WLAN 环境下拒绝服务攻击问题研究

夏新军　俞能海　刘　洋
(中国科学技术大学信息处理中心,合肥 230027)
E-mail:ynh@ustc.edu.cn

摘　要　文章探讨了 WLAN 环境下的拒绝服务(DoS,Denial of Service)攻击问题,提出了一种通过修改短帧隙(SIFS,Short Inter Frame Space)进行 DoS 攻击的方法,实验表明这种攻击具有较高的攻击效率。同时,对最近出现的一种针对物理层的攻击进行了具体的实验,分析了其攻击机理及危害程度。最后,结合现有协议提出了一些解决方案及安全建议,用以增强无线局域网抵抗攻击的能力。

关键词　拒绝服务　无线局域网　攻击　安全

文章编号 1002-8331-(2005)25-0129-04　**文献标识码** A　**中图分类号** TP393.08

Research of DoS Attack in WLAN

Xia Xinjun　Yu Nenghai　Liu Yang
(Information Processing Center,University of Science and Technology of China,Hefei 230027)

Abstract: In this article we have discussed deny of service(DoS) attacks in the environment of wireless LAN(WLAN) and proposed a novel attack method by modifying the short inter-frame space(SIFS).It is shown that the proposed method is effective in attacking.We have also analyzed the scheme of an emerging attack method aimed at the physical layer and investigated its potential damage by experiment.In the last we have given some solutions and advices on how to enhance the ability of the WLAN in resisting attacks based on the existing protocols.

Keywords: DoS,WLAN,attack,security

1　引言

自无线局域网出现以来,其安全问题就倍受关注,随着无线局域网安全问题研究的逐步深入,其安全措施也逐渐完善[1]:WLAN 的安全防护最初是由 WEP (Wired Equivalent Privacy,有线等效保密)协议[2]提供,但是由于其核心算法 RC4 算法本身的缺陷以及密钥调度算法过于简单,没有达到预期效果;后来 Wi-Fi 联盟吸取了 802.11i 工作组的一些研究成果,提出了自己的安全协议—WPA(Wi-Fi Protected Access),它使用基于 802.1x-EAP 的认证,通过 TKIP (Temporal Key Integrity Protocol,临时密钥完整性协议)改善密钥调度,而且使用新的校验算法。与 WEP 协议相比,WPA 更为安全。但是,它为了兼容当前仍然广泛使用的硬件设备,并没有放弃 RC4 算法,使得 WPA 仍然存在安全隐患;802.11i 工作组制定的 802.11i 规范[3],其核心内容就是解决 WEP 协议存在的一系列安全问题,其基本内容有:摒弃 RC4 算法,使用 AES-CCMP+TKIP 作为新的加密算法,使用一种可以支持双向认证的认证协议。这无疑将为无线网络提供更好的防护。

但是,上面所述的各种安全协议对于 DoS 这样的恶意攻击都没有提出明确的防护措施。"冲击波"病毒的出现,使我们再次认识了 DoS 攻击的严重性。在无线环境下,首先,因为攻击者利用极少的资源就能显著影响一个 WLAN 内的合法用户的通信效率(比如微波炉,2.4GHz 无绳电话等设备都能给 WLAN 带来干扰);再次 WLAN 使用微波传输数据,其范围无法有效控制,理论上只要在信号的范围内攻击者就能够发起攻击,其隐蔽性好,检测难度大。因此针对 WLAN 的 DoS 攻击必须得到应有的重视。

针对上面的问题,本文下面将进行具体的分析与研究。首先,结合现有的研究成果分析几类 DoS 攻击,并进行了一些攻击实验,用以验证攻击的可行性及攻击效率;其次,给出一些的解决方法及安全建议。

2　无线局域网 DoS 攻击方法分析

这里将详细分析三类 DoS 攻击,前两类分别是物理层和 MAC 层上的 DoS 攻击,第三类是利用不完善的认证机制进行的攻击。其它的比如 power saving DoS attack[4]和那些利用强信号进行干扰的暴力 DoS 攻击,由于可行性和效率的原因,通常使用不多,不属于本文的研究范围。

2.1　物理层的一种 DoS 攻击

IEEE 802.11 协议定义了两种媒体访问控制协议用来实现对无线信道的访问控制[2]:一种采用基于分布式协调功能(DCF:Distributed Coordination Function)的竞争模式来实现异步通信方式;另一种采用基于点协调功能(PCF:Point Coordination Function)的非竞争模式来实现同步通信方式。PCF 方式可扩展性很差,工作效率很低,极少被采用。目前的

基金项目:国家自然科学基金重大项目:未来移动通信系统基础理论与技术研究资助研究课题(编号:60496314)

作者简介:夏新军,男,中国科技大学硕士研究生(在读),研究方向:无线局域网安全。俞能海,男,中国科学技术大学教授,主要研究方向为图像处理与多媒体通信,信息隐藏与信息安全。刘洋,男,中国科学技术大学博士研究生,研究方向:无线局域网安全。

802.11 无线设备基本上都是采用 DCF 方式进行通信。在 DCF 中 IEEE 802.11 采用载波侦听/冲突避免(CSMA/CA:Carrier Sense Multiple Access with Collision Avoidance)机制进行无线介质共享,它的基本思想是让发送方激发接收方发出一个短帧,使得接收方附近的站点可以监听到将要进行的传输,从而避免它们在这个期间内向接收站点发送数据。而这一机制的实现是通过物理层的空闲信道评估(CCA)程序来完成的。它通过接收信号能量的强弱来确定信道是否空闲,每当信道由空闲转为忙或由忙转为空闲时,物理层的子层 PLCP(Physical Layer Convergence Procedure)都产生一种基元:PHY-CCA.indicate(STATE),STATE 为状态变量,当 PLCP 检测到信道忙时,其值为 BUSY,反之,为 IDLE。

最近澳大利亚电脑危机紧急响应小组宣布了一种 DoS 攻击[5],这种攻击就是利用 CCA 工作机理和 802.11 物理层管理实体(PLME)提供的一种测试模式(PLME_DSSSTESTMODE)来实施的。它攻击的对象是物理层采用直接序列扩频(DSSS)工作方式的无线设备。包括采用 IEEE802.11,802.11b 和低速(低于 20Mbps)802.11g 标准的 DSSS 无线设备。

下面将进行具体的攻击实验,选用五台配有 Orinoco 系列无线网卡的笔记本电脑(其中一台作为攻击设备)和一个接入点设备(AP),所有的笔记本电脑都使用 liunx 操作系统。将它们放置于不同的房间,其网络拓扑结构如图 1 所示。

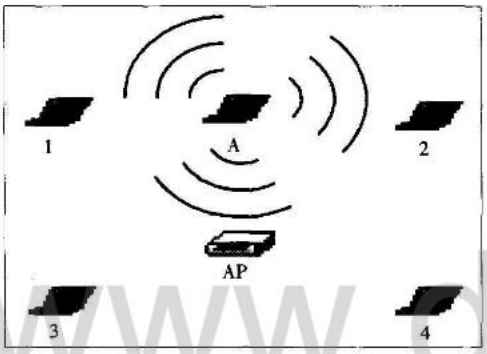


图 1 物理层的 DoS 攻击网络拓扑图

我们预先将攻击设备 A 的无线网卡设置为测试模式,这样它就可以连续发送 DSSS 信号。首先让 1 号与 2 号节点、3 号与 4 号节点分别建立 tcp 连接并开始通信,这时开启设备 A,让它连续发送测试信号,这时,我们观察到通信节点开始丢包以至于最后完全不能通信,同时我们发现,如果将 A 移动,使它离 AP 近一些,攻击效果会更明显。通过分析可以知道,攻击节点在选定的信道里连续地发送 DSSS 信号,这样,在攻击节点发射信号范围内的所有无线终端,包括 AP 的 MAC 层将收到 PHY-CCA.indicate(BUSY),这表明信道忙,数据传输将按照协议推迟进行,这种状态一直持续到攻击结束。该攻击方法简单,但效率很高,不需要特殊的设备与技术,另外,所使用的攻击设备无需高的发射功率,要发现并定位攻击者具有相当难度。

2.2 MAC 层的 DoS 攻击

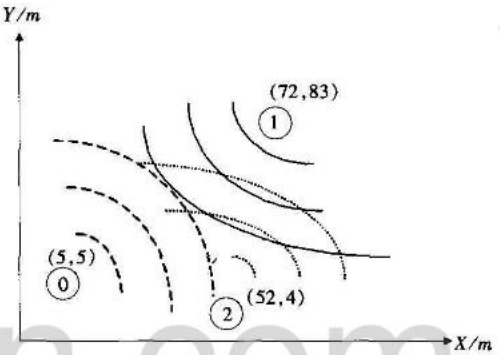
在 802.11 网络中,为了解决站点隐藏及报文碰撞等问题,采用了 RTS/CTS 等通讯控制机制,在 WPA 中采用消息完整性校验(MIC)机制[6]来防范伪造报文,这些机制在提高网络性能的同时,也带来了新的安全隐患。

2.2.1 利用 SIFS 实现的攻击

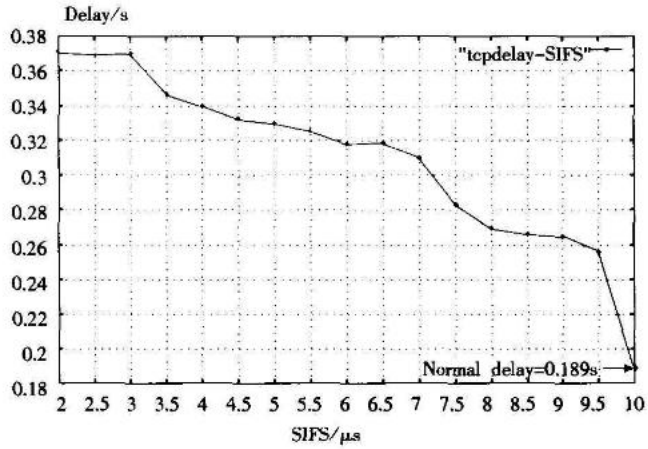
在 802.11 协议中,使用 CSMA/CA 技术来实现多路访问。为了避免一个节点长时间占用信道从而导致其他的节点无法传送数据,要求每个节点在发送完一个 MAC 层的协议数据单元(MPDU)之后都必须等待一个 SIFS(Short Inter Frame Space)时间,由此我们提出一种攻击方法,其核心思想就是通过修改攻击设备上的通信模块程序,将它的 SIFS 设得更短,那么在同等发包速率的情况下,攻击者将以很高的概率占有信道,从而使合法节点的通信推迟进行。

我们通过网络仿真软件 NS2 对这一想法进行了验证,实验中使用一台主频 2.5G、操作系统为 FreeBSD 的 Pentium4 电脑。攻击场景如图 2(a)所示,节点 1 和节点 2 为合法节点,其 SIFS 使用 802.11b 协议(物理层采用 DSSS)的缺省值 10μs。实验过程如下。

节点 1 与节点 2 之间建立 tcp 连接,攻击节点 0 以恒定速率向节点 1 发送数据包,数据包的大小与合法节点所发的数据包的大小基本相等。我们将节点 0 的 SIFS 值从 10μs 逐渐减小,记录并计算节点 1 和节点 2 之间的平均 tcp 时延,如图 2(b)所示:横坐标代表攻击节点的 SIFS 值,纵坐标代表节点 1 和节点 2 的 tcp 平均时延。从中我们可以发现,随着攻击节点的 SIFS 的逐渐减小,tcp 时延在不断增大。



(a)攻击场景



(b)SIFS-TCP delay 曲线

图 2 攻击场景及 SIFS-TCP delay 曲线

在实验中,我们为了比较合法节点与攻击节点竞争时隙的能力,使它们的发包速率相等。但在实际的网络中,攻击者通常会采用较快的发包速率,这样合法节点将较难抢到时隙来传送数据。为了便于说明问题,我们这里只列举了一对节点通信的

情况。我们利用这种方法还对多合法节点通信的情况进行了攻击模拟，实验结果表明，这种攻击方法是非常有效的。增加攻击节点的数目，合法节点间的通信将会变得更加糟糕甚至会使整个网络陷入瘫痪。

2.2.2 NAV 攻击[7]

CSMA/CA 为了解决隐藏节点问题引入了 RTS/CTS 控制机制，它能够为一个节点保留一定时间的信道。想要发送数据的节点首先必须向目的节点发送一个 RTS 帧，这个 RTS 帧中包含该节点的 ID 以及一个 duration 域，duration 域用于告知需要为该节点保留的随后数据传输所需要的时间，每个节点上都使用 NAV(Network Allocation Vector)来度量保留时间值，它的最大值为 $2^{15}-1=32\,767$，只有当 NAV=0 时该节点才可以发送数据，而这个值的更新是通过 duration 值进行的。目的节点一旦收到某个节点发来的 RTS 帧，就立即响应一个 CTS 帧，其中也包含 ID、duration 域，在信号覆盖范围内的其他的节点通过 CTS 帧来更新 NAV 值。这样可以解决由于隐藏节点造成的冲突问题。

这种 RTS/CTS 策略很容易引发 DoS 攻击。首先，我们知道 duration 域的设定是由发送节点决定的，如果增加它的值，那么其它节点的等待时间就会相应增加；其次，每个 802.11 帧中都包含 duration 域，因此攻击者有很多机会更改 duration 值。这样只要攻击者在自己发送的每个帧中都设置一个很大的 duration 值，就能使其它节点不能正常获得信道。这就造成了一种 DoS 攻击，参见图 3。这种攻击所需的资源要少得多，因为 duration 的最大值在 30ms 左右，这样差不多每秒发送 30 个帧就能够实现攻击。实际上，如果与合法节点进行“协作”，这种攻击持续的时间会更长，因为，如果攻击者不断发送包含较大 duration 值的 RTS 帧，那么，根据 CSMA/CA，收到 RTS 帧的合法节点会以 CTS 帧进行响应，响应后很快就会放弃对信道的控制，又因为合法节点要等待一个 SIFS 甚至一个 DIFS 后才能再次发送数据帧，而攻击者又不断发送 RTS，这样合法节点就很难抢到时隙，再加上这些节点对 CTS 的传播带来的影响，整个信道基本上将只会被攻击者占用，因此这种攻击会严重降低被攻击 WLAN 内节点的通信效率。

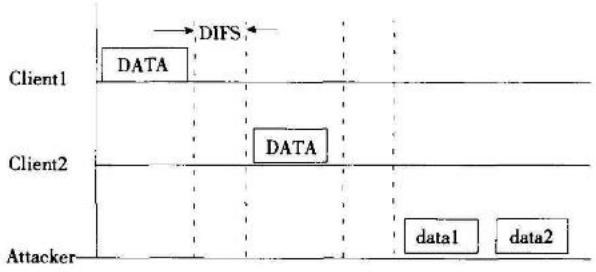


图 3 利用 Duration 实现的 DoS 攻击

2.2.3 Michael 攻击

我们知道，802.11 中的完整性校验值(ICV)的目的是为了保证数据在传输途中不会因为噪声等物理因素导致报文出错，因此采用了相对简单高效的 CRC 算法，但是攻击者可以通过修改 ICV 来使之和被篡改过的报文相吻合[8]，可以说没有任何安全功能；而 WPA 中的 MIC 则是为了防止攻击者的篡改而定制的，它利用 Michael 密钥并通过 Michael 算法求出一个 8 字节的消息完整性校验值(MIC)，加在每个数据分组(MSDU)后面，当一个无线客户或 AP 在一秒钟内收到两个或两个以上的 MIC 值有误的数据包，WPA 认为网络正在受到攻击，随后将采取一系列保护措施，包括中断通信一分钟，更换密钥等。下面将分析由此而可能引发的攻击。

首先，实现攻击的前提条件是伪造的报文要有正确 ICV 和初始化向量(IV)，因为接收方在收到报文后首先要核对报文的 ICV 和初始化向量(IV)，如果 ICV 不正确或 IV 值不大于前面已经收到报文的 IV 值，报文将会被直接丢掉，而不去检查它 MIC 值，从而也不会触发 MIC 错误保护措施。通过侦听和利用[8]中讲到的方法，攻击者是可以实现这个条件的。实际上，更简单的做法就是中途截获合法报文并阻止它发往目的节点，对此合法报文进行修改会更为方便。攻击者只需要每秒向目的节点发送至少两个这种 MIC 值有误的报文，就会使该节点触发 MIC 错误保护措施，中断通信一分钟，只要网络一恢复正常，攻击者就重复这样的攻击过程，最终将导致网络陷入瘫痪。

2.3 不完善的认证机制引发的 DoS 攻击

IEEE 802.11 标准提供两种类型的认证：开放系统认证和共享密钥认证。开放系统认证就其本质而言是一个空的认证过程，共享密钥认证基于一个预先共享的密钥，用 WEP 协议对客户进行认证：AP 发送一个质问串，并要求客户对其进行加密后返回，如果客户的响应被验证成功，则该客户通过验证。这一认证协议有着诸多公开化的缺陷[9]，攻击者可以利用这些缺陷对网络实施攻击。

2.3.1 网络接管

由于共享密钥认证是一种基于 WEP 协议的认证方法，如果攻击者同时知道了原始明文和相应的加密报文，那么就可以伪造认证报文。通过对无线网进行欺骗，攻击者可以积累许多验证请求，每个请求中包含有原始明文消息和相应的返回密文。进而，攻击者就可以很容易地破解出用来加密响应报文的密钥流来。然后利用这个密钥流可以伪造一个身份验证的报文，进而通过登录网络的身份验证，并且获许访问权。

现在假设一个非法用户通过上述方法绕过认证进入网络，那么他可以发送报文给路由设备和 AP，声称他的 MAC 地址是与一个已知 IP 地址相对应的。从那一时刻起，所有流经那个路由器并且目的地是被接管 IP 地址的通信量都将会传到攻击者的机器上。如果攻击者伪装成缺省网关或网络上某个特定的主机，那么所有希望连接该网络的机器或被欺骗的机器都将被连接到攻击者这里，而不是他们的目标机器。

另外，现行的 802.11 认证是单向的，即只用来验证无线客户，而不验证 AP。那么攻击者可以自己来伪装成 AP。一种方法是入侵者利用信号更强的 AP，放置在网络中，因为授权用户不能对 AP 的合法性进行认证，因此客户端就会无意识地连接到这个 AP 上来。一些对无线局域网友好的操作系统甚至在用户不知情的时候就会自动探测信号，然后建立连接。另一种假冒 AP 的方式是采用一些专用软件(如 HostAP)将入侵者的计算机伪装成 AP。这样，攻击者可以接收到身份认证的请求和来自终端工作站与密钥有关的信息，为进一步攻击准备了条件。同时，他可以发出大量的中止连接的命令，迫使周边用户断开与合法 AP 的连接，破坏正常的网络通信。

2.3.2 deauthentication 攻击[4]

在 802.11 认证协议里定义了一个认证请求帧(Authentication Request)，客户端(Client)可以通过发送这种帧请求接入网络，与认证请求帧相对应，协议里还定义了一个终止认证(deauthentication)帧，它用以结束认证，使认证双方回到非认证

状态。deauthentication DoS 攻击就是通过伪造 deauthentication 报文对无线局域网进行的攻击。如图 4 所示,Client 选定需要连接的 AP 后，首先由 Client 向 AP 发起认证请求 Authentication Request(或者由 AP 发起),接着 AP 向 Client 返回认证响应 Authentication Response，然后再进行后面身份验证。但是,由于此时认证双方都允许提出取消认证的请求来终止认证（因为 Client 和 AP 都可能因其它原因而不得不放弃认证),而且这个请求是不加密的,只是片面通知对方取消认证。所以,如果攻击者冒充客户端向 AP 发送了 deauthentication 报文,AP 则误以为是对方要终止认证，从而回应以 deauthentication 报文来终止认证过程。那么这以后客户端发来的报文将被 AP 视为非法而抛弃,攻击者如果长时间伪造这样的数据帧就能使得合法的节点长时间无法连接到该无线局域网中或不能进行正常的数据传输。

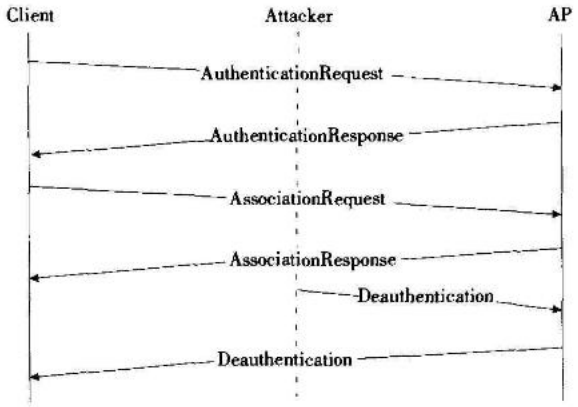


图 4 Deauthentication 攻击

相比之下,deauthentication DoS 攻击具有更大的灵活性。一方面发起这种攻击所需的数据量非常少,而且它所要求的对信道的干扰时间也少,隐蔽性比较好。另一方面,由于可以伪造针对某一个 client 的 deauthentication 数据帧,这样便可以阻止某个特定的 Client 访问网络,攻击的针对性很强,这样就可以配合其它的攻击方法实现危害性更大的网络攻击。

3 解决方案及安全建议

从上面的分析我们可以看出在 802.11 无线局域网中的确可以实现 DoS 攻击。随着无线局域网新的国际标准 IEEE802.11i 的正式颁布，由 WEP 造成的安全隐患基本消除,但 WLAN 环境下的 DoS 攻击却有上升的趋势，事实上现在已经发现了一些针对 IEEE802.11i 标准的 DoS 攻击，如 Michael 攻击及对四次握手的攻击[9]。因此 DoS 攻击问题应该引起我们高度的重视。结合上面对几种的 DoS 攻击的分析,我们给出一些解决方法及安全建议。

首先,增加检测和监控机制,对无线网络进行实时监控,随时剔除攻击节点。具体说就是在 AP 上集成一个入侵检测系统,监视网络数据,当网络长时间只被一两个节点占用时,触发检测模块,在检测模块中可以用简单的方法判断该节点是否为非法节点。因为 DoS 攻击要求攻击者大量地发送结构类似的数据帧，这样我们可以将连接关闭 1 秒钟然后重新开启连接,再判断该节点发送的后续数据是否和关闭连接之前类似,如果类似说明这是个节点是非法节点，然后可以利用 AP 的 MAC 过滤功能将它剔除。

其次,改进现行的认证协议,采用基于 802.1x 协议的认证方式,利用 802.1x 和 EAP(Extensible Authentication Protocol),实现用户与网络之间的双向认证;增加对每个数据帧,特别是像 deauthentication 这样的管理帧的合法性检验,例如可以加入信息完整性校验机制,使得 AP 与客户端都能够确定对方身份及所发报文的合法性。

另外,实现和升级防火墙,采用最新的杀毒软件,安装更新的安全补丁,配置诸如 AirMagnet 这样的 DoS 检测工具,对抵抗和防范 DoS 攻击,也会起到积极作用。

4 结论

本文在分析现行无线局域网标准的基础上,结合已有的研究成果,分析了在 WLAN 环境下的几种 DoS 攻击,并提出了通过修改 SIFS 值来进行攻击的方法,不难看出,WLAN 对于 DoS 攻击显得非常脆弱,我们应该修正现行协议中不合理的部分或者采用新的安全机制来保障 WLAN 的网络安全。从国内外最新研究也可以看出,针对 WLAN 的 DoS 攻击,目前还没有较为理想的防范机制,因此需要科研人员重视并致力于这方面的研究,以期建立更加安全高效的无线局域网。

(收稿日期:2005 年 3 月)

参考文献

1.Stanley Wong.The evolution of wireless security in 802.11 networks:WEP,WPA and 802.11 standards[S].SANS Reading Room,2003-07-11

2.L M S C OF THE IEEE COMPUTER SOCIETY.Wireless LAN medium access control(MAC)and physical layer(PHY)specifications[S].IEEE Standard 802.11,1999 Edition

3.IEEE 802.11i Group.IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11:Wireless LAN Medium Access Control(MAC)and Physical Layer(PHY)specifications Amendment 6:Medium Access Control(MAC)Security Enhancements[S].2004

4.John Bellardo,Stefan Savage.802.11 Denial-of- Service Attacks:Real vulnerabilities and Practical Solutions[S].11th USENIX Security Symposium,2003

5.Chris Wullems,Kevin Tham,Jason Smith et al.Technical Summary of Denial of Service Attack against IEEE 802.11 DSSS based Wireless LAN's.http://www.isrc.qut.edu.au/resource/techreport/wireless/

6.N Ferguson.Michael:an improved MIC 802.11 WEP.http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/2-020.zip,2002

7.Dazhi Chen,Jing Deng,Pramod K Varshney.Protecting Wireless Networks against a Denial of Service Attack Based on Virtual Jamming.http://www.sigmobile.org/mobicom/2003/posters/11-Chen.pdf

8.BORISOV N,GOLDBERG I,WAGNER D.Intercepting mobile communications:The insecurity of 802.11.MOBICOM 2001,2001

9.ChangHua He.1 Message Attack on the 4-Way Handshake.http://www.drizzle.com/~aboba/IEEE/