无线局域网自适应安全管理框架及其应用

刘振华[1,2,3]，周颢[1,2,3]，赵保华[1,2,3]
(1.中国科学技术大学计算机科学与技术系，230027，合肥；2.网络与交换技术国家重点实验室，100876，北京；
3.安徽省计算与通讯软件重点实验室，230027，合肥)

摘要：针对无线局域网易受攻击、入侵等诸多安全问题，提出一种分布式无线局域网(WLAN)安全管理框架(ASMF)，并基于该框架实现了自适应的安全管理系统(ASMS). ASMF框架依据协议分析和测试理论，即：应用主动分析法，通过构造、执行攻击测试用例，与待测协议进行交互，模拟WLAN漏洞的攻击行为，分析WLAN的防御能力；应用被动分析技术，通过实时的网络报文分析、网络性能监测和自适应调整监测策略进行综合的WLAN安全分析和安全管理. 与已有的安全系统相比，ASMF不仅能够被动地检测攻击，而且可以主动地探测未知漏洞与威胁，同时根据网络配置自适应调整防御策略，其良好的扩展性使得用户可针对新型攻击的测试、检测和自定制管理策略进行自由扩展.

关键词：无线局域网；安全管理系统；管理框架
中图分类号：TP393 **文献标志码**：A **文章编号**：0253-987X(2010)04-0034-05

An Adaptive Security Management Framework for Wireless Local Area Network and Its Application

LIU Zhenhua[1,2,3], ZHOU Hao[1,2,3], ZHAO Baohua[1,2,3]
(1. Department of Computer Science and Technology, University of Science and Technology of China, Hefei 230027, China; 2. State Key Laboratory of Networking and Switching Technology, Beijing 100876, China; 3. Province Key Laboratory of Software in Computing and Communication, Hefei 230027, China)

Abstract: An adaptive security manage framework (ASMF) for WLAN (wireless local area network) is presented to focus on security problems of of WLAN, based on which an adaptive security management system (ASMS) is built. The ASMF bases on the theory of protocol analyse and the theory of protocol testing. The active analysis method is applied to interact on the protocol by constructing the test case while the passive analysis method is applied to monitor the network data flow and the performance of WLAN. Hence, the ASMF can analyse the security of WLAN and manage the WLAN from integer. Compared with the existing security systems, the ASMF not only detects the attack passively, but also probes unknown threats. In addition the ASMF can adjust the defensive strategy according the configure of the WLAN. The good expansibility of ASMF allows users to extend new attacking testing, new attack detecting and customizing management strategy easily.

Keywords: wireless local area network; security management system; manage framework

IEEE802.11[1]无线局域网(WLAN)是计算机 网络和无线通信技术相结合的产物，它避免了有线

收稿日期：2009-09-11. 作者简介：刘振华(1983—)，男，博士生；赵保华(联系人)，男，教授，博士生导师. 基金项目：国家自然科学基金资助项目(60872009，60602016)；国家高技术研究发展计划资助项目(2007AA01Z428，2009AA01Z148)；安徽省自然科学研究计划重大项目(ZD2008005-2，ZD200904，JK2009A013，JK2009A025).

网络线缆对用户的束缚,发展迅速,但同时也带来了新的挑战. 传输介质的公开性使得 WLAN 更容易受到攻击,不但会受到与有线网络相同的 TCP/IP 攻击,而且还会受到针对 802.11 协议标准的特殊威胁[2-3]. 利用加密协议 WEP 固有的缺陷[4],最快可以在 60 s 内破解其密钥[5]. 为了保证安全通信,在无线局域网中制订了相应的安全标准 802.11i,但就目前的研究现状来看,这些安全标准并不能完全保证无线局域网的安全性,如 Martin Beck 等已经在实际环境中成功地对 WEP 及 802.11i 定义的 WPA 进行了攻击[6].

艾尔麦[7]和福禄克等公司[8-9]为 WLAN 提供了性能监测和安全分析系统,其中艾尔麦公司企业版无线局域网安全分析仪较为著名,它支持非法设备的识别,能检测多种攻击和异常行为,可自动阻塞非法设备等,并以被动的方式监测、分析网络的安全性. 该系统应用于匹配攻击或异常行为的模式库及管理策略,是不允许用户自由定制的,而且价格昂贵,一般中小企业难以负担,也不适合大量的布置.

本文提出的自适应安全管理框架(ASMF)能够主动探测 WLAN 未知漏洞,预警信息,并根据 WLAN 的网络设备、安全配置、网络拓扑、主动分析结果等信息,动态地生成具有针对性的安全管理策略,适时地调整攻击和异常行为的检测、处理策略.

1　分布式自适应安全管理框架

ASMF 采用分布式架构(如图 1),主要由 3 部分组成:控制中心、安全管理服务器、无线安全分析终端(Agent). 安全管理服务器与 Agent 通过配合来检测 WLAN 的安全性,并将网络状态实时地送往控制中心. 利用分布式架构,管理员同时可对多个无线局域网进行安全分析和管理,而无需亲临现场.

1.1　控制中心

控制中心由控制台和模式库组成. 控制台连接多个安全管理服务器,管理员通过控制台查看管理服务器中的网络性能状态和网络安全状态等,配置管理服务器中的用户信息库、模式库和决策库,向管理服务器发布网络分析和网络管理命令,例如执行主动分析,跟踪和阻塞指定接入设备或者 AP 等. 模式库存储的内容与管理服务器需保持同步,管理员在控制中心更新模式库,并将最新版分发到各地的安全管理服务器.

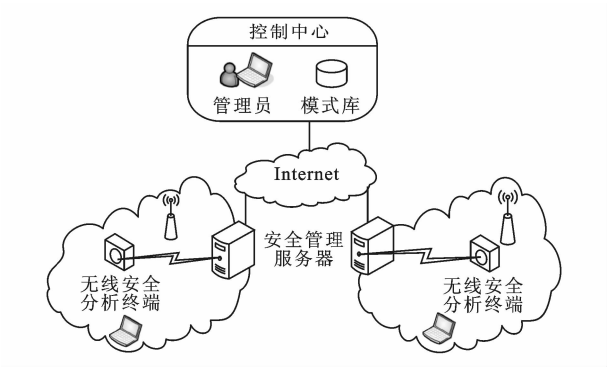

图 1　ASMF 分布式架构

1.2　安全管理服务器

安全管理服务器集成了 WLAN 主动分析技术、被动安全分析技术和无线网络管理技术,是本文框架的核心部分.

如图 2,管理服务器从若干个无线安全分析终端接收数据,数据经处理后放入存储模块,并根据数据的不同类型分别转发至被动安全分析模块、主动安全分析模块和安全管理模块. 主动分析模块和被动分析模块根据相应的模式库检测网络中是否存在攻击或异常行为,安全管理模块将结合主动与被动分析得出的结果分别送入决策模块和网络信息模块. 决策模块根据决策库的策略配置自动发布报警、防御等管理信息和管理指令. 安全管理模块以日志、安全报告、事件报警的形式向控制中心报告网络安全状况.

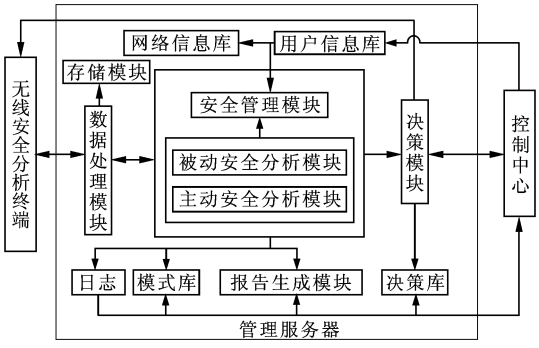

图 2　管理服务器框架

主动安全分析模块应用主动分析技术探测 WLAN 漏洞,检验网络对各种攻击的防御能力. 主动分析技术是依据协议测试理论[10],通过构造、执行攻击测试用例与待测协议进行交互,模拟 WLAN 漏洞的攻击行为,分析 WLAN 对模拟攻击的防御能力,最后确定 WLAN 是否存在安全漏洞. WLAN 的攻击测试方法结合了攻击者和测试者的特点,模

拟了任意情景下的无线网络攻击行为. 该方法适用于未知漏洞的检测和分析,可提前发布预警信息,为被动安全分析提供了导向,突出了重点防御的攻击类型.

被动安全分析模块通过实时的网络报文分析和网络性能监测来检测 WLAN 是否存在攻击或异常行为,主要功能如下.

(1)依据协议分析方法的攻击检测. 利用网络通信协议的高度规则性,通过对 WLAN 协议报文的内部结构、信息次序、信息前后一致性等分析,确定发生网络攻击时出现的协议异常等现象,生成对应的匹配模式库. 协议分析方法是基于状态的分析方法,入侵检测准确性高,误报率低,它的分布式攻击和拒绝服务的检测能力也优于其他入侵检测技术,如针对 802.1X 的检测[11].

(2)网络性能监测. 通过监测网络流量、接入点(AP)和终端(STA)的信噪比(SNR)、信道利用率、误码率、流量分布等的网络性能参数和网络拓扑,来检测 WLAN 是否存在异常行为,如误码率过高、信道利用率低下、管理帧或控制帧流量过大、Ad Hoc 网络被非法使用等.

(3)自适应调整监测策略. 被动分析模块通过 WLAN 的配置和主动分析结果,可以适时地调整入侵检测策略,降低或终止一些不必要的检测. 这样,不仅可以降低服务器的计算负担,而且更有利于加强系统的防御能力.

(4)安全防御指导. 除了安全检测以外,被动安全分析模块还通过对网络性能和配置的监测来指导用户合理配置网络设备,如信道选择、加密配置、信号强度调整等.

模式库是存储主动分析和被动分析匹配规则的规则库,由控制中心配置管理. 主动分析中的每一种攻击测试方法在模库中对应一个规则,被动分析模块针对每一种攻击或异常现象给出了协议异常定义及检测规则. 模式库采用开放式设计,用户可以自由扩展,如增加新的攻击测试方法或攻击检测方法等.

网络信息库由安全管理模块更新,用于存储当前 WLAN 的所有网络信息,包括 STA 或 AP 的基本信息(MAC 地址、协议、加密配置、SNR 变化曲线、速率、信道、站点报文收发统计、站点误码率、网络连接状态等)、网络拓扑、各类型帧流量统计、不同速率帧流量分布、信道利用率、总误码率等,可为被动分析及安全管理提供参考.

用户信息库指定了当前网络的合法用户,由控制中心配置. 系统可根据该信息库来阻塞未注册的非法用户. 通过配置用户信息库,可以在学校、医院、企业等环境中限制外部人员使用网络,避免产生诸多不安全因素.

安全管理模块的主要功能如下.

(1)可将结合主动分析和被动分析的检测结果送入决策模块,决策模块依据决策模式库发出报警、阻塞等命令.

(2)根据网络信息库和主动分析结果调整被动分析策略,并通知 Agent 做出相应调整,如停止某些攻击检测,更新 Agent 数据包返回的过滤规则等.

(3)生成日志和安全报告.

(4)调度多个 Agent 实现自适应的多点合作监测.

决策库由控制中心配置,决策库将针对每种攻击或异常系统做出反应,包括阻塞用户、阻塞网络、提出建议等. 决策模块根据决策库配置自发地对 WLAN 进行安全管理,无需人工干涉. 用户可以根据需要自定义管理策略.

报告生成模块可以针对当前 WLAN 的综合性能快速地生成安全报告,包括 WLAN 的网络设备信息、工作信息、安全性配置、对不同攻击的防御能力等. 日志模块记录了最近的网络安全状况,为定位攻击者和未来防御重点提供参考.

ASMF 框架允许用户通过扩展主动分析和被动分析模式库来支持新型的攻击测试及攻击检测,并可以通过配置决策库扩展管理策略,从而弥补当前管理软件无法自由配置的缺陷.

1.3 无线终端

Agent 是置于无线环境中的探测器,可捕获无线环境中的所有报文,并将自组报文注入任意信道,满足主动安全分析的要求. Agent 可监测所有使用 802.11 协议的网络设备,通过捕获 802.11 网络数据包来监测网络通信,它无需 AP 对简单网络管理协议(SNMP)等的支持,无需统一的网络设备,完全以第三方形式出现,所以不影响网络性能,不会受到无线环境的攻击. Agent 主要包括主动分析支撑模块、被动分析支撑模块、过滤规则库、分析终端管理模块,如图 3 所示.

主动分析支撑模块根据安全管理服务器发来的指令向信道中注入报文,在完成分析后,又向服务器返回攻击测试结果. 决策模块应用主动分析的攻击技术来阻塞非法用户,并根据威胁程度选择相应的

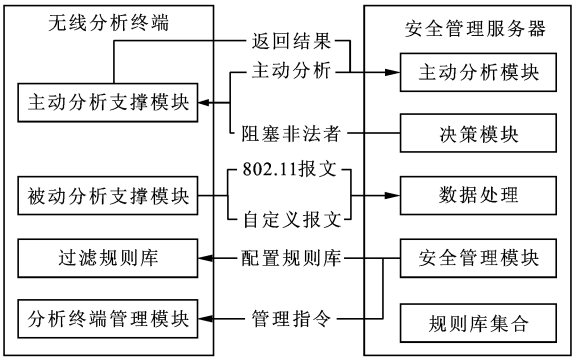

图 3　无线安全分析终端及通信

攻击模式和攻击时间等参数.

被动分析支撑模块返回 2 种报文：①在无线环境中捕获到的 802.11 报文；②自定义数据报文. 该模块负责监测网络性能，包括用户站点信号强度、网络吞吐量、各类型帧流量分布、不同速率帧流量分布等，并将统计结果通过自定义报文返回安全管理服务器.

由于 WLAN 中相邻 5 个信道相互重叠[1]，因此 Agent 可以捕获相邻的 5 个信道的报文，且无线网络速率最高可达 108 Mb/s. 安全管理模块在配置过滤规则库之后，不要求将某些攻击行为帧，如大量的 ACK 帧，返回服务器，仅需要对返回的 802.11 帧进行严格的过滤. 过滤规则库的内容包括：①802.11 报文和自定义报文的返回频率；②规定 802.11 帧返回类型及削减规则，如是否过滤请求发送(RTS)、清除发送(CTS)、确认(ACK)等帧，数据帧是否去除数据部分等；③规定不同类型帧返回频率，如对于同一个 AP，Beacon 帧发送速率约 10 s^{-1}，在一个月内，帧可能是完全相同的，因此一分钟或几分钟返回的信息足以反应网络配置情况. 在实际环境中测得，经过严格定义的过滤规则库可将返回数据的速率控制在 10 kb/s～15 kb/s.

分析终端管理模块负责一些辅助性工作，如：①在启动阶段发现并连接服务器，在工作阶段维护服务器的连接，在断开时恢复终端的初始状态；②根据管理服务器命令设定被动分析监测模式，如对固定信道或循环信道进行监测等；③支持多个主动分析实例进行组合执行，包括开启新线程、开设新端口、建立新的数据连接等，使得 Agent 可以同时执行多个攻击测试.

2　ASMF 框架的应用

基于 ASMF 框架，实现了自适应安全管理系统(ASMS)，其中 Agent 采用自主开发的支持 802.11 帧采集及信道注入的硬件终端，应用 TCL 脚本语言及 C++实现了安全管理服务器，集成了主动分析与被动分析技术，并应用 C# 语言在控制中心实现了图形化操作界面.

2.1　Agent 的实现

Agent 的硬件部分由自主研发的核心板和接口板组成，其结构如图 4 所示. 核心板集成了 Freescale 的 MPC8270 处理器，128 MB SDRAM 以及 16 MB 的 Flash. 底板上集成了非常丰富的外设接口：①2 个 10/100 Mb 以太网接口可接入本地局域网或直接连接安全管理服务器；②1 个两线 RS-232 串口(COM1)；③ 2 个 PCI 插槽.

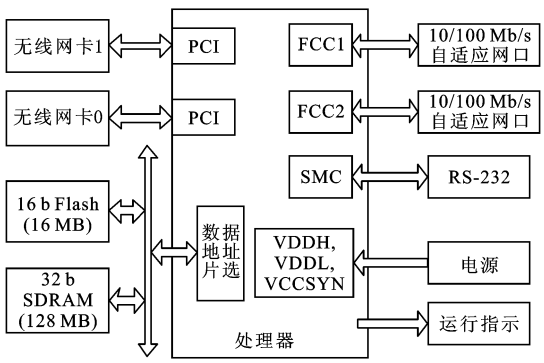

图 4　硬件结构图

Agent 软件包括 Linux 操作系统 2.6.20 、Madwifi-ng 网卡驱动程序、Libpcap. so. 0.9.4 函数库、TCL8.4 以及自主研发的 TCL 底层支撑库.

Libpcap 是 Unix/Linux 平台下的网络数据包捕获函数包，大多数网络监控软件都以它为基础. Madwifing 网卡驱动程序通过支持 Libpcap 函数库来捕获报文，并向信道中注入任意构造的报文. 系统采用 2 块 Atheros 公司 AR5005 系列芯片无线网卡，1 块网卡用于被动分析支持模块，捕获带有 802.11MAC 头的无线数据包，1 块用于主动分析支持模块，向信道中注入数据包，同时监测数据是否发送成功.

2.2　主动安全分析和被动安全分析技术

在主动安全分析中，每种攻击测试方法在模式库中对应一个测试套件，测试套件用 TCL 语言编写并基于自主开发的 TCL 扩展库. 套件分为主脚本和配置脚本，主脚本执行攻击测试，配置脚本配置主脚本中可变参数，所有脚本在管理服务器或控制中心进行编写和调试. 在执行主动分析时，主动分析模块将脚本发送到 Agent，Agent 执行后返回脚本收集

到的结果.本系统目前已支持45种攻击测试,支持协议有802.11协议(26种)、802.1X协议(7种)、移动IPv4协议(5种)、移动IPv6协议(7种).

被动分析分为两部分:一部分在无线分析终端执行一个可配置的TCL脚本,该脚本采集并统计与无线网性能相关的参数,如信道吞吐量、信道利用率、站点信号强度,脚本采用多线程,管理服务器通过发送配置脚本动态地改变主脚本的监测模式并返回信息等;另一部分在管理服务器完成,包括分析网络拓扑,分析STA或AP基本信息,分析入侵检测结果.入侵检测吸取了Wireshark[12]中的协议解析结构和Snort[13]入侵检测架构的特点,入侵检测采用动态链接库来实现,它针对每种攻击检测机制可以开发相应的动态链接库.所有动态链接库具有相同的数据入口、数据出口和调用接口,可以方便地加入到入侵检测链中,具有很强的扩展性.在进行被动分析执行时,可根据当前网络配置及主动分析中网络对每种攻击的防御能力,决定相应攻击检测动态链接库的挂载及数据包返回规则,从而控制每种攻击的检测力度.目前,系统支持51种攻击行为的检测和60种异常行为的检测.

2.3 与Airmagnet性能对比

Airmagnet是无线安全领域的著名艾尔麦公司开发的系统,与该系统企业版7.0(Airmgagnet7.0)相比(见表1),ASMS可主动探测WLAN未知漏洞,提前发布预警信息,指出网络防御重点,而Airmagnet只支持被动的网络攻击或入侵检测,不能根据网络配置自适应地调整检测策略.在管理策略配置方面,Airmgagnet7.0提供了策略管理器,它只允许用户从已有的管理策略中选取策略,所以不具扩展性,而ASMS不仅允许用户根据自身需要以TCL脚本的形式自由定制及扩展具有针对性的管理策略,还允许用户自由扩展安全检测及主动分析模式库,以检测新型攻击.

表1 ASMS与Airmagnet 7.0的性能比较

系统性能参数	Airmagnet 7.0	ASMS
可检测的攻击种数	54	51
主动分析的攻击种数	不支持	45
自动阻塞	支持	支持
性能分析	支持	支持
管理策略配置	不支持	支持
模式库配置	不支持	支持
非法设备定位	移动工具辅助定位	不支持

Airmagnet7.0在阻断入侵和定位非法设备方面性能良好,它除了支持无线阻断以外,还可以通过管理控制台集成SNMP,有线地阻断非法者,而对于非法设备,可根据预定义的网络所在物理环境的二维模型,利用三点定位技术进行追踪,这些是ASMS系统目前所不具备的.

3 结 论

本文提出了基于分布式架构的综合性安全管理框架,该框架同时具有安全分析和安全管理功能,能主动探测WLAN漏洞,并通过监测WLAN配置自适应地生成具有针对性的被动分析策略和防御机制.当检测到攻击或异常行为时,ASMF能够根据决策配置自发地进行防御和阻塞.除此之外,框架还具有良好的扩展性和灵活性,允许用户自由扩展新的攻击测试方法和新型攻击检测方法.同时,基于ASMF框架实现了原型系统ASMS,目前支持不同协议下共45种攻击测试、51种攻击检测和60种异常行为检测.下一步将继续完善模式库,以支持更多的攻击测试及攻击检测.

参考文献:

[1] IEEE. P802.11 IEEE standard for wireless LAN-Medium access control and physical layer specification [S]. Piscataway, NJ, USA: IEEE, 2007.

[2] TEWS E. Attacks on the wep protocol [EB/OL]. [2009-01-12]. http://eprint.iacr.org/.

[3] MISHRA A, ARBAUGH W A. An initial security analysis of the IEEE 802.1X standard CS-TR 4328 [R]. Maryland, USA: University of Maryland. Department of Computer Science, 2002.

[4] FLUHRER S, MANTIN I, SHAMIR A. Weaknesses in the key scheduling algorithm of RC4 [M]// Lecture Notes in Computer Science. Berlin, Germany: Springer, 2001:1-24.

[5] TEWS E, WEINMANN R P, PYSHKIN A. Breaking 104 bit WEP in less than 60 seconds [M]// Lecture Notes in Computer Science. Berlin, Germany: Springer, 2007:188-202.

[6] TEWS E, BECK M. Practical attacks against WEP and WPA [C]// Proceedings of the 2nd ACM Conference on Wireless Network Security. New York: USA: ACM, 2009: 79-86.

[7] Air Magnet Inc. Air magnet enterprise 24/7 WLAN security and performance monitoring [EB/OL]. [2009

-01-09]. http://www.airmagnet.com/products/enterprise/.

[8] Fluke Inc. Analyze air wi-fi spectrum analyzer[EB/OL]. [2009-01-09]. http://www.flukenetworks.com/fnet/en-us/products/AnalyzeAir/Overview.htm? wbc_purpose=BasiNewsListingsupp.

[9] Air Defense Inc. Enterprise wireless LAN security and WLAN monitoring [EB/OL]. [2009-1-20]. http://www.airdefense.net/.

[10] 陈伟琳，周颢，赵保华. 利用构造类别代数的协议安全测试方法 [J]. 西安交通大学学报，2008，42(12)：1481-1485.
XUE Yuyang，ZHOU Hao，ZHAO Baohua. The security analysis and detection of 802.1X WLAN [J]. Journal of Xi′an Jiaotong University，2009，43(10)：52-55.

[11] 薛雨杨，周颢，赵保华. 无线局域网 802.1X 协议安全性分析与检测 [J]. 西安交通大学学报，2009，43(10)：52-55.
CHEN Weilin，ZHOU Hao，ZHAO Baohua. Constructed type algebra based protocol security testing method [J]. Journal of Xi′an Jiaotong University，2008，42(12)：1481-1485.

[12] SHARPE R，WARNICKE E. Wireshark user's guide [EB/OL]. [2009-01-09]. http://www.wireshark.org/docs/wsug_html_chunked/index.html.

[13] Martin Roesch，Chris Green，Sourcefire Inc. SNORT users manual 2.8.5 [EB/OL]. [2009-01-09]. http://www.snort.org/assets/125/snort_manual-2_8_5_1.pdf.

（编辑　苗凌）