

基于主成分分析和多分类器融合的入侵检测

张瑞霞¹, 王 勇²

(桂林电子科技大学 计算机与控制学院, 广西 桂林 541004)

摘 要: 提出了利用主成分分析(PCA)提取入侵特征的多分类器融合的入侵检测算法. 首先, 利用 PCA 分类提取入侵子特征, 然后通过 KNN 分类器给出初步的识别结果, 最后采用 D-S 证据理论对识别结果进行融合, 得出最终识别结果. 通过在 KDD CUP'99 的标准入侵检测数据集上的实验表明, 该方法提高了入侵检测的整体性能.

关键词: 入侵检测; 主成分分析; D-S 证据理论; 分类器融合

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2010)04-0190-03

Intrusion Detection Methods Based on PCA and Multi-Classifier Fusion

ZHANG Rui-xia, WANG Yong

(Department of Computer and Control, Guilin University of Electronic Technology, Guilin 541004, China)

Abstract: An intrusion detection method using multi-classifier fusion based on Principal Component Analysis (PCA) feature analysis is presented. Firstly, PCA is applied to network intrusion feature extraction. then, initial intrusion detection result is done by three KNN classifiers. Next, the last step is form final result by fusing these results using the D-S evidence theory. Experiment has been done on dataset in KDD-99 and the results show that the intrusion detection performances can be improved by fusion three classifiers.

Key words: intrusion detection; PCA; D-S evidence theory; classifiers fusion

1 引言

入侵检测技术作为信息安全技术的重要方面得到了迅速发展. 入侵检测问题实质上就是一个 0-1 分类问题, 其关键问题是特征提取、选择和构造合适的分类器. 入侵检测数据在特征方面具有多维性的特点, 一方面需要降维以提高处理速度, 同时又需要保留入侵不同角度的特征以最大限度的区分不同的入侵, 进而提高检测率和减少误报率. 目前将模式识别技术应用到入侵检测中成为入侵检测领域研究的一个热点^[1-2]. 模式识别中的主成分分析(PCA)技术能够对样本空间进行降维, 从而使得匹配和识别在低维子空间进行. 因此它可以有效地提取攻击特征, 即在尽可能保留分类信息的前提下, 得到信息最大

的特征, 删除那些不利于分类或用途不大的信息或特征. 同时, 虽然入侵检测主要任务是设计一个高性能的 0-1 分类器, 如果单个分类器提取的特征具有独立性和互补性, 通过对现有的分类器融合获得比单个分类器更高的分类精度. 研究者利用多分类融合进行入侵检测来提高检测效果. 分类器融合的成功应用, 使得研究人员从理论上分析了分类器融合的条件、提高识别率的原因以及融合的策略, 从而给分类器融合提供了坚实的理论基础^[3].

文中提出利用主成分分析提取入侵的三个特征子空间来构造三个子分类器, 并利用证据理论融合子分类器的分类结果得到最终识别结果的入侵检测算法. 将该方法应用到 KDD CUP'99 数据集中, 实验结果表明, 该算法提高了入侵检测的整体性能.

收稿日期: 2009-03-09; 修回日期: 2009-06-18

基金项目: 广西自然科学基金(0575094)

2 PCA方法和D-S证据理论

2.1 主成分分析

主成分分析是通过K-L变换将训练样本集中的数据得到彼此正交互不相关特征.它使用了最大的几个特征值对应的特征向量组成变换矩阵,这些特征向量(基向量)构成一个子空间,基向量对应着原始空间变化最大的方向.该方法的最优性是从 N 个训练样本中提取 m 个主要特征,来达到降维的目的.

主成分分析按照式(1)中的线性变换把图像 X 投影到低维空间中的向量 Y

$$Y = W^T X \quad (1)$$

式中, $X \in R^N, Y \in R^M (N \gg M)$, W 代表投影矩阵.令 N 维向量 $X_i (i = 1, 2, \dots, L)$ 代表样本数据的 L 个属性特征, μ 代表它们的平均.则样本的协方差矩阵定义为:

$$W_{PCA} = \frac{1}{L} \sum_{i=1}^L [(X_i - \mu)(X_i - \mu)^T] \quad (2)$$

主成分分析投影矩阵的列向量则是由 W_{PCA} 的对应前 M 个最大特征值的特征向量组成.

2.2 D-S证据理论

证据理论^[4]又称为Dempster-Shafer理论,是一种不确定性推理方法.与传统的概率论相比,D-S理论能更好把握问题的未知性与不确定性,常用于信息融合^[5].D-S证据理论用识别框架 Θ 表示感兴趣的命题集,其上的布尔代数是分割组成的集类 R ,在其上定义基本概率赋值(BPAF - basic probability assignment):满足:

$$\sum m(A), A \subseteq \Theta \mid = 1, m(\Phi) = 0 \quad (3)$$

其中, $m(A)$ 表示证据支持命题 A 发生的程度,而不支持任何 A 的真子集. Φ 代表空集.

证据理论通过合成公式来合成多个证据源提供的证据.设有 n 个分类器,各分类器相应的基本概率赋值函数为 $m_i(A_j)$,表示第 i 个分类器对第 j 命题的后验可信度分配,则证据理论基本合成公式为:

$$m(\Phi) = 0$$

$$m(A) = \frac{1}{1-C} \sum_{\cap A_i \neq \Phi} \prod_{1 \leq i \leq n} m_i(A_i) \quad (4)$$

$$C = \sum_{\cap A_i \neq \Phi} \prod_{1 \leq i \leq n} m_i(A_i) \quad (5)$$

它反映了证据之间的冲突程度,称为冲突概率.系数 $1/(1-K)$ 称为归一化因子,它的作用是避免在合成证据时,将非零的概率赋给空集 Φ .

3 基于PCA和D-S证据理论的入侵检测

首先进行数据的预处理,然后对预处理后的数据应用PCA方法分别提取出三类子特征,并采用距离权重K-NN进行预分类得到一个识别结果,将这三个分类器的输出作为三条证据,利用证据理论合成规则对它们进行融合,根据定义的决策规则得到一个最终的识别结果.入侵检测原理框图如图1所示.

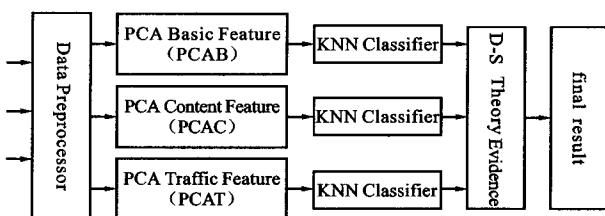


图1 基于PCA和多分类器融合的入侵检测

4 仿真实验与分析

4.1 数据预处理

文中采用MIT林肯实验室公开提供的DARPA入侵检测评价计划中的网络通信数据集,经过处理后形成的KDD Cup'99数据集进行仿真^[6].由于该数据集过于庞大,选取其中有代表性的10percent数据集作为实验数据集.随机分成Train Dataset训练数据集和两个Test Dataset测试数据集.一个用于测试单个分类器的正确识别率,另一个用于测试多分类融合系统的性能.

数据集中每条数据有42个特征,其中最后一条为攻击的类型特征,即分类标签.该特征分为5类,分别用0表示正常,1表示DOS攻击,2表示PRB攻击,3表示U2R攻击,4表示U2L攻击.根据分类标签我们定义证据理论中的识别框架 $\Theta = \{DOS, PRB, U2R, U2L, UNKNOWN\} = \{T_1, T_2, T_3, T_4, T_5\}$

KDD数据集的41个特征属性中,特征形式包含:连续的、离散的、字符串的.由于分类器只能接受数值型的数据,因而在分类训练之前要把这些离散型的数据连续化,把字符型的数据数字化,方法是将字符型数据除以符号型特征取值个数变换到 $[0, 1]$ 之间的连续数值数据.

4.2 训练单个分类器并得到其正确分类率

4.2.1 训练过程

对每一个分类器,给定一类入侵的训练集 $X_k, k = 1, 2, \dots, N$,根据式(2)计算协方差矩阵,然后求其 m 个最大特征值对应的特征向量构成PCA特征

投影矩阵 W_{pca} , 即 PCA 特征数据库. 重复执行得到矩阵 W_{ij} (其中 $i = 1, 2, 3; j = 1, 2, 3, 4, 5$), 表示第 i 个分类器对第 j 类攻击的 PCA 特征值.

$$W_{ij} = \begin{bmatrix} w_{11} & w_{12} & w_{13} & w_{14} & w_{15} \\ w_{21} & w_{22} & w_{23} & w_{24} & w_{25} \\ w_{31} & w_{32} & w_{33} & w_{34} & w_{35} \end{bmatrix}$$

4.2.2 单个分类器的正确分类率

计算测试样本集 1 到各类入侵训练样本投影特征的 KNN 距离, 分别是 $d_1^{pcab}, d_2^{pcab}, \dots, d_{k_1}^{pcab}$ 和 $d_1^{pcac}, d_2^{pcac}, \dots, d_{k_2}^{pcac}$ 和 $d_1^{pcat}, d_2^{pcat}, \dots, d_{k_3}^{pcat}$, 其中 $k'_1, k'_2, k'_3 < k$, 表示三个分类器与其最近邻的 k 个入侵样本对应的类别数. 根据 KNN 判别决策, 最终把测试样本判别为某类攻击, 从而得到单个分类器在测试集 1 上的正确识别率 ϵ_{ij} (其中 $i = 1, 2, 3; j = 1, 2, 3, 4, 5$), 表示第 i 个分类器对第 j 类攻击的正确识别率.

$$\epsilon_{35} = \begin{bmatrix} \epsilon_{11} & \epsilon_{12} & \epsilon_{13} & \epsilon_{14} & \epsilon_{15} \\ \epsilon_{21} & \epsilon_{22} & \epsilon_{23} & \epsilon_{24} & \epsilon_{25} \\ \epsilon_{31} & \epsilon_{32} & \epsilon_{33} & \epsilon_{34} & \epsilon_{35} \end{bmatrix} = \begin{bmatrix} \epsilon_1 \\ \epsilon_2 \\ \epsilon_3 \end{bmatrix}$$

4.3 D-S 融合决策

4.3.1 基本概率赋值获取

利用单个分类器的正确分类率转化为证据理论中的基本概率赋值. 考虑到一个 K-NN 分类器在做出最后决策之前对最多 K 个类别都有一定的支持度, 该支持度与前面得到的距离权重相对应. 为了提供更多的分类信息, 将归一化的距离权重作为 K-NN 分类器的输出. 同时由于分类器的输出不是完全可信的, 将不可信的部分赋值给整个的框架. 根据在一个测试集 1 上得到的三个距离权重 K-NN 分类器的正确分类率为 ϵ_i ($i = 1, 2, 3$), 它们对整个识别框架 $\Theta = \{T_1, T_2, \dots, T_5\}$ 的支持度分别为 $1 - \epsilon_i$ ($i = 1, 2, 3$). 对某一个分类器, 给定一组测试数据, 设对应于 PCA 特征的与其最近邻的 K 个入侵样本对应的类别数为 K'_1 ($K'_1 < K$), 对应的距离权重分别为 $d_1^i, d_2^i, \dots, d_{k_1}^i$, 将 K'_1 这个距离权重归一化, 并转化到 5 个类别变成 $q_1^i, q_2^i, \dots, q_5^i$, 其中只有 K'_1 个不为零. 对应三个分类器给出的三条证据的基本概率分配如下:

$$\begin{bmatrix} m_i(T_1) \\ m_i(T_2) \\ m_i(T_3) \\ m_i(T_4) \\ m_i(T_5) \end{bmatrix} = \begin{bmatrix} q_1^i \\ q_2^i \\ q_3^i \\ q_4^i \\ q_5^i \end{bmatrix} [\epsilon_{i1} \epsilon_{i2} \epsilon_{i3} \epsilon_{i4} \epsilon_{i5}]$$

$$m_i(\Phi) = 0, m_i(\Theta) = 1 - \epsilon_i^i$$

其中 $i = 1, 2, 3$.

4.3.2 证据理论融合过程

在测试集 2 上计算到每个分类器的距离权重, 将距离权重归一化处理, 并转化到 M 个类别, 得到三个分类器给出的三条证据的基本概率分配, 利用证据合成公式 (5) 融合三条证据得到新的证据 m , 对应的信任函数为:

$$\text{Bel}(T_i) = m(T_i), \quad i = 1, 2, \dots, 5$$

取具有最大信度函数对应的类别作为融合后的识别结果, 最终判别为 g 类.

$$g = \arg \max(m(T_i)), \quad i = 1, 2, \dots, 5$$

4.4 实验结果分析

表 1 给出了直接应用 PCA 方法和融合分类器的性能对比. 结果表明融合单个分类器后, 误报率提高不明显, 但是检测率提高了 4%, 虚警率由 0.57 降低到 0.32.

表 1 单个 PCA 和融合 PCA 的对比 (%)

分类方法	检测率	误报率	虚警率
PCA + KNN	94.56	2.28	0.57
Fusion	98.34	2.27	0.32

表 2 给出了采用不同融合方法的对比情况. 为了方便比较, 同时给出了平均方法、贝叶斯方法和证据理论融合方法的检测结果. 实验结果表明, 采用证据理论融合的方法, 虽然检测率没有明显的优势, 但是虚警率明显降低. 这正是 D-S 证据理论的优势, 降低了不确定性. 同时看到误报率增加了少许, 少许的误报率的增加换来了虚警率的明显下降, 这对一个检测系统来说是值得的.

表 2 采用不同融合方法的对比 (%)

融合方法	检测率	误报率	虚警率
Average	98.23	2.54	1.20
Bayesian	98.30	2.26	1.13
D-S theory	98.34	2.27	0.32

5 结束语

文中提出了利用主成分分析 (PCA) 提取入侵特征的多分类器融合入侵检测算法, 采用 PCA 方法分别提取攻击子特征建立分类器, 对入侵进行初步识别, 然后采用证据理论对三个分类器的检测结果进行融合. 从实验结果可知, 该方法提高了检测率, 同时降低了虚警率, 从提高了入侵检测的整体性能.

(下转第 197 页)

协议进行修改,因此额外开销比较少,易于在已经部署了 802.11i 设施的构件中升级.

5 结束语

802.11i 标准提供了较为完整的动态密钥管理机制,通过四步握手协议为 STA 和 AP 协商临时会话密钥提供了每次会话的安全性.但协议中的设计缺陷使它容易遭受 DoS 攻击,文中从降低协议遭受攻击的发生入手,给出了两种改进设计方案,较好地避免了 DoS 攻击.在改进协议安全性的同时如何提高执行效率,是需要进一步研究的内容之一.

参考文献:

- [1] 王小军,陆建德.基于 802.11i 四次握手协议的攻击分析与改进[J].计算机工程,2007,33(2):171.
- [2] 王曼珠,何文才,杨亚涛,等.无线局域网 IEEE 802.11 的安全缺陷分析[J].微电子学与计算机,2005,22(7):189-192.
- [3] 孙树峰,贺樑,石兴方,等.802.11 无线局域网安全技术研究[J].计算机工程与应用,2003,39(7):40-42.

- [4] Sithirasanen E, Muthukkumarasamy V. An early warning system for IEEE 802.11i wireless networks [C]// AusWireless'06: Proceedings the of 1st Australian Conference on Broadband Wireless and Ultra Wideband. Australian, 2006:25-30.
- [5] 张文革,马玉祥.基于 OPNET 的 IEEE802.11 战场 WLAN 增援救助仿真及性能评估[J].微电子学与计算机,2006,23(2):42-44.
- [6] Tim Moore. Suggested changes to robust security network (RSN) for IEEE 802.11[R]. IEEE P802.11 Task Group I Meeting Update, 2002.
- [7] 苏鹏,胡志远.802.11 无线局域网安全现状及其解决方案[J].计算机工程,2003,29(4):112-114.
- [8] Sithirasanen E, Muthukkumarasamy V, Powell D. IEEE 802.11i WLAN security protocol - a software engineer's model[C]// AusCERT'05: Proceedings of the 4th Asia Pacific Information Technology Security Conference. Sydney, 2005:39-50.

作者简介:

赵伟艇 男,(1966-),副教授.研究方向为计算机网络安全、网络管理等.

(上接第 192 页)

参考文献:

- [1] Khaled labid, Rao Venuri V. Application of principal component analysis to the detection and visualization of computer network attacks[C]// Annals of Telecommunications. France, 2005.
- [2] 朱永宣.入侵检测系统中基于主成份分析特征提取研究[J].微电子学与计算机,2006,23(7):91-96.
- [3] 张家超,孔媛媛.结合 SVM 与免疫遗传算法设计 IDS 的检测算法[J].微电子学与计算机,2008,25(10):206-209.
- [4] 徐耀红.数据融合理论与应用[M].西安:西安电子科技大学出版社,1998.

- [5] 孙即祥.现代模式识别[M].北京:国防科技大学出版社,2003.
- [6] Ludmila I. Kuncheva. A theoretical study on six classifier fusion strategies[J]. IEEE Trans On PAMI, 2002, 24(2):281-286.

作者简介:

张瑞霞 女,(1973-),硕士,讲师.研究方向为计算机信息与网络安全、入侵检测等.

王勇 男,(1964-),博士,教授.研究方向为信息安全、智能入侵检测等.