文章编号:1671-251X(2014)08-0067-05　　DOI:10.13272/j.issn.1671-251x.2014.08.017
罗尚平.介质访问控制层拒绝服务攻击的入侵检测系统[J].工矿自动化,2014,40(8):67-71.

介质访问控制层拒绝服务攻击的入侵检测系统

罗尚平

(乐山师范学院 计算机科学学院,四川 乐山　614004)

摘要:针对无线局域网安全防护手段的不足,结合无线局域网介质访问控制层拒绝服务攻击的特点,设计了基于支持向量机算法的入侵检测系统。该系统利用支持向量机分类准确性高的特点,构建支持向量机最优分类超平面和分类判决函数,对网络流量进行分类识别,完成对异常流量的检测。在 OPNET 平台下进行无线局域网环境入侵检测仿真,仿真结果表明,该系统能有效地检测出针对无线局域网介质访问控制层的拒绝服务攻击。

关键词:无线局域网;入侵检测;支持向量机;介质访问控制层;拒绝服务攻击
中图分类号:TD67　　文献标志码:A　　网络出版时间:
网络出版地址:

Intrusion detection system for denial of service attack in MAC layer

LUO Shangping
(School of Computer Science, Leshan Normal University, Leshan 614004, China)

Abstract: For insufficient of safety protection means and characteristics of denial of service attack in MAC layer of WLAN, the paper designed an intrusion detection system based on support vector machine. The system uses characteristics of high classification accuracy of support vector machine to build hyper-plane of optimal classification and classification decision function, and achieves classification and identification of network traffic, and completes detection of abnormal traffic. The intrusion detection of WLAN was simulated on OPNET platform, and the result indicates that the system can detect denial of service attack in MAC layer efficiently.

Key words: WLAN; intrusion detection; support vector machine; MAC layer; denial of service attack

0　引言

WLAN(无线局域网)利用无线电波在空中辐射传播进行数据传输,发射数据可被预期之外的、安装在辐射范围内不同地点的接收设备以及恶意侵入者接收,因此,数据传输的机密性、可靠性、完整性、抗干扰性和防窃听是 WLAN 应用中的关键[1]。WLAN 自身的特性使得它不但会遭受常规有线网络中的拒绝服务(Denial of Service,DoS)攻击,而且易遭受 WLAN 中所特有的 DoS 攻击[2]。WLAN 遭受 DoS 攻击会导致接入点和站点的连接中断,攻击者可伪造站点窃取数据情报。目前针对 WLAN 中的 DoS 攻击还没有很好的防范机制[3]。因此,研究针对该种攻击的检测和防御方法,对于保障 WLAN 的可用性,进而提升 WLAN 的安全性具有很重要的价值。本文设计了针对 WLAN MAC 层(介质访问控制层)DoS 攻击的入侵检测系统,该系统利用支持向量机(SVM)算法改进了分析处理模块,并根据其最优分类超平面分类原理对网络流量进行分类,实现了对 DoS 攻击的有效检测。

收稿日期:2013-11-28;**修回日期**:2014-06-19;**责任编辑**:胡娴。
基金项目:国家自然科学基金青年项目(61203268)。
作者简介:罗尚平(1977—),男,四川富顺人,实验师,硕士,研究方向为网络及安全,E-mail:710280046@qq.com。

1 MAC 层的 DoS 攻击原理

针对 MAC 层的 DoS 攻击，攻击者常通过伪造控制帧与管理帧发送正常的连接请求，利用载波监听多址接入技术(Carrier Sense Multiple Access with Collision Avoidance，CSMA/CA)及控制帧与管理帧缺乏有效认证机制的缺陷[4]，大幅提高攻击节点接入信道的概率，从而达到长时间持续占用通信信道的目的，使合法的站(Station，STA)与接入点(Access Point，AP)无法正常通信。

MAC 帧是构成 MAC 协议和保证有效数据通信的基础。MAC 帧由帧头(包括帧控制字段、持续时间、地址和序列控制信息)、可变长度的帧体 Body 和帧校验序列(Frame Check Sequence，FCS)3 个部分构成[5]。IEEE 802.11 的 MAC 层定义了 3 种类型的帧：数据帧、控制帧和管理帧[6]。帧控制字段的类型(Type)与子类型(Subtype)决定了具体的帧类型。攻击者在针对 MAC 层进行 DoS 攻击时，首先截获 MAC 帧的帧头部分。由于 MAC 帧的帧头部分有一个用来标识发送该帧的源地址字段是用明文方式传输的，攻击者可以从该字段分析得到源站的 MAC 地址，然后假冒源站进行数据传送。接收端在接到假冒源站发送的伪造 MAC 帧后，由于没有身份认证方法，无法判断帧的合法性。于是攻击者就可以假冒源站的 MAC 地址进行 DoS 攻击。

常见的 DoS 攻击方式有 Beacon Flood 攻击、Probe Request 攻击、Authentication Flood 攻击、Association Request Flood 攻击、Deauthentication Flood 攻击、Disassociation Flood 攻击。以上 6 种 DoS 攻击都是以破坏网络可用性为目的，其攻击方式包括发送大量帧致使 AP 和 STA 之间连接请求帧无法碰撞，或者耗尽 AP 存储资源导致网络瘫痪等。攻击进行时，网络流量会发生大幅度的变化，依据此原理，本文对网络流量进行分析，并通过观察其数值变化来判定网络是否受到攻击。

2 基于 SVM 的分析处理模块

2.1 分析处理模块概念模型

借鉴参考文献[7]中用 SVM 分类网络数据流的方法，分析了基于 SVM 的检测算法，并对 SVM 的相关参数进行了选取。分析处理模块利用 SVM 最优分类超平面的分类判别函数，对经过预处理的未知网络流量进行分类判别，进而得出检测结果。

分析处理模块采用特征检测、异常检测等方法对经过采集模块预处理后的数据进行分析，然后采用特定的融合算法对分析结果进行融合，从而得到检测结果。分析处理模块概念模型如图 1 所示。

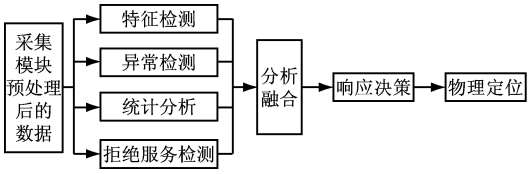

图 1 分析处理模块概念模型

对网络流量的入侵检测是一个二分类问题，需要判别待检测流量是否有异于正常网络流量，所以可以利用异常入侵检测技术进行检测。异常入侵检测技术的优点是可以检测出未知攻击行为。分析处理模块首先读取经过采集模块处理后的网络流量，然后用异常检测的方法将待检测流量与正常网络环境下的特征向量参数值进行比较，判断其是否为正常网络流量。若待检测流量为正常网络流量，则针对该流量的检测结束；若为不正常网络流量，则将此行为记录到日志库，同时发警告到主控程序，根据主控程序进行响应决策。

2.2 SVM 算法

SVM 问题可归结为一个二次型方程求解问题，针对线性不可分的两类问题进行最优分类，即将两类数据无错误地分开并使两类数据的分类间隙最大，从而得到全局最优解，解决了在神经网络中无法避免的局部极小问题。在 SVM 理论中，SVM 形成一个具有严格限制条件的最优分类超平面，然后将数据集合点分布在这个超平面两侧，如图 2 所示。

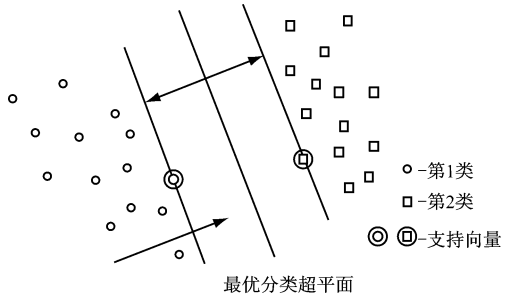

图 2 最优分类超平面

假定训练数据$(x_1,y_1),\cdots,(x_i,y_i),x\in R^n,y\in\{\pm1\}$可以被式(1)所示的超平面无错误地分开，且距离超平面最近的向量与超平面间的距离最大，则称向量集合被最优分类超平面(最大间隔超平面)分开[8]。

$$\boldsymbol{\omega}^{\mathrm{T}}\varphi(x)+b=0 \tag{1}$$

式中：$\boldsymbol{\omega}$ 表示该超平面的法向量；$\varphi(x)$表示训练样本特征的取值；b 表示偏移量。

在线性可分情况下，$\boldsymbol{\omega}^{\mathrm{T}}\varphi(x)+b\geqslant 1$ 时，$y_i=1$；$\boldsymbol{\omega}^{\mathrm{T}}\varphi(x)+b\leqslant -1$ 时，$y_i=-1$，所以可以将其合并为

$$y_i(\boldsymbol{\omega}^{\mathrm{T}}\varphi(x)+b)\geqslant 1,\ i=1,\cdots,l \tag{2}$$

式中：l 表示训练样本数。

容易验证，超平面就是满足式(2)且使得自定义函数 $\Psi(\boldsymbol{\omega})$ 关于向量 $\boldsymbol{\omega}$ 和标量 b 最小化的平面。自定义函数 $\Psi(\boldsymbol{\omega})$ 表达式为

$$\Psi(\boldsymbol{\omega})=\|\boldsymbol{\omega}\|^2 \tag{3}$$

SVM 利用边缘最大化原则，通过最优分类超平面来构造判决函数，避免了对训练集的过度拟合，保证了 SVM 的分类能力。经过训练集上的学习后，对测试集中数据进行分类的正确率非常高。同时核函数的引进使得特征空间的维数变得不再重要，不必知道特征映射的具体形式，从而避免了维数灾难，因此，SVM 适用于处理高维数据。

2.3　改进的分析处理模块

将 SVM 作为分析处理模块的主体算法，对分析处理模块进行了改进，其工作流程如图 3 所示。

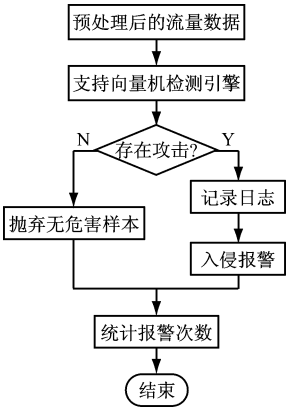

图 3　SVM 分析处理模块工作流程

检测算法效率的高低直接决定了入侵检测系统的性能。用 SVM 对测试样本集进行入侵检测，实际上就是由分类判别函数对数据进行分类的问题，分类判别以后得到预测输出值 y，y 表示网络流量是否正常。当 y 为 $+1$ 时判定该网络流量正常；y 为 -1 则表示存在攻击行为。

由式(1)可知，SVM 是基于结构风险的原理机器学习。在线性不可分的情况下，需要转换成二次优化问题求解。设 $\min J(\boldsymbol{\omega},\boldsymbol{\xi})$ 为将非线性问题转换成二次优化问题时定义的函数，J 表示支持向量的集合，则有

$$\min J(\boldsymbol{\omega},\boldsymbol{\xi})=\frac{1}{2}\|\boldsymbol{\omega}\|^2+C\sum_{i=1}^{n}\xi_i \tag{4}$$

$$\text{s.t.}:\ y_i(\boldsymbol{\omega}\varphi(x_i)+b)\geqslant 1-\xi_i \tag{5}$$

$$\xi_i\geqslant 0,\ i=1,\cdots,l \tag{6}$$

式中：$\boldsymbol{\xi}=(\xi_i,\cdots,\xi_l)^{\mathrm{T}}$ 为非负松弛变量；C 表示惩罚因子。

当分类出现错误时，$\xi_i>0$，因此，$\sum_i\xi_i$ 是训练集中错分样本数的上界。这就需要在目标函数中为分类误差分配一个额外的代价函数，即引入错误惩罚分量。惩罚因子 C 控制对错分样本的惩罚程度，C 越大表示对错误分类的惩罚越大。C 控制了模型复杂度和经验风险之间的折中，等价于对核函数作了附加的常数调整：

$$\boldsymbol{K}(\cdot)\leftarrow\boldsymbol{K}(\cdot)+\frac{1}{C}\boldsymbol{I} \tag{7}$$

式中：$\boldsymbol{K}(\cdot)$ 表示核矩阵；$\boldsymbol{I}$ 表示单位矩阵。

在训练 SVM 时，如果无限制地增加惩罚因子 C，使得 $1/C\to 0$，就会使 SVM 等价于可分模型。随着 C 的增大，它对性能的影响越来越弱。为了客观分析 C 对分类性能的影响，本文在 Wisconsin Breast Cancer 数据集上进行实验，当使用径向基核函数，并保持核参数 σ 不变时(设定为 0.000 1)，观察 LooRate(留一法推广能力估计值)、SVR(Support Vectors Rate，支持向量率)和 TestRate(实际测试错误率)随 C 的变化情况，如图 4 所示。

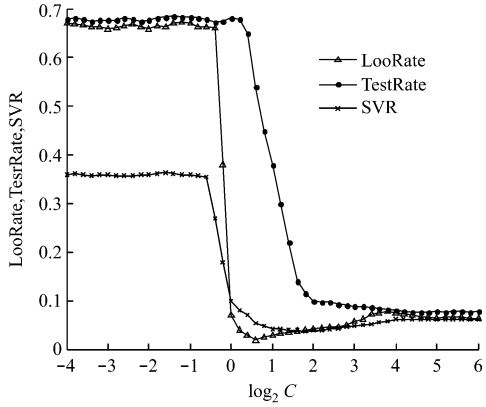

图 4　各性能参数随惩罚因子 C 的变化曲线

SVR 是 SVM 数目或支持向量数目与样本数目的比值，是留一法推广能力的上界。从图 4 可以看出，当 C 较小时，LooRate 和 TestRate 的值都比较高；而当 C 增加时，两者的值都急剧降低，此时性能迅速提高；继续增加 C，曲线波动不明显，此时性能的变化较小；当 C 增加到一定值后，性能不再受 C 的影响。因此，在较大的范围内，推广能力对 C 的变化不敏感。对应的 SVM 分类面在特征空间中越来越复杂，训练集中分类错误的样本越来越少，C 是算法中唯一可以调节的参数。

SVM 通过引入 Lagrange 因子将大样本分类问题转化为对偶问题，拉格朗日函数为

$$L(\boldsymbol{\omega},b,\alpha)=\frac{1}{2}\|\boldsymbol{\omega}\|^2+C\sum_{i=1}^{l}\xi_i-\sum_{i=1}^{l}\alpha_i(y_i(\boldsymbol{\omega}\varphi(x_i)+b)-1+\xi_i)-\sum_{i=1}^{l}\beta_i\xi_i \tag{8}$$

式中：$\boldsymbol{\alpha}=(\alpha_1,\cdots,\alpha_l)^{\mathrm{T}}$，$\boldsymbol{\beta}=(\beta_1,\cdots,\beta_l)^{\mathrm{T}}$，是 Lagrange 因子；$\alpha_i\geqslant 0$，$\beta_i\geqslant 0$。

求拉格朗日函数关于 $\boldsymbol{\omega}$，b，ξ 的偏导数，由极值条件可得

$$\begin{cases}\nabla_b L(\boldsymbol{\omega},b,\alpha)=0\\ \nabla_{\boldsymbol{\omega}} L(\boldsymbol{\omega},b,\alpha)=0\\ \nabla_{\xi} L(\boldsymbol{\omega},b,\alpha)=0\end{cases} \tag{9}$$

从而推出

$$\begin{cases}\sum_{i=1}^{l}y_i\alpha_i=0\\ \boldsymbol{\omega}=\sum_{i=1}^{l}y_i\alpha_i\varphi(x_i)\\ C-\alpha_i-\beta_i=0\end{cases} \tag{10}$$

将式(10)代入式(8)，得到对偶函数：

$$\max_{\alpha}:\sum_{i=1}^{l}\alpha_i-\frac{1}{2}\sum_{i=1}^{l}\sum_{j=1}^{l}y_iy_j\alpha_i\alpha_j\varphi(x_i)\varphi(x_j) \tag{11}$$

$$\text{s.t.}\sum_{i=1}^{l}y_i\alpha_i=0$$

式中：$0<\alpha_i<C$，$i=1,\cdots,l$。

构造对偶问题后求得

$$f(x)=\operatorname{sign}\Big\{\sum_{i=1}^{l}\alpha_iy_i[\varphi(x)\varphi(x_i)]+b\Big\} \tag{12}$$

将核函数 $K(x_i\cdot x)=\varphi(x)\varphi(x_i)$ 代入式(12)，得到分类判别函数：

$$f(x)=\operatorname{sign}\Big[\sum_{i=1}^{l}\alpha_iy_iK(x_i\cdot x)+b\Big] \tag{13}$$

Lagrange 乘子与约束的积在最优点为 0，即

$$\begin{cases}\alpha_i[y_i(\boldsymbol{\omega}\varphi(x_i)+b)-1+\xi_i]=0\\ \beta_i\xi_i=0\end{cases} \tag{14}$$

对于标准支持向量($0<\alpha_i<C$)，由式(10)得到 $\beta_i>0$，则由式(14)得到 $\xi_i=0$，因此，对于任意标准支持向量，满足：

$$y_i[\boldsymbol{\omega}\varphi(x_i)+b]=1 \tag{15}$$

从而得到参数 b 为

$$b=y_i-\boldsymbol{\omega}\varphi(x_i)=y_i-\sum_{x_j\in J}\alpha_jy_j\varphi(x_j)\varphi(x_i) \tag{16}$$

为了保证计算可靠，还需要对所有标准支持向量分别计算 b 的值，然后再求取平均值。

$$b=\frac{1}{N_{\mathrm{NSV}}}\sum_{x_i\in JN}\Big[y_i-\sum_{x_j\in J}\alpha_jy_j\varphi(x_j)\varphi(x_i)\Big] \tag{17}$$

式中：N_{NSV} 为标准支持向量的总数；JN 为标准支持向量的集合，J 为支持向量的集合。

在求解过程中，只考虑支持向量的大小，不考虑支持向量的方向。

3 仿真分析

在 OPNET 仿真平台建立一个 WLAN 环境，并在该网络环境下进行入侵攻击检测仿真。仿真中 DoS 攻击帧的生成由 Attack 节点实现。Attack 节点实行 DoS 攻击仿真的网络拓扑如图 5 所示。其中 jam 表示无线移动干扰节点，其分析出 MAC 帧头部分，并进行帧的伪造；tx 表示无线固定发信机，其向 WLAN 发送伪造的攻击帧；rx 表示无线固定收信机，其捕获 MAC 帧；数据速率为2 Mbit/s。

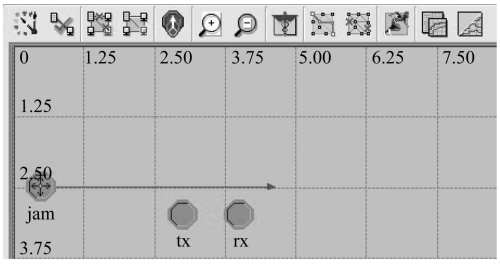

图 5 DoS 攻击 OPNET 仿真网络拓扑结构

在进行入侵攻击检测仿真时，为了使检测结果具有可比性，设置了对照样本集。实验过程如下：

(1) 随机在每种已知攻击类型的测试数据中选取 2 000 份攻击样本，构成攻击类型已知的攻击样本集，同时选取 2 000 份正常网络流量样本作为对照，构成正常流量样本集。

(2) 选取 6 种攻击的攻击样本各 2 000 份，将其混合，并从混合集中随机抽取 2 000 份攻击样本，作为混合攻击样本集，同样构造正常流量样本集进行对照。

(3) 经过上面 2 个步骤后，就得到了 7 种已知攻击类型的攻击样本集和用于对照的正常流量样本集，每个测试样本集中包含 2 000 份样本。

(4) 对每种攻击，取同类型的攻击样本 1 000 份构建一个待检测流量包，得到 7 个已知攻击类型的待检测流量包，同时构建等量用于对比的正常流量包。

(5) 在 WLAN 正常工作的实验环境下，对已知攻击类型的待检测流量包中测试样本集进行入侵检测实验，若检测判定为入侵攻击，则系统进行报警，并记录此次报警。

(6) 最后通过统计正确检测出的待检测流量包中的攻击样本集数目、错判为攻击样本集的正常流

量样本集数目、检测率 adr、漏检率 ldr 和虚警率 fpr 的值来判断无线入侵检测系统的性能。

以 Beacon Flood 攻击的入侵攻击检测实验为例,其入侵攻击检测实验流程如图 6 所示。检测出的 Beacon 攻击测试样本个数如图 7 所示。图中横坐标为时间变化,纵坐标为检测出攻击样本集并进行报警的次数累计,中间小图部分是对照流量包中 1 000 份正常流量样本检测结果的放大。

图 6　Beacon Flood 攻击检测流程

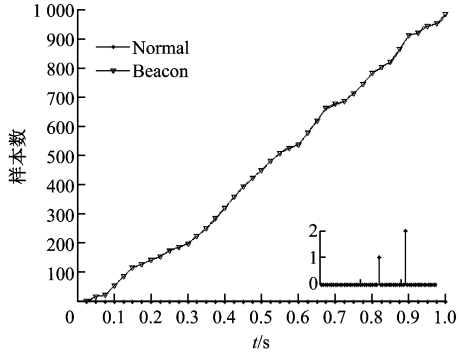

图 7　检测出的 Beacon 攻击测试样本个数

对入侵检测系统检测结果的统计见表 1。针对某个已知攻击类型的待检测流量包,正确检测表示检测出的攻击样本集的数目,错误检测表示将正常流量样本集错判为攻击样本集的数目,正确检测对应的概率统计为检测率,错误检测对应的概率统计为虚警率。

表 1　检测主机的检测结果

测试样本集类型	正确检测	错误检测	检测率/%	虚警率/%	漏检率/%
Beacon Flood	992	2	99.2	0.2	0.8
Probe Request	988	0	98.8	0.0	1.2
Authentication	983	0	98.3	0.0	1.7
Association	976	3	97.6	0.3	2.4
Deauthentication	971	0	97.1	0.0	2.9
Disassociation	962	6	96.2	0.6	3.8
Mixed	988	3	98.8	0.3	1.2

实验结果表明,针对 MAC 层的 6 种 DoS 攻击,检测主机取得了较高的检测率、较低的虚警率和漏检率。在 6 种攻击单独进行时,检测主机针对每种攻击方式的检测都取得了 96%以上的检测率,基于 SVM 原理的分类算法极大地提高了入侵检测系统的检测率;虚警率则低于 0.6%,漏检率低于 4%,特别是在进行 Probe Request、Authentication、Deauthentication 的攻击检测时,其虚警率一度达到了 0,在进行 Beacon Flood 攻击检测时其虚警率也仅为 0.2%,且漏检率为 0.8%;在对混合攻击测试样本集进行入侵检测时,检测主机的检测率为 98.8%,虚警率和漏检率分别为 0.3%和 1.2%。

4　结语

将 SVM 引入到 WLAN MAC 层 DoS 攻击的入侵检测系统,设计了改进的分析处理模块。基于 SVM 算法的入侵检测系统能有效地检测出常见的 6 种类型的 DoS 攻击,由于这 6 种 DoS 攻击具备了针对 WLAN MAC 层 DoS 攻击的所有特点,所以可以将本文设计的入侵检测系统推广到不同的无线网络入侵检测环境中。在检测出入侵攻击以后,只要用无线定位技术对攻击源进行定位,然后屏蔽掉该攻击源发送的一切信息,就能从本质上清除 DoS 攻击的威胁,最大程度地保护网络的可用性和安全性。

参考文献:

[1] GEIER J. 无线局域网[M]. 王群,李馥娟,叶清扬,译. 北京:人民邮电出版社,2001:18-27.

[2] 李林. WLAN 安全机制的分析与研究[D]. 西安:西安电子科技大学,2005.

[3] MALEKZADEH M. An experimental evaluation of DoS attack and its impact on throughput of IEEE 802.11 wireless networks[J]. International Journal of Computer Science and Network Security, 2008, 8(8): 96-103.

[4] ADARSHPAL S S, HNATYSHIN V Y. The OPNET user guide for practical computer network simulation[M]. Chapman & Hall/CRC, 2012: 2-10.

[5] 张帆,马建峰. WAPI 实施方案的安全性分析[J]. 西安电子科技大学学报:自然科学版,2005,32(4):545-548, 592.

[6] 邓达. WLAN 安全性问题研究与改进[D]. 成都:电子科技大学,2007.

[7] ZHU Li, YUAN Ruixi, GUAN Xiaohong. Accurate classification of the Internet traffic based on the SVM method [C]//IEEE International Conference on Communications, 2007: 1373-1378.

[8] VLADIMIR V. The nature of statistical learning theory[M]. 2nd ed. New York: Springer-Verlag New York Inc., 2000.