

文章编号:1001-9081(2005)03-0546-02

## 基于 IEEE 802.11 认证协议的 DoS 攻击

冯柳平<sup>1,2</sup>, 刘祥南<sup>3</sup>

(1. 北京理工大学 信息科学技术学院, 北京 100081;  
2. 桂林电子工业学院 通信与信息工程系, 广西 桂林 541004;  
3. 厦门大学 计算机与信息工程学院, 福建 厦门 361005)  
(lpfeng@inetcop.com.cn)

**摘要:**对 IEEE 802.11 认证协议的漏洞和无线网络受到的拒绝服务 (DoS) 攻击进行了深入的剖析。捕获并分析 IEEE 802.11 MAC 帧, 利用序列号分析的方法, 对授权的合法客户受到的 DoS 攻击进行检测; 利用统计分析方法, 对访问接入点 AP 受到的 DoS 攻击进行检测。

**关键词:**无线网络; DoS 攻击; MAC 地址欺骗; 序列号分析; 统计分析

**中图分类号:** TP393.08 **文献标识码:** A

## DoS attack based on IEEE 802.11 authentication protocol

FENG Liu-ping<sup>1,2</sup>, LIU Xiang-nan<sup>3</sup>

(1. School of Information Science and Technology, Beijing Institute of Technology, Beijing 100081, China;  
2. Department of Communication and Information Engineering, Guilin University of Electronic Technology, Guilin Guangxi 541004, China;  
3. School of Computer and Information Engineering, Xiamen University, Xiamen Fujian 365001, China)

**Abstract:** Vulnerability in IEEE 802.11 authentication protocol and Denial of Service (DoS) attacks against wireless network were anatomized. IEEE 802.11 MAC frames were captured and analysed. DoS attacks against authorized legitimate clients were detected by sequence number analysis method. DoS attacks against access points were detected by statistic analysis method.

**Key words:** wireless network; DoS attack; MAC address spoofing; sequence number analysis; statistic analysis

基于 IEEE 802.11 的无线网络得到了广泛的应用,但也成为极有吸引力的攻击目标。目前的研究表明, IEEE 802.11 的 WEP 加密机制和认证协议存在着严重的缺陷<sup>[1,2]</sup>。经过大量的研究,产生了一系列的扩展协议,以加强无线网络的访问控制和机密性<sup>[3]</sup>。但无线网络由于其开放特性,还是很容易受到攻击,尤其是来自数据链路层的攻击。而拒绝服务攻击 (DoS) 是最难于检测和控制的。

本文主要讨论 IEEE 802.11 认证协议的漏洞及由此导致的 DoS 攻击,并对无线网络受到的 DoS 攻击进行检测。

### 1 IEEE 802.11 认证协议的漏洞与 DoS 攻击

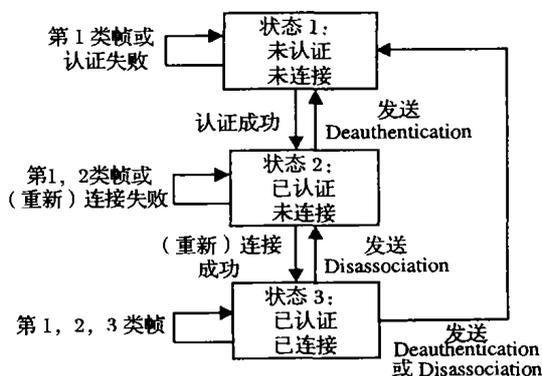


图 1 IEEE 802.11 状态图

客户要加入一个无线网络,它首先要向访问接入点 AP

(Access Point) 进行认证。在认证之后,客户和 AP 连接,得到 AP 的传输率和其他参数。当客户要离开无线网络,它和 AP 断开连接。一个无线站点有三种状态<sup>[4]</sup>: 1) 未认证和未连接; 2) 已认证和未连接; 3) 已认证和已连接(如图 1 所示)。当客户进入状态 3 之后,就可以和 AP 进行通信了。但是在这种状态下,如果发送 Deauthentication 帧或 Disassociation 帧,客户就会和 AP 断开连接,回到状态 1。

在无线网络中,MAC 地址很容易被攻击者监听到。IEEE 802.11 的管理帧和控制帧都是不加密的,数据帧的加密,也只是对数据进行加密,而 MAC 头部则为明文。因此即使采用了 WEP 加密,MAC 地址也是以明文的形式在空中传播。攻击者通过对网络被动地监听,可以得到授权的 MAC 地址列表。

改变无线网卡的 MAC 地址是很简单的事情,几乎所有的无线网卡都允许通过软件的方式去改变它们的 MAC 地址。例如,在 Linux 下,可用 ifconfig 工具或在 C 程序中调用 ioctl() 函数对 MAC 地址进行更改。在 Windows 下也允许在网络控制面板上进行相应的设置。因此,攻击者可以将他们的 MAC 地址设置成任何授权的合法地址。

SSID 值、身份认证和 MAC 地址控制常常用于鉴别客户是否授权允许访问无线网络。然而,当攻击者获取了授权的 SSID 值和 MAC 地址,就能伪装成合法的客户。即使无线网络采用了 WEP 共享密钥认证,密钥也能在数小时内破译。

窃取授权的合法客户的身份对无线网络造成了很大的威胁。作为认证协议的一部分,IEEE 802.11 允许客户或访问

收稿日期:2004-08-28; 修订日期:2004-11-16

作者简介:冯柳平(1964-),女,广西玉林人,副教授,博士研究生,主要研究方向:网络安全; 刘祥南(1937-),男,福建厦门人,教授,主要研究方向:网络安全。

接入点发送 Deauthentication 或 Disassociation 请求与对方断开连接。因此,攻击者通过 MAC 地址欺骗,假扮成授权的客户或 AP,构造并发送一个 Deauthentication 帧或 Disassociation 帧,就可使客户断开和网络的连接<sup>[5]</sup>(如图 2 所示)。

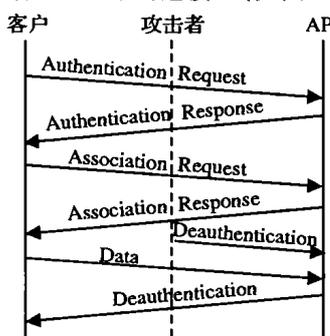


图 2 对无线客户的 DoS 攻击

攻击者对 AP 的 DoS 攻击是在很短的时间间隔内,不断地向 AP 发送认证请求 (Authentication Request) 帧。当客户发送了一个认证请求而又未进行连接之前,AP 必须停留在状态 2,等待该客户的连接请求。一个客户对 AP 持续不断的认证请求使 AP 没有能力接收更多其他客户的请求。

## 2 DoS 攻击检测

### 2.1 IEEE 802.11 帧结构

在 IEEE 802.11 的 MAC 帧中,开始两个字节为帧控制 (Frame Control) 字段 (如图 3 所示)。帧控制字段的第 2~3 位表示帧类型;00 表示管理帧;01 表示控制帧;10 表示数据帧。4~7 位表示子类型。当 Type = 00 (即类型为管理帧): Subtype = 0000 时,表示 Authentication Request 帧; Subtype = 1100 时,表示 Deauthentication 帧; Subtype = 1010 时,表示 Disassociation 帧<sup>[6]</sup>。

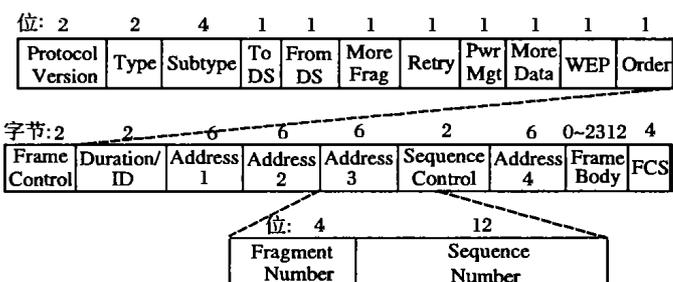


图 3 IEEE 802.11 的 MAC 帧结构

IEEE 802.11 的 MAC 层的设计比其他的 IEEE 802 协议的设计要复杂得多。为了保证传输的可靠性和漫游的透明性,在 IEEE 802.11 的头部增加一个序列控制字段。通过使用帧序列控制字段,对大的管理帧和数据帧实行分片。每个帧用 2 个字节来作为序列控制字段:4 位作为分片号 (Fragment Number),12 位作为序列号 (Sequence Number) (如图 3 所示)。

序列号字段是连续记数的,从 0 开始,模为 4096。当管理帧或数据帧需要分片的时候,在分片的每部分带有一个相同的序列号和一个递增的分片号。对于所有在序列控制字段中具有相同序列号的传输,接收站点将对其进行重组。对于不分片的帧,分片号总是 0。

利用 Libpcap 库,捕获 IEEE 802.11 的 MAC 帧,并进行协议分析。通过协议分析,我们可以从捕获的 IEEE 802.11 的 MAC 帧中,找出 Deauthentication 帧和 Disassociation 帧,并得到发送该帧的源 MAC 地址和序列号。

### 2.2 序列号分析

攻击者通过窃取授权的 MAC 地址把自己装扮成合法的客户端,伪造并发送 Deauthentication 帧或 Disassociation 帧,对合法客户端进行 DoS 攻击。这种独特的方式使我们很难检测到攻击者,对 DoS 攻击进行检测,首先要识别 MAC 地址欺骗。

IEEE 802.11 的 MAC 帧序列控制字段和网络层的 IP 标识字段很相似。然而,和 IP 标识字段不同的是,序列控制字段的值不能通过软件或程序的方式去修改<sup>[7]</sup>。因此,攻击者能伪造一个 IEEE 802.11 的 MAC 帧,但却没有能力把序列控制字段设置为任意值。通过分析序列号分析,我们就能识别 MAC 地址欺骗。

对合法的 MAC 地址,建立一个序列号基线,捕获信号范围内的所有无线网络传输,并对与该 MAC 地址相同的帧进行序列号跟踪,将其序列号与序列号基线进行比较,若超出了一定的阈值,就视为 MAC 地址欺骗。

合法客户的信息存储在双向链表中。双向链表的节点结构为:

```

typedef struct _CLIENT {
    u_int8_t not_flag;
    u_int8_t addr[6]; //客户的 MAC 地址
    u_int16_t seq_ctrl; //序列号基线
    time_t timestamp; //时间戳
    struct _CLIENT * next, * prev; //后继指针和前趋指针
} CLIENT;
  
```

在节点结构中,addr 数组为合法的授权客户端的 MAC 地址,序列号 seq\_ctrl 记录了该客户端的序列号基线。当合法客户端和网络连接的时候,我们建立该客户端的信息,并插入到该双向链表中。序列号字段是连续记数的,即使因为掉包等原因有所偏差,也不会相差太远。因此当捕获到使用该 MAC 地址发送的帧,而其序列号偏离 seq\_ctrl 超出了给定的阈值,那么该帧为伪造的。

当我们从无线传输中检测到一个客户端伪装成授权的合法客户端或访问接入点 AP 给另一客户端发送 Deauthentication 帧或 Disassociation 帧,就能断定这是一个恶意的客户端对无线网络的 DoS 攻击。

### 2.3 统计分析

如果一个客户端不断地向 AP 发送 Authentication 帧,那它就有向 AP 进行 DoS 攻击的可能。因此,监控无线信道上的网络传输,并对网络传输进行分析和分类统计。然后,利用统计分析检测算法,对一定时间间隔内访问接入点 AP 接收的 Authentication 帧进行统计,从而检测对 AP 的 DoS 攻击。

为了对 AP 接收的 Authentication 帧进行统计,建立一个存储 AP 信息的双向链表。链表的节点结构为:

```

typedef struct _AP {
    u_int8_t addr[6]; //访问接入点 AP 的 MAC 地址
    int alert_flag;
    int auth_cnt; //Authentication 帧计数器
    time_t ts_init, ts_last; //监控的开始时间和结束时间
    struct _DoS * next, * prev; //后继指针和前趋指针
} AP;

同时定义:
int threshold; //在时间间隔内发送 Authentication 帧的阈值
time_t dos_period; //时间间隔
time_t expire_timeout; //监控时间
  
```

码等用户信息。DoPathDevelopment, 根据用户信息, 查询、更新路径库或重新构造路径。EndPathDevelopment, 返回所有路径或失败代码。RedoPathDevelopment, 根据用户对路径验证后返回的验证失败代码或路径库查询失败代码, 请求重新构造路径。Terminate, 清除运行环境。

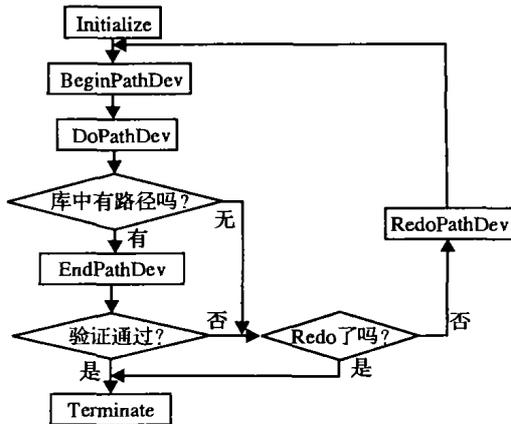


图4 用户请求响应流程

### 3 分析

实际应用中, 签发 10000 个 EE 证书的 PKI 11 个, 它们的 CA 层数为 2~3 层; 签发 50000 个 EE 证书的 PKI 3 个, 它们的 CA 层数为 3~4 层。根据各系统的日志数据统计得到: 90% 的业务在 PKI 内处理; 在代理处理的路径构造请求中, 98% 通过查询路径库得到。

在代理中, 查询成功用户等待响应的平均时间为 1s, 查询失败重新构造的平均处理时间是 120s, 用户的等待时间较长。由于实际应用规模较小, PKI 间的路径长度一般不超过 4, 随着域间节点的增多, 时间开销很高, 查询失败时用户的等待时间会很长。

用证书主体别名存储 PKI 内路径, 使得 PKI 内路径构造的平均时间为 10ms, 对于层次结构的 PKI, 若它签发了  $N$  个 EE 证书, 则 EE 证书主体别名中的路径长度为  $\log N$ , 因此, 随着域内节点的增加, 对于 PKI 内证书路径构造时间的影响是很小的。

### 4 结语

实际应用中, 当 PKI 增多时, 为了路径的可信, 要限制 PKI 间路径的长度。

利用代理, 可以实现后台处理, 具有 PKI 桥<sup>[11,12]</sup> 的功能,

并且省去庞大的建桥开销; 另外, PKI 间无耦合, 利于 PKI 的扩展; 同时, 为将来入桥留有统一的表示结构。

如果各 PKI 对外支持多个信任锚, 则要复杂一些; 如果证书别名中没有存放其 PKI 内的证书路径且没有 PKI 间代理的支持, 那么路径构造蜕化为基本的前向和逆向构造, 如果两者缺一, 则为局部蜕化; 如果证书没有 AKID 和 SKID 扩展, 那么用证书的签发者名和主体名构造证书路径, 则构造过程要确保证书识别名的唯一及证书中的公钥与签名私钥的一致。

#### 参考文献:

- [1] COOPER M, DZAMBASOW Y, HESSE P. Internet X.509 Public Key Infrastructure: Certification Path Building [EB/OL]. <http://www.ietf.org/internet-drafts/draft-ietf-pkix-certpathbuild-03.txt>, 2003-12.
- [2] RIVEST RL, SHAMIR A, ADLEMAN LM. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.
- [3] MILLER VS. Use of Elliptic Curves in Cryptography[A]. Advances in Cryptology - CRYPTO'85[C]. LNCS 218, 1986. 417-426.
- [4] SILVA AR, STANTON MA. Pequi: A PKIX Implementation for Secure Communication[A]. Proceedings of the 1999 International Networking Conference (INET'99)[C], 1999.
- [5] HOUSLEY R, FORD W, POLK W. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [EB/OL]. <http://www.ietf.org/rfc/rfc3280.txt>, 2002-04.
- [6] WAHL M, HOWES T, KILLE S. Lightweight Directory Access Protocol (v3)[EB/OL]. <http://www.ietf.org/rfc/rfc2251.txt>, 1997-12.
- [7] BOEYEN S, HOWES T, RICHARD P. Internet X.509 Public Key Infrastructure LDAPv2 Schema [EB/OL]. <http://www.ietf.org/rfc/rfc2587.txt>, 1999-06.
- [8] BOEYEN S, HOWES T, RICHARD P. Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2 [EB/OL]. <http://www.ietf.org/rfc/rfc2559.txt>, 1999-04.
- [9] LLOYD S. Understanding Certification Path Construction[EB/OL]. [http://www.pkiforum.org/dpfs/understanding\\_path\\_construction\\_DS2.pdf](http://www.pkiforum.org/dpfs/understanding_path_construction_DS2.pdf), 2002-09.
- [10] ELLEY Y, ANDERSON A, HANNA S. Building Certification Paths: Forward vs. Reverse[EB/OL]. <http://www.isoc.org/isoc/conferences/ndss/01/2001/papers/elley.pdf>, 2001.
- [11] Report of Federal Bridge Certification Authority Initiative and Demonstration[EB/OL]. [http://csrc.nist.gov/pki/documents/emareport\\_20001015.pdf](http://csrc.nist.gov/pki/documents/emareport_20001015.pdf), 2000.
- [12] BURR B. Federal Bridge CA Concept [EB/OL]. [http://csrc.nist.gov/pki/twg/archive/y2000/presentations/twg\\_00\\_14.pdf](http://csrc.nist.gov/pki/twg/archive/y2000/presentations/twg_00_14.pdf), 2000.

(上接第 547 页)

当捕获到一个 Authentication 帧, 在双向链表中查找与 Authentication 帧匹配的 AP 的 MAC 地址, 将其 Authentication 帧计数器 auth\_cnt 加 1, 并对其进行检测。若在设定的时间间隔内, 该 AP 接收的 Authentication 帧的次数超出了指定的阈值, 则产生报警信息, 表明该 AP 正在受到 DoS 攻击。

为了捕捉到攻击源, 可在 AP 结构中增加一项, 记录在该时间间隔内向该 AP 发送 Authentication 帧的客户的 MAC 地址。但由于攻击者一般是采用 MAC 地址欺骗的手段对 AP 进行 DoS 攻击, 所以一般很难找到真正的攻击源。

#### 参考文献:

- [1] BORISOV N, GOLDBERG I, WAGNER D. Intercepting Mobile Communications: The Insecurity of 802.11[A]. Proceedings of the Seventh Annual International Conference[C], 2001.
- [2] FLUHRER S, MANTIN I, SHAMIR A. Weakness in the Key

Scheduling Algorithm of RC4[A]. 8th Annual Workshop on Selected Areas in Cryptography[C], 2001.

- [3] FARIA DB, CHERITON DR. DoS and authentication in wireless public access networks[A]. Proceedings of the ACM workshop on Wireless security[C], 2002. 47-56.
- [4] LOUGH DL. A Taxonomy of Computer Attacks with Applications to Wireless Networks[D]. Virginia Poly Technic Institute, 2001.
- [5] BELLARDO J, SAVAGE S. 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions[A]. 12th USENIX Security Symposium[C], 2003.
- [6] GAST MS. Gast. 802.11 Wireless Networks: The Definitive Guide (影印版)[M]. 北京: 清华大学出版社, 2002.
- [7] WRIGHT J. Detecting Wireless LAN MAC Address Spoofing[EB/OL]. <http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf>, 2003.