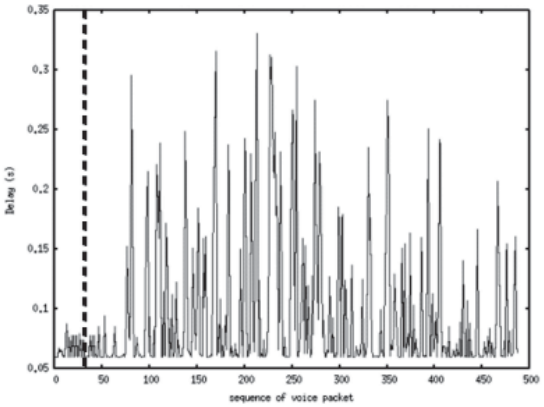

图6　R=1Mb/s时，无线VoIP语音通信延迟

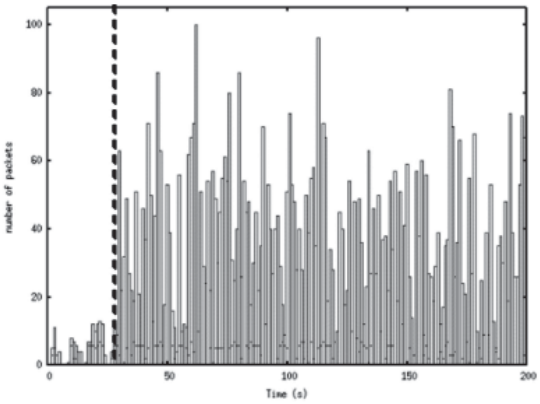

图7　R=1Mb/s时，AP节点收到数据包直方图

接下来深入讨论CW　Spoofing攻击对无线VoIP系统产生的影响。本文设计了两个实验场景。实验场景一：攻击节点修改CWMin值，攻击速率R不变；实验场景二：改变攻击速率R，CWMin值不变。

在场景一中，攻击节点保持攻击速率R为2Mb/s，平均攻击速率为1/5×2Mb/s=400kb/s。表5给出了不同CWMin值对无线VoIP系统的影响情况。

从表5中可以看到，当将CWMin值减小时，无线VoIP系统的服务质量（QoS）受到影响。影响程度随CWMin值的减小而增大。

表5　RoQ攻击对无线VoIP系统的影响(实验场景一)

CWMin值	无线VoIP语音平均延迟(ms)	语音数据包丢包率
CWMin=15	93.807751	0.84%
CWMin=20	92.429368	0.54%
CWMin=25	91.962987	0.39%
CWMin=31	90.558982	0.42%

在场景二中，CW　Spoofing攻击节点的CWMin值为15。改变攻击速率R，实验结果见表6。CWMin值保持不变，增大攻击速率R，语音数据包延时不断增加，丢包率不断增大。当攻击速率达到3Mb/s时，平均延迟达到121.29ms，包丢率为2.95%，有超过1/4的通信时间处于不能忍受的状态。当攻击速率R达到5Mb/s时，平均延迟达到156.61ms，丢包率为14.97%，此时无线VoIP用户将无法实现语音通信。总的来说，随着RoQ攻击速率的变大，其对无线VoIP系统产生的影响也越来越大。

5　总结

本文介绍了无线VoIP系统MAC层的RoQ攻击原理，使用NS2网络仿真软件模拟了CW　Spoofing攻击情况，讨论了该攻击对无线VoIP系统的影响。模拟结果表明，RoQ攻击对无线VoIP系统产生了严重影响。今后的工作将继续探讨RoQ攻击，并深入研究如何在无线VoIP系统中检测与防御该类攻击。

表6　RoQ攻击对无线VoIP系统的影响(实验场景二)

攻击速率		0kb/s	1Mb/s	2Mb/s	3Mb/s	4Mb/s	5Mb/s
语音	好	0.2%	0%	0%	0%	0%	0%
	较好	82.4%	67.0%	57.1%	49.5%	47.7%	45.8%
延迟	一般	17.2%	20.1%	13.3%	13.9%	10.9%	8.7%
	可以忍受	0%	10.4%	13.9%	10%	9.70%	9.6%
等级	不能忍受	0%	2.5%	15.7%	26.6%	31.7%	35.9%
	平均延迟(ms)	64.07	72.61	93.81	121.29	134.04	156.61
百分	最大延迟(ms)	88.07	218.66	150.86	525.89	519.85	535.74
比(%)	最小延迟(ms)	32.03	60.23	69.90	60.22	60.23	60.21
丢包率(%)		0%	0%	0.61%	2.95%	6.28%	14.97%

参考文献

[1] IEEE P802.11.Standard for Wireless LAN Medium Access Control(MAC)and Physical Layer(PHY)Specifications,1997

[2] 付晓蕊,张连芳.具有最低竞争吞吐率保证的准入控制算法[J]. 软件学报, 2005,16(7)

[3] 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):20-23

[4] 郑康锋,杨义先,钮心忻,等. 针对VoIP系统的拒绝服务攻击研究[D].2005通信理论与技术新进展:第十届全国青年通信学术会议论文集.北京:北京邮电大学出版社,2005

[5] VoIP Security and Privacy Threat Taxonomy[EB/OL](2005-10)[2009-11-10]. www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf

[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):77-82

[7] A Kuzmanovic,E W Knightly.Low-rate TCP-targeted denial of service attacks. Proc of the conf on Applications,Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM2003).New York, 2003

[8] The Network Simulator version 2(NS2)[EB/OL](2006-3)[2009-11-10].http://nsnam.isi.edu/nsnam/index.php

[9] 时培昕,雷振明.Internet流量模型的研究[J].计算机科学.2004:31(2):26-29

[10] 杨光华,王行刚.基于网络模拟时的VoIP性能评价方法.计算机应用[J].2002,22(1):29-31

[11] ITU-T Recommendation G.114.One-Way transmission time,2003

作者简历

李鹏勇

山西阳城广播电视局工程师。

Simulation Research on RoQ Attack at MAC Layer in Wireless VoIP System

Li Pengyong | Radio and Television Bureau of Yangcheng, Yangcheng 048100, China

Abstract With the development of wireless VoIP technology, its security problem has been paid more attention recently. The Reduction of Quality (RoQ) attack principle at MAC layer in wireless VoIP system is discussed and the simulation of RoQ attack is implemented with NS2 (network simulation version 2). The experiment results show that RoQ attack wastes more resources of wireless channel to cause longer delays and more voice packet loss rate, thus, destroy common communication service.

Keywords Wireless VoIP; Reduction of Quality Attack; IEEE802.11; MAC