轻量级无线网络入侵检测系统①

殷立峰，吴 剑，马 宾

(山东政法学院 信息科学技术系, 济南 250014)

摘 要：针对当前流行的无线拒绝服务 DoS、伪装 STA、伪装 AP、WarDriving、暴力破解等无线网络攻击，采用误用检测和异常检测结合的方式，设计并实现了一个针对无线局域网的轻量级无线网络入侵检测系统。系统采用用户自定义攻击规则库、自定义授权 AP/STA 名单、自定义非法 AP/STA 名单等方式，能针对无线网络具体环境和用户的不同需要，合理调整入侵检测灵敏度和攻击检测阈值。仿真试验表明，与市场上同类系统相比较，本系统能有效提高无线网络入侵检测效率，大大降低误报率和漏报率。

关键词：无线网络; 入侵检测; 误用检测; 异常检测; 攻击密度检测

Lightweight Wireless Lan Intrusion Detection System

YIN Li-Feng, WU Jian, MA Bin

(Department of Information Science and Technology, Shandong University of Political Science and Law, Jinan 250014, China)

Abstract: Aiming at wireless network attacks such as DoS attacks,rouge STA, rouge AP,WarDriving attacks and bruteforce attacks, a Lightweight Intrusion Detection System for WLAN is implemented by combining the misuse detection and anomaly detection. In this system,the user can define attack rule set, authorization AP/STA list, illegal AP/STA list, and the sensitivity and the threshold value of detection can adjust according to the circumstance and user requirement. The test shows that this system has a better detecting effect than other WLAN intrusion detection in market.

Key words: WLAN; intrusion detection; misuse detection; anomaly detection; detection of attack density

随着无线网络技术的迅猛发展，无线网络已经遍及家庭、高校、企业、政府等各个生产和生活领域，日益受到网络用户的追捧，但是用户的无线网络安全意识并没有像无线网络一样普及[1]。由于无线网络自身的特点，攻击者无需物理连接就可以对其进行攻击，致使无线网络较之有线网络更容易受到不法侵害，随着网络入侵技术的提高，无线网络受到的威胁也越来越多，如何对无线网络攻击行为进行充分研究，并在研究基础上提出解决办法，以此维护无线网络的安全，使合法用户免受非法侵害就显得越来越重要[2]。

本文在对现有无线网络入侵行为充分研究的基础上，设计并实现了一个无线网络入侵检测系统，系统主要由数据包捕获模块、解码模块、过滤模块、解析模块、统计模块和日志记录存储模块以及可视化操作界面构成。可以对入侵行为进行实时检测、记录、处理、阻止和报警。系统设计的目的是研究常见无线网络攻击类型和攻击特征，探讨未知无线网络攻击类型的特征和组成要素。通过对检测数据的分类组织和存储，聚类分析和统计，进一步研究异常检测、误用检测和 AP/STA 实时授权维护的有机结合对提高入侵检测效率的影响。仿真试验表明，与市场上同类系统相比较，本系统能有效提高无线入侵检测效率，大大减少误报率和漏报率。

① 基金项目:山东省自然科学基金(ZR2011FQ019D);济南市科技发展计划(201010002)
收稿时间:2011-11-23;收到修改稿时间:2011-01-09

1　系统结构及设计原理

本系统是一款安装有 libpcap、mysql 与 aircrack-ng 软件的 Linux 操作系统平台，具有图形界面用户接口的无线网络入侵检测系统。硬件环境为配置具备 monitor 监视功能无线网卡的计算机。系统运行时首先将无线网卡切换到 Monitor 模式，然后调用 libpcap、aircrack-ng 功能函数捕获该无线网卡可接受范围内的所有数据包，并对捕获的数据包进行解码、分析、检测与统计等操作，从而实现无线网络的入侵检测。系统总体结构如图 1 所示：

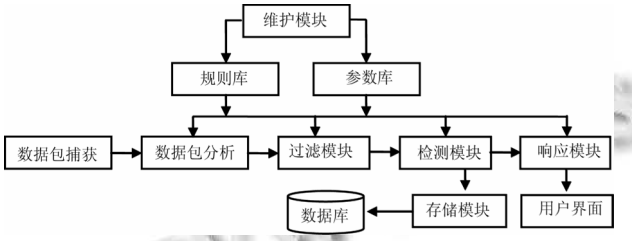

图 1　入侵检测系统总体结构图

图 1 中，数据包捕获模块在 monitor 模式下捕获所有可侦测到的数据包。将其交给数据包分析模块进行分析，根据分析结果，将具有可疑行为的数据包传送给检测模块，检测模块调用异常检测插件对数据包进行检测，并视检测情况调用响应模块作出相关响应，完成检测结果的存储并以适当方式对用户发出警示。在数据包分析、数据包检测和检测响应环节，系统会根据处理要求自动加载规则库和参数库，以此合理调整入侵检测灵敏度和攻击检测阈值，提高入侵检测效率，减少误报率和漏报率。系统允许用户采用自定义攻击规则库、授权 AP/STA 名单、非法 AP/STA 名单等方式实现功能扩展，在程序设计上采用多线程技术，将用户界面、数据包分析、数据包检测、异常检测插件调用、检测响应、检测结果存储等程序模块分别作为单个线程进行设计，保证系统操作的顺畅和数据捕获、检测、处理的连续性。

2　系统主要模块及其工作原理

2.1 数据包捕获模块

数据包捕获模块首先查找并启动捕获数据包的设备，获取设备相关信息，创建捕获句柄，完成数据包的捕获准备。数据包的捕获主要利用 libpcap 提供的网络数据包捕获接口 pcap_loop 函数和 iwconfig 网卡信息获取接口完成，数据包捕获模块循环捕获数据包存入内存，然后根据过滤条件调用回调函数进行处理，每捕获到一个数据包就调用一次回调函数，把数据包传到系统的数据包分析模块接口。

2.2 数据包分析模块

数据包分析模块主要对捕获的数据包进行解析。其任务是完成被捕获数据包链路层首部的解码，为系统检测模块做数据准备。无线网络数据包由如图 2 所示的三部分组成，其中 Radiotap 是结构型数据，主要存储诸如协议版本、数据包长度、无线网络信号的频率、强度、质量、信噪比、天线、信号衰减、数据重传等信息[3]，通过对该部分的解析，主要判断数据包长度是否正常，如正常则将该 u_char*类型指针强制转化为 libtrace_radiotap_t* 类型，根据 radiotap 结构信息，将 1 左移指定位后与 it_present 变量进行按位与运算，从而获得解码后的数值。将解码后的数值全部存储于一个 radiotap 结构体，以备检测模块检测，主要实现代码如下：

```
if (rtap->it_present &(1<<TRACE_RADIOTAP_
TSFT))
{ pkt.rt.TFST = ((uint64_t)(*((uint64_t *)p)));
  p += sizeof (uint64_t);
  rtap_real_len += sizeof (uint64_t);
}
```

完成首部 Radiotap 部分解码后，接下来对图 2 中的 802.11MAC 部分进行解码。通过对 802.11MAC 帧格式分析可知，802.11MAC 部分的 framecontrol 字段(占 2 个 bytes)的 Type 部分定义了数据帧、管理帧、控制帧三种数据包类型，在程序中定义 framecontrol 类型结构体变量，将捕获的数据包信息转存到 framecontrol 类型变量中，根据变量值获取数据包类型，然后调用数据帧解码函数、管理帧解码函数、控制帧解码函数分别对数据帧、管理帧、控制帧进行解码，解码完毕后，所有解码获取的数据信息传送给检测模块，进行下一步操作。

图 2　无线网络数据包格式

2.3 数据包过滤模块

主要根据黑名单中的 AP/STA 和非授权的 AP/STA

过滤掉非正常的广播帧。在过滤部分实现时并非匹配上用户自定义的名单后就报警或者记入日志，而是继续匹配动态黑名单，在动态黑名单里控制报警次数，减少误报率。此外还可以存储、显示未授权的 STA/AP，实时提醒用户是否对未授权的用户进行授权和阻止。

2.4 数据包检测模块

数据包检测模块由异常检测子模块和误用检测子模块构成，限于篇幅，下面主要介绍异常检测模块的工作原理和算法实现。

2.4.1 异常检测子模块

异常检测是通过分析用户行为模式与标准，判断检测出当前未知入侵行为的一种方法。方法是将所观察对象的正常行为特征轮廓描述为行为参数及其阈值的集合[4]。当用户行为模式与正常行为有重大偏离且偏离密度较大时，则判定为是入侵。行为参数及其阈值的制定依据是常见攻击的攻击特征。

异常检测算法及其实现步骤是：

1) 通过对 WLAN 入侵和攻击方式的研究，制作攻击特征树如图 3 所示:

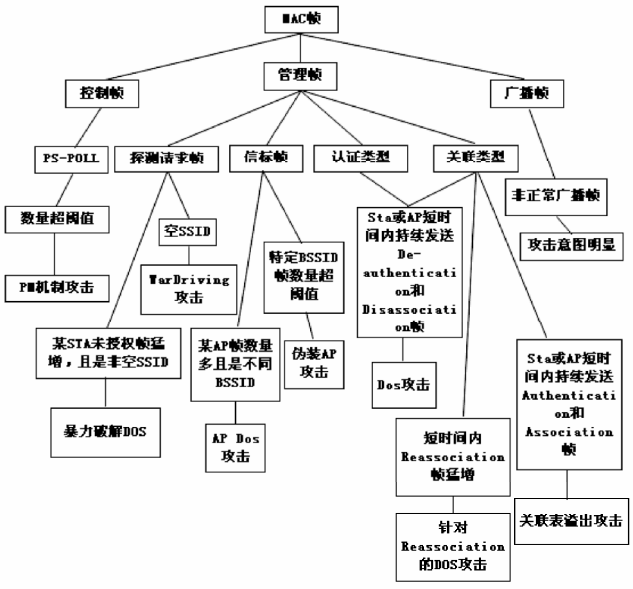

图 3 无线网络攻击特征树

2) 采用攻击密度检测算法进行检测

攻击密度检测算法主要思想是用可疑报文行为特征与攻击特征树叶结点进行匹配，如果短时间内可疑特征报文匹配的数量达到一定的阈值并且达到阈值的次数达到一定的密度则判定为攻击行为，进行标记包为异常和报警等相关处理，算法实现如图 4 所示：

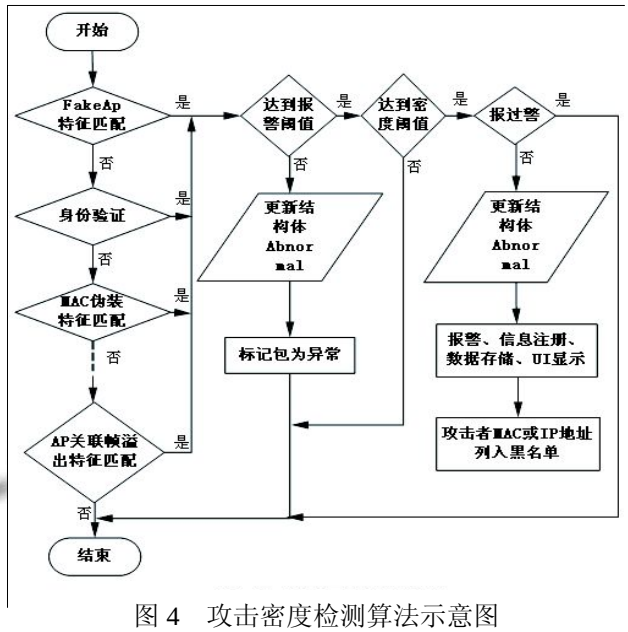

图 4 攻击密度检测算法示意图

设计 abnormal 结构体作为对各种攻击、警告、异常进行记录、分类统计和查询的数据接口。通过它可以把程序运行期间发现的攻击、警告、异常等信息进行分类标记、记录和统计，方便查询和对攻击检测扩展的实现。结构体定义如下：

```
struct abnormal
{
  Short flag_abnormal;//错误标记位
  QString abnormal_code;//错误代码
  QString MAC_addr;//发生错误的 MAC
  QString AP;//发生错误的 AP
  QString errstring;//错误信息描述
  };
```

2.4.2 序列号统计算法子模块

序列号统计算法原理是根据帧的不规则序列号在短时间内数量达到一定阈值则进行报警，报警阈值的不同也会使系统的灵敏度不同。比如普通的黑白名单检测虽然能够检测出伪装 MAC 和伪装 AP，但当有伪装成合法的 STA 和 AP 入侵发生时，采用这种方式就检测不出来了，因此采用序列号统计算法作为黑名单过滤法的补充。

无线局域网协议 MAC 帧格式中有一序列控制字段，由分段号子字段和序列号子字段构成。其中分段号子字段表明一个特定的介质数据单元(MSDU)的分

段号; 序列号子字段从 0 开始，每发送一个帧，序列号依次加1。无线网络设备的MAC地址虽然可以修改，但是 MSDU 序列号是由硬件决定的，用户无法任意修改，如果入侵者伪装成合法用户，就会有两个设备共用一个 MAC 地址，这样的话检测到的序列号一定会是时大时小没有严格的递增的，所以可以据此来检测是否有人盗用了合法的 MAC。

当然下列几种特殊情况也会导致序列号不是严格递增：

① 无线网断开重连，数据包的序列号会从 0 重新开始依次递增。

② 数据包的序列号是模 4096 的所以数据包的序列号到 4095 后，会跳变为 0。

③ 无线工作站漫游出检测范围，然后又漫游回来。

由于上述情况的存在，所以系统首先对序列号的跳变不应该太敏感，而是应该保证跳变在一定范围内是正常的。其次对跳变次数也不应太敏感，应该允许在一定的阈值内的跳变次数是正常的。在此基础上便可以实现密度检测算法的改良版本序列号统计算法。

2.4.2 统计模块

主要完成各种检测数据的分析统计，方便用户直观了解系统的运行状况，系统统计内容如下：

① 事故分类统计。主要统计数据包总数、攻击次数、警告次数、事故次数、事故率等;

② AP 和 STA 统计。统计 AP 总数、未授权 AP 总数、STA 总数、未授权 STA 总数、授权 STA 总数;

③ 帧数据统计。主要有帧总数、数据帧数量、管理帧数量、控制帧数量以及广播帧数量统计;

④ 数据包长度范围统计。主要统计数据包字节数在 0~100、100~300、300~500、500~900 之间和字节数大于 900 的数据包个数;

⑤ 速率统计。主要进行数据帧捕获速率、管理帧速率、控制帧速率、抓包平均速率、实时抓包速率统计;

⑥ 统计抓包开始时间、抓包持续时间、抓包流量等;

⑦ 攻击统计。统计非用户定义的已知和未知攻击类型、用户定义的已知攻击类型和用户定义的未知攻击类型的攻击次数和频度。

3 结语

根据上述模块功能和性能设计，针对验证帧洪水攻击、FakeAP 攻击、取消验证及取消关联帧洪水攻击、MAC 伪装、误用检测、AP 过滤、STA 过滤、数据统计以及系统稳定性等内容，应用本系统和目前流行的无线入侵检测软件 Kismet 进行了比较性测试。测试结果分析表明，和目前流行的无线入侵检测软件 Kismet 相比较。本系统具有在持续运行的情况下稳定性好，可靠性高，检测攻击种类多，AP/STA 过滤功能好，检测攻击灵敏度高，误报率、漏报率低，操作界面友好，可信度高，统计数据齐全，日志查看更方便等优点。

参考文献

1 朱建明,马建峰.无线局域网安全—方法与技术.第 2 版.北京:机械工业出版,2009.53−77.

2 杨哲.无线网络安全攻防实战进阶.北京:电子工业出版社,2011.67−69.

3 邢长明.无线网络中分布式入侵检测系统的研究.济南:山东师范大学,2007.113−116.

4 齐建东,陶兰,孙总参.网络异常行为的检测方法.计算机工程,2004,30(5):104−105.

(上接第 9 页)

ment,2008,1(2),1265−1276.

5 Yick J, Mukherjee B, Ghosal D. Wireless sensor network survey. Computer Networks,2008,52(12):2292−2330.

6 Oracle Real Application Clusters.http://www.oracle.com/technology/products/database/clustering.

7 Hadoop.http://hadoop.apache.org/.

8 HBase.http://hadoop.apache.org/hbase/.

9 Chang F, Dean J, Ghemawat S, et al. BigTablel:A distributed storage system for structured data.ACM Trans.on Computer Systems,2008,26(2):1−26.

10 ZooKeeper. http:// zookeeper.Apache.org/.

11 Remote Procedure Calls. http://www.Cs.cf.ac.uk/Dave/C/node33.html.

12 Google-Gson.http://code.google.com/p/google-gson.