基于 IEEE 802.11 的无线阻断及数据伪装技术研究①

Interruption of WLAN and Data Camouflaging Based on IEEE 802.11 Protocol

章晨衍　张华熊　朱诗威　(浙江理工大学 信息电子学院 浙江 杭州 310018)

摘　要： 对IEEE 802.11 协议以及无线局域网存在的安全问题进行了深入的剖析，根据IEEE 802.11 的 MAC 头格式，提出了一种基于 MAC 头序列号的阻断算法和一种基于 Beacon 帧的 AP 伪装算法。通过此二种方法，成功实现了对非法接入主机的阻断和对 AP 信息的伪装。

关键词： WLAN 无线阻断 IEEE 802.11 数据伪装

1　引言

无线局域网(WLAN)由于其可移动性、布线容易、组网灵活等特性，在企业和家庭得到了广泛应用。但由于无线局域网采用公共的电磁波作为载体，因此对越权存取和窃听的行为也更不容易防备，使其成为了极有吸引力的攻击目标。由于无线传输的特点，对 AP 入口的管理不像传统网络那么容易，未授权实体可以在公司外部或者内部进入网络，并浏览存放在网络上的信息，或者是让网络感染上病毒；其次，未授权实体进入网络，利用该网络作为攻击第三方网络的出发点(致使受危害的网络却被误认为攻击始发者)；第三，入侵者对移动终端发动攻击，或为了浏览移动终端上的信息，或为了通过受危害的移动设备访问网络[1]。

目前的研究表明，IEEE 802.11 标准的 MAC 协议设计存在着严重的缺陷[2,3]。所以，对于一个安全健壮的 WLAN 来说，一个可以实时地发现攻击行为，并对其进行阻断的网络检测系统是非常关键的。本文提出了基于 Disassociation 的无线局域网阻断技术和基于 Beacon Frame 的数据伪装技术。

2　基于IEEE 802.11的无线阻断技术的实现原理

2.1 IEEE 802.11 介绍[4]

1990 年，IEEE 802 标准化委员会成立了 IEEE 802.11 无线局域网标准工作组。工作组的任务是研究 1Mbps 和 2Mbps 的数据传输速率、工作在 2.4GHz 开放频段的无线设备和网络发展的全球标准。工作组于 1997 年 6 月公布了该标准，它是第一代无线局域网标准之一。该标准定义了物理层(PHY)和介质访问控制层(MAC)的规范，为无线局域网及无线网络设备之间提供了互操作性。

2.2 无线阻断技术实现原理

当客户机试图连接到无线网络时，首先要通过 IEEE802.11 的认证协议，向 AP 请求身份认证。当认证成功后，客户机可与 AP 进行连接[5]。一个无线站点有三种状态:1)未认证和未连接；2)已认证和未连接；3)已认证和已连接(如图一所示)[6]。当客户进入状态 3 之后，就可以和 AP 进行通信了。当处于连接状态时，发送 Disassociation 帧，客户机就会断开连接，回到状态 1，如图 1 所示。

2.3 AP 伪装实现原理

在客户机试图连接到无线网络前，首先需要获取当前空间中的 AP 信息，而 AP 新的获取则是要通过读取 AP 发送的 Beacon 帧的方式来实现。因此，我们可以对 Beacon 帧的伪装，伪造数个，乃至数十个不同 MAC 地址不同 SSID 的 AP，此时非法接入主机将很难判断哪一个才是真实 AP。 同时，我们还可以通过构造并发送与合法 AP 拥有相同的 SSID，不同的 MAC

① 基金项目:浙江省新苗人才计划(2007R40G2060030)
收稿时间:2008-10-29

地址加密伪装 Beacon 帧，来影响非法主机接入，造成其连接时断时续。

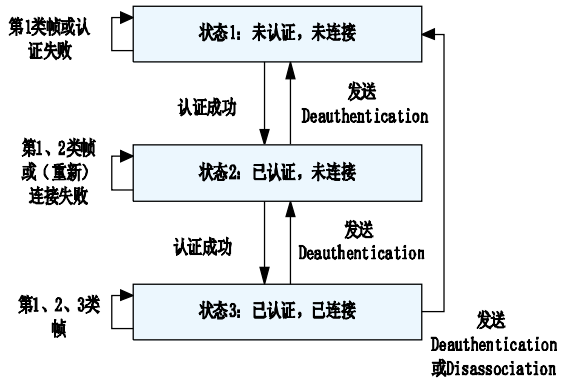

图 1　IEEE802.11 状态图

3　基于IEEE802.11无线阻断技术实现

3.1 实现方式

我们通过采用使用 Atheros v4.2.1 版本驱动的无线网卡进行实时侦听，当有非法主机接入合法无线 AP 中，或者有合法主机接入非法 AP 中时，发出报警，并根据抓获的 MAC 地址，帧序列号等信息，伪装客户机向 AP 发送数个阻断包。如图 2:

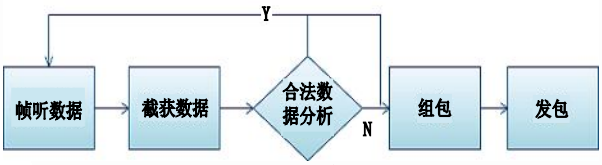

图 2　系统实现框图

在收到 Disassociation 伪造的帧后 AP 和终端的连接将会中断，通过这种方法，我们实现了阻断非法主机接入，防止机密数据流出的目的。实现原理如图 3 所示[7]。

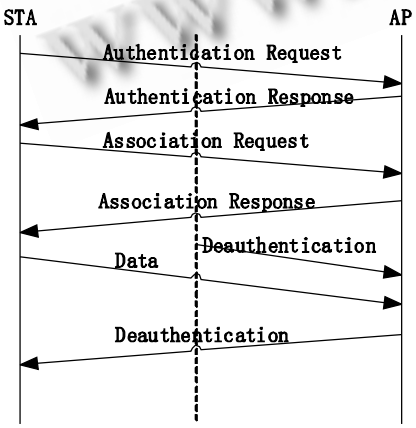

图 3　伪装主机阻断

3.2 IEEE802.11 Disassociation 帧构造算法

IEEE802.11 开始两个字节为帧控制字，0-1 位为协议版本号，2-3 位为帧类型，00 为管理帧，01 为控制帧，10 为数据帧，11 为保留值，当 TYPE=00，即管理帧时，且子类型即 SUBTYPE 为 1010 时为去关联帧，即 Disassociation 帧[8]。当 TYPE=00，SUBTYPE 为 1000 时为信标帧，即 Beacon 帧。如图 4 所示。

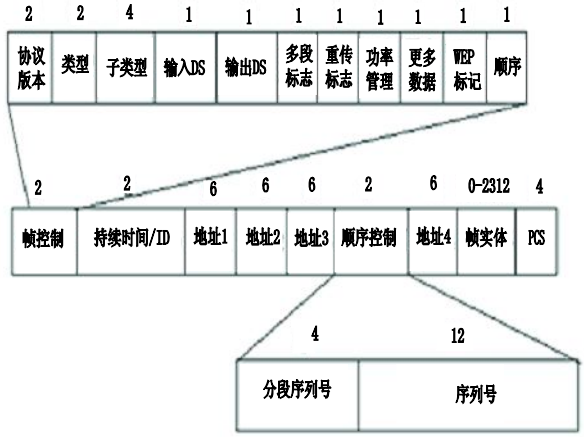

图 4　IEEE20.11 帧结构

当根据帧控制字段中的输入 DS，输出 DS 字段，我们可以得到地址 1，地址 2，地址 3，地址 4 含义如表 1 所示。

表 1　数据帧中的地址域内容

输入 DS	输出 DS	地址 1	地址 2	地址 3	地址 4
0	0	目标地址	源地址	BSSID	不可用
0	1	目标地址	BSSID	源地址	不可用
1	0	BSSID	源地址	目标地址	不可用
1	1	接收地址域	发送地址域	目标地址	源地址

根据获得的 AP 的 MAC 地址，我们构造 Disassociation 帧，并发送至 AP 使连接中断。而吕何甲、冯柳平[5,7]等人都在他们的文章中提到过几种对伪装 Disassociation 帧的判断机制，他们通过对顺序控制中的序列号，以阈值法或是是否乱序。对此，我们通过对无线数据的实时截获技术，根据 IEEE 802.11 的帧结构，进行分析，获取当前在传的数据

包序列号。

首次截获非法主机连接时，我们以截获的数据帧为基数设为 N，构造的 Disassociation 帧的序列号 G：G=N+500。

当三秒钟以上再次截获非法主机连接时，我们以三秒为单位，设首次截获序列号为 Ni，再次截获为 Ni+1，间隔时间为 t 秒，，此时我们构造的帧序列号为：G=(Ni+1- Ni，)*3/t。

3.3 IEEE802.11 Beacon 帧构造

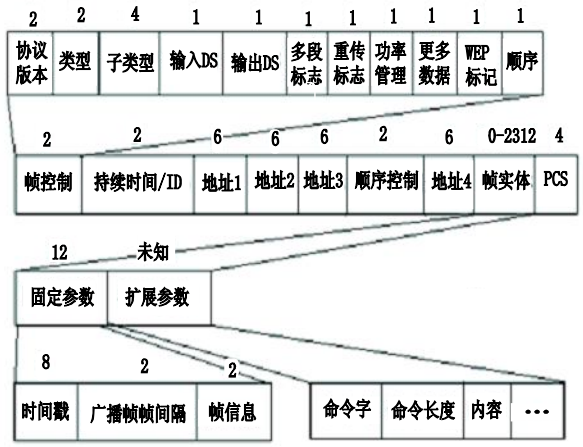

图 5　Beacon 帧结构

前面我们提到过当 TYPE=00，SUBTYPE 为 1000 时为 Beacon 帧，而 Beacon 帧的帧实体中主要包括两部分，固定参数部分和扩展参数部分。如图 5 所示。其中，固定参数部分的帧信息中包括以下信息：本广播帧类型(由 AP 发出还是由终端发出(第 0 位))，本 AP 是否加密(第 4 位)等信息，而扩展参数则由命令字，命令长度，命令内容循环出现的方式来表示，当命令字即 Tag Num 为 0 时，其内容，即 Tag interpretation 为 SSID 名，其命令长度即 Tag length 为 SSID 长，当 Tag Num=3 时，Tag interpretation 为 AP 的工作信道，而当 TAG Num 为 211 时，且 Tag interpretation 为 0050f2010100 开始时，此 AP 以 WPA 的方式进行加密。

经过实验发现，本系统通过 Disassociation 帧能够有效实现非法主机连接的阻断，能够成功实现 5 个以上的 AP 伪装，并通过伪装 AP 的手段影响非法主机的接入。

我们的系统在一个小型 WLAN 局域网中实现，基于 WINDOWS XP 操作系统，采用了 Atheros v4.2.1 版本驱动的无线网卡，需要无线 AP 一个，非法接入主机一台，阻断主机一台。其中 Atheros v4.2.1 版本驱动的无线网卡用于阻断和伪装的抓发包，非法接入主机采用的是 TP-LINK TL-WN620G 无线网卡。

4　结论

本系统能够实现在不接入目标网络的情况下，对主机的非法接入进行实时的报警，提出了一个基于 MAC 头序列号的阻断算法，和一个基于 IEEE 802.11 的 AP 伪装算法。经实验证明，能够在 1 秒内即对非法接入主机进行阻断，能够实现 5 个以上的 AP 伪装，从而提高无线局域网的安全性。

参考文献

1 张黎.VoIP 在 IEEE802.11 无线局域网中的安全问题.西华师范大学学报, 2007,9:257－261.

2 Bellardo J, Savage S. 802.11 Denial-of- Service Attacks: Real Vulnerabilities and Practical Solutions. Washington D.C. Proceedings of the USENIX Security Symposium, 2003.

3 Mishra A, Arbaugh WA. An Initial Security Analysis of the IEEE 802.1X Standard. CSTR 4328, Department of Computer Science, College Park:University of Maryland, 2002.

4 张彬彬.无线局域网攻击技术研究[硕士学位论文].武汉:华中科技大学, 2006.

5 吕何甲,任新.IEEE 802.11 M AC 地址欺骗及其检测技术.电脑开发与应用, 2007,3:51－55.

6 Lough DL.A Taxonomy of Computer Attacks with Applications to Wireless Networks.Virginia Poly Technic Institute, 2001.

7 冯柳平,刘祥南.基于 IEEE 802.11 认证协议的 DoS 攻击.计算机应用, 2005,(5):546－550.

8 金纯,陈林星,杨吉云.IEEE 802.11 无线局域网.2004,1:34－44.