基于马尔可夫链的CSMA/CA接入攻击

王 巍 曹春杰
(通信信息控制和安全技术重点实验室 嘉兴 314033)
(中国电子科技集团公司第三十六研究所 嘉兴 314033)

摘 要 首先对CSMA/CA机制进行形式化建模,然后基于马尔可夫链从随机性能模型和带宽占用模型两方面给出了对其进行攻击的理论分析,在此基础上给出了对CSMA/CA机制的具体攻击方法。在仅掌握数据帧部分字段的情况下对接入机制攻击进行了实验,并对吞吐量、通信效率、碰撞次数几方面进行了性能分析。实验结果验证了利用马尔可夫链理论对CSMA/CA机制进行攻击分析的可行性和有效性。

关键词 马尔可夫链,CSMA/CA,接入机制攻击
中图法分类号 TP393 **文献标识码** A

Markov Chain Based Attack on the CSMA/CA Mechanism

WANG Wei CAO Chun-jie
(Science and Technology on Communication Information Security Control Laboratory, Jiaxing 314033, China)
(No. 36 Research Institute of CETC, Jiaxing 314033, China)

Abstract The CSMA/CA mechanism was formally modeled firstly. Based on the Markov Chain theory, the analysis of attack on CSMA/CA is introduced from two aspects, such as the stochastic performance model and bandwidth share model. After discussing the typical attack methods, the experiments was performed with the knowledge of partial fields in frames. The attack performance was analyzed by throughput, communication efficiency and collision numbers, which validated the feasibility and efficiency of attack method based on Markov Chain theory.

Keywords Markov chain, CSMA/CA, Access mechanism attack

1 引言

无线通信网络攻击对于研究网络安全有着十分重要的意义,众多研究者进行了大量相关工作的研究[1-9]。由于未来无线网络自组织、多节点、高带宽、突发通信的特点,固定多点接入技术如FDMA、TDMA等在应用时可能会受到限制,而类ALOHA机制的动态多点接入技术又由于其自身的吞吐量问题不适用于无线网络;CSMA/CA机制由于其自身具有实时性、可扩展性、支持突发通信、避免隐终端/暴露终端问题等特点,必会受到无线网络研究人员越来越多的关注。张君毅讨论了根据MAC协议的信息对Ad hoc网络进行智能阻塞攻击和欺骗干扰的单节点工作方式和多节点协同工作方式,比较了不同方式能够达到的干扰效果[5]。文献[10-12]通过伪造NAV值的违规行为节点周期性发送RTS帧和CTS帧来实现攻击,这种攻击的后果是在违规节点一跳范围之内的节点根据RTS帧和CTS帧中的NAV值字段错误地更新本地的NAV值,使其误认为信道繁忙,增加了它们接入信道的时延。曾弘毅等人提出了一种针对CSMA/CA的攻出模式,通过相关的网络仿真和数据处理,分析了该攻击模式的效用及其影响,同时提出一种衡量网络攻击效率的评价标准,最后分析了攻击方式和对随机退避算法的改进[13]。曹春杰等人针对IEEE 802.11 CSMA/CA提出了一种RTS-CTS攻击,攻击者通过修改竞争窗口,优先抢占业务信道。该攻击可使目标工作站或者网络接入点保持静默,甚至造成网络瘫痪[14]。

上述已有工作在技术方面讨论了针对CSMA机制进行攻击的可性能,但在理论分析方面还有待进一步探讨。本文重点针对CSMA/CA信道接入机制进行研究,通过理论分析和研究,讨论了针对CSMA/CA信道接入机制的攻击方法的可行性和有效性。

2 CSMA/CA接入攻击可行性分析

带冲突避免的载波侦听多路访问机制(CSMA/CA,Carrier Sense Multiple Access with Collision Avoidance)是未来无线网络的一种主要信道接入协议。该机制下,节点在发送数据时,首先监听信道的工作状态,如果信道忙,则延迟发送以避免数据碰撞。而延迟发送的随机时隙通常采用二进制指数退避算法产生,并且由各个通信节点自主随机选择,选到最小时隙的节点可接入信道发送数据。该协议假定通信节点都严格遵循协议规则随机选择时隙,但缺乏直接的控制机制,攻击者可以利用这一缺陷对网络通信进行攻击。

本文受国家自然科学基金项目(60872041,61072066)资助。

王 巍(1980—),男,博士,高级工程师,主要研究方向为网络攻击,E-mail:wwzwh@sohu.com;曹春杰(1977—),男,博士,高级工程师,主要研究方向为网络安全。

2.1 CSMA/CA 工作原理

在下面的分析中，假设无线网络环境中的所有节点都执行 CSMA/CA，并且所有的单播数据包都采用 ACK 确认，没有收到 ACK 则重新传输。CSMA/CA 主要涉及 RTS-CTS 握手和二进制指数退避两方面的内容。

RTS-CTS 握手：RTS 和 CTS 是 CSMA/CA 的控制帧，用于预约接下来的信道时隙。在发送实际的数据帧之前交换 RTS 和 CTS 是一种主要的信道预约方式，并且可以解决 CSMA/CA 基本访问方式存在的“隐终端”和“暴露终端”问题以及大量数据同时发送而导致的碰撞问题。RTS 和 CTS 帧包含持续时间字段，定义了数据帧及其 ACK 占用信道的时间。所有源站和目的站覆盖范围之内的工作站都会获得媒介预约信息。具体实现是：发送节点先监听信道，如果信道持续 DIFS(竞争服务帧间间隔)时间间隔都为空闲，它就发送一个 RTS 帧。否则在等到当前传输结束和接下来的一个 DIFS 时间间隔后激活二进制指数退避算法。当目的节点收到 RTS，在一个 SIFS(最短帧间间隔)时间间隔后它传送一个 CTS。当源站收到这个 CTS 后，等待一个 SIFS 时间间隔就可以发送 DATA 帧，目的站收到 DATA 帧，等待一个 SIFS 时间间隔就发送 ACK 帧，源站收到 ACK 帧后确认此次数据传送成功。所有其他监听到 RTS 和 CTS 帧的站，通过在 RTS 和 CTS 帧中的持续时间字段，更新它们的 NAV(Network Allocation Vector，网络分配矢量)值，并在该段时间内保持沉默。RTS 帧的持续时间字段中的值是 CTS 帧时间，加上 DATA 帧传输时间，加上 ACK 帧时间，加上 3 个 SIFS 时间间隔。CTS 帧持续时间字段是 DATA 传输时间，加上 ACK 帧加上两个 SIFS 间隔。所有节点在 NAV 值的时间段结束后(即此次数据传输已经结束)重新竞争信道。图 1 给出了 RTS-CTS 握手的示意图。上述 DIFS、SIFS 都由多个时隙 slot 组成。

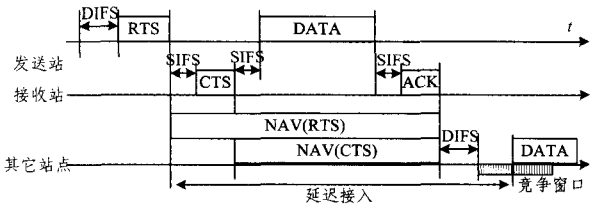

图 1 RTS-CTS 握手 2

二进制指数退避机制：对于要发送数据帧的节点来说，一旦发现链路忙，则激活退避过程。或者节点发送的帧没有收到 ACK，也要激活退避过程，生成一个等待时隙的递减计数器。执行退避过程的节点用载波监听机制决定每个退避时隙媒介是否空闲：如果空闲，则计数器为 -1；如果忙，则暂停计数器，等待媒介空闲时间达到 DIFS 或 EIFS 后，继续执行计数器。当计数器为 0 时，可以发送帧。

2.2 接入攻击可行性分析

首先给出一些符号说明，如表 1 所列。

表 1 符号说明

n	通信节点下标
$w=\langle w_{\min}, L\rangle$	退避配置信息
$w=(w_1,\cdots,w_N)$	配置集
t,c,s	一个时隙内的试图传输、冲突和成功概率
T,S	所有节点试图传输概率之和、成功概率之和
b	通信节点占用的带宽

我们首先通过介绍 CSMA/CA 的网络运行方式给出基于 Bianchi 马尔可夫链模型的单个节点带宽占用模型，然后扩展此模型以适应接入攻击下的 CSMA/CA 特性。

2.2.1 CSMA/CA 退避机制的形式化表述

退避机制是指网络节点在通信时一般处于等待状态，除非信道空闲了一段时长为 DIFS 的时间，当从等待状态恢复时，节点将自己的退避计数器置为[0，CW)间的随机数，这里 CW 是当前的退避窗口。最开始的时候，CW 被设置为一个最小值 $w_{\min}$。若在一个时隙 slot 内信道是空闲的，则退避计数器自减；一旦信道处于忙状态则将计数器的值固定不变，之后一旦信道再次空闲了一段时长为 DIFS 的时间后，节点就又恢复计算器的自减操作。若使用基本访问方法(非 RTS/CTS 模式)，当计数器为 0 时节点就开始传输数据帧。若传输成功，节点收到接收方的 ACK 并将 CW 置为 $w_{\min}$；否则，若多个数据帧冲突，每个数据帧的发送方得到冲突信息，将 CW 加倍，令退避计数器取[0，CW)间的随机数，开始下一次计数器自减操作。最短帧间间隔 SIFS 用来保证 DATA+ACK 的交互方式不被打断。在 RTS/CTS 访问机制中，节点当退避计数器为 0 时发送 RTS 帧，若成功，发送节点收到接收方的 CTS 帧，并发送数据帧。若多个 RTS 帧冲突，它们的发送方将收到冲突信息，并进行类似上述的操作。SIFS 同时能够保证 RTS+CTS+DATA+ACK 的交互方式不会被打断。

令 L 是竞争冲突后 CW 加倍的最大次数，即 $w_{\max}=w_{\min}\cdot 2L$，二元组 $w=\langle w_{\min}, L\rangle$ 称为节点的退避配置信息。

2.2.2 随机性能模型

考虑一个有 N 个节点的 Ad hoc 无线网络，其在 MAC 层使用 CSMA/CA 机制。假设网络节点运行在业务发送状态，也就是说一旦成功传输 DATA 帧，节点需要立即传输另一帧，即可以认为 N 个节点进行大文件传输或进行 CBR 传输。为了对接入攻击进行建模，我们假设发送节点对接受节点是“匿名”的，即其物理位置由于自身移动性和跟踪设备的不确定性是无法定位的，且它的逻辑身份可以由伪造 MAC 地址隐藏。

由于没有已知的 CSMA/CA 网络模型，我们使用马尔可夫链作为建模基础工具。建模的核心思想是“独立性假设”：具有 $w=\langle w_{\min}, L\rangle$ 的节点被表示为一个马尔可夫链，若其存在冲突概率常量 c(即在一个时隙内其他节点传输数据的概率)。根据文献，节点在一个时隙内试图发送数据帧的稳态概率为 $t=((w_{\min}+1)/2+(w_{\min}/4)\cdot\sum_{l=1}^{L}(2c)^l)^{-1}$。退避计算器不变的概率可以利用已有方法计算，因此有

$$t=\frac{1-c}{1-c+\frac{w_{\min}-1}{2}+\frac{w_{\min}}{4}\cdot\sum_{l=1}^{L}(2c)^l} \tag{1}$$

式中，t 表示为 c 的函数。根据独立性假设，c 又可以表示为非线性等式 $c=1-(1-t)^{N-1}$。

假设每个节点 n 使用 $w_n=\langle w_{n,\min}, L_n\rangle$ 作为其退避配置信息。节点 n 的相应概率 t_n 和 c_n 也有类似式(1)的关系。由独立性假设，当前时隙中至少有一个节点试图发送数据帧的概率为

$$T=1-\prod_{n=1}^{N}(1-t_n) \tag{2}$$

由于 $c_n=1-\prod_{m\neq n}(1-t_m)$，我们有

$$t_n=(T-c_n)/(1-c_n) \tag{3}$$

将式(3)代入式(1)可以得到：对 $n=1,\cdots,N$

$$\frac{1+c_n\cdot(T-2)}{T-c_n}=\frac{w_{n,\min}+1}{2}+\frac{w_{n,\min}}{4}\cdot\sum_{l=1}^{L_n}(2c_n)^l \tag{4}$$

2.2.3 带宽占用模型

通过式(4)解非线性等式(2)得到 c_n 和 t_n 后，可确定节点 n 的带宽占用模型

$$b_n=\frac{\tau_{DATA\text{-}payload}\cdot s_n}{\tau_{DIFS+RTS}-\tau_{slot}+\tau_{slot}/T+\tau_X\cdot S} \tag{5}$$

式中，$sn=tn\cdot(1-cn)/T$ 是节点 n 的成功发送概率(在非空时隙成功发送数据帧的概率)，$S=\sum_{m=1}^{N}s_m$ 是所有节点成功发送概率之和，$\tau(\cdot)$ 是指定的时间或帧传输时间，$X=SIFS+CTS+SIFS+DATA+SIFS+ACK$。对于基本访问方式，由于 *CSMA/CA* 中 $\tau_{RTS+DIFS}>\tau_{slot}$ 且 $\tau_{DATA+DIFS}>\tau_{slot}$，因此可用 *DATA* 代替 *RTS*，并令 $X=SIFS+ACK$，仍然可以得到类似式(5)的等式。

令 $\boldsymbol{w}=(w_1,\cdots,w_N)$ 为全体网络节点的退避配置信息集。若不考虑 CSMA/CA 的多稳定性，则式(2)－式(4)有唯一解 $(t_n^*(w),n=1,\cdots,N)$。此解的充分条件和部分说明由下面的定理给出。

定理 1 令 $\tilde{n}$ 表示具有如下性质的网络节点：①具有最小 $w_{n,\min}$ 值的节点，②满足①的节点中具有最小 L_n 值的节点；令 $w_{\tilde{n}}=\langle\tilde{w}_{\min},\tilde{L}\rangle$。若

$$\tilde{w}_{\min}\geqslant 1+\sqrt{2\cdot\tilde{w}_{\min}\cdot 1_{\tilde{L}}>0} \tag{6}$$

这里 $1_{(\cdot)}$ 为指标函数，则下述情况成立：

(I)解 $(t_n^*(w),n=1,\cdots,N)$ 存在且唯一；

(II)令 $w'<w$，$\boldsymbol{w}=(w_1,\cdots,w_{n-1},w,w_{n+1},\cdots,w_N)$，且 $\boldsymbol{w}'=(w_1,\cdots,w_{n-1},w',w_{n+1},\cdots,w_N)$。则对于带宽占用值，有 $b_n(\boldsymbol{w}')>b_n(\boldsymbol{w})$。

条件(6)不适用于配置信息 $\tilde{w}_{\min}\leqslant 3,\tilde{L}>0$ 的情况，但在 $\tilde{w}_{\min}\leqslant 3$ 时，网络节点 n 一定会占用尽可能大的带宽，这使得即使不考虑外部攻击的情况，这种配置本身也会导致网络节点自身产生接入攻击。定理的(II)部分给出了导致接入攻击的可能性：为了增加传输机会，配置信息本身会导致冲突率的提升，这使得网络性能看上去依赖于其他节点的配置；也就是说使用 CSMA/CA 机制可能产生接入攻击。

3 针对 CSMA/CA 信道接入机制的接入攻击方法

在无线网络中，信道接入功能一般使用网络控制数据包/数据帧实现，而由于控制数据包/数据帧一般不进行加密的特点，对其进行字段识别、运行机制分析较为容易实现。本节针对 CSMA/CA 提出一种信道接入扰乱攻击方法，给出只掌握控制帧(RTS、CTS)部分字段："类型"和"持续时间"时对信道分配/接入/共享机制进行接入攻击的思路。在攻击过程中，攻击节点利用 CSMA/CA 机制的特点，优先抢占业务信道，发送攻击数据。该攻击方法可以使目标节点或者网络接入点保持静默，甚至使所有的工作站与接入点解除关联，造成网络瘫痪。同时该方法也是实现对目标网络非合作接入以及对目标节点进行无线注入攻击的必要步骤，并且可扩展到对其它网络信道接入机制的攻击方法中。

在通信过程中，工作节点一旦通过 RTS 和 CTS 预约到信道，就独占信道，直到其数据发送完成。假设攻击者得到了控制帧中的"类型"和"持续时间"字段的位置和作用，如图 2 所示。由于在预约信道的过程中，"持续时间"字段用来记录 NAV 的值，且通信双方访问无线介质的时间限制由 NAV 指定。因此，攻击者可以通过这种方式发起针对这种机制的攻击，从而达到占用信道，阻止工作站进行数据传输，甚至阻塞网络接入点，瘫痪整个无线网络的目的。

未知	类型	未知	持续时间	未知

图 2 只掌握持续时间字段的信道接入控制帧

攻击者发起攻击的方式：攻击可以采取多种方式，即可以针对网络接入点，也可以针对移动终端节点，或者同时针对上述两者发起攻击。攻击者需要监听网络传输数据，进行 NAV 同步。另外，该攻击方法既可以单独利用 RTS 来实现，也可以利用 RTS-CTS 来实现。主要的攻击方式如下：

(a)攻击一个或几个节点：如图 3 所示，攻击者首先根据"类型"字段截获 RTS 帧并修改其"持续时间"字段，然后向目标节点定向发送 RTS 帧，来通告当前无线网络中有数据正在发送，使其执行退避过程，从而让目标节点在一段时间内无法发送数据。被攻击节点由于执行了正常的退避过程，因此没有异常行为。其他的节点由于没有收到该 RTS 帧，因此进行正常通信。从整体来看，网络通信是正常的。这种攻击方式不易检测，也便于对目标节点进一步进行无线注入攻击。

(b)攻击接入点：如图 4 所示，由于无线网络中网络接入点和其他网络节点共同竞争同一信道，因此，同样可以向网络接入点重发修改"持续时间"字段后 RTS 帧，使其执行退避过程。由于攻击过程中，网络接入点无法发送数据，也就无法响应所有节点的请求，造成所有的节点会自动与该网络接入点解除安全关联，使整个网络无法通信。

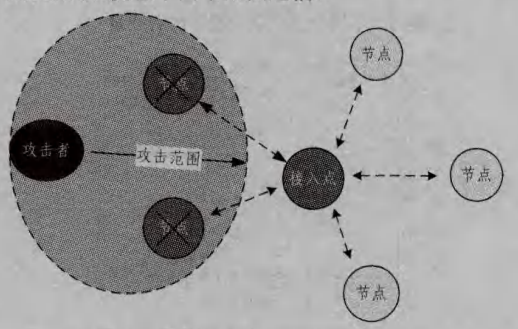

图 3 针对节点的攻击

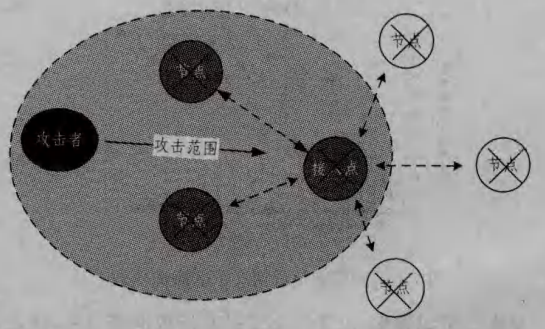

图 4 针对网络接入点的攻击

攻击者成功抢占信道的概率：设最小信道竞争窗口为 CW，网络节点数量为 n，帧最大重传次为 r。并且网络节点采用二进制指数退避机制。攻击者始终选择 0 号竞争窗口。因此，只有第一次和攻击者发生碰撞的节点才有可能与其发生

第二次碰撞，第一个帧时之后，攻击者会马上发送第二个帧。因此，第一次没有碰撞的节点的 NAV 在第二个帧时是不会减 1 的，只有第一次碰撞的节点才有可能在随机选择窗口的时候选到 0 号窗口。

由 RTS-CTS 工作机制可知，攻击者一旦抢占到信道，则后续的帧会在短帧间间隔 SIFS 之内发送，其他网络节点是无法获得信道的使用权的。那么，攻击者在一帧的发送周期内成功抢占到信道的概率 Prsuccess 如下所示。

$$Pr_{success}=1-Pr_{fail};Pr_{fail}=Pr_{fail,r}$$

$$Pr_{fail,r}=\frac{1}{2^{r-2}}Pr_{fail,r-1}\cdot(1-(\frac{2^{r-2}CW-1}{2^{r-2}CW})^{n})$$

$$Pr_{fail,1}=1-(\frac{CW-1}{CW})^{n}$$

4 性能分析

对于 $n=30$，$r=6$，$CW=32$，$Pr_{fail}=8.84e-6$ 的无线网络，我们给出利用上述攻击方式对其 CSMA/CA 机制进行攻击的效果分析图。图 5 为不同信道负载情况下的吞吐量，图 6 为不同信道负载情况下的通信效率，图 7 为不同信道负载情况下的退避次数。

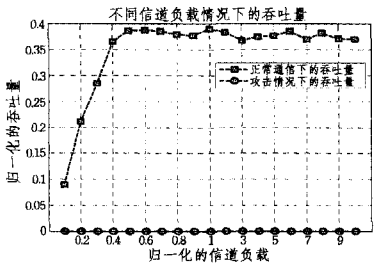

图 5 不同信道负载情况下的吞吐量

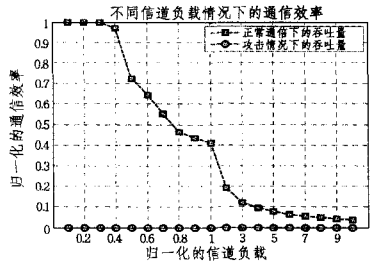

图 6 不同信道负载情况下的通信效率

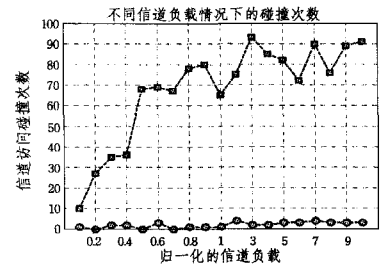

图 7 不同信道负载情况下的碰撞次数

从图 5 可以看出，由于采用二进制指数退避过程，在正常通信情况下，网络吞吐量维持在一个比较稳定的状态，不会因负载的增加引起网络性能的下降。在攻击情况下，由于攻击者一直占用信道，网络节点由于检测到信道忙而持续等待，网络节点始终无法发送数据，因此，实际有效吞吐量为 0。

从图 6 可以看出，正常通信情况下，网络通信效率（发送成功的数据与网络负载的比值）在网络负载较低时能够达到 100%，即所有的数据均能成功发送。在遭受攻击的情况下，由于攻击者信息的大量注入导致网络正常通信吞吐量为 0，因此实际网络通信效率也为 0。这导致网络节点的数据帧被迫驻留缓冲队列，在待发送帧缓冲队列已满的情况下，大量的数据将被丢弃，网络通信陷入瘫痪。

从图 7 可以看出，正常通信情况下，两个节点由于选择同一个时隙发送数据而导致的碰撞次数随着网络负载的增加而增大。攻击情况下，网络碰撞次数极大降低。所以二进制指数退避机制为了均衡网络流量而采取的随机选择时隙的方法反而为攻击者提供了便利条件。极低的碰撞概率可使攻击者随时接入信道发送数据。

结束语 本文首先通过对 CSMA/CA 机制进行建模，然后基于马尔可夫链从随机性能模型和带宽占用模型两方面给出了对其进行攻击的理论分析，最后给出了具体攻击方法及其性能分析，验证了对 CSMA/CA 机制进行攻击的可行性和有效性。但是，上述信道接入攻击方法较适合于采用简单 CSMA/CA 机制的无线网络协议，当无线网络采用接入功能更复杂的类 CSMA/CA 机制时，上述攻击方法的攻击效果还有待研究。

参 考 文 献

[1] 陶源，刘增良，张智南，等. 基于因素神经网络理论的网络攻击态势小生境模型研究[J]. 高技术通讯，2010，7：680-684

[2] 王前，冯亚军，杨兆民，等. 基于本体的网络攻击模型及其应用[J]. 计算机科学，2010，37(6)：114-117

[3] 王国玉，王会梅，陈志杰，等. 基于攻击图的计算机网络攻击建模方法[J]. 国防科技大学学报，2009，31(4)：74-80

[4] 赵芳芳，陈秀真，李建华. 基于权限提升的网络攻击图生成方法[J]. 计算机工程，2008，34(23)：158-160

[5] 张君毅. 基于 MAC 协议的 Ad Hoc 网络攻击技术研究[J]. 无线电工程，2008，38(10)：4-6

[6] 陈峰，罗养霞，陈晓江，等. 网络攻击技术研究进展[J]. 西北大学学报：自然科学版，2007，37(2)：208-212

[7] 诸葛建伟，韩心慧，叶志远，等. 基于扩展目标规划图的网络攻击规划识别算法[J]. 计算机学报，2006，29(8)：1356-1366

[8] 于泠，陈波，肖军模. 一种网络攻击路径重构方案[J]. 电子科技大学学报，2006，35(3)：392-395

[9] 张岳公，李大兴. IPv6 下的网络攻击和入侵分析[J]. 计算机科学，2006，33(2)：100-102

[10] Guevara N，Lin Guo-long. Low power DoS attacks in data wireless LANs and counter measures[J]. ACM Mobihoc，2003，26(12)：62-69

[11] Maxim R，Jean-Pierre H，Imad A. DOMINO：A system to detect greedy misbehavior in ieee 802.11 hotspots[C]//Proceedings of the 2nd international conference on Mobile systems，applications，and services. New York，NY，USA：ACM，2004：84-97

[12] John R. The Sybil Attack[R/OL]. http://www.cs.rice.edu/Conferences/IPTPS02/101.pdf

[13] 曾弘毅，张文铸，徐赞新，等. 一种针对 IEEE 802.11 MAC 子层攻击模式的研究[J]. 网络安全技术与应用，2007，9：39-41

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