

基于 KKT 和超球结构的增量 SVM 算法的云架构入侵检测系统

张文兴¹, 樊捷杰^{2*}

(1. 内蒙古科技大学 机械工程学院, 内蒙古 包头 014010; 2. 内蒙古科技大学 信息工程学院, 内蒙古 包头 014010)

(* 通信作者电子邮箱 fanjiejie777@hotmail.com)

摘要:针对传统入侵检测系统(IDS)处理数据负载过重,不支持多主机数据联合分析,以及大规则库维护的问题,提出一种云架构的基于卡罗需-库恩-塔克(KKT)条件和超球结构的增量支持向量机(KS-ISVM)入侵检测系统。将客户端抓取的数据包经过预处理生成样本空间,然后发送至云端使用KS-ISVM进行建模分析,利用KKT条件对增量样本进行筛选,选取违反KKT条件的样本作为有用样本,剔除KKT范围内的所有样本;此外,为了保证剔除的样本为冗余样本,进一步采用超球结构的方法对样本进行第二次筛选,将超球范围内的样本作为有用样本,剔除其余样本;最后将选取的样本进行合并,对SVM进行更新训练。利用KDDCUP99数据进行实验验证,并与SVM、批量支持向量机(Batch-SVM)、互检KKT条件的增量学习(K-ISVM)算法进行对比,结果表明,KS-ISVM具有良好的预测能力和样本淘汰能力,准确率达到90.3%,而SVM、Batch-SVM和K-ISVM三种方法准确率均在89%以下;同时还对并行KS-ISVM进程联合分析,发现单进程的分析时间由6351s降低到16进程的146s,分析时间大大降低,说明了多进程的有效性,满足云计算环境中的入侵检测系统对效率和精度的要求。

关键词:入侵检测系统;云架构;增量支持向量机;卡罗需-库恩-塔克条件;超球结构

中图分类号: TP393.0 **文献标志码:** A

Cloud architecture intrusion detection system based on KKT condition and hyper-sphere incremental SVM algorithm

ZHANG Wenxing¹, FAN Jiejie^{2*}

(1. School of Mechanical Engineering, Inner Mongolia University of Science and Technology, Baotou Nei Mongol 014010, China;

2. School of Information Engineering, Inner Mongolia University of Science and Technology, Baotou Nei Mongol 014010, China)

Abstract: In view of overload, nonsupport of multi-computer conjunction analysis and maintenance of huge rule database in traditional Intrusion Detection System (IDS), a new kind of cloud architecture IDS with Incremental Support Vector Machine (ISVM) algorithm based on KKT condition and hyper-sphere, namely KS-ISVM was proposed. The network data captured by client were preprocessed and sent to the cloud as samples. The KS-ISVM was used to analyze these samples in cloud. According to the KKT condition, the samples that violated the KKT condition were selected as useful samples, and the others that met the KKT condition were removed. In addition, in order to ensure that the removed samples were redundant, they were screened again by hyper-sphere, after that, the samples which met the hyper-sphere rule were regarded as useful samples, while the others were deleted. Finally, the SVM was trained and updated by merging those selected useful samples. Contrast experiments with SVM, Batch-SVM and Incremental SVM based on KKT (K-ISVM) were carried out on KDDCUP 99. The results show that KS-ISVM has good performance in prediction and selection of samples, its accuracy can reach 90.3%, but the accuracy of SVM, Batch-SVM and K-ISVM are all below 89%. Through analyzing the parallel KS-ISVM processes, the analyzing time of the single process is 6351 s, while that of 16 processes is 146 s, which proves that the multi-process techniques is effective, and it can meet the efficiency and accuracy requirements of IDS in cloud computing environment.

Key words: Intrusion Detection System (IDS); cloud architecture; Incremental Support Vector Machine (ISVM); Karush-Kuhn-Tucker (KKT) condition; hyper-sphere

0 引言

入侵检测系统(Intrusion Detection System, IDS)是通过分析网络数据包、系统日志、配置文件改变等数据特征,来推测系统是否发生入侵事件的安全机制。随着互联网的不断演化改变,IDS的形式也逐渐日新月异。除了要维护巨大的本地

规则库外,传统IDS要耗费大量计算资源来分析本机所接收到的数据包,并对包含大量冗余信息的数据作重复分析工作。为减轻主机工作负担,提高入侵检测效率,Gogoi等^[1]提出一种多层混合入侵检测算法,将多种算法结合在一起,提升入侵检测精度和速度;林洋等^[2]提出改进支持向量机(Support Vector Machine, SVM)算法和井小沛等^[3]提出的特征选择算

收稿日期:2015-04-20;修回日期:2015-07-27。 基金项目:国家自然科学基金资助项目(21366017)。

作者简介:张文兴(1983-),男,江西上饶人,讲师,硕士,主要研究方向:数据挖掘、工业过程建模;樊捷杰(1985-),男,江西上饶人,硕士研究生,主要研究方向:信息安全、大数据处理、入侵检测。

法,均是将基于概率学的 SVM 算法应用于单机入侵检测环境;张永俊等^[4]提出的基于云模型的增量 SVM 入侵检测方法将增量 SVM 算法应用到了样本分析。

针对传统入侵检测系统处理数据负载过重且不支持多主机数据联合分析,以及需对大规则库进行维护的问题,本文提出一种基于卡罗需-库恩-塔克(KKT)和超球结构的增量支持向量机(KKT and Supper-ball Incremental SVM, KS-ISVM)算法的云架构入侵检测系统。用户端可通过对数据的抓取和初步处理,得到该数据包的特征集 $C(f_1, f_2, \dots, f_n)$; 将特征集所构成的样本空间发送到云端进行处理,云端使用 KS-ISVM 算法模块对样本空间进行并行分析,并得到最终入侵检测结果。

1 生成数据包特征集

为给云端 KS-ISVM 提供分析样本空间,须将主机上抓取的网络数据包所包含的各个属性进行量化,形成特征集。在量化数据包特征集方面,朱映映等提出从数据包协议,通过连接属性等方法提取特征值^[5];很多学者也提出了从数据包的各个层面上提取有效信息特征的方法^[6-8]。在本文中,对数据包属性特征的提取遵循以下三个方面。

1) 头部属性。

从 IP 层捕获的数据报文分为头部和内容部两部分。头部包含数据包的各种协议信息,如源地址、目的地址、数据包长度、上层协议、连接属性、标志位等。使用 $W(W_1, W_2, \dots, W_n)$, 表示从头部获取的属性,头部属性亦称协议属性。

2) 内容属性。

内容即数据包携带的有效数据信息。内容属性通常指经过关键字匹配后得到的内容检测结果。设规则库内容匹配关键字字符串数量为 m , 则经过 m 次匹配算法生成的内容属性集合为: $T = (t_1, t_2, \dots, t_n)$ 。为避免内容属性过于庞大,使用 $F(T)$ 对匹配结果进行如式(1)所示处理,进而得到 n 个新的属性集合。

$$F(T) = Q(q_1, q_2, \dots, q_n); n \ll m \quad (1)$$

通过设置阈值 α_1 和 α_2 来对是否入侵进行检测判断。当 $F(T)$ 中存在属性项 $q > \alpha_2$, 认为此数据包已经检测出入侵行为;当 $F(T)$ 中存在属性项 $q < \alpha_1$, 则认为数据包属于普通数据包。

3) 会话属性。

在网络通信过程中,数据包存在通信属性,也称为会话属性,如 TCP 连接的时间、连接频度等。这些属性集合用 $S = (S_1, S_2, \dots, S_n)$ 表示。

在获取上述属性后,使用加权评估函数 F_n 对这些属性进行处理:

$$F_n(b_1 W, b_2 Q, b_3 S) = C(f_1, f_2, \dots, f_n) \quad (2)$$

其中: b_1, b_2, b_3 为加权因子。经过进一步处理,数据包可以转换成 $D = (d_1, d_2, \dots, d_n, C)$ 的形式,作为样本空间提供给云端处理。其中: d 为数据包的附加属性,如所属主机号、数据包编号等,用来管理数据包; C 则是 KS-ISVM 处理的样本属性部分。

2 增量支持向量机

许多学者为解决海量数据的训练问题,提出了多种 SVM

增量学习算法^[9]。如: Syed 等^[10]提出的批量支持向量机(Batch-SVM)增量学习算法,淘汰历史样本集中的非支持向量,将支持向量同新增样本一起训练,达到增量学习的目的。该算法快速降低了参与增量训练的历史样本数目,但对于新增样本集未加筛选,不论新增样本中是否含有新的信息,全部加入增量学习,从而造成浪费。曾文华等^[11]提出了一种互检 KKT 条件的增量学习(Incremental SVM based on KKT, K-ISVM)方法,分别对初始和增量样本集训练,得到各自的分类器和支持向量集,然后互相找出违反对方 KKT 条件的样本,加入到各自的支持向量集一起训练得到最终分类器,样本分类精度有所提高,但对那些最有可能成为最终支持向量的违反 KKT 条件的样本欠考虑。为了解决这些问题,本文在上述研究的基础上,提出了一种基于 KKT 条件超球结构的增量支持向量机(KS-ISVM)。

3 基于 KKT 条件和超球结构的 KS-ISVM

基于超球结构的 SVM 增量学习算法利用超球结构对增量学习中的训练样本进行选取^[12]。超球结构通过在高维希尔伯特核空间中构造出一个超球,然后从超球上选取符合条件的边缘样本。KS-ISVM 算法是将每一类数据在希尔伯特核空间中用最小超球来界定,整个数据的希尔伯特核空间就变成了若干个超球的组合。

在增量学习过程中,只需对新增样本构造其对应的超球,不需要额外的参数修改且计算量小。但由于超球包围的数据有可能是非支持向量,该类数据对模型的训练毫无意义,还需要消耗训练时间。因此采用 KKT 条件的方法来找出非支持向量并将其删除,同时将违反 KKT 条件的新增样本加入到模型的增量学习当中,提高模型精度和训练速度。

3.1 超球结构支持向量机

针对 $k \geq 2$ 类的数据分类问题,超球结构的数学描述如下: 给定 k 个 n 维空间的集合 $A^m (m = 1, 2, \dots, k)$, $x_i^m \in A^m (i = 1, 2, \dots, l^m)$ 。对于集合 A^m , 找出一个球 (a^m, R^m) , 其中: R^m 是球的半径, a^m 是球心。在半径尽量小的前提下, 使球 (a^m, R^m) 包含几乎所有样本点 x_i^m 。为避免各别样本点偏离球心太远,引入松弛变量 ξ_i^m 对较远的样本点进行如式(3) ~ (4)所示的约束。

$$\|x_i^m - a^m\| \leq R^m + \xi_i^m \quad (3)$$

$$\begin{cases} i = 1, 2, \dots, l \\ \xi_i^m \geq 0 \end{cases} \quad (4)$$

以超球半径最小化为优化目标,其函数如式(5)所示:

$$F(R^m, a^m, \xi_i^m) = R^m + C^m \sum_i \xi_i^m \quad (5)$$

其中: C^m 为惩罚系数,控制球的大小及错分样本的惩罚程度。利用 Lagrange 乘子法解该优化问题如式(6)所示:

$$\max(L(\alpha_i^m)) = \sum_i \alpha_i^m k(x_i^m, x_i^m) - \sum_{i,j} \alpha_i^m \alpha_j^m k(x_i^m, x_j^m) \quad (6)$$

$$\text{s.t.} \quad \sum_i \alpha_i^m = 1; i, j = 1, 2, \dots, l^m \quad (7)$$

$$0 \leq \alpha_i^m \leq C^m$$

其中: $\alpha_i, \alpha_j \geq 0$ 为 Lagrange 乘子。

传统增量学习方法各个增量学习步骤都是基于新增样本

与原有样本在希尔伯特核空间中的分布特点有关,有些样本由于不是支持向量而被删除,而在后续新增样本到来之后,这些原来被删除的样本有可能在新的 KKT 条件下成为支持向量^[13]。然而由于这些样本被删除导致无法参与模型的更新训练,从而不可避免地影响到模型精度。基于超球结构的样本选择实际上就是一个在希尔伯特核空间中超球边缘数据选取问题,选取方法具体如图1所示。

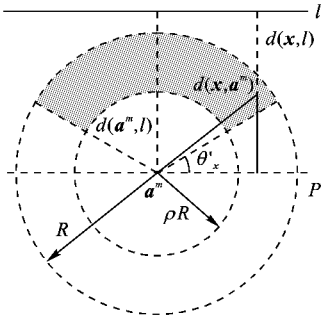


图1 基于超球结构的边缘样本选取方法

如图1所示,通过超球算法可求出球心为 a^m ,半径为 R 的超球。为选取超球边缘附近的样本点,定义一个半径为 ρR 的同心超球,其中 $\rho \in [0,1]$ 。将 SVM 模型的决策超平面 l 作为参照,取经过球心且平行于 l 的超平面 P ,设点 x 与球心的连线与超平面 P 的夹角为 θ'_x ($\theta'_x \in [-\pi/2, \theta]$)。计算方法如式(8)所示:

$$\theta'_x = \arcsin\left(\frac{d(x, l) - d(a^m, l)}{d(x, a^m)}\right) \quad (8)$$

其中: $d(x, l)$ 表示点 x 到超平面 l 的距离, $d(a^m, l)$ 表示球心 a^m 到超平面 l 的距离, $d(x, a^m)$ 表示点 x 到球心 a^m 的距离。

根据上述距离和角度的结果,得超球边缘附近点 x 被选取的条件为式(9)所示:

$$\rho R \leq d(x, a^m) \leq R; 0 \leq \theta'_x \leq \theta \quad (9)$$

由式(8)可知,只要适当选取 θ 与 ρ ,就可选取潜在的有用样本,即处于阴影区域的样本。其选取过程如图2所示。

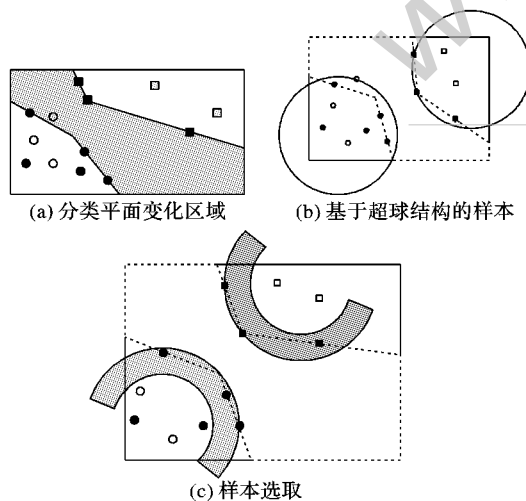


图2 超球样本选取过程

对于选取的样本,进一步采用 KKT 方法进行过滤,一般认为,违反式(10)所示 KKT 条件的样本包含大量有用信息,且是以前模型所未学习到信息,因此,选取违反 KKT 条件的样本作为最终有用的样本,删除在 KKT 条件范围内的样本。

KKT 条件如下:

$$\begin{cases} a_i^{(*)} = 0 & \Rightarrow y_i \cdot f(x_i) \geq 1 \\ 0 < a_i^{(*)} < c & \Rightarrow y_i \cdot f(x_i) = 1 \\ a_i^{(*)} = c & \Rightarrow y_i \cdot f(x_i) \leq 1 \end{cases} \quad (10)$$

选取满足 $y_i \cdot f(x_i) \leq 1$ 的样本作为本文所需的样本进行模型的增量更新。

3.2 KS-ISVM 处理数据包特征集

假设存在历史样本集 A ,增量样本集 B ,基于超球结构的支持向量增量分类算法步骤如下:

- 1) 利用样本集 A 训练支持向量机初始分类器;
- 2) 利用初始分类器对样本集 B 分类;若达到预定分类精度,则计算结束,否则转3);
- 3) 令集合 $M = A \cup B$,根据样本所属类别分别构造超球,根据设定的 ρ 和 θ ,从集合 M 中完成训练样本选取;
- 4) 对选取样本进行 KKT 条件验证,选取违反 KKT 条件的样本;
- 5) 利用4)所选取的样本对支持向量机进行训练,求得新的支持向量机分类器。

4 系统设计及测试

4.1 系统设计

为论证 KS-ISVM 算法在云架构入侵系统中应用的可行性,通过对云架构入侵检测系统的分析,本文对其结构进行了模块设计,如图3所示。

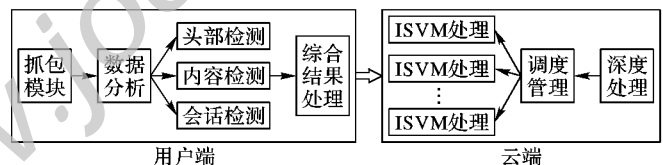


图3 云架构入侵检测结构

系统分为用户端与云端两部分。用户端包含数据抓取模块、数据分析模块、检测模块以及综合处理模块;云端则通过调度管理模块调度多个 KS-ISVM 模块进行并发处理用户端发送来的样本空间,并包含深度处理模块。整个系统工作流程如下:

- 1) 用户端使用数据包抓取模块进行数据抓取;
- 2) 对数据进行初步处理,过滤掉无须分析的数据包;
- 3) 使用头部检测、内容检测及会话检测3种检测方式生成对应的属性集合 W, Q, S ;
- 4) 对属性集合综合处理,得到属性 $D(d_1, d_2, d_3, \dots, C(f_1, f_2, \dots, f_n))$ 的样本集并发往云端;
- 5) 云端调度模块调度 KS-ISVM 算法模块进行样本分析;
- 6) 对 KS-ISVM 处理结果进行更深一步处理。

4.2 算法实现及结果分析

4.2.1 实验环境

实验在实验室搭建的云服务平台上进行。实验平台配置为:CPU 四核 2.4 GHz \times 2,内存 16 GB,硬盘 4 TB,双 100 GB/s 网卡的一台塔式服务器上安装 VmWare ESXI 5.1 作为云端虚拟服务平台。使用 CentOS 6.4 64bit 作为虚拟机操作系统,可同时开启 1~8 个虚拟操作系统,在一台虚拟机上开启 1~4 个 KS-ISVM 处理进程来处理样本。

为准确地模拟攻击环境,用户端数据从 10% 的

KDDCUP99 中随机抽取 6000 个正常数据包和 6000 个受攻击的数据包,使用特征集处理模块进行预处理,生成样本空间(为便于测试,样本取六维属性 $C(f_1, f_2, \dots, f_6)$),且不作样本过滤处理。选取 5000 个普通样本和 5000 个受攻击样本作为训练样本,其余 2000 样本进行预测验证,分别进行单进程和多进程两组实验。

4.2.2 实验结果分析

实验1 单进程实验。

将 10 000 个训练样本并平均分成 5 等份,得到 5 个训练样本集。首先对其中一个样本集进行 SVM 训练;然后,利用 KKT 条件和超球结构方法,对训练样本及 SVM 的支持向量进行数据筛选;最后,将筛选出的数据和下一个训练集样本进行混合并重新训练 SVM 模型,完成一次增量学习。对后面 3 个训练集以此类推,共完成 4 次增量学习训练,使用单进程的 KS-ISVM 进行分析,并与标准 SVM、Batch-SVM 和 K-ISVM 分析的准确率对比,其预测精度和训练时间结果如图 4~5 所示。

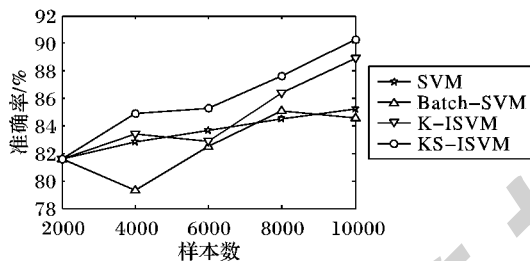


图4 不同算法的准确率对比

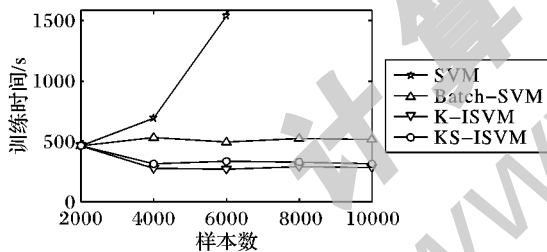


图5 不同算法的训练时间对比

从图 4 的实验结果可得出,KS-ISVM 相对其余的 3 种分析算法在精度上有一定的优势,并且算法精度的稳定性也较其他的算法更优。由图 5 的实验结果可知,传统 SVM 算法随着样本数量的增加训练时间明显增长,且大大超过其他 3 种算法,因此,传统 SVM 训练效率太差,不适合大规模样本的训练;Batch-SVM 由于将上次模型的支持向量样本和增量样本合在一起进行模型的更新训练,相比传统 SVM,其训练样本大大减少从而导致训练时间明显减少,但由于没有对新增样本进行筛选,相比 K-ISVM 和 KS-ISVM 算法,其训练时间仍然偏高;K-ISVM 的训练样本既选择了上次模型的支持向量,又选择了增量样本中违反 KKT 条件的样本,训练样本数量最少且训练时间最短;KS-ISVM 在 K-ISVM 的基础上利用超球结构选择了潜在的支持向量,导致训练时间增长,但模型的精度要明显高于 K-ISVM。

实验2 多进程实验。

该实验采用 1 进程、4 进程、8 进程、16 进程的方式进行训练,按照对应的进程规模以此启动多台虚拟机参与运算。为便于计算,按照进程数量规模,依次对训练样本、增量样本

和测试样本进行均分。其预测精度和训练时间如表 1 和图 6 所示。

KS-ISVM 进程整个处理过程如图 6 所示。单进程耗时 6351 s;4 进程减少到 2158 s;8 进程为 578 s;而 16 进程则为 146 s。可见处理时间随进程数量的增加而迅速下降。4 种算法精度对比如图 7 所示。对于 KS-ISVM 来说,进程数量增加准确率平缓上升,且较其余 3 种算法精度略有优势。

实验结果表明,对于大样本的训练集,单进程 KS-ISVM 需耗费大量处理时间,实际应用会造成主机计算的巨大负担,使用多主机多线程并行处理可使处理时间呈指数曲线降低,并且准确率略有提升,这表明 KS-ISVM 算法更加适合云架构环境中联合分析。

表1 KDDCUP99 数据集多进程算法的准确率比较

进程数	准确率/%			
	SVM	Batch-SVM	K-ISVM	KS-ISVM
1	85.3	83.6	84.1	84.6
4	85.3	84.5	86.4	85.9
8	85.3	86.7	87.7	89.3
16	85.3	88.1	90.6	91.5

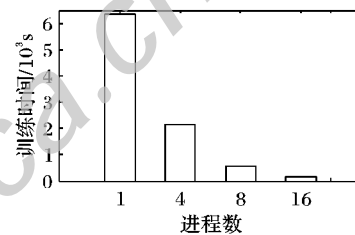


图6 多 KS-ISVM 进程的训练时间对比

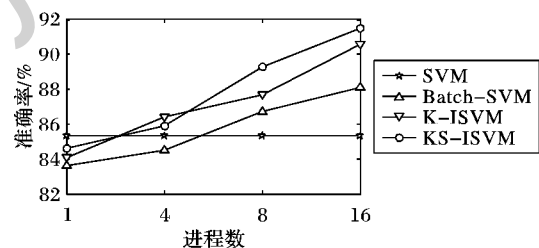


图7 不同进程的准确率对比

5 结语

针对传统入侵检测系统对数据处理负载过重,不支持多主机数据联合分析的问题且难以维护规则库的问题,本文提出一种基于 KS-ISVM 算法的云架构的入侵检测系统,并在实验室搭建的硬件平台上对所提算法进行实验验证。通过将用户端数据处理的中间结果作为样本点集合,使用 KS-ISVM 算法对其进行分析。KS-ISVM 算法还充分考虑增量学习中新增样本,对于新增样本利用超球结构选取有用样本,将违反 KKT 条件的新增样本且最有可能成为支持向量的边界向量加入增量学习,并淘汰对后继回归预测影响不大的样本^[14]。实验结果表明:本文算法可在保证一定学习速度的基础上有效提高支持向量机的精度,满足云端分布式入侵检测系统对速度和准确性的要求。

参考文献:

- [1] GOGOI P, HATTACHARYYA D K, BORAH B, et al. MLH-IDS: a multi-level hybrid intrusion detection method[J]. The Computer Journal, 2014, 57(4): 602-623.

- [2] LIN Y, LIU G, YANG L. Intrusion detection based on improved SVM algorithm [J]. *Computer Engineering*, 2007, 33(14): 151 – 153. (林杨, 刘贵全, 杨立身. 基于改进 SVM 方法的入侵检测[J]. *计算机工程*, 2007, 33(14): 151 – 153.)
- [3] JING X, WANG H, NIE K. Feature selection algorithm based on IMGA and MKSVM to intrusion detection [J]. *Computer Science*, 2012, 39(7): 96 – 99. (井小沛, 汪厚祥, 聂凯, 等. 面向入侵检测的基于 IMGA 和 MKSVM 的特征选择算法[J]. *计算机科学*, 2012, 39(7): 96 – 99.)
- [4] ZHANG Y, MU Q, BI X. Incremental SVM intrusion detection based on cloud model [J]. *Computer Applications and Software*, 2013, 30(3): 311 – 314. (张永俊, 牟琦, 毕孝儒. 基于云模型的增量 SVM 入侵检测方法[J]. *计算机应用与软件*, 2013, 30(3): 311 – 314.)
- [5] ZHU Y, WU J, ZHU Y, *et al.* Deep protocol analysis method in network intrusion detection [J]. *Application Research of Computers*, 2012, 29(5): 1891 – 1895. (朱映映, 吴锦锋, 朱艳艳, 等. 网络入侵检测中的深度协议分析方法[J]. *计算机应用研究*, 2012, 29(5): 1891 – 1895.)
- [6] ZHANG R, QIAN D, ZHANG W, *et al.* A survey of intrusion detection technology research [J]. *Mini-Micro Systems*, 2003, 24(7): 1113 – 1118. (张然, 钱德沛, 张文杰, 等. 入侵检测技术研究综述[J]. *小型微型计算机系统*, 2003, 24(7): 1113 – 1118.)
- [7] LUO S. Intrusion detection [M]. Beijing: Beijing University of Posts and Telecommunications Press, 2004: 168 – 192. (罗守山. 入侵检测[M]. 北京: 北京邮电大学出版社, 2004: 168 – 192.)
- [8] ZHENG H, HOU M, WANG Y. Fast method for feature selection in intrusion detection [J]. *Computer Engineering*, 2010, 36(6): 262 – 264. (郑洪英, 侯梅菊, 王渝. 入侵检测中的快速特征选择方法[J]. *计算机工程*, 2010, 36(6): 262 – 264.)
- [9] ZHANG X. Introduction to statistical learning theory and support vector machines [J]. *Acta Automatica Sinica*, 2000, 26(1): 32 – 42. (张学工. 关于统计学习理论与支持向量机[J]. *自动化学报*, 2000, 26(1): 32 – 42.)
- [10] SYED N, LIU H, SUNG K. Incremental learning with support vector machines [EB/OL]. [2015-04-10]. <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.46.6367>.
- [11] ZENG W, MA J. A novel approach to incremental SVM learning algorithm [J]. *Journal of Xiamen University: Natural Science*, 2002, 41(6): 687 – 691. (曾文华, 马健. 一种新的支持向量机增量学习算法[J]. *厦门大学学报: 自然科学版*, 2002, 41(6): 687 – 691.)
- [12] XU Z, MAO Z. Incremental learning of support vector machine based on hyperspheres [J]. *Journal of Northeastern University: Natural Science*, 2010, 31(1): 16 – 19. (徐喆, 毛志忠. 基于超球的支持向量机增量学习算法[J]. *东北大学学报: 自然科学版*, 2010, 31(1): 16 – 19.)
- [13] ZHANG G, LANG R, ZHOU K. Support vector machine classification based on fuzzy kernel function clustering [J]. *Journal of Computer Applications*, 2013, 33(S2): 108 – 110. (张国兵, 郎荣玲, 周凯. 基于模糊核聚类的支持向量分类[J]. *计算机应用*, 2013, 33(增刊2): 108 – 110.)
- [14] TENG S, CHEN H, ZHANG W. Multi-pose cooperative face detection based on hypersphere support vector machine [J]. *Journal of Computer Applications*, 2013, 33(7): 1988 – 1990. (滕少华, 陈海涛, 张巍. 基于超球支持向量机的多姿态协同人脸检测[J]. *计算机应用*, 2013, 33(7): 1988 – 1990.)

(上接第 2882 页)

- [6] SUN D, LI J, FENG Z, *et al.* On the security and improvement of a two-factor user authentication scheme in wireless sensor networks [J]. *Personal and Ubiquitous Computing*, 2013, 17(5): 895 – 905.
- [7] KUMAR P, LEE H J. Cryptanalysis on two user authentication protocols using smart card for wireless sensor networks[C]// *Proceedings of the 2011 IEEE Wireless Advanced*. Piscataway: IEEE Press, 2011: 241 – 245.
- [8] FAN R, HE D, PAN X. An efficient and DoS-resistant user authentication scheme for two-tiered wireless sensor networks[J]. *Journal of Zhejiang University Science C*, 2011, 12(7): 550 – 560.
- [9] VAIDYA B, MAKRAKIS D, MOUFTAH H T. Improved two-factor user authentication in wireless sensor networks[C]// *Proceedings of the 2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications*. Piscataway: IEEE Press, 2010: 600 – 606.
- [10] YUAN J J. An enhanced two-factor user authentication in wireless sensor networks[J]. *Telecommunication Systems*, 2014, 55(1): 105 – 113.
- [11] YEH H L, CHEN T H, LIU P C, *et al.* A secured authentication protocol for wireless sensor networks using elliptic curves cryptography[J]. *Sensors*, 2011, 11(5): 4767 – 4779.
- [12] CHEN T H, SHIH W K. A robust mutual authentication protocol for wireless sensor networks[J]. *Etri Journal*, 2010, 32(5): 704 – 712.
- [13] YOO S G, PARK K Y, KIM J. A security-performance-balanced user authentication scheme for wireless sensor networks[J]. *International Journal of Distributed Sensor Networks*, 2012, 2012, Article ID 382810.
- [14] SHI W, GONG P. A new user authentication protocol for wireless sensor networks using elliptic curves cryptography[J]. *International Journal of Distributed Sensor Networks*, 2013, 2013, Article ID 730831.
- [15] KUMAR P, CHOUDHURY A J, SAIN M, *et al.* RUASN: a robust user authentication framework for wireless sensor networks[J]. *Sensors*, 2011, 11(5): 5020 – 5046.
- [16] XUE K, MA C, HONG P, *et al.* A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks[J]. *Journal of Network and Computer Applications*, 2013, 36(1): 316 – 323.
- [17] NAM J, KIM M, PAIK J, *et al.* A provably-secure ECC-based authentication scheme for wireless sensor networks [J]. *Sensors*, 2014, 14(11): 21023 – 21044.
- [18] FAN R, FU J, PAN X. A secure and efficient user authentication protocol for two-tiered wireless sensor networks [C]// *Proceedings of the 2010 Second Pacific-Asia Conference on Circuits, Communications and System*. Piscataway: IEEE Press, 2010, 1: 425 – 428.
- [19] KALRA S, SOOD S K. Advanced password based authentication scheme for wireless sensor networks[J]. *Journal of Information Security and Applications*, 2015, 20: 37 – 46.
- [20] LI C T, LEE C C, WANG L J, *et al.* A secure billing service with two-factor user authentication in wireless sensor networks[J]. *International Journal of Innovative Computing, Information and Control*, 2011, 7(8): 4821 – 4832.
- [21] LI X, BAO F, LI S, *et al.* FLAP: an efficient WLAN initial access authentication protocol[J]. *Parallel and Distributed Systems*, 2014, 25(2): 488 – 497.