

引用格式:张娅. 基于深度学习的物联网非法入侵识别研究 [J]. 微电子学与计算机, 2020, 37(6): 75-78. [ZHANG Ya. Research on internet of things illegal intrusion recognition based on deep learning network [J]. Microelectronics & Computer, 2020, 37(6): 75-78.]

基于深度学习的物联网非法入侵识别研究

张 娅

(电子科技大学, 四川 成都 611731)

摘 要: 为了获得理想的物联网非法入侵自动识别结果, 提出基于深度学习的物联网非法入侵自动识别方法. 首先采用物联网非法入侵的数据, 并从中提取数据的异常入侵行为特征, 然后将特征作为深度学习的输入, 物联网非法入侵类型作为输出, 通过深度学习的训练建立物联网非法入侵识别分类器, 最后与其它方法进行了物联网非法入侵识别仿真实验, 结果表明, 深度学习网络获得了高精度的物联网入侵行为识别结果, 能够有效保证物联网安全, 具有一定的实际应用价值.

关键词: 深度学习网络; 物联网案例; 非法入侵; 行为识别; 特征向量

中图分类号: TP391

文献标识码: A

文章编号: 1000—7180(2020)06—0075—04

Research on internet of things illegal intrusion recognition based on deep learning network

ZHANG Ya

(University of Electronic Science and Technology of China, Chengdu 611731, China)

Abstract: In order to obtain the ideal results of the automatic identification of the illegal invasion of the Internet of things, an automatic identification method of the illegal invasion of the Internet of things based on the deep learning network is proposed. Firstly, we use the signal of Internet of things illegal invasion, and extract the time-domain and frequency-domain characteristics of abnormal invasion signal, then take the characteristics as the input of deep learning network, and the type of Internet of things illegal invasion is as the output. Through the training of deep learning network, we establish the Internet of things illegal invasion recognition classifier. Finally, we carry out the simulation experiment of Internet of things illegal invasion recognition with other methods. The results show that the deep learning network can obtain high-precision pattern recognition results of Internet of things intrusion behavior, which can effectively ensure the security of Internet of things, and has a certain practical value.

Key words: deep learning network; Internet of things cases; illegal intrusion; behavior recognition; feature vector

1 引言

物联网在许多领域得到了广泛的应用, 其中物联网安全十分重要, 因为经常有一些非法入侵破坏行为对物联网中的重要信息进行截取, 为了对非法入侵进行有效防御, 需要对非法入侵行为进行识别, 因此设计高精度的物联网非法入侵识别, 具有十分

重要的意义^[1,2].

传统物联网防御系统受到自身技术条件约束限制, 已经无法满足物联网安全实际应用需求^[3]. 物联网非法入侵识别研究技术可以划分为两类: 定性分析的物联网非法入侵识别方法和定量的物联网非法入侵识别方法^[4], 其中定性分析方法主要包括专家系统的物联网非法入侵识别方法, 定性分析的物联

网非法入侵识别方法的识别的效果与规则库的好坏密切相关,识别结果极不稳定,缺陷十分明显^[5]. 定量分析的物联网非法入侵识别方法主要包括人工神经网络、贝叶斯网络等,它们从物联网非法入侵数据中提取可以区别物联网非法入侵行为的特征,然后通过自动学习以及训练,对物联网非法入侵变化特点进行拟合,从而实现物联网非法入侵类型的分类,定量分析的物联网非法入侵识别效果要明显优于专家系统,成为当前主要的研究方向^[6-8]. 在实际应用中,这些方法同样存在一些不足,如:对新的或者变异的物联网非法入侵类型,难以进行有效识别,学习过程复杂,导致物联网非法入侵识别效率低等^[9,10].

为了获得理想的物联网非法入侵自动识别结果,提出基于深度学习网络的物联网非法入侵自动识别方法,并与其它方法进行了物联网非法入侵识别仿真对比实验,验证了深度学习网络用于物联网非法入侵行为识别的有效性和优越性.

2 深度学习网络的物联网非法入侵自动识别方法

2.1 物联网非法入侵自动识别的基本思路

基于深度学习网络的物联网非法入侵自动识别思路为:首先采用物联网非法入侵的数据,然后从中提取数据的异常入侵行为特征,并采用核主成分分析算法选择最优特征子集,最后将特征作为深度学习网络的输入,物联网非法入侵类型作为输出,通过深度学习网络的训练建立物联网非法入侵识别分类器,对物联网非法入侵识别分类器的参数进行优化,并根据物联网非法入侵识别结果决定是否进行拦截,具体如图 1 所示.

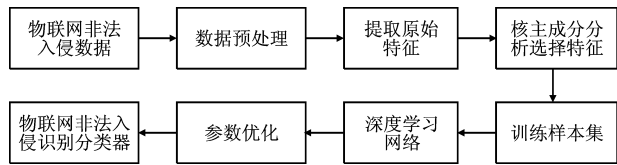


图 1 物联网非法入侵自动识别的基本思路

2.2 物联网非法入侵识别的特征选择

物联网非法入侵自动识别的原始特征数量比较多,特征与特征之间的信息有一定的重复,重复信息会对物联网非法入侵自动识别结果产生负面影响,为此采用核主成分分析对原始物联网非法入侵自动识别特征进行处理和变换,得到一些可以代表原始特征的物联网非法入侵自动识别重要特征子集,抑制重复信息的负面影响,同时可以减少物联网非法

入侵自动识别时间. 设物联网非法入侵自动识别的原始特征为: $x_i, i = 1, 2, \dots, N, N$ 表示原始特征数量,核主成分分析算法引入映射函数 $\Phi(x_i)$ 对其进行变换,可以得到特征的方差矩阵计算公式为:

$$C = \frac{1}{N} \sum_{i=1}^N \Phi(x_i) \Phi(x_i)^T \quad (1)$$

式中, $\sum_{k=1}^N \Phi(x_k) = 0$.

对式(1) 进行求解,建立如下的特征方程:

$$\lambda v = Cv \quad (2)$$

式中, v 表示投影向量,其可以描述为:

$$v = \sum_{i=1}^N \alpha_i \Phi(x_i) \quad (3)$$

式中, $\alpha_i (i = 1, \dots, N)$ 为常数.

采用核函数替换内积操作,降低求解的复杂度,即: $k(x_i, x_j) = \Phi(x_i)^T \Phi(x_j)$, 那么可以得到:

$$\lambda N \alpha = K \alpha \quad (4)$$

根据上式可以得到特征值 λ 和特征向量 $(\alpha_1, \alpha_1, \dots, \alpha_N)$.

对特征向量根据特征值进行排序,选取多个特征值较大的特征向量作为物联网非法入侵自动识别特征子集,其数量要少于原始物联网非法入侵自动识别特征.

2.3 深度学习网络建立物联网非法入侵识别的分类器设计

最小二乘支持向量机是深度学习网络的一个重要分支,相对于传统人工神经网络,最小二乘支持向量机不仅泛化性能更优,而且收敛速度明显加快,因此本文将引入到物联网非法入侵自动识别的分类器设计中.

设经过核主成分分析对原始物联网非法入侵特征进行选择后,最后特征数是为 n , 第 i 个样本的特征向量为 $x_i \in R^n$, 训练样本含有 N 个样本,它们组合的集合为: $\{x_i, y_i\}, i = 1, 2, \dots, N, y_i \in R$ 表示物联网非法入侵类型,那么可以建立一个分类平面对物联网非法入侵类型进行识别,分类平面可以表示为:

$$y(x) = w^T \varphi(x) + b \quad (5)$$

根据深度学习理论法则,上式可以变换为:

$$\min J(w, e) = \frac{1}{2} w^T w + \frac{1}{2} C \sum_{i=1}^N e_i^2 \quad (6)$$

s. t.

$$y_i = w^T \varphi(x_i) + b + e_i$$

式中, $\varphi(x)$ 为空间变换函数; J 为分类结果的损失函

数; C 为惩罚参数,主要用于物联网非法入侵识别结果误差的处理.

为了降低物联网非法入侵计算的时间复杂度,引入 Lagrange 乘子 $\alpha_i \in R$ 对式(6) 约束条件进行处理,建立如下 Lagrange 函数:

$$L(w,b,e;a) =$$
$$J(w,e) - \sum_{i=1}^N \alpha_i (w^T \varphi(x_i) + b + e_i - y_i) \quad (7)$$

基于 Karush-Kuhn-Tucker 理论,对式(7) 求偏导,建立物联网非法入侵识别分类器的决策函数具体为:

$$\hat{y}(x) = \sum_{i=1}^N \alpha_i K(x_i, x_j) + b \quad (8)$$

式中, $K(x_i, x_j)$ 具体设置为:

$$K(x_i, x_j) = \exp\left(\frac{-\|x_i - x_j\|^2}{2\delta^2}\right) \quad (9)$$

式中, δ 为核函数宽度参数.

2.4 物联网非法入侵识别的分类器参数优化

在构建物联网非法入侵识别的分类器过程中,参数 C 和 δ 对物联网非法入侵识别结果影响非常重要,决定了是否能够获得理想的物联网非法入侵识别结果,因此首先需要解决参数 C 和 δ 优化问题,本文采用混沌算法确定参数 C 和 δ 的最优值. 设物联网非法入侵识别目标即误差最小,则可以建立如下的参数 C 和 δ 优化目标函数:

$$\min J = \min f(z_i) = \frac{1}{L} \sum_{i=1}^N (y_i - \hat{y}_i)^2$$

s. t.

$$\begin{cases} C \in [C_{\min}, C_{\max}] \\ \sigma \in [\sigma_{\min}, \sigma_{\max}] \end{cases} \quad (10)$$

物联网非法入侵识别的分类器参数 C 和 δ 优化步骤如下:

Step1:根据物联网非法入侵识别的训练样本集合 $\{x_i, y_i\}, i = 1, 2, \dots, N$ 初始化 2 个随机数 x_0 .

Step2:根据 Logistic 映射产生混沌变量,具体如下:

$$x_{n+1} = \mu x_n (1 - x_n) \quad (11)$$

Step3:根据式(11) 得到混沌变量 $z_{n,i}$

$$z_{n,i} = c_i^r + d_i^r x_{n,i} \quad (12)$$

Step4:式(10) 的目标函数 J 实际就是描述分类器参数 C 和 δ 的函数,采用混沌变量在分类器参数 C 和 δ 范围内进行搜索,使目标函数 J 的值不断减小,即物联网非法入侵识别误差不断减少,最后收敛到最小值 J^* ,那么此时对应的 C 和 δ 即为物联网非法

入侵识别的分类器参数的最优值.

Step5:最小二乘支持向量机根据参数最优值对训练样本进行重新训练,建立物联网非法入侵识别的最佳分类器.

3 仿真实验

3.1 仿真平台及对象

为了测试基于深度学习网络的物联网非法入侵自动识别效果,选择一个物联网作为研究对象,该物联网共有 5 类非法入侵类型,它们样本分布情况具体如表 1 所示. 仿实验的平台参数设置如表 2 所示.

表 1 5 类物联网非法入侵类型的样本分布情况

物联网入侵类型编号	样本数量
1	1000
2	500
3	800
4	1000
5	1200

表 2 物联网非法入侵识别的仿真平台

平台参数名称	具体设置
CPU	4 核 Intel 3.2GHz
RAM	32GB
OS	WIN7
编程语言	Java
5	1200

3.2 特征提取结果

采用核主成分分析对 5 类物联网非法入侵类型特征进行选择,最后选择的特征子集特征和原始特征数量如图 2 所示. 从图 2 可以看出,相对于所列举的 5 类物联网非法入侵类型,选择的特征子集数量均有了一定程度的减少,这样减少了物联网非法入侵识别的输入向量数量,不仅简化了物联网非法入侵识别的结构,而且有利于后续的物联网非法入侵识别分类器的设计.

3.3 最优参数的确定

采用混沌算法分别确定 5 类物联网非法入侵的分类器参数,具体如表 3 所示. 从表 3 可以看出,不同类型的联网非法入侵类型,参数差异性比较明显,因此需要确定最合理的参数,这表明本文的参数优化思想正确的.

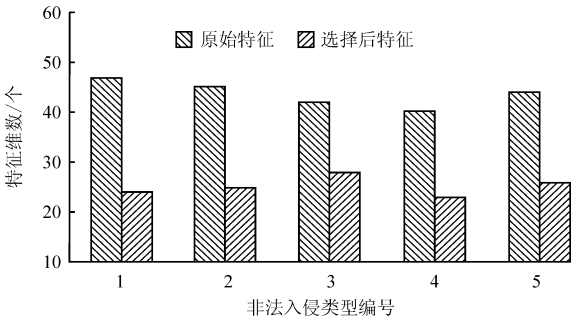


图 2 原始和重要特征子集的特征维数

表 3 5 类物联网非法入侵类型的参数

物联网入侵类型编号	C	δ
1	64. 03	64. 03
2	386. 10	30. 21
3	665. 56	27. 79
4	143. 87	66. 88
5	650. 95	22. 25

3.4 非法入侵识别效果分析

为了测试本文设计的物联网非法入侵自动识别结果的优越性,在相同仿真平台下,选择 BP 神经网络、贝叶斯网络进行物联网非法入侵自动识别仿真,统计它们的物联网非法入侵自动识别率和训练时间,结果如图 3 和图 4 所示。从图 3 可以看出,相对于 BP 神经网络、贝叶斯网络,本文设计的物联网非法入侵自动识别率得到相应的提升,这说明了物联网非法入侵的误识现象比较少,本文方法提高了成功率。从图 4 可以看出,贝叶斯网络的物联网非法入侵识别训练时间最长,次之为 BP 神经网络,而本文方法的物联网非法入侵识别训练时间最少,这表明本文方法加快了物联网非法入侵识别训练收敛速度。

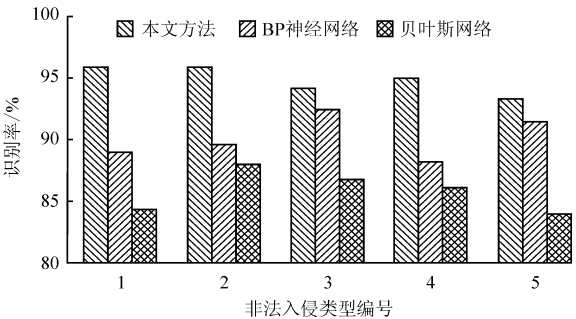


图 3 不同方法的物联网非法入侵识别率对比

4 结束语

物联网非法入侵受到了人们的高度关注,结合非法入侵时变性和动态性,以提高物联网非法入侵

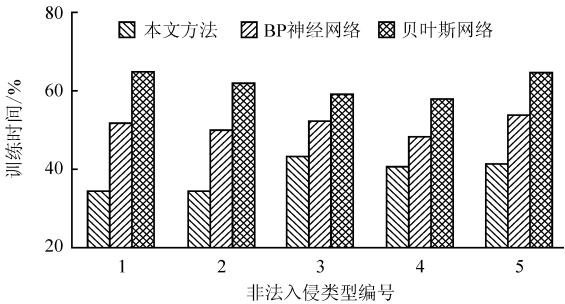


图 4 不同方法的物联网非法入侵识别训练时间对比

自动识别率为目标,提出了基于深度学习网络的物联网非法入侵自动识别方法,结果表明,深度学习网络不仅得到了理想的物联网入侵行为识别结果,而且物联网入侵行为识别效率高,可以满足物联网安全保障的要求。

参考文献:

[1] 张玉清,周威,彭安妮. 物联网安全综述[J]. 计算机研究与发展,2017,54(10):2130-2143.

[2] 左军. 物联网中重复博弈论入侵检测模型[J]. 重庆大学学报,2014,37(6):90-96.

[3] 胡向东,韩恺敏,许宏如. 智能家居物联网的安全性设计与验证[J]. 重庆邮电大学学报(自然科学版),2014,26(2):171-176.

[4] 程子轩,乔木. 物联网入侵的最优通信节点选取算法[J]. 吉林大学学报(理学版),2019,57(4):903-909.

[5] 胡向东,贾子漠. 一种面向物联网的轻量级入侵检测方法[J]. 重庆邮电大学学报(自然科学版),2015,27(2):255-259.

[6] 刘雅菲,刘宴兵. WSN 中一种新的基于重复博弈的入侵检测研究[J]. 计算机应用研究,2013,30(5):1540-1543.

[7] 楼晓俊,鲍比赛,刘海涛. 分布式信息融合的物联网事件检测方法[J]. 南京邮电大学学报(自然科学版),2012,32(1):12-16.

[8] 罗世亮,程良伦,任斌. 面向医疗物联网的一种行为规则入侵检测方法[J]. 科学技术与工程,2014,14(5):86-91.

[9] 潘建国,李豪. 基于实用拜占庭容错的物联网入侵检测方法[J]. 计算机应用,2019,39(6):1742-1746.

[10] 王国卿,庄雷,王瑞民,等. 基于时间自动机的物联网网关安全系统的建模及验证[J]. 通信学报,2018,39(3):63-75.

作者简介:

张 娅 女,(1980-),硕士,副教授. 研究方向为软件工程、大数据. E-mail:zhangya8018@163.com.