Maintenance and Security System for PLC Railway LED Sign Communication Infrastructure

Tomasz Andrysiak(✉) and Łukasz Saganowski

Institute of Telecommunications and Computer Science,
Faculty of Telecommunications, Information Technology and Electrical Engineering, UTP University of Science and Technology,
Al. Prof. Kaliskiego 7, 85-796 Bydgoszcz, Poland
{andrys,luksag}@utp.edu.pl

Abstract. LED marking systems are currently becoming key elements of every Smart Transport System. Ensuring proper level of security, protection and continuity of failure-free operation seems to be not a completely solved issue. In the article, a system is present allowing to detect different types of anomalies and failures/damage in critical infrastructure of railway transport realized by means of Power Line Communication. There is also described the structure of the examined LED Sign Communications Network. Other discussed topics include significant security problems and maintenance of LED sign system which have direct impact on correct operation of critical communication infrastructure. A two-stage method of anomaly/damage detection is proposed. In the first step, all the outlying observations are detected and eliminated from the analysed network traffic parameters by means of the Cook's distance. So prepared data is used in stage two to create models on the basis of autoregressive neural network describing variability of the analysed LED Sign Communications Network parameters. Next, relations between the expected network traffic and its real variability are examined in order to detect abnormal behaviour which could indicate an attempt of an attack or failure/damage. There is also proposed a procedure of recurrent learning of the exploited neural networks in case there emerge significant fluctuations in the real PLC traffic. A number of scientific research was realized, which fully confirmed efficiency of the proposed solution and accuracy of autoregressive type of neural network for prediction of the analysed time series.

Keywords: Anomaly and fault detection · Time series analysis · Outliers detection · Network traffic prediction · Autoregressive neural networks · Critical infrastructure · LED sign communications network

1 Introduction

Intelligent Transport Systems (ITS) are different types of solutions which are an answer to increasing demand for goods and human mobility. By their means we can create vast, fully-functional and efficient systems of managing transport in real time. To achieve these aims, there are used diverse information and telecommunication technologies (e.g. Internet of Things (IoT), Wireless Sensor Network (WSN) or Power Line

V. V. Krzhizhanovskaya et al. (Eds.): ICCS 2020, LNCS 12140, pp. 170–183, 2020.
https://doi.org/10.1007/978-3-030-50423-6_13

Communication (PLC)) but also automation solutions for mobile objects including infrastructure, vehicles and their users. The main objective of ITS is boosting the capacity of transport systems and enhancement of quality of their services [1]. A special solution of ITS are variable LED sign systems, which visualize traditional signs used in the utility transport system. These signs are switched on by the operator, or they can be connected to the smart steering system. Their typical function is showing appropriate marking and/or defined information [2]. An important aspect of every Intelligent Transport System is proper solving of potential problems connected with protection and security of its own infrastructure. One of possible solutions is anomaly/damage detection systems allowing to recognize occurring threats, i.e. noticing variation from normal behavior or situation. Identification of abnormal incidents which are an aftermath of an attack, abuse or harm is crucial from the system's security point of view, because it may lead to critical states in the protected infrastructure and may require instant remedial activities [3].

The article presents possible solutions allowing to detect different type of anomalies and failures/damage for critical infrastructure of railway signs. There is proposed and described the structure of constructed LED Sign Communications Network realized with the use of PLC technology. There are presented key security problems which have direct impact on proper operation of the critical communication infrastructure. Furthermore, numerous experiments were conducted which fully confirmed efficiency and efficacy of the suggested solution.

The article is organized as follows. After the Introduction, Sect. 2 presents related work on existing security and maintenance solutions for PLC Railway LED Sign Communication Infrastructure. Next, Sect. 3 presents the structure and operation of the proposed solution. In Sect. 4, experimental results are presented and discussed. Finally, Sect. 5 concludes our work.

2 Related Work

Internet of things and solutions in industrial and consumer applications has been spreading rapidly in recent years. As an example, we can mention solutions connected to Smart Grids like metering systems [4, 5], smart lights [6, 7], intelligent transportation and city systems [8, 9]. Anomalies in communication systems may be caused by various factors, i.e. deliberate or undeliberate human activities, damage of elements of communication infrastructure or any possible sorts of abuse. When analyzing related literature, one can notice many works concentrating on solutions of anomaly detection in computer network as well as in Smart Grid systems [4] including the last mile of communication network [10]. There exist various solutions for detecting anomalies in wireless sensor networks, intelligent measure networks or PLC infrastructure [11, 12]. They usually concentrate on protecting communication in last mile network.

The problems of anomaly detection are also noticeable in different smart-solutions concerning environment protection. In [13] authors propose a completely data-driven and machine-learning-based approach for water demand forecasting and online anomaly detection (such as smart meter faults, frauds or possible cyber-physical attacks) through the comparison between forecast and actual values. Another solution

to the problem are methods for finding anomalies in gas consumption that can identify causes of wasting energy, presented in [14].

Power Line Communication technology so far was used mainly in smart lights and smart metering systems [5, 7] where the requirements regarding safety and speed of operation are much smaller than in railway critical infrastructure application [15]. In the article we propose original solution for control, maintenance and security of railway signs critical infrastructure.

So far, new LED based signalization devices usually replace old signalization without additional functionalities for control and maintenance. Railway automation systems control only level of current consumption for such devices and detect only on/off and failure states of a signalization device. Such solutions are provided today by main suppliers of railway automation systems, like Bombardier Transportation [16]. Even in computer based railway, automation systems' state of railway signs is controlled by means of current level measurement by microcontroller cards dedicated for a given railway sign circuit.

That is why we have noticed the need for proposing and implementing solution of LED railway signs with new control and maintenance functionalities. We can control the state of the railway sign and transmit by means of Power Line Communication technology packets between LED sign and LED sign controller interface maintenance information to railway automation system without additional investments in cable infrastructure.

In the article we propose solution for improving safety and maintenance functionalities in the network consisting of the proposed railway PLC LED signs.

3 Maintenance and Security System: The Proposed Solution

Traffic from railway LED signs is transmitted by means of PLC point to point links between a LED sign controller and a LED sign. We collected cumulative PLC traffic from point to point links with the use of LED signs controllers interfaces (e.g. RS232, RS485, Ethernet depending on installation). There are two main steps in the proposed method (see Fig. 1).

In the first step we calculated railway PLC signs traffic models for cumulative traffic of railway signs. At the beginning we select and calculate traffic in a form of univariate time series of PLC traffic features presented in Table 1. Next, all the outlying observations are detected and eliminated from the analyzed network traffic parameters by means of the Cook's distance (see Sect. 3.1). Subsequently, traffic features' time series are used for neural network autoregression learning (see Sect. 3.2). Based on neural network prediction intervals and Bollinger bands, we achieve models of variability for every railway PLC sign traffic feature (see Sect. 3.3).

Second branch of the proposed method consist of real time steps for railway LED signs anomaly/attack detection method. First, we select and calculate traffic features from cumulative traffic of railway PLC signs. Next, we check if every value of univariate time series representing traffic feature does not exceed boundaries represented by calculated models in the first step of the proposed method. If values are outside boundaries set for a given traffic feature, we generate detection report. The proposed

methodology has also possibility of traffic model recalculation in case of significant changes in traffic characteristic of the examined network. Condition of models recalculation/update is presented in Sect. 3.4.

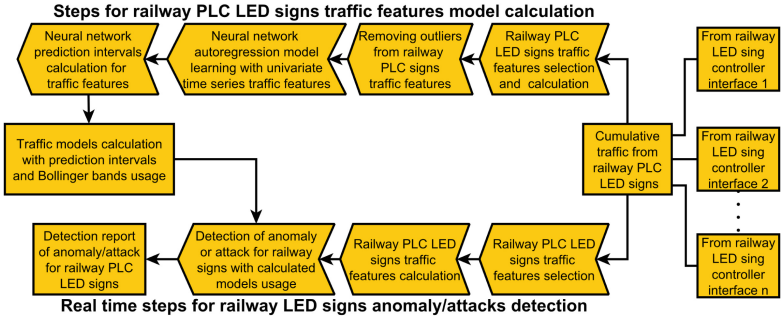

Fig. 1. Block representation of main steps in the proposed algorithm for anomaly/attack detection in railway PLC signs network.

3.1 Outliers' Detection and Elimination Based On Cook's Distance

The Cook's Distance [17] was chosen to recognize outliers in the examined PLC traffic parameters. By means of this approach we calculate the distance stating the level of data corresponding for two models: *(i)* a full model with all observations from the learning set, and *(ii)* a model lacking one observation i from its data set

$$D_i = \frac{\sum_{j=1}^{n} \left(\hat{Y}_j - \hat{Y}_{j(i)}\right)^2}{m \cdot MSE}, \tag{1}$$

where $\hat{Y}_j$ is the forecasted value of x variable for observations number j in the full model, i.e. built on the complete learning set; $\hat{Y}_{j(i)}$ is the predicted value of x variable for observations number j in the model built on the set in which the i - number observation was temporarily deactivated, MSE is the mean-model error, and m is the number of parameters used in the analyzed model.

For the Cook's distance D_i threshold value, over which the given observation should be understood as an outlier, according to criterion (1), 1 is accepted, or alternatively $4/(n - m - 2)$, where n is the number of observations in the learning set. The above rules are performed in order to detect and eliminate outliers from the PLC network traffic parameters. So prepared data is ready for stage of creating models.

3.2 The PLC Traffic Features Forecasting Using Neural Networks

The nonlinear autoregressive model of order p, $NAR(p)$, defined as

$$z_t = h\left(z_{t-1}, \ldots, z_{t-p}\right) + \in_t \tag{2}$$

is a direct generalization of linear AR model, where $h(\cdot)$ is a nonlinear known function [18]. It is presumed that $\{\in_t\}$ is a sequence of random independent variables identically distributed with zero mean and finite variance σ^2. The autoregressive neural network (NNAR) is a feedforward network and constitutes a nonlinear approximation $h(\cdot)$, which is defined as

$$\widehat{z}_t = \widehat{h}\left(z_{t-1}, \ldots, z_{t-p}\right), \widehat{z}_t = \beta_0 + \sum\nolimits_{i=1}^{I} \beta_i f\left(\alpha_i + \sum\nolimits_{j=1}^{P} \omega_{ij} z_{t-j}\right), \tag{3}$$

where $f(\cdot)$ is the activation function, and $\Theta = (\beta_0, \ldots, \beta_I, \alpha_1, \ldots, \alpha_I, \omega_{11}, \ldots, \omega_{IP})$ is the parameters vector, p denotes the number of neurons in the hidden layers [18].

The NNAR model is a parametric non-linear model of forecasting. The process of forecasting is conducted in two steps. In the first stage, we determine the auto-regression order for the examined time series. It indicates the number of former values on which the current values of time series depend. In the second stage, we train the NN by means of the set previously prepared with order of auto-regression. Next, we determine the total of input nodes in the auto-regression order, the inputs to the NN being the former, lagged observations in forecasting of univariate time series. Finally, the forecasted values constitute the NN model's output. There are two possibilities to check for hidden nodes, namely, trial-and-error and experimentation, as there is no constituted theoretical ground for their selection. It is crucial though that the number of iterations is correct not to meet the issue of over-fitting [19].

3.3 Estimation of the Forecast Variability Based on Bollinger Bands

Bollinger's Bands is a tool of technical analysis invented at the beginning of 1980-ties [20]. The main idea of this tool is the condition that when variability of data is low (their standard variation is decreasing) then the bands are shrinking. On the other hand, in case of increase of data changeability, the bands are expanding. Therefore, this tool presents dynamics of data variation in a given time window. In the presented solution, we used the Bollinger's Bands to estimate changeability of forecasts of the used models. As the middle band (not presented in the pictures) we accepted the calculated values of used models' forecasts, and with upper and lower bands we tied their double standard variation [21].

3.4 The Condition of Neural Network Model's Update

It is highly likely that the character and nature of the examined parameters of the railway LED Sign Communication Network imply possibility of appearance of significant data variabilities in the analyzed time series. The reasons of such phenomenon are to be found in possible changes in the communication infrastructure (ageing of devices, exchange into new/different models, or extension/modification of already existing infrastructure). Therefore, the following statistical condition can be formulated, fulfilling of which should cause launching of the recurrent learning procedure of the neural network

$$x_i \notin (\mu - 3\sigma, \mu + 3\sigma),\ i = 1, 2, \ldots, n, \tag{4}$$

where $\{x_1, x_2, \ldots, x_n\}$ is time series limited by n elements' analysis window, μ is mean estimated from forecasts of the neural network in the analysis window, and σ is standard deviation of elements of the examined time series in reference to such mean.

4 Experimental Results

The proposed new solution of railway LED Sign Communicating through PLC link is implemented to work with existing solutions of rail automation systems [16]. A PLC sign controller can work with classic analog systems and computer based systems. The novelty of the proposed solutions comes from the fact of existence of digital transmission with actual signaling cables to signs used for railway traffic control. In existing analog or computer based rail automation system the interface is analog (the state of device is controlled by level of current consumption [16]. In this article we put emphasis on security and maintenance issues of the proposed solution. In Fig. 2 we presented placing of our PLC controlled LED signs in typical part of rail automation system responsible for control and maintenance of railway signs. Every sign controller is connected to a dedicated interface responsible for a given LED sign.

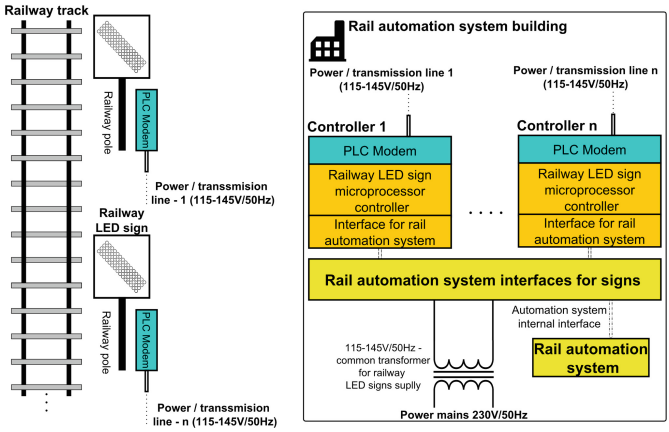

Fig. 2. Place of PLC controlled railway LED signs in typical rail automation system responsible for signs control and maintenance.

The railway sign is mounted on a railway pole on the one side of railway track. Communication between the sign controller and the LED sign is performed through standard signalization cable so the proposed solution can be implemented without big investments in new cable infrastructure. In Fig. 3 we can see internal block scheme of railway sign controller, LED signs and transmission links between signs and

controllers. Every pair of a sign and a controller is connected by a PLC communication link where typical distance is approximately 1 km. Every sign controller is supplied from common power source (transformer). Between a sign controller and a LED sign, the packets are transmitted through point to point link. Every point-to-point link is separated by proposed by authors PLC transmission separation filter. Such a filter isolates transmission of PLC packets in common medium (signaling cable) for a given point-to-point link and avoids to reach packets from one point-to-point link to another point-to-point links connected to the same common medium (see Fig. 3). Separation of transmission is necessary to ensure safety and reliability in signs critical infrastructure. Sign's controller may be equipped with different communication interfaces (e.g. relay, RS232, RS485, CAN etc.) depending on railway automation system type. A sign controller and LED sign is constructed in order to meet highest Safety Integrity Level 4 (SIL4) standard [15].

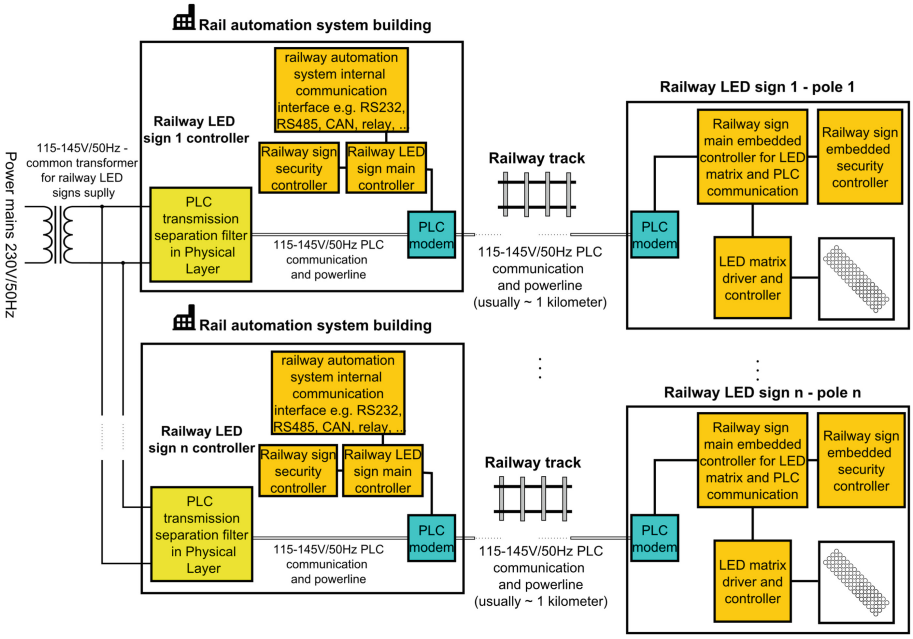

Fig. 3. Connections between elements of the proposed railway PLC controlled LED signs.

For analysis of PLC railway signs traffic's anomaly and attack detection we captured traffic features that are connected to network features (data link and network layers) from Table 1 and for maintenance purposes (see Table 2). Traffic features are processed into form of univariate time series where every sample arrives in constant period of time. After traffic features selection and calculation time series are used for neural network auto-regression models' learning.

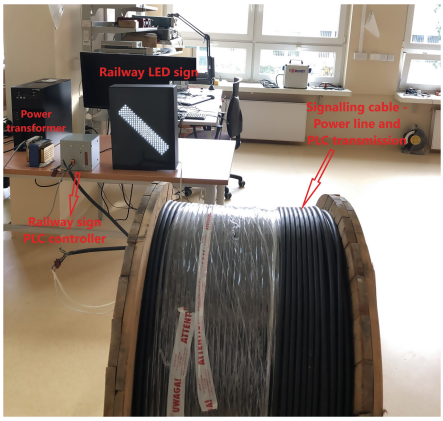

Fig. 4. Part of experimental testbed used for measurements and methodology verification representing connections between main elements of railway PLC signs together with power and transmission line (1 km length).

Part of experimental test bed used for the proposed methodology verification is presented in Fig. 4. We can see there an example set of devices communicating through signaling cable where we can set point-to-point link from 1 to 5 km.

Table 1. Railway PLC signs network features.

Traffic feature	Railway PLC sign feature description
SF1P	RSSIP: received signal strength indication for PLC transmission in [dBm] for a given railway LED sign point to point link
SF2P	SNRP: signal-to-noise ratio in [dBu] for a given railway LED sign point to point link
SF3P	NPRP: number of packet retransmissions per time interval for a given railway LED sign point to point link
SF4P	PERP: packet error rate per time interval in [%] for a given railway LED sign point to point link
SF5P	CNPTP: Cumulative number of packets per time interval for railway signs point to point links
SF6P	ACKPRP: Number of acknowledgements of proper packet receiving and configuration sent by LED controller for a given point to point sign link
SF7P	SPSP: Number of status packet sent by LED sign for a given railway LED sign point to point link

We gathered traffic features connected with physical PLC signal parameters like SF1P (RSSIP: received signal strength indication for PLC), SF2P (SNRP: signal-to-noise ratio) and features related to transmission protocol e.g. SF3P (NPRP: number of packet retransmissions) or SF6P (ACKPRP: Number of acknowledgements of proper packet receiving and configuration).

Table 2. Railway PLC signs maintenance features.

Traffic feature	Railway PLC sign feature description
MF1P	LEDP: Health status of railway sign LED matrix for a given railway LED sign point-to-point link
MF2P	RSLLP: Railway LED sign luminosity level in [%] (changes from 0–100%) for a given railway LED sign
MF3P	MTP: Temperatures of PLC modems communicating through point-to-point link
MF4P	SCCP: Number of safety circuit activation for a given LED sign
MF5P	TOT: Railway LED sign total operation time for a given railway LED sign

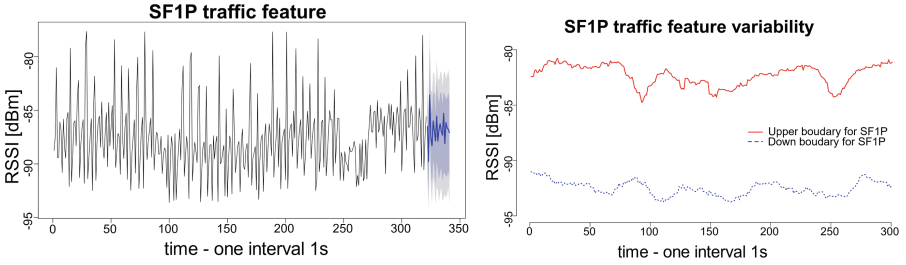

Fig. 5. Railway PLC sign traffic feature SF1P (RSSI [dBm]) neural network prediction intervals (20 samples horizon) with narrower (80%) and wider (90%) prediction intervals (on the left) and SF1P traffic feature variability used for model calculation (on the right).

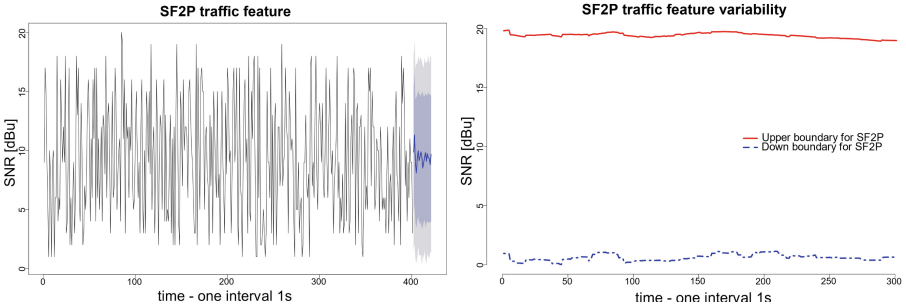

Fig. 6. Railway PLC sign traffic feature SF2P (SNR [dBu]) neural network prediction intervals (20 samples horizon) with narrower (80%) and wider (90%) prediction intervals (on the left) and SF2P traffic feature variability used for model calculation (on the right).

Maintenance traffic features from Table 2 are mainly used by railway automation system staff to assess railway LED signs condition and to plan mandatory technical inspections. Maintenance features are connected to status information sent by LED sign in packet payload to a sign controller. As an example, we can mention MF1P

(LEDP: Health status of railway sign LED matrix for a given railway LED sign) where information about a broken LED is transmitted (number of shortened LED and number of opened LED).

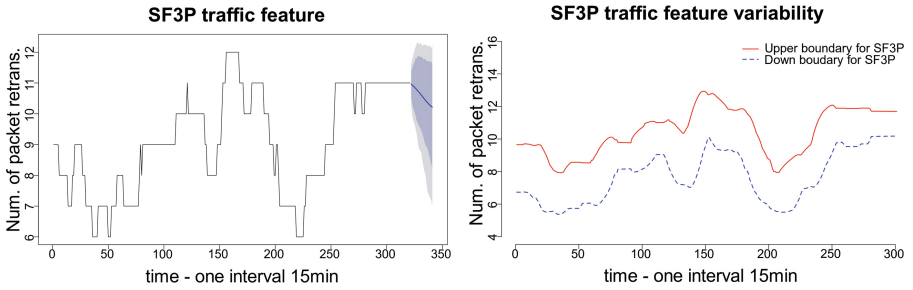

Fig. 7. Railway PLC sign traffic feature SF3P (number of packet retransmissions) neural network prediction intervals (20 samples horizon) with narrower (80%) and wider (90%) prediction intervals (on the left) and SF3P traffic feature variability used for model calculation (on the right).

Graphics representations of exemplary traffic features are presented in Fig. 5, 6 and Fig. 7. An instance of SF1P-SF3P traffic features captured from examined railway signs network are presented in a form of univariate time series (see left sides of Fig. 5, 6 and 7). We can also see there examples of 20 samples prediction intervals calculated by neural network auto-regression model in order to assess how this type of neural network manages with examined signals (time series). Two intervals represent 80% (narrower) and 90% (wider) prediction intervals. Proposed maintenance and security system is complementary to functions available inherently in railway automation system. We have to mention here that our solution is an advisory element for maintenance staff but for physical on/off operations is responsible railway automation system. First of all our additional system can't be responsible for increasing number of railway traffic stops and in consequence substantial economic losses caused by alarms from our systems. That's why prediction intervals from our traffic model have to be wide enough even in unusual situations caused by testing scenarios TS1–TS3. In standard work condition of our PLC signs network our anomaly detection system won't trigger an alarm. For every traffic feature we used these prediction intervals in order to achieve variability of traffic feature for a given traffic feature. In order to evaluate neural network prediction accuracy we presented in Table 3 Root Mean Square Error

Table 3. RMSE and MAE calculated for 10 sample prediction intervals for SF1P, SF2P and SF3P traffic features.

Neural Network	RMSE SF1P	MAE SF1P	RMSE SF2P	MAE SF2P	RMSE SF3P	MAE SF3P
NNAR	4.28	33.53	4.81	37.04	2.32	21.98

(RMSE) and Mean Absolute Error (MAE) parameters calculated with the use of 10 sample prediction intervals. Values were calculated for SF1P–SF3P traffic features. In the next step we calculate Bollinger bands (see Sect. 3.3) in order to achieve upper and down boundary values for a given traffic feature.

Variability for SF1P – SF3P traffic features are presented on the right sides of Fig. 5, 6 and 7. The final PLC railway signs traffic model can be generated based on one on more traffic feature variability time series depending on observation period of time. When more than one set of Bollinger bands is calculated for given period of time for a given traffic feature then final boundaries are calculated as a time series representing maximum or minimum values for higher or down boundary respectively (see Sect. 3.3). Variabilities of traffic features represent models of traffic feature behavior in our case. Online steps of our algorithm start with railway traffic features selection and calculation. Selected values of time series for a given traffic feature is subsequently compared to calculated models representing traffic features variability. If value of traffic feature exceeds boundaries set by calculated model then we generate detection report for a given railway sign and traffic feature. We also propose condition for models recalculation (see Sect. 3.4). Models recalculation is necessary in case of significant change of railway signs PLC traffic behavior or changes in physical structure of the examined network. Without models recalculation false positive values would rise to unacceptable levels. In order to evaluate anomaly/attack detection solution we proposed subsequent Testing Scenarios TS1–TS3:

- **TS1**
  First testing methodology requires generation of disturbance signals by means of equipment used for Electromagnetic Compatibility (EMC) conformance tests. Tests were performed by generating for example Electrical Fast Transient (EFT)/Burst disturbance signal according to IEC 61000-4-4 or Radio Frequency disturbances by current injection clamp according to IEC 61000-4-6 standard. Simpler attack may be performed also by connecting capacitor close to PLC modems. These methods are used for attacking Physical layer of PLC signs communication link. As a result of the proposed attacks, we are degrading physical parameters of PLC transmission line. Week parameters of PLC transmission signal has a big impact on communication reliability also in higher layers of PLC communication protocol stack.
- **TS2**
  Next testing scenario is based on connecting additional PLC communication device to railway sign communication link. Fake transmission node with PLC modem generates and transmits random packets. In different mode untrusted device capture arriving PLC packets, change/disturb them and retransmit to railway PLC sign modems. These packets disturb communication process between PLC sign controller and LED sign. Influence of this type of attack can be observed especially for traffic features connected to data link and network layers.
- **TS3**
  Subsequent testing scenario requires adding devices that create untrusted communication tunnel with the use of the same carrier frequency that is used by railway sign modems. One of the fake PLC node captures arriving packets and transmit them to other untrusted device. Another fake communication tunnel has an impact

on reliability of communication between PLC sign controller and LED sign. Another way of attack is a replay attack where untrusted device copy the received PLC packets that arrive to its PLC modem and transmit copy of this packet to legitimate PLC modems with certain delay. Abuses described in this scenario have the biggest impact especially on traffic features connected to data link and network layer and may have indirect influence on some maintenance features.

Taking into consideration all simulated attack or anomalies described in Testing Scenarios TS1–TS3, we achieve cumulative results presented in Table 4. Detection rate (DR) changes from 98.22%–90.14%, while false positive (FP) 5.83%–2.82%. The best results were achieved for SF4P (PERP: packet error rate per time interval) and SF2P (SNRP: signal-to-noise ratio in [dBu]). Based on literature analysis and solutions proposed by railway industry [16] we couldn't make straight comparison to similar solution for railway LED signs controlling. Present used interfaces for railway LED signs are based on analog interface to digital railway automation systems [16]. Our solution based on PLC transmission for railway LED signs is our novel proposition to digital control of railway LED signs signalization by existing railway infrastructure (classic signalization cable). From these reasons we can only indirectly compare our solution to anomaly/attack detections systems which utilize PLC transmission as a communication. For anomaly detection class systems (which also utilize PLC transmission) where we try to recognize abuses with unknown behavior signature, false positive values about 5% are treated as acceptable [10, 22]. We have to mention that anomaly detection class systems try to recognize unknown traffic behavior (so called 0 day attacks) on the contrary to the Intrusion Detection Systems (IDS) where patterns of malicious activity are already known. That's why false positive indications from anomaly detection system can be higher than in case of IDS systems.

Table 4. Detection rate and false positive for railway PLC signs network features.

Traffic feature	DR [%]	FP [%]
SF1P	96.20	3.20
SF2P	97.40	2.82
SF3P	95.63	4.35
SF4P	98.22	3.27
SF5P	90.14	5.83
SF6P	95.45	4.65
SF7P	90.27	5.64

There can also be observed some correlations between different types of testing scenarios. For example generation of electromagnetic disturbances or hardware modifications have an impact on testing scenarios TS2 and TS3 by disturbing packet exchange process in data link and network layers by sign controller and LED sign. The same type of coincidences can also be observed between different traffic features. For example, when values of SF2P (SNRP: signal-to-noise ratio in [dBu]) decrease in

consequence SF3P (NPRP: number of packet retransmissions per time interval) and SF4P (PERP: packet error rate per time interval) increases. Less obvious and indirect coincidences can be observed for maintenance features from Table 2. Maintenance features are usually used by railway automatic system engineers to assess technical condition of railway signs by analyzing features like MF1P (LEDP: Health status of railway sign LED matrix), MF2P (RSLLP: Railway LED sign luminosity level) or MF4P (SCCP: Number of safety circuit activation for a given LED sign) in order to plan service schedule for given signs. For example, coincidence may be observed when SF5P (CNPTP: Cumulative number of packets per time interval) increases then MF3P (MTP: Temperatures of PLC modems communicating through point to point link) also rises.

5 Conclusions

Continuous monitoring of resources and systems of critical infrastructures in order to ensure proper level of security and protection is currently a field of intense research. It is apparent that due to their nature, rail marking systems, especially those based on PLC technology, are susceptible to a great number of threats originating both inside and outside their own infrastructure. Significant problems connected to their safety are caused by attacks with increasingly great range and complexity level, as well as failures and damage of communication infrastructure elements. Most often implemented solutions which are supposed to ensure adequate level of security and protection are methods of detection and classification which allow to identify untypical behaviors reflected in the analyzed network traffic. In the present work, there were provided proposals of a system allowing to detect different types of anomalies and failures/damage in critical infrastructure of rail transport realized with the use of PLC technology. The structure and features of the examined LED Sign Communication Network were described. Furthermore, key aspects of security and system maintenance were analyzed, which influence correct operation of the critical communication infrastructure. There were also performed numerous experiments which confirmed effectiveness and efficiency of the proposed solution. We evaluated proposed solution by means of real world railway LED signs test bed. We analyzed 7 network features and 5 maintenance features in order to detect anomaly or attack in network of LED signs. Achieved DR changes from 98.22%–90.14%, while FP 5.83%–2.82%.

References

1. An, S., Lee, B., Shin, D.: A survey of intelligent transportation systems. In: Proceedings of the 3rd International Conference on Computational Intelligence, Communication Systems and Networks, pp. 332–337 (2011)
2. Qureshi, K., Abdullah, A.: A survey on intelligent transportation systems. Middle East J. Sci. Res. **15**(5), 629–642 (2013)
3. Fadlil, J., Pao, H.K., Lee, Y.J.: Anomaly detection on ITS data via view association. In: Proceedings of the ACM SIGKDD Workshop on Outlier Detection and Description, pp. 22–30 (2013)

4. Rossi, B., Chren, S., Buhnova, B., Pitner, T.: Anomaly detection in smart grid data: an experience report. In: Proceedings of the 2016 IEEE International Conference on Systems, Man, and Cybernetics, pp. 9–12 (2016)
5. Lloret, J., Tomas, J., Canovas, A.: An integrated IoT architecture for smart metering. IEEE Commun. Mag. **54**(12), 50–57 (2016)
6. Daely, L., Red, P.T., Satrya, H.T., Kim, J.W., Shin, S.Y.: Design of smart LED streetlight system for smart city with web-based management system. IEEE Sens. J. **17**(18), 6100–6110 (2017)
7. Mahoor, M., Salmasi, F.R., Najafabadi, T.A.: A hierarchical smart street lighting system with brute-force energy optimization. IEEE Sens. J. **17**(9), 2871–2879 (2017)
8. Garcia-Font, V., Garrigues, C., Rifà-Pous, H.: Attack classification schema for smart city WSNs. Sensors **17**(4), 1–24 (2017)
9. Leccese, F., Cagnetti, M., Trinca, D.: A smart city application: a fully controlled street lighting isle based on Raspberry-Pi card, a ZigBee sensor network and WiMAX. Sensors **14**(12), 24408–24424 (2014)
10. Xie, M., Han, S., Tian, B., Parvin, S.: Anomaly detection in wireless sensor networks: a survey. J. Netw. Comput. Appl. **34**(4), 1302–1325 (2011)
11. Rajasegarar, S., Leckie, C., Palaniswami, M.: Anomaly detection in wireless sensor networks. IEEE Wirel. Commun. Mag. **15**(4), 34–40 (2008)
12. Yau, K., Chow, K.P., Yiu, S.M., Chan, C.F.: Detecting anomalous behavior of PLC using semi-supervised machine learning. In: Proceedings of the 2017 IEEE Conference on Communications and Network Security, pp. 580–585 (2017)
13. Candelieri, A.: Clustering and support vector regression for water demand forecasting and anomaly detection. Sensors **9**(3), 1–19 (2017)
14. De Nadai, M., Someren, M.: Short-term anomaly detection in gas consumption through ARIMA and artificial neural network forecast. In: Proceedings of the 2015 IEEE Workshop on Environmental, Energy and Structural Monitoring Systems, pp. 250–255 (2015)
15. IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems (2010). https://www.iec.ch/functionalsafety/. Accessed 10 Jan 2020
16. Bombardier Transportation. https://www.bombardier.com/en/transportation.html. Accessed 12 Jan 2020
17. Cook, R.D.: Detection of influential observations in linear regression. Technometrics **19**(1), 15–18 (1977)
18. Cogollo, M.R., Velasquez, J.D.: Are neural networks able to forecast nonlinear time series with moving average components? IEEE Lat. Am. Trans. **13**(7), 2292–2300 (2015)
19. Zhang, G.P., Patuwo, B.E., Hu, M.Y.: A simulation study of artificial neural networks for nonlinear time series forecasting. Comput. Oper. Res. **28**, 381–396 (2001)
20. Bollinger, J.: Bollinger on Bollinger Bands. McGraw Hill (2002)
21. Vervoort, S.: Smoothing the Bollinger bands. Tech. Anal. Stocks Commod. **28**(6), 40–44 (2010)
22. Garcia-Font, V., Garrigues, C., Rifà-Pous, H.: A comparative study of anomaly detection techniques for smart city wireless sensor networks. Sensors **16**(6), 868 (2016)