基于 MAC 帧分类匹配的 WLAN 入侵检测*

张绍辉,陈 晨,韩宪忠
(河北农业大学 信息科学与技术学院,河北 保定 071001)

摘 要:在研究 WLAN 入侵检测技术的基础上,给出一种基于数据链路层的无线局域网入侵检测方法。该方法使用协议分析技术,采用 MAC 帧分类的方法匹配入侵特征,实现对 WLAN 的入侵检测。

关键词:无线局域网;入侵检测;协议分析;分类匹配

中图分类号:TP393.1 **文献标识码**:A **文章编号**:1674-7720(2011)01-0057-02

WLAN intrusion detection based on MAC frame classification matching

Zhang Shaohui, Chen Chen, Han Xianzhong
(College of Information Science and Technology, Agricultural University of Hebei, Baoding 071001, China)

Abstract: The paper posts an intrusion detection arithmetic which in the data link layer that based on WLAN intrusion detection technology. This arithmetic uses protocol analysis techniques that classified MAC frame to mach invasion characteristics, achieving WLAN intrusion detection.

Key words: WLAN; intrusion detection; protocol analysis; classification matches

无线网络依靠其无可比拟的灵活性和可扩容性,使其网络无线化已是大势所趋。但由于无线信道的开放性和 802.11 协议自身的诸多漏洞[1-2],无线局域网的安全一直受到各种入侵方式的威胁[3],这使得无线网络的发展空间受到了严重制约。尤其是随着无线加密协议破解技术的发展,各种针对无线加密协议的攻击平台层出不穷(如 Back Track 3、Back Track 4[4]),国内赵春生最近开发的 Beini[5]攻击平台,非专业技术人员利用这些平台破解任何一个使用 WEP 加密的 AP 点用时不会超过 3 min,即使加密协议使用 WPA、WPA2,只要获得足够的握手包,暴力破解密钥也只是时间问题。更何况如今计算机运算技术的飞速发展,单机的 CPU+GPU 运算可达 100 K keys/s,如果使用云计算,运算时间更会显著缩短。为确保无线局域网数据安全,十分有必要建立 WLAN 入侵检测系统。

本文在研究入侵检测技术的基础上,设计了一种基于数据链路层的 WLAN 入侵检测方案,并针对 WLAN 的特性,在协议分析[6]的入侵检测过程中使用 MAC 帧分类检测技术,针对每一种子类型的 MAC 帧使用与其相对应的子类型协议分析器进行分析检测,使得检测策略灵活多变,特征码提取更加准确、迅捷,可进行准确的分类统计,提高了匹配效率。

1 系统架构

无线网络由若干个 AP 覆盖的 WLAN 组成,WLAN 入侵检测系统包括控制中心和监测代理两部分。每个 WLAN 中分别设置一个监测代理,每个监测代理配置一块无线网卡和一块以太网卡。无线网卡设置成混杂模式,负责监听该 WLAN 中的无线数据包,以检测是否存在针对该无线网络相关节点的入侵行为,并将检测到的异常数据通过以太网传送给控制中心。控制中心负责处理各监测代理发来的警告信息并进行相应的处理,如图 1 所示。

检测代理单元由报文捕获模块、协议分析模块、入侵检测模块、通信模块和阻断模块组成。报文捕获模块捕获相应数据后,传给协议分析模块,首先进行协议解码,然后入侵检测模块对协议解码后的数据进行检测,若发现入侵,将产生报警,记录攻击特征,并通过通信模块将报警信息发给控制中心,控制中心根据各检测代理单元上报的报警信息进行综合分析,判断入侵情况,通知阻断模块进行相应处理。

*基金项目:河北省自然科学基金资助项目(F2009000653);河北省科技厅计划资助项目(072135126)

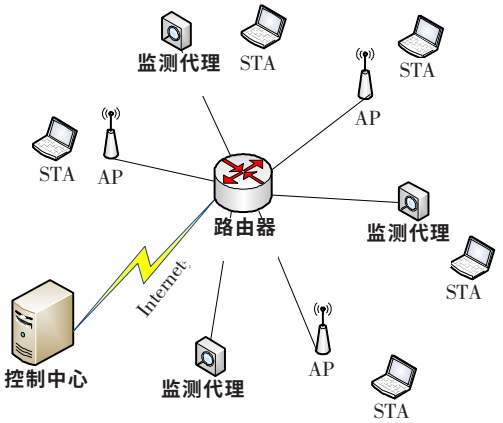

图 1 无线网络系统架构

控制中心主要包含配置模块、通信模块、数据库管理模块、人机交互界面和响应模块。配置模块可对各个检测代理进行各种配置。通信模块负责与监测代理进行通信。数据库管理模块负责存储入侵行为特征。人机交互界面提供给管理员直观的图形界面。响应模块接收各监测代理发送的检测结果,并生成报表写入日志。

WLAN 入侵检测系统工作流程如图 2 所示。

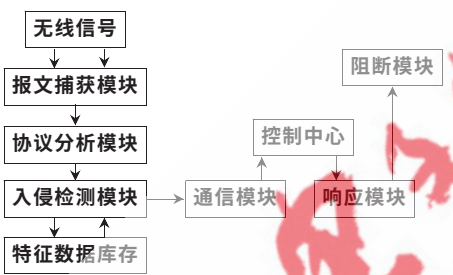

图 2 WLAN 入侵检测系统工作流程图

2 基于 MAC 帧分类匹配的入侵检测

2.1 报文捕获

本文通过在 Linux 系统下的射频监听模式进行报文捕获,通过 Libpcap 开发库实现开发。射频监听模式需要特殊的网卡与特殊的驱动程序,通过查询资料,本系统选用 Atheros 芯片的无线网卡及其相应的 Madwifi 驱动。操作系统选用对无线网卡驱动支持较好的 Ubuntu Linux。无线网卡在射频监听模式下不接入任何 WLAN,能捕获网卡接收范围内所有的原始 802.11 协议报文。

Libpcap 能捕获到底层的所有报文,并且通过设置命令使得 Libpcap 捕获到带 prism 头结构的所有 802.11 原始报文,Prism Monitor Header 长度为 144 B,这是网卡在捕获无线帧时添加在 802.11MAC 帧头前的数据,主要包括信号强度、传输速率等信息。报文捕获命令如表 1 所示。

表 1 报文捕获命令

命令	功能
/sbin/ifconfig ath0 mode monitor	设置监听模式
/sbin/sysctl-w dev.ath0.rawdev=1	产生新的监听接口
/sbin/ifconfig ath0raw up	启动新接口
/sbin/sysctl-w dev.ath0.rawdev_type=1	设置带上 prism 头结构

2.2 协议分析及 MAC 帧分类

MAC 帧分类树如图 3 所示,树的根节点是对 MAC 帧的总体分析,中间节点根据 Type 值进行了 MAC 帧的分类,而每一个叶子节点代表一种实现不同子功能的 MAC 帧。本文针对每一个叶子节点使用相对应的子类型协议分析器,因为针对 AP 的每一种入侵,不管是 AP 关联表溢出攻击、STA 各种认证攻击还是最近很“流行”的针对 WEP、WPA、WPA2 等加密技术的口令破解攻击,其最明显的特征都是在短时间内向 AP 频繁发送某一种特定的帧。MAC 帧分类的优点在于检测策略灵活多变,特征码提取更加准确、迅捷,可进行准确的分类统计,提高了匹配效率。

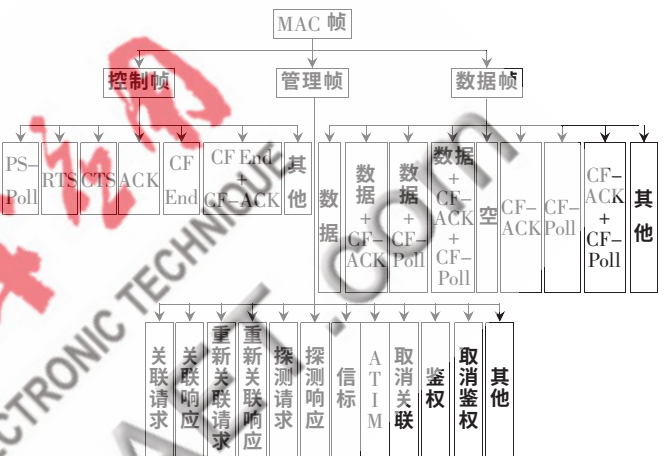

图 3 MAC 帧分类树

协议分析的过程就是一条从根节点到某个叶子节点的路径。根部是 MAC 帧的总体分析,对所有 MAC 帧,首先提取帧头信息,提取 MAC 帧的控制字段以及地址 1-4。根据控制字段中 Type 值分别分析管理帧、控制帧以及数据帧,再根据 Subtype 值确定该帧的具体子类型,然后将控制字段及地址 1-4 提交给相应的子类型协议分析器。在每个子类型协议分析器中,通过分析检测得到入侵检测规则所需要的帧体元素值,采用模式匹配来检测攻击,并且对收到的该子类型 MAC 帧进行来源区分和目标地址的时间段统计。

2.3 分类匹配检测

(1)捕获 802.11 原始 MAC 帧。

(2)分析帧头的 Frame Control 字段,根据变量 Type 值判别该帧类型,根据变量 Subtype 值进一步判断帧功能,使用相应的子类型协议分析器检测,其流程如图 4 所示。

(3)特征码提取。协议分析技术利用网络协议的高度规则性,能理解数据流,利用网络协议分析网络字段,从而不再需要匹配整个数据包,只需要匹配特殊字段,减少了计算量,提高了检测效率,可以快速探测攻击的存在。由于多数黑客软件攻击时所发送的报文均为特殊的

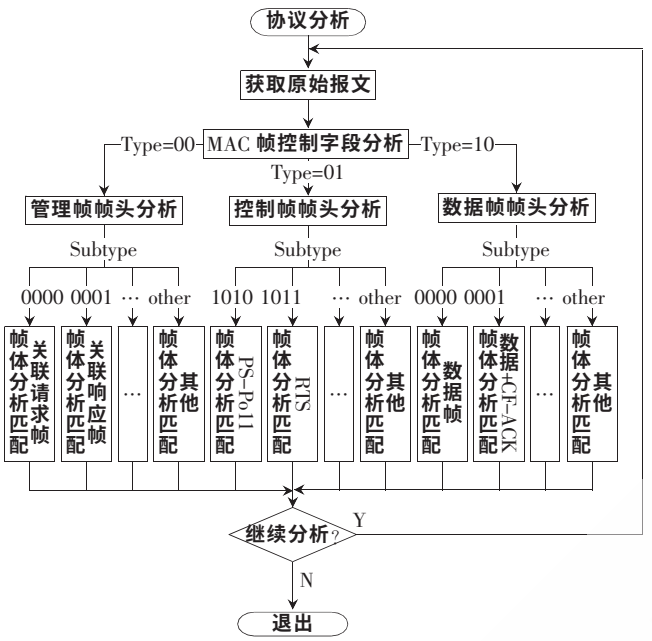

图 4 分类区配检测流程图

字符串,所以只要在报文中检索到此类标志性信息便可认定存在攻击。

(4)特征码匹配检测。各检测模块在入侵检测过程中采用 MAC 帧,分类检测技术,针对每一种子类型的 MAC 帧,使用与其相对应的子类型协议分析器与特征数据库中的攻击特征码进行匹配检测。根据匹配结果,判别此通信是否属于网络入侵行为,并利用统计分析检测所捕获的报文中可能存在的异常。对于已经确定的网络入侵行为,通过通信模块向控制中心传输检测结果,并由控制中心通知阻断模块对其采取相应的处理操作。对 MAC 帧进行子类型分类检测的原因在于,针对 AP 的每一种入侵,不管是 AP 关联表溢出攻击、STA 各种认证攻击还是最近很"流行"的针对 WEP、WPA、WPA2 等加密技术的口令破解攻击,其最明显的特征都是在短时间内频繁发送某些特定的帧以达到入侵的目的。MAC 帧分类的优点在于,检测策略灵活多变,特征码提取更加准确、迅捷,可进行准确分类统计,提高了匹配效率。

本系统是在 Linux 下实现了一个基于网络的 WLAN 入侵检测系统,并在 Linux 下进行了模拟实现。实验表明,本系统能快速检测出较常见的 WLAN 入侵行为,具有实时处理和低误报率的特点,对 WLAN 的安全保障具有一定的实用价值。利用该系统和其他安全策略,可对无线局域网的安全提供基本的保障。如何进一步实现原型系统来验证其有效性,如何在加密的网络环境中更加有效地进行入侵检测以及有效融合分析结果等问题还需要进一步的研究和探讨。

无线入侵检测技术仍处于研究阶段,还存在很多不足之处。随着无线网络的普及,人们越来越关注无线网络的安全性,采用入侵检测技术加强无线网络的安全是非常必要的,无线网络入侵检测技术必将受到人们的高度重视。

参考文献

[1] KING J S. An IEEE 802.11 wireless LAN security white paper [R]. U.S. Department of Energy, Lawrence Livermore National Laboratory UCRL-ID-147478, 2001.10.

[2] STUBBLEFIELD A, IOANNIDIS J, RUBIN A D. Using the Fluhrer, Mantin, and Shamir attack to break WEP [C]. Network and Distributed System Security Symposium, 2002: 100-122.

[3] 孙树峰,石兴方,顾君忠.关于 802.11 协议的攻击研究[J].网络安全技术与应用,2002,33(10):33-36

[4] Muts, Emgent, Pure_hate [CP/OL]. http://www.backtrack-linux.org/,2010-09-01.

[5] 赵春生.Beini [CP/OL].http://www.ibeini.com/index.htm,2010-09-01.

[6] 杜建国,郭巧.协议分析和命令解析在入侵检测中的应用[J].计算机工程与应用,2004,18:159-162.

(收稿日期:2010-09-13)

作者简介:

张绍辉,男,1980 年生,硕士研究生,主要研究方向:计算机网络与数据库。

陈晨,男,1983 年生,硕士,讲师,主要研究方向:计算机网络与数据库。

韩宪忠,男,1965 年生,硕士,教授,主要研究方向:计算机网络与数据库。