文章编号：2095-2163(2021)03-0038-06 中图分类号：U463.6 文献标志码：A

基于 LSTM 的 CAN 总线入侵检测

黄 迪，陈凌珊
（上海工程技术大学 机械与汽车工程学院，上海 201620）

摘 要：提出结合 CAN 矩阵对报文数据场信号的具体定义提取特征，训练 LSTM 网络在多个时间步长上，对一些重要的信号进行预测，引入观测值得到预测误差矩阵。使用多元高斯分布对误差矩阵建立异常概率模型，根据误报率、漏报率调整阈值大小。得到完整模型后，模拟总线攻击，并实验验证了模型的精度。

关键词：CAN 总线；LSTM；异常检测；入侵检测；车联网

CAN bus intrusion detection based on LSTM

HUANG Di, CHEN Lingshan
(School of Mechanical and Automotive Engineering, Shanghai University of Engineering Science, Shanghai 201620, China)

【Abstract】 Combining with the specific definition of message data field signal in CAN matrix, the paper extracts features, trains LSTM network to predict some important signals in multiple time steps, and introduces observation value to forecast error matrix. According to the probability of false positive rate and false negative rate, the threshold value is adjusted by using the probability distribution of multiple variables. After getting the completed model, the bus attack is simulated and the accuracy of the model is verified by experiments.

【Key words】 CAN bus; LSTM; anomaly detection; intrusion detection; intelligent connected vehicle

0 引 言

随着智能网联概念和自动驾驶技术的发展，当代汽车的发展重心已经从传统的动力系统、传动总成和汽车轻量化转移到汽车电子上。汽车电子系统越发地庞大，一些传统的机械部件也由电子电气所取代，且在不断地增加汽车对外界的接口，使汽车变得更加地智能化、电动化、共享化、网联化[1]。

在 80 年代，就已开发出 CAN 总线用来解决当时分布式控制的行业要求，甫一问世，就因其优秀的数据传输稳定性，多主机的总线结构，灵活的总线扩展性能以及较高的性价比赢得了汽车市场的认可和青睐，直至如今国内外的大部分车型依然使用的是 CAN 总线。而当时的控制器并未对外界的智能设备提供接口，所以 CAN 总线设计上在网络安全方面就存在明显的不足。时下，若要发展和普及汽车网联技术和自动驾驶技术，CAN 总线的网络安全则亟待获得保障。于赫[2]即分析了 CAN 总线的入侵形式，并基于信息熵和决策树的方法设计了入侵检测系统，但基于信息熵的方法只能识别总线上有大量异常报文的情况。Miller 等人[3]根据 CAN 总线上报文的固定周期特性，识别异常报文，研究中不仅某 ID 的发送周期不变，且不同 ID 报文之间的发送周期都是一个固定值，然而近年来，为了减轻总线负载，提高报文信息量，在发送报文策略方面引入事件的概念，即不同的条件触发不同的发送周期。Kang 等人[4]把报文数据场按字节作为特征使用 RBM (restricted Boltzman machine)算法训练模型，估计异常的可能性，并标记超过阈值的报文为异常报文。Cortes 等人[5]根据总线上一段时间窗里数据流的统计数据使用 OCSVM 支持向量机来识别异常总线上的异常行为。Song 等人[6]研究基于 CAN 总线广播的特征，分析总线上的时间间隙、报文的序列来识别异常。Weber 等人[7]结合 CAN 的定义，使用机器学习算法从总线流的角度部署了入侵检测系统。Tomlinson 等人[8]用预先定义 CAN 总线广播的平均时间间隙值并结合 ARIMA 方法来检测总线上的时间变化。Marchetti 等人[9]提出基于总线上不同 ID 报文之间的传输序列的入侵检测算法。

综上论述可知，现有研究主要分析了 CAN 总线的入侵形式，以及基于报文 ID 或数据场对周期性的报文做出检测，在机器学习领域把数据场里的数据按照单个字节作为特征输入，并未考虑总线数据时间上的关联性。基于此，本文使用多层 LSTM 神经网络，并充分考虑 CAN 通信矩阵对数据场里信号的定义，把 CAN 数据场里不同的信号作为特征提取，

作者简介：黄 迪(1995-)，男，硕士研究生，主要研究方向：车载网络安全。

收稿日期：2020-10-20

以此提高算法的精度，减少计算代价。

1　CAN 总线概述

1.1　报文格式和 CAN 通信矩阵

1.1.1　报文格式

CAN 总线有 2 种协议单元格式，区别主要在于仲裁场的大小，对于分析 CAN 总线的传输特性影响不大，因此这里将基于行业内广泛应用的 ISO11898 的报文格式展开论述。

CAN 总线在设计初期的目的是为了减少车辆线束、给分布在汽车不同位置的多个 ECU 提供通信服务。因此 CAN 总线是以报文为基础，在总线上多个 ECU 以广播的形式通信，在网络上的所有节点都可以自由地收发报文。当多个 ECU 同时发送报文时，防止报文冲突多是取决于发送报文的仲裁场，也就是 ID 大小，越小的 ID 则有越高的优先权占用总线。CAN 总线共有 4 种不同的报文帧，分别为：数据帧、错误帧、远程帧、超载帧。文中将重点关注正常通信时使用的数据帧。研究可知，数据帧的基本结构如图 1 所示。由图 1 可知，对其中涉及的每一位的功能含义拟做分述如下。

（1）SoF。为帧起始，在总线上以一个显性位表示一个报文的开始。

（2）ID，场定义报文的标识以及优先级。ID 的值越小，优先级越高。

（3）RTR。当报文为远程帧的时候置为显性。

（4）IDE。在使用拓展帧的时候置为显性。

（5）R0。为保留位。

（6）DLC。定义数据场的大小，最大为 8 个字节。

（7）DATA，数据场用来传输实际的数据。一个报文最大传输 8 个字节的数据。

（8）CRC，循环冗余校验码。通过对数据场数据计算出一个 CRC 码来确保发送端和接收端收到正确的数据。

（9）ACK。接收端收到报文后的应答场。

（10）EoF。帧结束 7 比特隐性位，标识一帧报文结束。

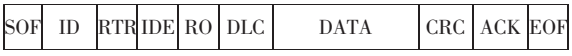

图 1　报文格式

Fig. 1　CAN frame

1.1.2　CAN 通信矩阵

通常，CAN 通信矩阵是由主机厂和供应商共同定义确定的，用于描述整车电子系统上各个网段下不同节点需要在总线上收发什么 ID 的报文，以及收发的方式，数据场里比特位与信号的映射关系，信号的原始值与物理值的映射关系等。

一个 ID 为 0x121 的报文内容见表 1。由 ESP 发送，周期为 20 ms，数据场长度 DLC 为 8 个字节，在第一个字节的第 0 位至第二个字节的第 3 位长度 12 比特的数据场为车速信号，此信号的解析方式为原始整形值乘上 0.068 75，得到精度为 0.068 75 的车速物理值，第二个字节的第 7 位长度 1 比特的数据场为车速状态位，表征此报文的车速信号是否有效，0x0 为有效，0x1 为无效。还有一些空的数据场没有被使用到。

其他报文也以类似的方式在 CAN 矩阵里被定义。在 CAN 总线上接收到报文后，可以使用 Vector 公司的工具，载入带有 CAN 矩阵信息的 dbc 文件，在线解析每个报文里的每个信号。

表 1　CAN 通信矩阵

Tab. 1　CAN matrix

发送节点	ID	发送类型	DLC	实时性/ms	位	长度	信号名称	signal value
ESP_1	0x121	fixed period	8	20	1.0-2.3	12	Vehicle_speed	PH=INT * 0.068 75 km/h [0;281.462 5] km/h [0x000;0xFFE] invalid:0xFFF Init:0x000/Default:0xFFF
ESP_1	0x121	fixed period	8	20	2.7	1	Vehicle_speed_Status	0x0:Valid 0x1:Invalid Init:0x0/Default:0x1
ESP_1	0x121	fixed period	8	20	7.0-7.3	4	ESP1_MSG_Counter	[0,15] Init/Default:0x0
ESP_1	0x121	fixed period	8	20	8.0-8.7	8	ESP1_Checksum	Checksum=(Byte1+Byte2...+Byte7) XOR 0xFF

1.2 CAN 总线缺陷分析

由 1.1 节研究可知,CAN 总线是基于报文设计的通信方式,所有节点在总线上接收与自己有关的报文 ID 获取数据,而不会涉及到发送端和接收端的任何信息,因此就并不能判断接收到的报文的源头。进一步地,也将无法判断这一条是不是入侵报文。同时在 CAN 通信里,所有报文数据场中的数据都没有经过加密。另外,在 CAN 总线增加或减少节点是非常便利的,只是在物理上接入总线,并不需要对新接入的节点进行验证就能在总线上正常收发报文。

综上 CAN 总线的不足,加上各种 ECU 对外界的无线接口,使得车载网络的网络安全面临严峻的挑战。

1.3 入侵方式分析

根据 CAN 总线的易接入性,在车上的自带的诊断接口 OBD 可以轻易地接入整车车载网络,监听总线上的报文,由 CAN 总线的仲裁机制可知,ID 越小有越高的优先级,攻击者就可以向总线上以高频率的方式发送高优先级的报文,即使没有任何节点接收此报文,总线也会由于超负载而陷入瘫痪,这种攻击模式即称为洪泛攻击。

除了车上的 OBD 口可以入侵车载网络,现在越来越多的远程接入方式带来更大的隐患,比如 4G、5G、WiFi、蓝牙等。

另外在接入总线、监听了总线上正常的通信后,将其记录下来再重放到总线上去,每个 ID 和数据都是正常的,但接收端接收到的数据并不符合当前的工况,造成安全威胁。这种攻击模式被称为回放攻击。

更隐秘的攻击方式是先入侵总线上的节点,解析 CAN 矩阵,使节点发送合法 ID 的报文,而改变数据场中的内容。比如入侵整车上的一个网关,通过网关在总线上发送正确的车速报文 ID 和错误的车速信息,这时如果车辆上有主动安全功能,就有可能会引起误报,或者触发刹车信号及转向信号。这种攻击模式被称为伪装攻击,是一种很难准确检测出来的攻击方式,因为除了数据场里的数据不符合当时的工况以外,其他特征均与正常报文一致,而且与回放攻击比起来,则几乎不会在总线流的角度上产生异常,从而躲过监控总线统计数据的入侵检测系统。

2 异常检测

2.1 异常检测

异常检测是指分析数据在正常情况下的行为特征,并能识别不具备这些特征的数据点,这些点被称为异常。

要识别出异常首先需要分析数据的分布情况,得到数据的可能性分布,如图 2 所示。由图 2 可知,数据有 2 种分布模式:蓝色点和红色点,在最密集的地方可能性的值最高,在边缘的点可能性更低。在低于某个阈值之后被异常检测算法标识为一个异常,比如图 2 中在边缘线外的点。

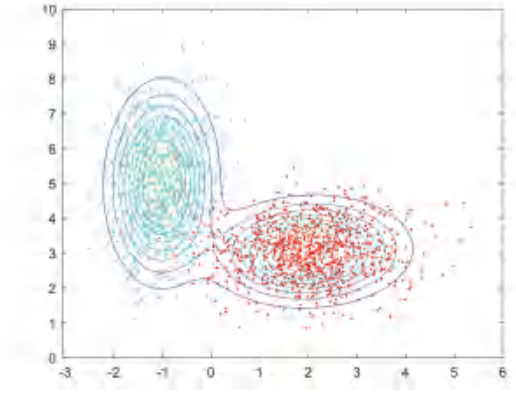

图 2 异常检测

Fig. 2 Anomaly detection

2.2 多元高斯分布

对于本文分析的问题,CAN 总线上的信号通常有较强的关联性,比如挡位信号、车速信号和发动机转速信号等。因此采用多元高斯分布来分析数据的可能性分布。

研究中,假设一个 d 维的矢量 $\boldsymbol{x} \in \mathbb{R}^d$ 服从多元高斯分布,其概率密度为:

$$N(\boldsymbol{x} \mid \boldsymbol{\mu}, \boldsymbol{\Sigma}) \triangleq \frac{1}{(2\pi)^{d/2} |\Sigma|^{1/2}} \exp\left(-\frac{1}{2}(\boldsymbol{x}-\boldsymbol{\mu})^{\mathrm{T}} \boldsymbol{\Sigma}^{-1} (\boldsymbol{x}-\boldsymbol{\mu})\right). \quad (1)$$

其中,$\boldsymbol{\mu}$ 表示 $\boldsymbol{x}$ 的 d 维均值向量,$\boldsymbol{\Sigma}$ 表示 $\boldsymbol{x}$ 变量 $d * d$ 维对称、正定的协方差矩阵。

$\boldsymbol{\mu}$ 向量与 $\boldsymbol{\Sigma}$ 协方差矩阵对多元高斯分布的影响如图 3 所示。$\boldsymbol{\mu} = [0,0]$,$\boldsymbol{\Sigma} = \begin{pmatrix} 0.5 & 0.3 \\ 0.3 & 0.5 \end{pmatrix}$,通过调整 $\boldsymbol{\mu}$ 和 $\boldsymbol{\Sigma}$ 的值可以捕捉数据之间的相关性。

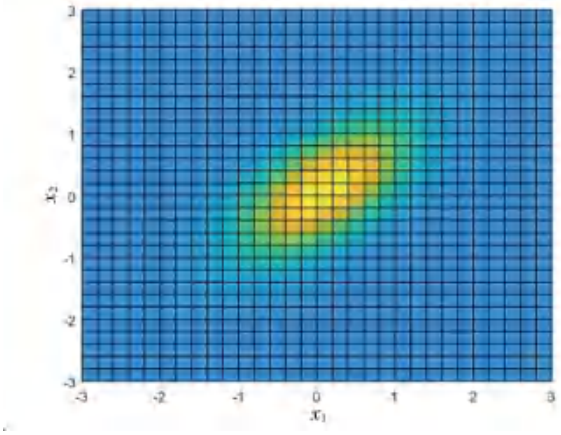

图 3 二元高斯分布

Fig. 3 Bivariate gaussian distribution

3　长短期记忆 LSTM

长短期记忆网络 LSTM 是 recurrent neural network(RNN)中的一种，其特点是对数据有长期记忆性，对一些对历史状态有依赖性的数据预测有较好的表现。长短期记忆网络的单元结构如图 4 所示。

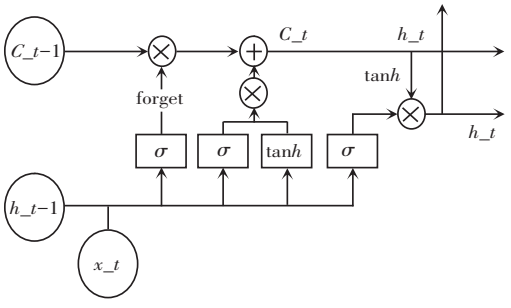

图 4　LSTM 单元

Fig. 4　LSTM cell

为了使网络记忆历史数据里的重要信息，对未来的预测以历史条件和输入作为限制，做出质量更高的预测。LSTM 中要处理的数据除了当前的外部输入 $\boldsymbol{x}(t)$ 以外，还有前一时刻的反馈 $\boldsymbol{h}(t-1)$，记新输入为：

$$\hat{\boldsymbol{C}}(t)=\tanh(\boldsymbol{w}_C\cdot[\boldsymbol{h}_{t-1},\boldsymbol{x}_t]+\boldsymbol{b}_C),\tag{2}$$

其中，$[\boldsymbol{h}_{t-1},\boldsymbol{x}_t]$ 表示当前输入向量与前一时刻输出向量的拼接向量；$\boldsymbol{w}_C$ 为输入权重矩阵；$\boldsymbol{b}_C$ 为偏移向量。

图 4 中，$\boldsymbol{C}(t)$ 是 LSTM 的长期记忆单元，包含了 t 时段的状态信息，$\boldsymbol{C}(t-1)$ 为上一个时间步的长期记忆单元，$\boldsymbol{h}(t-1)$ 为上一个时间步的短期记忆单元，$\boldsymbol{X}(t)$ 为当前时间步的输入，σ 为 sigmoid 层，输出 0~1 之间的值，控制遗忘、记忆及输出的大小，3 个门都是与 $\boldsymbol{h}(t-1)$ 及当前输入 $\boldsymbol{X}(t)$ 相关的。对其内容原理及定义公式可解析分述如下。

遗忘门数学表达为：

$$f_t=\sigma(\boldsymbol{W}_f\cdot[\boldsymbol{h}_{t-1},\boldsymbol{x}_t]+\boldsymbol{b}_f),\tag{3}$$

输入门数学表达为：

$$i_t=\sigma(\boldsymbol{W}_i\cdot[\boldsymbol{h}_{t-1},\boldsymbol{x}_t]+\boldsymbol{b}_i),\tag{4}$$

输出门数学表达为：

$$o_t=\sigma(\boldsymbol{W}_o\cdot[\boldsymbol{h}_{t-1},\boldsymbol{x}_t]+\boldsymbol{b}_o),\tag{5}$$

一个 LSTM 在 t 时间步上对当前长期记忆单元进行更新要经过 2 步，即：

$$\boldsymbol{C}_t=f_t*\boldsymbol{C}_{t-1}+i_t*\hat{\boldsymbol{C}}_t,\tag{6}$$

对输入的新信息 $\hat{\boldsymbol{C}}$ 做选择性记忆，对上一时间步长的长期记忆单元 $\boldsymbol{C}_t$ 做选择性遗忘。

代入公式(2)~公式(4)到公式(6)，得到 LSTM 状态更新数学表达式，即：

$$\boldsymbol{C}_t=\sigma(\boldsymbol{W}_f\cdot[\boldsymbol{h}_{t-1},\boldsymbol{x}_t]+\boldsymbol{b}_f)*\boldsymbol{C}_{t-1}+\sigma(\boldsymbol{W}_i\cdot[\boldsymbol{h}_{t-1},\boldsymbol{x}_t]+\boldsymbol{b}_i)*\tanh(\boldsymbol{w}_C\cdot[\boldsymbol{h}_{t-1},\boldsymbol{x}_t]+\boldsymbol{b}_C),\tag{7}$$

更新完当前长期记忆单元 $\boldsymbol{C}_t$ 后，激活长期记忆单元并对其作用输出门，提取到与当前时间步相关性强的输出，并作为短期记忆单元传递到下一时间步去：

$$h(t)=o_t*f(\boldsymbol{C}_t).\tag{8}$$

4　实验

4.1　数据处理

本文搭建了一个基于 LSTM 的以汽车系统时间上的相关性为基础的总线入侵检测模型，图 5 中数据为国内某款汽车正常行驶状态下的实车总线数据形式。包括时间戳、收发信息、数据长度、数据场、ID 场。

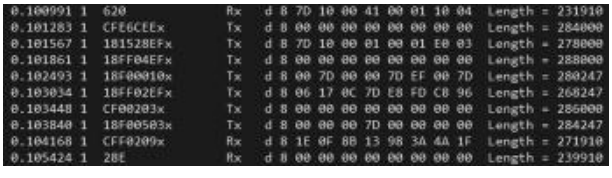

图 5　总线数据

Fig. 5　CAN bus data

通过 vector 公司的上位机软件 CANoe 加载 DBC 后可以从图 5 的数据中解析出每帧报文的具体信号的物理值，车辆航向角信号物理值如图 6 所示。

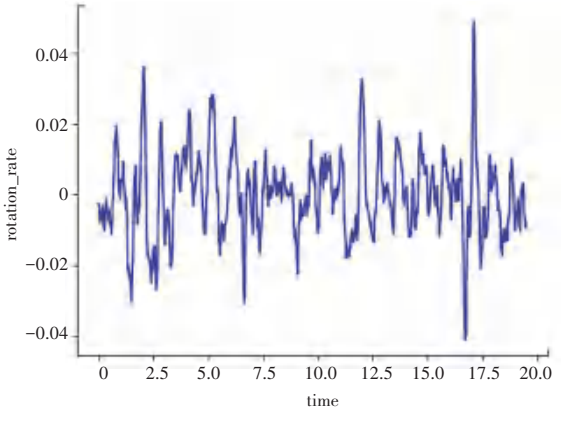

图 6　航向角

Fig. 6　Azimuth

由于总线上信号太多，为了确保准确率的同时减少计算量，文中人工选取了多个重要且不冗余的信号作为 LSTM 的输入，分别为：图 6 中的车速信号、方向盘转角信号、加速度信号、加速踏板信号、制动踏板信号、挡位信号、发动机扭矩 7 个特征。选取

的特征如图 7 所示。数据集为 200 个正常行驶工况下的车辆数据,由于在总线上的报文发送周期不同,取 100 Hz 的采样数据,共有 200 * 7 维度的时间序列数据集。

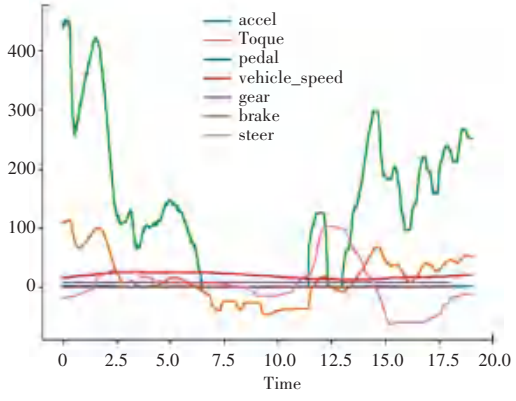

图 7 选取的特征

Fig. 7 Picked features

4.2 LSTM 建模及预测

将实录的正常数据分为 85% 训练集和 15% 验证集,用训练集对 LSTM 模型进行训练,并用验证集验证模型的性能,最后用测试集得到一个误差矩阵。计算误差矩阵的多元高斯分布特征。

将数据集定义为 $X = \{x^{(1)}, x^{(2)}, \ldots, x^{(t)}, \ldots, x^{(n)}\}$,$t$ 时刻的数据点在时间序列上是 m 维 $\{x_1^{(t)}, x_2^{(t)}, \ldots, x_m^{(t)}\}$ 为 LSTM 训练模型的 m 维输入。LSTM 在 t 时刻对所有输入特征里的 d 个特征在 l 个时间步长里做出预测。

本文选取 7 个特征,因此 LSTM 的输入层为 7 个单元,d 为 6,因此 LSTM 的输出层应为 6 个单元,隐藏层设为 15 和 30 个单元,预测时间长度定为 100 个周期,因此 LSTM 在 50 个周期后的每个时刻输出为 6 * 100 的矩阵。

研究后可得,训练 30 次后模型对其中一个特征的表现见图 8。

由此得到形状为 $e(6,100,t)$ 的误差张量,其中 $e[0] = 6$ 表示预测的 6 个特征,$e[1] = 100$ 表示时间序列上的预测长度,$e[2] = t$ 表示时间维度。其中,3 个误差在 t 时刻分布的可视化如图 9 所示。

4.3 异常检测

4.3.1 异常数据仿真

考虑到实车入侵的危险性和成本,本文的异常数据为仿真数据,分别对车速 ID_0x121,发动机转速 ID_0x10D,方向盘转角 ID_11F 做仿真伪装报文入侵报文攻击整车总线,对 3 个不同 ID 的报文数据场注入一个突变的异常,如图 10 所示。

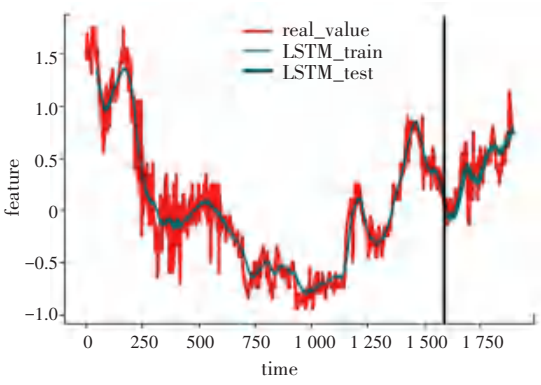

图 8 LSTM 模型

Fig. 8 LSTM model

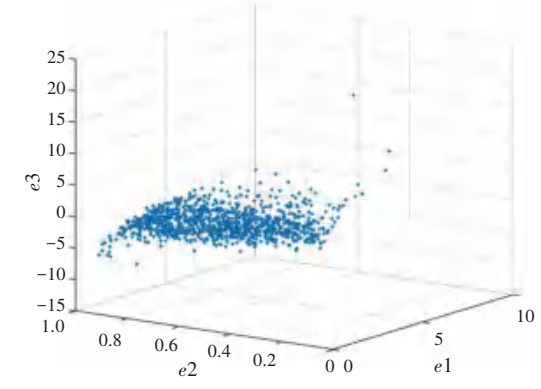

图 9 误差分布

Fig. 9 Error distribution

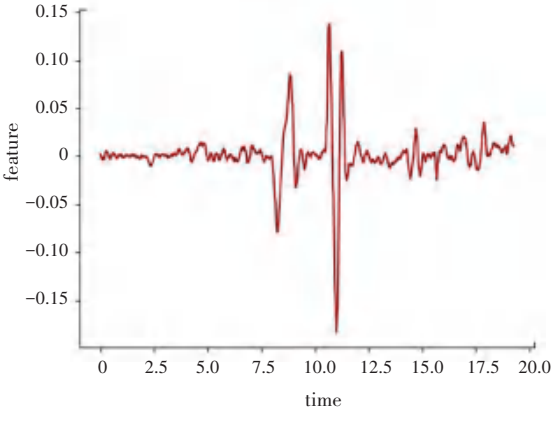

图 10 注入攻击

Fig. 10 Injection attack

4.3.2 异常检测

经过上述步骤得到通过正常行驶的数据集训练好的 LSTM 预测模型和通过仿真得到的异常数据集,把异常数据集输入到 LSTM 预测模型,得到异常数据集的误差张量后使其符合多元高斯分布,求得其分布均值向量、协方差矩阵和每个误差点对应的可能性 $p(e)$。

当 $p^{(t)} < \tau$ 时对应的输入特征 $x^{(t)}$ 将会被归为‘异常’。通过尽可能地最大化 F_β -score 来确定阈

值 τ 。

本文选用 $\beta = 0.1$ 的评价方法来评估模型的性能，因为本文讨论的异常检测其正常数据的样本数远大于异常样本，入侵检测的准确率要比查全率重要得多。$F_{0.1}$ - score 在不同单元数隐藏层下的评估结果见表 2。

表 2　$F_{0.1}$-score

Tab. 2　$F_{0.1}$-score

单元数	准确率	查全率	$F_{0.1}$ -score
15~30	0.97	0.05	0.82
20~35	0.98	0.12	0.92

5　结束语

本文通过先对 CAN 总线上原始数据解析处理后再输入到多层 LSTM 模型，对多个特征在多时间步上做预测，把得到的误差张量服从多元高斯分布，求得其均值向量、协方差向量和可能性 $p^{(t)}$。通过 $F_{0.1}$ - score 评价指标，确定阈值 τ，得到一个较高的准确率。

参考文献

[1] 宋昊辰，杨林，徐华伟，等. 智能网联汽车信息安全综述[J]. 信息安全与通信保密，2020(7)：106-114.

[2] 于赫. 网联汽车信息安全问题及 CAN 总线异常检测技术研究[D]. 长春：吉林大学，2016.

[3] MILLER C，VALASEK C. Adventures in automotive networks and control units[C]// DEFCON 21 Hacking Conference. Las Vegas：DEF CON Communications，Inc.，2013：260-264.

[4] KANG M J，KANG J W. Intrusion detection system using deep neural network for in-vehicle network security[J]. PLoS One，2016，11(6)：e0155781.

[5] CORTES C，VAPNIK V. Support-vector networks[J]. Machine Learning，1995，20(3)：273-297.

[6] SONG H M，KIM H R，KIM H K. Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network[C]// 2016 international conference on information networking (ICOIN). Kota Kinabalu，Malaysia：IEEE，2016：63-68.

[7] WEBER M，KLUG S，ZIMMER B，et al. Embedded hybrid anomaly detection for automotive CAN communication[C]//9th European Congress on Embedded Real Time Software and Systems. Toulouse，France：Pierre Baudis Congress Center，2018：1-11.

[8] TOMLINSON A，BRYANS J，SHAIKH S A，et al. Detection of automotive CAN cyber-Attacks by identifying packet timing anomalies in time Windows[C]// 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W). Luxembourg City：IEEE，2018：231-238.

[9] MARCHETTI M，STABILI D. Anomaly detection of CAN bus messages through analysis of ID sequences (Los Angeles，2017)[C]//2017 IEEE Intelligent Vehicles Symposium (IV). Los Angeles，CA：IEEE，2017：1577 - 1583.

(上接第 37 页)

高负荷预测的精度，本文提出了含注意力机制的 EMD-GRU 负荷预测方法。模型首先对原始数据进行了 EMD 分解，然后再对平稳性的 *IMF* 分量进行预测，降低了直接对非平稳性负荷数据进行预测带来的误差；构建多层 GRU 网络并加入了 Attention 机制，深入挖掘当前数据与历史数据在关键时间上的相关性特征，进一步提高预测精度；使用贵州某地实际负荷数据进行实例分析并与不同模型进行指标对比，验证了本文所提方法的有效性。

参考文献

[1] 陆继翔，张琪培，杨志宏，等. 基于 CNN-LSTM 混合神经网络模型的短期负荷预测方法[J]. 电力系统自动化，2019，43(8)：131-137.

[2] 李春涛，李啸骢，袁辉，等. 基于改进灰色模型的短期负荷预测[J]. 电气开关，2017，55(2)：11-13，96.

[3] 杨正瓴，张广涛，林孔元. 时间序列法短期负荷预测准确度上限估计[J]. 电力系统及其自动化学报，2004(2)：36-39.

[4] CHARLTON N，SINGLETON C. A refined parametric model for short term load forecasting[J]. International Journal of Forecasting，2014，30(2)：364-368.

[5] QIU Xueheng，REN Ye，SUGANTHAN P N，et al. Empirical mode decomposition based ensemble deep learning for load demand time series forecasting[J]. Applied Soft Computing，2017，54：246-255.

[6] 赵峰，孙波，张承慧. 基于多变量相空间重构和卡尔曼滤波的冷热电联供系统负荷预测方法[J]. 中国电机工程学报，2016，36(2)：399-406.

[7] ZHENG J，XU J A，ZHANG C A，et al. Electric load forecasting in smart grids using long-short-term-memory based recurrent neural network[C]// 2017 51st Annual Conference on Information Sciences and Systems (CISS). Baltimore，MD，USA：IEEE，2017：1-6.

[8] 陈卓，孙龙祥. 基于深度学习 LSTM 网络的短期电力负荷预测方法[J]. 电子技术，2018，47(1)：39-41.

[9] 张立峰，刘旭. 基于 CNN-GRU 神经网络的短期负荷预测[J]. 电力科学与工程，2020，36(11)：53-57.

[10] 任成国，肖儿良，简献忠，等. EMD-LSTM 算法在短期电力负荷预测中的应用[J]. 电力科学与工程，2019，35(8)：12-16.

[11] 彭文，王金睿，尹山青. 电力市场中基于 Attention-LSTM 的短期负荷预测模型[J]. 电网技术，2019，43(5)：1745-1751.

[12] 李鹏，何帅，韩鹏飞，等. 基于长短期记忆的实时电价条件下智能电网短期负荷预测[J]. 电网技术，2018，42(12)：4045-4052.

[13] 邓带雨，李坚，张真源，等. 基于 EEMD-GRU-MLR 的短期电力负荷预测[J]. 电网技术，2020，44(2)：593-602.

[14] 朱伟，孙运全，钱尧，等. 基于 CEEMD-GRU 模型的短期电力负荷预测方法[J/OL]. 电测与仪表：1-8[2020-07-28]. http://kns.cnki.net/kcms/detail/23.1202.TH.20200727.1613.026.html.

[15] 赵兵，王增平，纪维佳，等. 基于注意力机制的 CNN-GRU 短期电力负荷预测方法[J]. 电网技术，2019，43(12)：4370-4376.