基于隐马尔可夫模型的无线局域网媒体接入控制层入侵检测方法

李金铃[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：将无线局域网媒体接入控制(MAC)层字段作为检测入侵的分析对象，提出了基于隐马尔可夫模型(HMM)的无线局域网MAC层入侵检测方法.采用了基于控制台、服务器、代理的3层分布式无线局域网入侵检测框架；基于HMM模型对无线局域网的MAC帧头部进行建模；利用正常的无线局域网络数据对HMM进行训练，并记忆正常系统下的数据包行为.由此，检测发现了出现概率小的数据包或数据包序列，并制定了入侵检测阈值.试验结果表明，所提方法对已有的无线局域网MAC层攻击的误报率和漏报率比较低，并能检测未知攻击.

关键词：无线局域网；入侵检测；隐马尔可夫模型
中图分类号：TP393 **文献标志码**：A **文章编号**：0253-987X(2009)12-0026-05

Intrusion Detection Method of Wireless Local Area Network MAC Layer Based on Hidden Markov Model

LI Jinling[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. Anhui Province Key Laboratory of Software in Computing and Communication, Hefei 230027, China)

Abstract: The packet field of wireless local area network (WLAN) medium access control (MAC) layer is taken for the analytical object of detecting intrusion. An intrusion detection method of WLAN MAC layer is proposed based on the hidden Markov model(HMM). A three layers frame including console, server and agents is given; the data of WLAN MAC layer is used to model the HMM; then the normal data of WLAN is used to train the HMM and to memorialize the normal action of WLAN. An intrusion will be detected when the occuring probability of a packet data or a sequence of packet data is smaller than a given threshold. Experimental results show that the proposed method has low false positive rate and missing report rate when detecting the known attacks on WLAN MAC layers, and also detects unknown attacks.

Keywords: wireless local area network; intrusion detection; hidden Markov model

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，它避免了有线网络线缆对用户的束缚，具有强有力的市场竞争力，发展迅速，但同时也带来了很多的安全隐患.由于传输介质的公开性，所以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

收稿日期：2009-03-17. 作者简介：李金铃(1984—)，男，硕士生；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).

802.11 协议标准的特殊威胁,因此提高 WLAN 的安全性具有重要意义.

采用入侵检测系统(IDS)来加强 WLAN 的安全性是一种很好的选择,尽管该技术在有线网络中已得到认可,但无线网络的特殊性使其应用于 WLAN 尚需进一步研究. 当前,对 WLAN 的入侵检测大都处于试验阶段,如开源入侵检测系统 Snort-Wireless[1]采用了规则匹配的方法进行入侵检测,但该规则无有效的定义,使得检测功能有限,即不能很好地检测媒体访问控制(MAC)地址欺骗和泛洪拒绝服务攻击,对未知攻击更是无能为力. 作为概念模型设计的 WIDZ[2] 系统实现了访问点(AP)监控和泛洪拒绝服务检测,但它没有一个较好的体系架构,存在局限性. 2003 年 IBM 提出 WLAN 入侵检测方案,即采用无线感应器进行监测,该方案需要联入有线网络,应用范围有限且系统成本昂贵.

隐马尔可夫模型(HMM)[3-4]具有研究透彻、算法成熟、效率高、效果好、易于训练等优点,应用于入侵检测可以减小误报率、漏报率. 目前,基于 HMM 异常检测技术的数据主要来源于主机[5](如系统调用),并且取得了很多有效的实验结果. 基于主机的入侵检测技术对于 WLAN 的作用是有限的,而 HMM 应用于 WLAN 网络入侵检测的主要困难在于 HMM 的观测值千差万别、难以确定.

本文提出一种基于隐马尔可夫模型的无线局域网入侵检测方法,该方法根据无线网络数据包的 MAC 帧头部建立 HMM,并将 WLAN 的 MAC 帧头部的字段作为模型的输入.

1　隐马尔可夫模型

HMM 是一个双重随机过程,由两部分组成:描述状态转移的马尔可夫链;描述状态与观测序列间关系的一般随机过程,是观测值的概率描述. HMM 的状态是不确定、不可见的,只有通过观测序列的随机过程才能表现出来. 观测到的事件与状态并不是一一对应的,而是通过一组概率分布矩阵来表示两者之间的关系.

一个 HMM 由五元组 $\boldsymbol{\lambda}=(N,M,\boldsymbol{\pi},\boldsymbol{A},\boldsymbol{B})$构成,其中 N 是系统状态数,M 是每个状态可能的观测值数,$\boldsymbol{\pi}$ 为状态初始概率分布,$\boldsymbol{A}$ 是与时间无关的状态转移概率矩阵,$\boldsymbol{B}$ 是给定状态下的观测值概率分布矩阵.

HMM 可以简写为 $\boldsymbol{\lambda}=(\boldsymbol{\pi},\boldsymbol{A},\boldsymbol{B})$,其中状态转移矩阵 $\boldsymbol{A}=\{a_{ij}\}$,观测值概率矩阵 $\boldsymbol{B}=\{b_j(k)\}$,初始状态概率分布 $\boldsymbol{\pi}=\{\pi_i\}$. 观测符号集合 $\boldsymbol{V}=\{v_1,v_2,\cdots,v_M\}$,观测符号序列 $\boldsymbol{O}=\{o_1,o_2,\cdots,o_T\}$($T$ 是观测时间),状态数为 N. HMM 的 3 个基本问题如下.

(1)给出一个 $\boldsymbol{\lambda}=(\boldsymbol{A},\boldsymbol{B},\boldsymbol{\pi})$,如何高效率地计算出某个输出序列 $\boldsymbol{O}=\{o_1,o_2,\cdots,o_T\}$ 的概率 $P(\boldsymbol{O}|\boldsymbol{\lambda})$?

(2)给出一个 $\boldsymbol{O}=\{o_1,o_2,\cdots,o_T\}$ 及 $\boldsymbol{\lambda}$,如何选择状态序列,使得它最符合观测序列?

(3)给出一个 $\boldsymbol{O}=\{o_1,o_2,\cdots,o_T\}$,如何调整参数 $\boldsymbol{A}$、$\boldsymbol{B}$、$\boldsymbol{\pi}$,使得 $P(\boldsymbol{O}|\boldsymbol{\lambda})$最大?

本文将利用问题(1)来评估 WLAN 网络数据包序列出现的概率,利用问题(3)对模型参数进行学习训练.

根据前向-后向算法[3-4],计算前向变量 $a_t(i)$ 和后向变量 $\beta_t(j)$ 的步骤如下.

(1)初始化

$$a_1(i)=\pi_i b_i \quad 1\leqslant i\leqslant N \tag{1}$$

$$\beta_T(i)=1 \quad 1\leqslant i\leqslant N \tag{2}$$

(2)归纳

$$a_t(j)=\Big[\sum_{i=1}^{N}a_{t-1}(i)a_{ij}\Big]b_j(o_t)$$
$$2\leqslant t\leqslant T \quad 1\leqslant j\leqslant N \tag{3}$$

$$\beta_t(i)=\Big[\sum_{j=1}^{N}a_{ij}b_j(o_{t+1})\beta_{t+1}(j)\Big]$$
$$t=T-1,\cdots,1 \quad 1\leqslant i\leqslant N \tag{4}$$

(3)计算结果

$$P(\boldsymbol{O}\mid\boldsymbol{\lambda})=\sum_{i=1}^{N}\alpha_T(i) \tag{5}$$

模型参数训练是入侵检测中的关键问题. Baum-Welch 算法[3-4]是 HMM 常用的一种算法,它采取递归思想,使得 $P(\boldsymbol{O}|\boldsymbol{\lambda})$局部最大. 利用该算法训练 HMM 时,不同的初始参数会产生不同的训练结果. 一般认为,$\boldsymbol{\pi}$ 和 $\boldsymbol{A}$ 的初值对训练结果的影响较小,在满足一定条件时可以随机选取,而 $\boldsymbol{B}$ 的初值对训练结果影响较大.

给定 $\boldsymbol{\lambda}$ 和 $\boldsymbol{O}$,从 i 到 j 的转移概率定义为

$$\xi_t(i,j)=P(s_t=i,s_{t+1}=j\mid X,\boldsymbol{\lambda})=\frac{\alpha_t(i)a_{ij}b_j(O_{t+1})\beta_{t+1}(j)}{\sum_{i=1}^{N}\sum_{j=1}^{N}\alpha_t(i)a_{ij}b_j(O_{t+1})\beta_{t+1}(j)} \tag{6}$$

用

$$\gamma_t(i)=\sum_{j=1}^{N}\xi_t(i,j) \tag{7}$$

表示 t 时刻处于状态 S_i 的概率,用

$$\sum_{t=1}^{T-1}\gamma_t(i) \tag{8}$$

表示整个过程中从状态 S_i 转出的次数的预期，用

$$\sum_{t=1}^{T-1}\xi_t(i,j) \tag{9}$$

表示从 S_i 跳转到 S_j 的次数的预期，从而得到

$$\bar{\pi}_i = \gamma_1(i) \tag{10}$$

$$\bar{a}_{ij} = \frac{\sum_{t=1}^{T-1}\varepsilon_t(i,j)}{\sum_{t=1}^{T-1}\gamma_t(i)} \tag{11}$$

$$\bar{b}_j(k) = \frac{\sum_{t=1,\ \text{s.t.}\ o_t=v_k}^{T}\gamma_t(j)}{\sum_{t=1}^{T}\gamma_t(j)} \tag{12}$$

2 HMM 检测 WLAN 入侵

WLAN 的 MAC 层攻击主要分为两种：①洪泛攻击，此类攻击以消耗可用资源或带宽为目的，通过大量发送伪造的数据报文，占用网络可用的带宽或资源，导致合法用户无法获取正常的服务；②针对协议的攻击，此类攻击主要是针对协议自身固有的缺陷，达到破坏用户访问或获取信息的目的. 以上两种攻击都会带来网络流量或者网络数据包序列异常，通过分析网络数据包可以提前发现这种异常. 本文对 MAC 层的头部进行建模，通过计算数据包序列概率 $P(\boldsymbol{O}|\boldsymbol{\lambda})$来发现 WLAN 入侵.

2.1 模型的建立

将 WLAN 网络数据包作为 HMM 的观测序列的一个观察值，取值为 2^n（n 为网络数据包长度的二进制位数），这个数值相当大，会产生以下两种问题：观测符号集合 $\boldsymbol{V}$ 过大，集合元素总数为 2^n；观测符号概率矩阵 $\boldsymbol{B}$ 过大. 它们会导致模型训练时间过长，甚至无法完成. 为了解决这个问题，本文只对 WLAN 的 MAC 帧头部进行分析，采取了网络数据包分段处理的方法，并以网络数据包分段后的一个字段作为一个观测值. 设每个分段长度为 m，则网络数据包分段数为 n/m. 如果 m 太小，网络数据包分段过多会影响检测的准确率；如果 m 过大，会影响模型训练的速度. 试验证实，m 取值为的 8 时候效果较好.

因为选择 WLAN 的 MAC 头部进行建模，所以 n 的值是 MAC 头部的二进制位数长度. 根据 IEEE 802.11 标准 2007 年版本[6]，MAC 头部为 32 B，所以 n 的值为 256. 用 $L=n/m$ 表示一个网络数据包的分段数，其值为 32，则基于 WLAN 网络数据包的 HMM 描述如下.

（1）观测符号集合 $\boldsymbol{V}=\{0,1,2,\cdots,255\}$，观测符号总数 $M=2^8=256$.

（2）正常状态的观测符号概率矩阵

$$\boldsymbol{B}=[b_i(k)]_{L\times M}$$

（3）以一个数据包头部的所有字段为一个观测序列，该观测序列为 $\boldsymbol{O}=\{o_1,o_2,\cdots,o_T\}$，其中的 o_i 是观测序列的第 i 个观测值，同时又是观测对象（网络数据包头部）的第 i 个字段的值.

2.2 模型的简化

WLAN 的基于 MAC 层的常见攻击有 Flood（洪泛）攻击、Spoof（欺骗）攻击、MAC 地址欺骗攻击、NAV 攻击等.

ARF（Authentication Request Flood）是一种典型的 Flood 攻击. 攻击者通过向 AP（Access Point）发送大量的 AR（Authentication Request）帧，使 AP 资源耗尽，从而实现攻击. 如果 AP 在很短的时间内接收到大量 AR 帧，而收不到 STA（Station）的连接请求，则可能存在 ARF 攻击. 类似 Flood 攻击的还有 Beacon Flood、Probe Request Frame Flood、Association Flood、Reassociation Request Frame Flood、Probe Response Frame Flood 等，检测方式类似. 通过分析 MAC 头部帧控制字段可以得到帧的类型，所以分析一段就时间内帧控制字段可以发现 Flood 攻击.

SDF（Spoof Deauthentication Frame）攻击是一种典型的 Spoof 攻击. 攻击者伪造 STA 发送 Deauthentication 帧，持续地向 AP 发送该帧，或者伪造 AP 向 STA 发送该帧，使得 STA 长时间无法连接. 如果在 WLAN 范围内检测到某个 STA 设备（或 AP）向连接着的 AP（或 STA）发送了 Deauthentication 帧，之后在很短的时间内且在还未再次建立连接的情况下又试图进行数据传输等，则说明该设备有可能遭到了 SDF 攻击. 从另一种角度看，在一段连续的数据帧中，帧的类型顺序出现了异常，其检测方式和 Flood 攻击很相似. 检测 Flood 攻击是检测一段连续的数据帧中有大量相同类型的帧，而检测 Spoof 攻击是检测一段连续的数据帧有异常类型序列出现. 类似的 Spoof 攻击有 SDF、Spoof Disassociation、Spoof Disassociation Broadcast Frame、Spoof Sleep State Indication Frame、Spoof PS-Poll Frame、Spoof No Data TIM Frame 等.

MAC 地址欺骗是很多 WLAN 攻击的前提,攻击者通过伪装成合法的 AP、STA 来获取 WLAN 的信息或者进行下一步的攻击. 在 WLAN 的 MAC 帧头中有一个序列控制字段,如图 1 所示. 序列控制字段分为分段号子字段和序列号子字段. 分段号子字段标出了一个特定的介质服务数据单元的分段号;序列号子字段从 0 开始,对于每一个发送 MAC 层协议数据单元(MSDU)序列号加 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,用户无法随意修改. 如果 WLAN 收到 MAC 欺骗攻击,序列号将不是严格递增,所以序列控制字段需要作为 HMM 的观测值.

NAV 攻击是攻击者不断发送 Duration(以时间戳单元表示的数字信号宽度)值很大的请求发送(RTS)帧,使得其他节点不能正常获得信道. 如果在 WLAN 范围内检测到某个 STA 或 AP 的地址,在一段时间内发送了大量的 Duration 域值很大的控制发送/请求发送(CTS/RTS)帧,则说明可能存在 NAV DoS 攻击,所以 MAC 中的 Duration/ID 字段需要作为 HMM 的观测值.

通过以上分析得出,只要把一段连续的网络数据包中的帧控制、Duration/ID 以及帧序列控制字段作为 HMM 的观测值,通过分析帧的类型可以发现 Flood 和 Spoof 攻击,通过分析 Duration/ID 域可以发现 NAV 攻击,通过分析帧序列控制字段可以发现 MAC 欺骗攻击. 所以,我们不用分析整个 32 B 的 MAC 帧头部,只需分析 3 个域,而这 3 个域只有 6 B,从而大大简化了模型复杂度. 针对这 3 个域分别存在的不同攻击,为了提高检测的正确率,对这 3 个域建立了各自的 HMM:FC-HMM (帧控制)、DI-HMM(Duration/ID)、SC-HMM (序列控制),使得各个 HMM 的检测率更高.

2.3　滑动窗口

通过对 HMM 基本问题(1)的求解,得到的 $P(\boldsymbol{O}|\boldsymbol{\lambda})$往往是一个非常小的数值,解决 $P(\boldsymbol{O}|\boldsymbol{\lambda})$值太小的方法之一是采用滑动窗口,基本思想是:在观测序列上建立一个宽度固定的滑动窗口,计算观测序列上的所有滑动窗口概率的最小值,用这个最小值来判断该数据包是否正常. 评价入侵检测系统的检测性能主要有两个指标,即检测率和误报率. 当滑动窗口过小时误报率提高,检测率降低,当滑动窗口过大时训练速度过慢,所以必须通过试验来选择合适的滑动窗口.

2.4　阈值的确定

阈值的大小直接决定入侵检测系统的检测性能. 如果增大阈值,入侵检测率将提高,但误报率也会提高. 相反,如果减小阈值,误报率会降低,但入侵检测率也会降低. 所以,在选择阈值时,应该在入侵检测率和误报率之间折中考虑.

2.5　模型结构

本模型主要由以下 5 个模块组成:数据包捕获模块、数据包解析模块、预处理模块、基于隐马尔可夫模型的学习模块和基于隐马尔可夫模型的异常检测模块.

2.5.1　*数据包捕获模块*　用于整个 WLAN 的数据包,但需将无线网卡设置成混杂模式. 该模式可以捕获所有的数据包,而不管地址如何,即通过 libpcap 进行数据包的捕获.

2.5.2　*数据包解析模块*　负责对捕获的数据包进行分析,即分析结构、检查报头、确定类型,从而提取出该类数据包的特征. 根据建模需要,只需提取出 MAC 头部. 在简化的模型中,只需提取出帧控制、Duration/ID 以及帧序列控制 3 个字段.

2.5.3　*预处理模块*　将解析过的数据包字段进行处理,以便作为隐马尔可夫模型的观测值. 本文采取分段处理,以 FC-HMM 为例,帧控制字段为 2 B,占 16 b,把整个字段以 8 为单位分成 2 段处理.

2.5.4　*训练模块*　在建立的入侵检测系统模型中,建立了 3 个隐马尔可夫模型,其分别经帧控制、Duration/ID、帧序列控制字段分段处理后作为观测值进行学习训练. 训练模块通过 Baum-Welch 算法对一组观测值序列进行训练,然后建立隐马尔可夫检测模型.

2.5.5　*异常检测模块*　利用前向算法计算捕获得到的观测值序列的概率,再通过与阈值的比较来确定捕获到的数据包是否异常,是否对WLAN存在

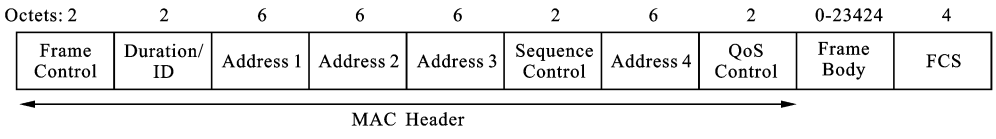

图 1　无线局域网 MAC 帧头部结构图

威胁. 利用前向算法计算出一个观测值序列的概率 $P(\boldsymbol{O}|\boldsymbol{\lambda})$，此时的 $P(\boldsymbol{O}|\boldsymbol{\lambda})$表示 WLAN 数据包字段序列的概率. 因为 $P(\boldsymbol{O}|\boldsymbol{\lambda})$是一个相当小的数值，为了方便比较，需计算 $\lg P(\boldsymbol{O}|\boldsymbol{\lambda})$. 设置 2 个阈值 p 和 q，如果 $\lg P(\boldsymbol{O}|\boldsymbol{\lambda})<p$，表示网络中出现了异常；如果 $\lg P(\boldsymbol{O}|\boldsymbol{\lambda})>q$，表示网络出现了入侵. 阈值的确定是至关重要的，直接决定系统的检测效率，这需要根据实际情况，再经过大量的测试来确定.

2.6 系统实现

由于 WLAN 的开放性和移动性，所以要收集 WLAN 的全部数据是相当困难的. 收集网络数据包是用本文方法进行入侵检测的基础，为了尽可能收集 WLAN 的所有数据包，可采用一个分布式框架，由下述 3 部分构成，结构框架如图 2 所示.

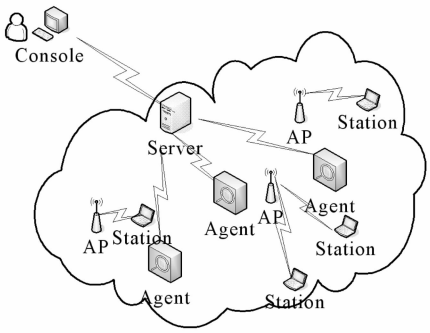

图 2 分布式 WLAN 入侵检测框架结构图

(1)控制台(Console). 用来连接服务器、用户显示和控制.

(2)管理服务器(Server). 管理多个 Agent 节点处理采集到的数据，存储网络数据，分析网络数据包，实现数据包解析模块、预处理模块、训练模块、异常检测模块.

(3)无线分析终端(Agent). 终端分布在 WLAN 中的各个地段，采集 WLAN 数据包，实现数据包捕获模块，执行攻击测试脚本，进行攻击试验.

3 模型的测试和结果分析

利用 HMM 检测入侵，首先要通过训练来建立正常情况下的 HMM. 收集 WLAN 处于正常情况的 10^6 个数据包，在收集数据包的过程中，必须保证 WLAN 未处于入侵状态，否则 HMM 会把入侵当作正常行为，这将导致检测率下降. 编辑攻击脚本，对 WLAN 进行入侵攻击，模拟入侵，再用训练过的 HMM 模型来测试模型的可靠性. 因为 MAC 地址欺骗攻击是很多其他攻击的前提，所以用 SC-HMM 来检测处理后的数据会提前发现很多入侵，从而提高检测效率. 由表 1 结果可见，本文方法具有比较好的检测效果.

表 1 检测结果

模型	FC-HMM	DI-HMM	SC-HMM
误报率/%	6.5	6.3	7.0
漏报率/%	2.3	2.6	3.0

4 结束语

本文提出一种基于 HMM 的 WLAN MAC 层入侵检测方法，采用 WLAN 网络数据包 MAC 帧头部建模，利用分段处理的方法简化模型复杂度，并通过分析 WLAN 攻击的特点对模型进行简化. 试验证明，这是一种有效的方法，对 WLAN 入侵检测具有参考价值.

参考文献：

[1] Andrew Lockhart. Snort-wireless [EB/OL]. [2009-01-15]. http://www. snort-wireless. org/.

[2] Fatblock Working Group. WIDZ [EB/OL]. [2009-01-15]. http://www. loud-fat-bloke. co. uk/w80211. html.

[3] RABINER L R, JUANG B H. An introduction to hidden Markov models [J]. ASSP Magazine, 1986, 3(1): 4-16.

[4] RABINER L R. A tutorial on hidden Markov models and selected applications in speech recognition [J]. Proceedings of the IEEE, 1989, 77(2): 257-286.

[5] WARRENDER C, FORREST S, PEARLMUTTER B. Detecting intrusions using system calls: alternative data models [C]// Proceedings of the 1999 IEEE Symposium on Security and Privacy. Los Alamitos, CA, USA: IEEE Computer Society, 1999: 133-145.

[6] IEEE. Telecommunications and information exchange between systems: local and metropolitan area networks —specific requirements part 11(wireless LAN medium access control (MAC) and physical layer (PHY) specifications 2007) [EB/OL]. [2009-01-02]. http://standards. ieee. org/getieee802/download/802.11-2007. pdf.

(编辑 苗凌)