Journal of Universal Computer Science, vol. 26, no. 4 (2020), 508-527
submitted: 4/11/2019, accepted: 5/2/2020, appeared: 28/4/2020

Anomaly Detection for Smart Lighting Infrastructure with the Use of Time Series Analysis

Tomasz Andrysiak
(Institute of Telecommunications and Computer Science
Faculty of Telecommunications, Computer Science and Electrical Engineering
UTP University of Science and Technology, Al. S. Kaliskiego 7, 85-796 Bydgoszcz, Poland
andrys@utp.edu.pl)

Łukasz Saganowski
(Institute of Telecommunications and Computer Science
Faculty of Telecommunications, Computer Science and Electrical Engineering
UTP University of Science and Technology, Al. S. Kaliskiego 7, 85-796 Bydgoszcz, Poland
luksag@utp.edu.pl)

Abstract: One of the basic elements of every Smart City is currently a system of managing urban infrastructure, in particular, smart systems controlling street lighting. Ensuring proper level of security, continuity and failure-free operation of such systems, in practice, seems not yet a solved problem. In this article we present proposals of a system allowing to detect different types of anomalies in network traffic for Smart Lighting critical infrastructure realized with the use of Power Line Communication technology. Furthermore, there is proposed and described the structure of the examined Smart Lighting Communications Network along with its particular elements. We discuss key security aspects which affect proper operation of advance communication infrastructure, i.e. possibility of occurrence of abuse connected both to activity of external factors which could disturb transmission of steering signals, as well as active forms of attack aiming at influencing the informative content of the transmitted data. In the article, there is also presented an effective and quick anomaly detection method in the tested network traffic represented by suitable time series. At the initial stage of the method, the process of detection and elimination of potential outlying observations was realized by one-dimensional quartile criterion. Data prepared in this manner was used for learning recurrent neural networks, i.e. Long and Short-Term Memory types, in order to predict values of the analyzed time series. Further, tests were performed on relations between the forecasted network traffic and its real variability in order to detect abnormal behavior which could mean an attempt of an attack or abuse. Due to a possibility of occurrence of significant fluctuations in real network traffic of the tested Smart Lighting infrastructure, we propose a procedure of recurrent learning with the use of neural networks to obtain more accurate forecasting. The results achieved by means of the performed experiments confirmed effectiveness of the presented method and proper choice of the Long Short-Term Memory neural network for forecasting the analyzed time series.

Keywords: Anomaly detection, time series analysis, outliers detection, network traffic prediction, neural networks, Smart Lighting Communications Network
Categories: C.2.0, K.6.5

1 Introduction

One of the key elements of a Smart City (SC) infrastructure are systems of management, monitoring and steering of street lighting. They allow for optimal utilization of lighting network but also enable significant decrease in cost consumption by means of: *(i)* reduction of lighting intensity of particular lamps within specified time frames and space; *(ii)* precise turning on and off of particular lamps, and *(iii)* counting for changeable capacity of light sources in long-term exploitation. The use of the above mentioned activities usually ensures optimization of lighting management methods and limits the costs of electric energy consumption [Castro, 13].

The „smartness" of the systems of street lighting steering and management usually consists in adjusting the levels of illuminance to the current demand of the users, weather conditions, and requirements posed by binding norms and provisions of law. For this reason, most often sensors of traffic and weather are installed so that the smart steering system could collect information from those sensors and, depending on the current situation, automatically adjust procedures of the street lighting operation [Rong, 13].

The most important functions of the Smart Lighting (SL) system of street lighting management are: *(i)* different procedures of steering particular lamps in given time units, *(ii)* lamp grouping with regard to needs and established steering algorithm, *(iii)* counting energetic parameters of individual lamps, groups of lamps and additional devices, *(iv)* parameter monitoring and detection of correct operation of the exploited lamps [Wu, 10].

While constructing SL infrastructure which is responsible for data transmission, further referred to as Smart Light Communication Network (SLCN), the following aspects are most often taken into consideration: Power Line Communication (PLC) networks and Long Term Evolution (LTE) solutions. Main advantage of the PLC network is its ability to use for data communication the already existing network infrastructure, without the need to install additional wiring. In consequence, it is possible to limit the costs of constructing such a network. The costs would include wiring, its maintenance and conservation. LTE networks can, on the other hand, be competition to PLC networks in this regard, because they also do not require erecting additional infrastructure, however, still in many cases they are not capable of ensuring full territorial cover. Range and speed of data communication in radio networks can be negatively affected by presence of other wireless devices and muting signals caused by urban obstacles and natural barriers, e.g. high buildings and greater hills [Kiedrowski, 15].

SLCN networks, by their character, are subject to an increasing number of threats (different type of abuses) originating both inside and outside their own communication infrastructure. Serious security problems within the SLCN infrastructure are threats coming from intruders whose aim is to destabilize or significantly influence operation of SL network. They can be connected to realization of destructive activities in relation to the SLCN infrastructure, consisting in hampering its correct operation or hindering transmission of the already existing signals. However, the key security problem is usually ensuring proper level of protection against the external abuses realized as network attacks [Elmaghraby, 14].

In Figure 1 we can see smart lighting network overall scheme. Smart lamp is connected to power network supplying every lamp by means of a PLC modem. Every segment of PLC smart light network consist of a PLC traffic concentrator. Smart lamps from different locations are connected to PLC traffic concentrators which play a role of protocol translator from smart lamps network to, for example, Internet Protocol (IP) network. Access Point Name Server gives us functionality of access to PLC network by means of different packet transmissions, like LTE. Smart Lighting Server is a host for maintenance applications for entire PLC smart lights network.

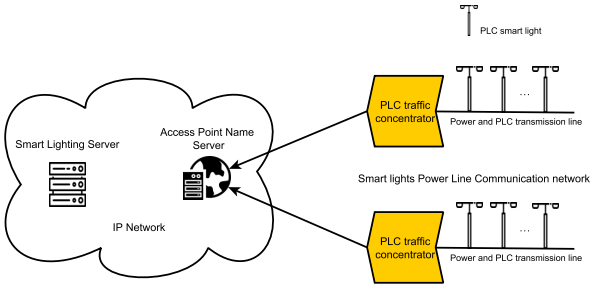


Figure 1: Smart lighting network overview

The Article presents effective solutions concerning detection of different types of anomalies in the tested SL infrastructure realized with the use of PLC technology. The structure of the examined SLCN network is described and we present an analysis of proper operation of a critical communication infrastructure. Further, we propose an efficient protection system against attacks based on recurrent neural networks, i.e. Long Short-Term Memory networks in order to forecast values of the analyzed time series representing appropriate SLCN network parameters. There have also been presented numerous scientific experiments which confirmed effectiveness and efficacy of the described solution. The anomaly detection processes consisted in examining relations between the forecasted network traffic and its real variability in order to detect behavior which might signal an attempt of attack or abuse. The obtained results showed that the anomalies contained in the network traffic signal can be successfully detected by means of the proposed solution.

The article is organized as follows. After the Introduction, Section 2 presents motivation and related work on existing anomaly detection systems for Smart Lighting network. In Section 3 the main security issues related to Smart Lighting Communications Network are categorized and characterized. Next, Section 4 shows the structure and operation of the proposed solution. In Section 5, a real-life experimental setup and experimental results are presented and discussed. Finally, Section 6 concludes our work.

2 Motivation and related work

Complexity and diversity of processes occurring in contemporary computer networks and challenges currently posed in the field of analysis and signal transformation (in particular those concerning construction of network traffic models, in case of which it is crucial to have detailed knowledge on phenomena arising inside their communication infrastructure) were basis for the undertaken activities and conducted experiments. Undoubtedly, having reliable knowledge about communication infrastructure usually allows for modelling and forecasting the network traffic to identify and/or recognize different type of disorders (anomalies), which are significant from the quality point of view of the realized network services and the adopted security level [Bhuyan, 14].

To detect and analyze such phenomena, most often two technologies are joined: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). Considering a proper level of security for network infrastructures, the systems are usually located just after protection elements, such as firewall. The aim of solutions such as IPS is undertaking activities which would stop the attack, minimize its effects and/ or active response to security rules' violation. The basic task of these solutions is comparison of parameters of the real-life network traffic and the memorized attacks' signatures. The IDS systems, on the other hand, are used to increase the security level of the protected infrastructure, both from the inside and from the outside. Their advantage is that they can be used for network traffic analysis and utilize diverse techniques of threat identification [Jackson, 99][Esposito, 05]. One of them is based on the idea of monitoring normal network operation to spot deviation from norm (detect an anomaly), which may indicate a hack into a protected network infrastructure [Lim, 08].

Anomaly detection usually consists in recognizing nonstandard patterns of behaviors reflected in parameters of the analyzed network traffic. All the occurrences diverging from those patterns (models describing the network traffic behavior) are classified as potentially dangerous and can indicate an attempt of attack or abuse. High efficiency and efficacy of methods based on anomaly detection is closely connected to ability of recognizing unknown attacks, i.e. zero-day exploits. The fundament of these types of actions are methods of anomaly detection and/or identification, working on the basis of knowledge not how the given attack happens, but what is beyond the predefined moral model of the network traffic [Barford, 02].

Analyzing work of the examined domain, a complete list of methods and techniques concerning anomaly detection can be found in numerous overview papers [Sample, 13][Chondola, 09]. They present different approach to problems of anomaly detection, beginning with machine learning methods, data exploration and information theory, up to spectral solutions. However, the analysis of these solutions needs to be carried out with strict relation to their implementation.

Anomalies in communication systems, in particular SLCN, can be caused by different factors, i.e. deliberate or accidental human activities, damaged element of the communication infrastructure, or any other kind of abuses. While analyzing field literature, it can be easily noticed that there are many works concentrating on anomaly detection solutions in communication networks, as well as in Smart Grid systems. However, the authors of these articles usually concentrate on solutions detecting anomalies in different fields on the basis of protocol stacks, i.e. Transmission Control Protocol (TCP)/Internet Protocol (IP) or User Datagram Protocol (UDP) [Rossi, 16].

Despite extensive searches, no publications were found (besides works of the authors [Liu, 12]) which would concentrate on the problems of anomaly/attack detection for Smart Lighting network realized with the use of PLC/LTE technology.

It can be stated that there are different anomaly detection methods which are used in wireless networks of sensors, smart measuring networks or PLC infrastructure [Rajasegarar, 08][Yau, 17]. Nevertheless, most of the tests focus on the problem of reliability of data transmission in communication networks.

In our article we propose a new solution for improving security for PLC Smart Lighting network.

3 Overview of security problems in SLCN

In Smart Cities security of critical infrastructures have key role due to the size of area they operate on, potentially great number and variability of their communication devices, and exploitation costs they generate. Therefore, providing an adequate level of safety and protection to them becomes an extremely important element of the proposed solutions, especially those concerning SLCN infrastructures [Rinaldi, 01] [Kiedrowski, 15].

It is known that the aim of every SL system is not only to light the streets but also, depending on the type of surface, to control brightness and homogeneity of lighting and reflections in order to provide the drivers and pedestrians with best possible visibility. Therefore, Smart Lighting solutions are characterized by high functionality and flexibility in operation, however, due to their smart nature, they can be subject to different type of abuses (attacks). Such activities can be realized not only by the recipient of the service but also by criminals who want to impose a particular state of SLCN infrastructure [Castro, 13][Elmaghraby, 14].

The recipient most often causes destructive actions in relation to SLCN consisting in disturbing transmission of controlling signals in order to achieve a change of period and/or intensity of lighting. Such actions may have conscious or unconscious nature. Unconscious (non-deliberate) interference usually occurs when loads which do not comply with electromagnetic compatibility are introduced into the supply network. Conscious form of interference into communication system, on the other hand, is connected to deliberate action consisting in connecting to the SLCN infrastructure such elements as: capacitors, disturbing generators, hub emulation terminals. Attaching such devices is not difficult, and their utilization by an intruder may be hard to detect for longer period of time [Liu, 12] .

A more complex problem seems to be protection against intentional attacks realized for criminal purposes, whose aim is disturbing the steering system, turning off the lighting or reduction of its intensity. In such a case, every light of the Smart Lighting system may become a point, through which SLCN can be attacked.

Attacks against safety of the SLCN can be divided into two basic groups: passive and active. Passive attacks are understood as any activities aiming at unauthorized access to SLCN infrastructure, in which the attacker does not use emission of signals which could disturb and/or disable correct operation of the system. Active attacks, on the other hand, are all the attempts of unauthorized access to the SLCN infrastructure with the use of emission of any signals or actions that can be detected [Macaulay, 12].

Realizing a passive attack, an intruder disguises his presence and attempts to obtain access to the transmitted data by passive listening to such a network by: *(i)* imitating a hub, *(ii)* imitating a particular lamp, or *(iii)* participating in transmission of frames. Another type of a passive attack onto SLCN are activities aiming to analyze traffic inside such network by attempts of obtaining topological knowledge that would allow to recognize the structure of the attacked infrastructure [Liu, 12].

In case an active attack is realized, the intruder influences actively or passively the content of the transmitted data and/or functionality of the system. Attacks of this type are much easier to detect because they cause visible disturbances in the correct work of SLCN. Due to form, aim and manner of realization, active attacks can be divided into three groups: *(i)* physical attacks by means of Electromagnetic Pulse (EMP) [Smoleński, 12], *(ii)* attacks onto integrity and confidentiality of the steering signals' transmission, and *(iii)* attacks oriented onto particular layers of the SLCN network.

Physical attacks are any type of destructive actions whose aim is complete destruction or damage of SLCN infrastructure. However, attacks directed onto integrity or confidentiality of the steering signals' transmission are actions consisting in compromising legal element of the network and overtaking its function.

Another kind of attack in SLCN networks depends on overloading the affected network infrastructure, which is usually manifested by lack of possibility to use particular services. Activities of this kind usually occur when the network is introduced with greater traffic than can be serviced. They can also have a different form, e.g. appear in physical layer, realizing jamming actions, and in data link layer by flooding with packets causing data collision and imposing a need for their retransmission [Wang, 16].

In order to protect from the above listed threats, in particular different types of active and passive attacks, it is necessary to ensure a high level of security to the SLCN critical infrastructure by means of its continuous monitoring and control of the network traffic. One of the possible solutions to so stated a problem may be implementation of detection system of anomalies reflected in particular parameters of the SLCN network traffic. In consequence, the detected non-standard behaviors of defined parameters may manifest a possibility of appearing an abuse or any form of attack. The latter is the main focus of the present paper.

4 Anomaly/attack detection system in Smart Lighting infrastructure - the proposed approach

For ensuring high level of security and protection of the implemented Smart Lighting solutions, it is necessary to utilize methods and techniques providing both passive actions, i.e. network monitoring, storing occurrences, and reporting; and active solutions, such as continuous supervision in order to execute the adopted security policy. Realization of so stated tasks is most often provided by Network Anomaly Detection System (NADS) type of solution [Lim, 08].

Then, anomaly detection consists in recognizing nonstandard patterns of behavior reflected in parameters of the analyzed network traffic. All the occurrences diverging from those patterns (describing normal behavior of network traffic) are classified as potentially hazardous, and may indicate an attempt of an attack or abuse. High efficiency and effectiveness of the methods based on anomaly detection are closely related to capacity of recognizing unknown attacks/abuses, because these methods operate on the basis of knowledge: not how particular attack/abuse works (what is its signature), but what goes beyond the defined pattern of network traffic. Therefore, systems based on anomaly/abuse detection are much better than systems using signatures while spotting new, unknown types of attacks/abuses [Esposito, 05].

In the present work we are proposing predictive system of anomaly/attack detection for PLC Smart Lighting Network based on Long Short-Term Memory (LSTM) neural network for forecasting the analyzed time series.

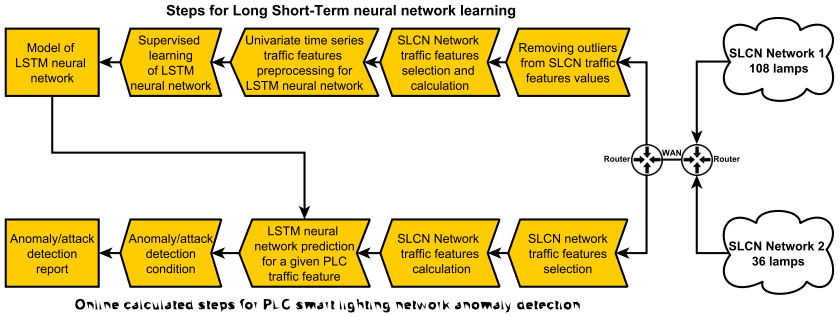


Figure 2: Presentation of main steps in the proposed anomaly detection algorithm for PLC Smart Lighting Network

Schematic presentation of main steps in the proposed method is presented in Figure 2. PLC traffic from the two examined SLCN Network 1 and Network 2 is processed by the suggested anomaly detection method. There are two main branches in the presented methodology. Firstly, we have to obtain a model of LSTM neural network. At the beginning we do some pre-processing operations on every PLC traffic feature from Table 1, starting from removing outliers (see Chapter 4.1). Every traffic feature from Table 1 is represented in a form of univariate time series where every consecutive PLC traffic feature value arrives in constant time periods.

Before neural network learning process (supervised learning) we performed some pre-processing operations on univariate time series representing traffic features. Firstly, we transform input data into stationary by differencing consecutive values in time series. Next, time series are transformed with the use of lagging operation. After that dataset is split into training and testing datasets (e.g. 70% training and 30% testing stets) and normalize/rescale data to the range of activation function. For the LSTM neural network model compilation process, we chose mean squared error as the loss function and Adaptive Monument Estimation (ADAM) for optimization algorithm. Subsequently, univariate time series is used for supervised learning of the LSTM neural network model. After model fitting process, we use the LSTM neural network for

prediction process (see Chapter 4.2) which is carried out during online performed step of the proposed anomaly detection algorithm.

Second branch of the proposed algorithm consists of online calculated steps performed for anomalies/attacks detection. Pre-processing steps are responsible for extracting and calculating univariate times series presented in Table 1. For every PLC smart light traffic feature we calculate prediction intervals with the use of LSTM neural network model calculated by first branch of the proposed algorithm. Based on parameters calculated by the LSTM neural network, we check anomaly/attack detection condition in order to classify PLC traffic (for more details concerning anomaly/ attack detection conditions, see Chapter 4.2).

4.1 Outliers' detection and elimination based on one-dimensional quartile criterion

While analysing structure and character of the SLCN infrastructure, it can be assumed that there is a real threat of great fluctuations in the examined network traffic parameters, i.e. high likelihood of outliers' occurrence in the analysed time series. These fluctuations may originate differently, e.g. *(i)* can be caused by technical changes to the infrastructure, *(ii)* can be a result of physical damage of devices, *(iii)* they can be an aftermath of a network attack or *(iv)* can be intended deceit of users. Constructing solution on grounds of a set of such data can lead to numerous adverse consequences. It is then highly likely that inference, prediction, and decision-making on such basis may have significant error occurrence possibility, and the proposed solution will not be reflecting main mechanisms controlling behaviour of the examined phenomenon. Therefore, an important element of data pre-processing phase should be detection of outlying observations, evaluation of their influence on prediction results and, alternatively, their elimination from the analysed data set.

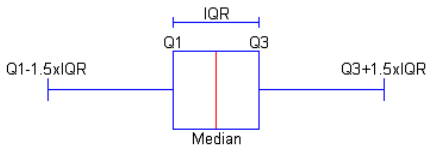


Figure 3: Identification of outliers – box plot

In our attempt, identification of outlying observations in the analysed SLCN network parameters is performed by means of one-dimensional quartile criterion, which is used for creation of box plots, developed by [Tukey, 77]. Outliers' detection and elimination based on one-dimensional quartile criterion in our algorithm is only calculated during first off-line stage of our algorithm (see Figure 2). First branch of our algorithm, where outliers' detection and elimination is performed, is responsible for calculation of initial LSTM neural network model and in case of neural network model recalculation (see Chapter 4.3). We eliminate outlying observations from every examined SLCN traffic feature (see Table 1) in order to limit influence of such values on prediction results. For every parameter we calculate first Q1 and third Q3 quartile and interquartile range (IQR), where IRQ=Q3-Q1. In such circumstances, outliers (see

Fig. 3) are those whose values exceed the range (Q1-1,5IQR, Q3+1,5IQR). To the contrary, observation of extreme outliers are identified as those for which the attributes are outside the range (Q1-3IQR, Q3 + 3IRQR).

4.2 The SLCN traffic features forecasting using neural networks

In the forecasting processes of the analyzed time series' future values (representing chosen features of the network traffic) more and more often there are used approaches based on different type of artificial neural networks (such as unidirectional multilayer, recurrent or self-organizing networks), which acquire ability to predict due to the course of learning processes. It is known that neural networks provide a possibility to build models mapping complex dependencies between input and output data for phenomena whose structure, rights of action or casual relationships have not been acknowledged to sufficient extent so as to create effective mathematical models. Then, neural analysis and prediction of variables represented in the form of time series requires usage of methods which include changes occurring in time (i.e. character, dynamics, and structure of data). They can also describe regularities connected with them.

Among numerous types of artificial neural networks, the most effective tools for prognosing future values of time series are currently becoming neural networks in which there is a feedback loop. The loop should undergo the same rules that all the entrances do, i.e. weighting and backward error propagation. Then, the state of individual neurons depends not only on input data but also on the previous state of network *h(t-1)*, which theoretically enables to keep information within the network's structure between consecutive iterations, so in a way it works as some kind of memory. Theoretically, such network should have an ability to react to a set of input data that has already appeared before at the entrance and was preserved in its structure. In practice, it is not that obvious.

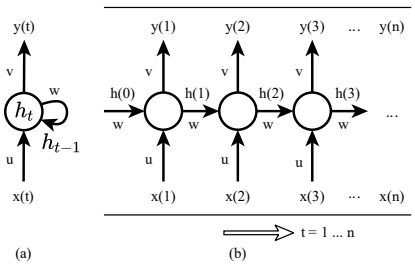


Figure 4: Scheme presenting a neuron's „developing in time" in a recurrent network

If we were to imagine an operational scheme of such a network, then in moment *t* every neuron with feedback loop (Fig. 4a) would be as it were an expansion (Fig. 4b) of all its states *h(t-n)*, corrected by weight coefficients *w*. Here is where the main problem lies. Weight coefficients in this chain multiply, and if the chain is long, the result of such operation quickly approaches zero (if $w < 1$) or infinity (if $w > 1$). This

phenomenon, known as gradient fading or explosion, in practice, causes that in case of longer sequence the network is not able to learn any valuable data [Bengio, 94]. Solution to this problem was published in work of [Hochreiter, 97]. It consisted in integration in the structure of each neuron blocks with nonvolatile memory and additional switches controlling data flow. The new network was called Long Short-Term Memory, i.e. network with long memory of short range, which became insensitive to "forgetting" and remembering patterns.

Besides defining the structure of LSTM network and number of its hyperparameters, an essential factor of its correct operation is the properly prepared data which needs to be complete, deprived of outliers, normalized and stationary. Due to the fact that data gets into the network in sequences, it is necessary to understand what kind of sequence would be most proper for the task we want to perform and then prepare it correctly. In the end it is necessary to define the shape of tensor which gets at the input of the LSTM layer and to define properly parameters of this layer.

In the present work we propose predicative system of anomaly/abuse detection in SLCN network, based on recurrent neural network Long Short-Term Memory used for forecasting future values of the analyzed time series. At the initial stage we perform operation on data (i.e. values of the analyzed time series described in Table 1) which consists in elimination of outlying observations. Next, we transform input data to the stationary form by differentiation of consecutive values in the analyzed time series. In the next step, we transform time series by means of delaying operation. Further, we divide the data set into set of training and testing data (70% training and 30% testing sets), and we normalize/scale the data to the range of activation function. In the process of LSTM neural network model compilation we use mean square error as a loss function and Adaptive Monument Estimation (ADAM) for optimization algorithm [Brownlee, 18]. Then, we use one-dimensional time series for supervised learning process of the LSTM neural network model. In the process of adapting the model we use LSTM neural network for prediction of future values of the analyzed time series. These actions are realized at the online stage of the proposed algorithm of anomaly detection, in which the process of anomaly finding consisted in examining the following condition

$$x_i \notin \langle \Sigma - \Delta, \Sigma + \Delta \rangle \;\; i = 1,2, \dots, n \tag{1}$$

where $\{x_1, x_2, \dots, x_n\}$ is the examined time series limited by current n – element analysis window, Σ is mean calculated from forecasts/predictions of the neural network in analysis window, and Δ is value of three standard deviations of prediction errors in the previous analysis widow in relation to mean Σ.

Condition from Equation 1 is checked for every traffic feature from Table 1 during online detection steps. Variability for a given traffic feature is based on predictions calculated for current analysis window (Σ is a mean calculated from LSTM forecasts) and three standard deviations Δ calculated from LSTM prediction errors time series calculated based on predictions calculated by LSTM neural network for previous analysis window. In consequence, for subsequent analysis windows we achieve SLCN traffic feature variability channel with center Σ mean values and boundary values $\Sigma - \Delta$ and $\Sigma + \Delta$. When online extracted tested time series' traffic feature value x_i is outside the fixed channel $\langle \Sigma - \Delta, \Sigma + \Delta \rangle$ calculated for a given analysis window, we indicate detection of an attack/anomaly.

A detailed description of methods and techniques used for estimation of the proposed LSTM network, such as choice of parameters, network structure and description of learning processes, can be found in works by [Brownlee, 18][Brownlee, 19]. There are also described consecutive stages of the required data transformation adopted for the proposed solution.

4.3 The condition of neural network model's update

The character and nature of the tested dependencies, i.e. SLCN network traffic parameters, imply high probability of occurrence of significant data fluctuations in the analyzed time series. The reasons of such phenomenon are to be sought in possible variabilities (intended or unintended) in the SL infrastructure, namely, ageing of devices, exchange into new/different models, or development/modification of the existing lighting infrastructure but also emergence of permanent disturbances which can exert significant influence on the transmitted communication signals. These factors should cause adaptation of the proposed anomaly detection method to the variable conditions which are not a consequence of any attack or abuse. One of possible solutions to so formulated a problem is a procedure of recurrent learning of the used neural networks, realized on new learning sets (features/parameters), including the subject fluctuations.

Therefore, the condition of a neural network recurrent learning should be detection in the analyzed data set (elements of time series representing particular features or parameters) of significant and possibly permanent statistical variability. The observable duration of such variability should be much larger than the width of the potential analysis window, which would guarantee updates of the parameters of the used neural networks at the time of already established fluctuations.

Assuming data distribution close to normal, we can conclude that in a range with a width of six standard deviations there is over 99% of the data [Shiavi, 07]. Hence, if we define the average on the set of forecasts received on the basis of the used neural network and the standard deviation is calculated for real values of the analyzed data then significant non-compliance with the above condition may indicate a change in the statistical nature of the data analyzed.

Expression from Equation 2 is used only as a trigger condition responsible for LSTM neural network model relearning

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

where $\{x_1, x_2, \dots, x_n\}$ is a time series limited by n – element analysis window, μ is the mean calculated on the neural network forecasts in current analysis window, and σ is standard deviation of the tested time series' representing online extracted SLCN traffic feature elements in relation to such mean. In order to prevent the neural network from possible learning of the data set reflecting attacks/anomalies (i.e. outliers), the given set should undergo the procedure described in section 4.1 (outliers' detection and elimination).

In contrast to condition from Equation 2, three standard deviations Δ values from Equation 1 are calculated from LSTM prediction errors time series based on predictions calculated by LSTM neural network for previous analysis window. When the condition described in Equation 2 is not satisfied in over 50% analysis windows in a week's

period of time then we start the process of recurrent learning of the neural network used in our algorithm.

The size of analysis window was set by taking into consideration few aspects. First practical aspect comes from the fact that 10 samples' prediction interval (in our case traffic samples are acquired in 15 minutes intervals) used for neural network prediction is sufficient in the context of smart lighting infrastructure. Longer prediction period is not necessary for smart light infrastructure maintenance purposes.

Subsequent aspect that we take into consideration is a relationship between length of the neural network prediction interval and the model's prediction accuracy represented by, for example, MAE (Mean Average Error), RMSE (Root Mean Squared Error) or MAPE[%] (Mean Average Percentage Error). We experimentally checked that in case of prediction interval longer than 10 samples we achieve worse LSTM neural network model accuracy represented by RMSE, MAE and MAPE parameters.

5 Experimental installation and results

The testing Smart Lights Communication Network is an installation consisting of two networks in two geographical locations (see Figure 5). First installation includes real world implementation of 108 lamps situated on a three kilometres street. Second installation consists of 36 lamps of test network placed in a university building. In case of the first network, PLC communication is performed through dedicated lighting power installation located along the street. In the second location lamps are connected to standard building power mains 230VAC without separation from devices that usually work in university buildings (e.g. laboratories, administration etc.).

Packets from PLC networks are repacked into IP packets by means of PLC traffic concentrator which play a role of bridge between SLCN network and IP network. Packets from these two PLC networks are transmitted through WAN link and dedicated VPN connection to the machine responsible for Smart Light Communication Network anomaly/attack and maintenance purposes, where the algorithm proposed in the article was tested.

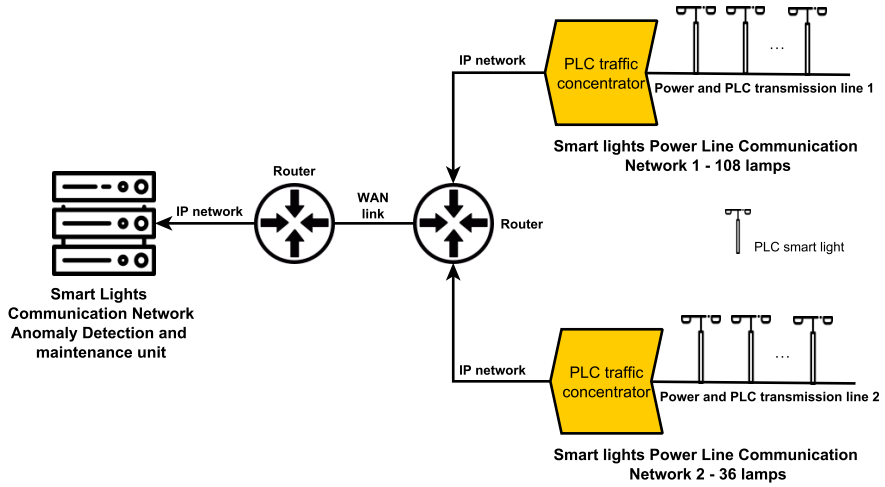


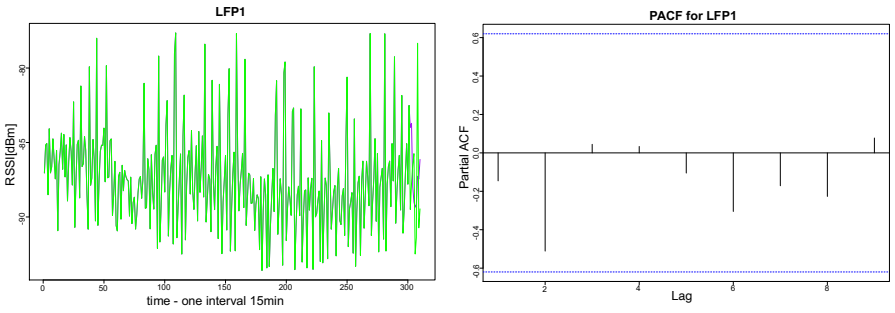
Figure 5: Smart Light Communication Network test bed used for experimental results

For anomaly/attack detection in SLCN, network traffic from two examined networks is transformed into a form of univariate time series where each value arrives in constant periods of time. In Table 1 we gathered SLCN PLC traffic features connected either for Data Link and Network Layers (LFP1 – LFP10) or for Application Layer (LFP11 – LFP13).

Parameters of PLC traffic features in case of Data Link and Network layers concern, for example, PLC signal parameters (LFP1 - RSSILF: received signal strength indication, LFP2 - SNRLF: signal-to-noise ratio) or parameters calculated based on communication protocol implemented in the tested network e.g. LFP6 - NOCCLF: number of Command copies received by PLC concentrator, LFP10 - ACCLF: ACK/CANCEL copies number received through PLC node.

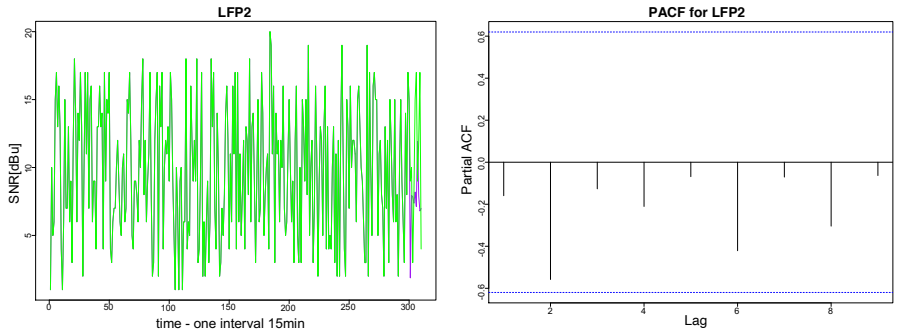
SLCN feature	SLCN feature description
LFP1	RSSILF: received signal strength indication for PLC lamps in [dBm]
LFP2	SNRLF: signal-to-noise ratio in [dBu]
LFP3	PERLF: packet error rate per time interval in [%]
LFP4	NPTLF: number of packets per time interval
LFP5	TTLLF: packet time-to-live value for PLC node
LFP6	NOCCLF: number of Command copies received by PLC concentrator
LFP7	NRCLF: number of RESPONSE copies received by PLC concentrator
LFP8	NLNLF: number of neighbours for a given lamp per time interval
LFP9	NPRLF: number of packet retransmissions by means of PLC communication (for a given lamp)
LFP10	ACCLF: ACK/CANCEL copies number received through PLC node
LFP11	MLOLF: maximum luminosity operation time for a given PLC lamp
LFP12	TOT: total operation time of PLC lamp
LFP13	PC: power consumption by PLC lamp in [Wh]

Table 1: Smart Lighting Network features captured for anomaly detection purposes



a) *b)*

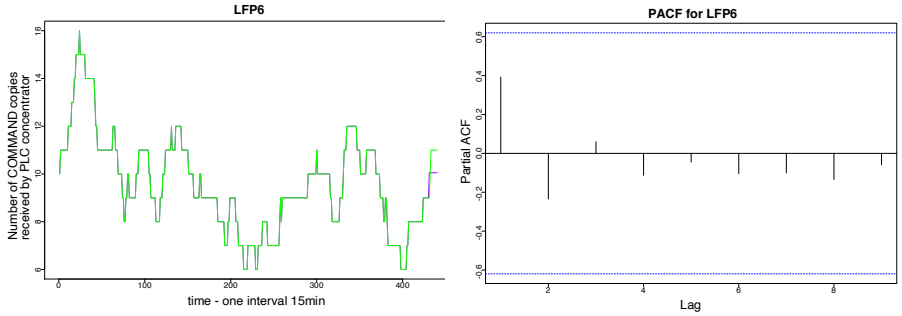
Figure 6: Smart Light network traffic LFP1 feature and PACF function (a) RSSI [dBm] traffic feature (green line) and 10 samples prediction interval (purple line) (b) Partial Autocorrelation Function PACF from model residuals for LFP1 feature



a) *b)*

Figure 7: Smart Light network traffic LFP2 feature and PACF function (a) SNR [dB] traffic feature (green line) and 10 samples prediction interval (purple line) (b) Partial Autocorrelation Function PACF from model residuals for LFP2 feature

In case of Application Layer we collected time series represented by LFP11 - MLOLF: maximum luminosity operation time for a given PLC lamp, LFP12 - TOT: total operation time of PLC lamp and LFP13 - PC: power consumption by PLC lamp in [Wh].



a) *b)*

Figure 8: Smart Light network traffic LFP6 feature and PACF function (a) NOCCLF Number of COMMAND copies received by PLC concentrator traffic feature (green line) and 10 samples prediction interval (purple line) (b) Partial Autocorrelation Function PACF from model residuals for LFP6 feature

Graphic representation of exemplary SLCN traffic features are presented in Figure 6 – Figure 8. Every traffic figure consists of two parts. First part, e.g. Figure 6.a, shows shape of time series representing a given feature (green line) and 10 samples of forecasting interval (purple line) calculated by means of LSTM neural network model which work in prediction mode. In order to evaluate model of LSTM neural network we calculated Partial Autocorrelation Function (PACF) for a given traffic feature (Figure 6.b – Figure 8.b). PACF function is calculated from residual values achieved after predictions calculated from LSTM neural network model. Values of PCAF for

subsequent lags should have insignificant amplitudes constrained by dashed horizontal lines in Figures 6.b – Figure 8.b. Insignificant values of PACF function mean that the proposed model fits enough to the characteristic of the examined univariate time series and may be used for PLC traffic prediction.

On the basis of prediction intervals achieved from LSTM neural network, we check anomaly/attack detection condition (for details see Chapter 4.2, condition 1) for every PLC traffic feature in order to classify possible anomaly in the examined traffic.

Evaluation process of the proposed algorithm was performed by simulating anomalies or attacks that belongs to different class and have an impact on traffic features from Table 1. Methodologies of conducted attacks/anomalies belong to different classes described in Testing methodology 1 – Testing methodology 3.

- Testing methodology 1

First testing methodology concerns anomaly/attack generation by means of hardware devices that generates conducted (e.g. EFT/Burst generator according to IEC 61000-4-4) or Radio Frequency disturbances (e.g. by current injection clamp according to IEC 61000-4-6). Such attack has an impact on quality of physical parameters of PLC communication between smart lamps. Physical parameters of PLC signal have an influence on communication reliability also in higher layers of PLC communication protocol stack.

- Testing methodology 2

Second testing methodology requires installation of additional transmission devices, like a PLC smart lamp or a traffic concentrator. They disturb communication process by generating number of random PLC packets or by changing PLC packets that arrive to their PLC modems and transmit to other PLC nodes. These devices have an impact on routing protocol used in the examined network. They disturb routing mechanism between the PLC lamps connected to a common PLC transmission medium. This kind of activity has an influence especially on communication process and traffic features connected to data link and network layers.

- Testing methodology 3

Another type of attack also requires a necessity of adding additional devices. In this case an untrusted PLC device copies the received packets and transmits them with certain delay to other PLC nodes or to different segments of PLC communication network.

Another way of usage for these additional/untrusted PLC nodes is creation of additional communication tunnels and transmission of the received PLC packets to another untrusted device. Such a tunnel also has an impact on communication reliability between smart lamps and an influence of this attack type can be observed not only in data link or network layers but also has indirect impact on some data connected to application layer that is used by maintenance services of Smart Lights communication network.

Taking into consideration all the described anomaly/attack methodologies and traffic features presented in Table 1, we collected cumulative results of detection rate and false positive values in Table 2. For all 13 PLC traffic features detection rate DR[%] changes from 97.68% for LFP2 feature to 83.43% for LFP6, while false positive values were in range from 2.41% to 5.32%. We have to mention here that the proposed algorithm belongs to anomaly detection class solutions where we try to recognize

unknown attacks or other anomalies whose false positive values are higher than in Intrusion Detection Systems IDS and where we recognize known attacks with already described signatures of attack behaviour. In anomaly detection system for IoT solutions, values of false positive are usually less than 10% [Garcia-Font, 17][Miao, 11][Cheng, 15]. The worst false positive values were achieved for LFP6 (5.32%) traffic feature, while the best false positive parameter we achieved for LFP2 feature (2.41%).

SLCN feature	**Detection Rate DR[%] for a given traffic feature**	**False Positive FP[%] for a given traffic feature**
LFP1	97.54	3.62
LFP2	97.68	2.41
LFP3	96.44	4.24
LFP4	95.86	4.43
LFP5	93.26	4.65
LFP6	83.43	5.32
LFP7	85.27	5.23
LFP8	96.86	3.71
LFP9	96.72	4.32
LFP10	95.67	4.15
LFP11	97.46	4.55
LFP12	95.63	4.54
LFP13	94.47	5.16

Table 2: Anomaly and attack detection results achieved for the examined PLC networks

When we take into consideration the achieved results (Table 2), we can observe for example influence of first testing methodology (where we have influence on physical parameters of PLC transmission) on more than one traffic feature. When SNR values degrades (LFP2) than we can observe impact on, for example, LFP3 (PERLF: packet error rate per time interval), LFP1 (RSSILF: received signal strength indication for PLC lamps) and LFP9 (NPRLF: Number of packet retransmissions by means of PLC communication) traffic features.

Another coincidence we can observe also when we take into consideration testing methodologies 2 and 3. Such an attack/anomaly simulation has especially direct impact on data link and network layer features (for example LFP3 – LFP10) and indirect impact on application layer features LFP11 – LFP13. Interferences caused by testing methodologies 2 and 3 have an impact on communication reliability between smart PLC lamps and on routing protocol used for the examined network. When smart lamps did not receive proper settings or they lost communication to other communication nodes in SLCN network, a PLC lamp switches to maximum luminosity operation. That is why we can observe indirect impact on application features like LFP11 (MLOLF: maximum luminosity operation time for a given PLC lamp) and LFP13 (PC: power consumption by PLC lamp in [Wh]).

The proposed anomaly/attack detection algorithm gives us promising results thanks to the used machine learning techniques, like LSTM neural network and proper pre-processing and postprocessing of selected traffic features. Its application to Smart Lights network will help to improve reliability of SLCN implementation. In consequence the proposed solution helps to increase public transport safety by higher immunity on anomaly/attacks or improved maintenance in case of Smart Light network infrastructure damage or failures.

6 Conclusions and Future Work

The key element of every Smart City is a system of monitoring and managing urban infrastructure, in particular smart systems steering street lighting. They enable optimal management of lighting facilities and significantly limit the amount of consumed electric power. However, to ensure proper level of security and protection of the signal transmitted therein, they require special care about safety of critical communication infrastructure. The most often implemented mechanisms to ensure the mentioned safety are methods of detection and classification of abnormal behaviors reflected in the analyzed network traffic. An advantage of such solutions is lack of need for prior defining and memorizing patterns of such behaviors, i.e. abuse signatures. Therefore, in the decisive process, it is only necessary to determine what is and what is not abnormal behavior in network traffic in order to detect a possible unknown attack or abuse.

It is known that SLCN networks due to their nature are currently subject to increasing number of threats originating both outside and inside their own communication infrastructure. Severe security problems inside the SLCN network are usually dangers coming from intruders aiming at performing destructive activities directed onto the SLCN infrastructure, consisting in interrupting correct operation or hampering transmission of the steering signals. However, the key security problem is ensuring proper level of protection against external abuses, i.e. safeguard from cyberattacks. In such situation, every not properly secured element of the SLCN infrastructure can possibly become a subject of such an attack.

In this article we presented effective solutions concerning different types of anomalies (abuses) reflected in the analyzed network traffic for critical SL infrastructure. We also proposed and discussed a structure of a SLCN network constructed for the purpose of this experiment based on PLC technology. Key security problems were discussed along with their direct impact on correct operation of critical SL infrastructure. Then, there was proposed an efficient and effective method of anomaly detection in the examined SL network traffic represented by suitable time series. At the initial phase of the proposed solution, we identified and further eliminated outlying observations with the use of criterion based on one-dimensional quartile criterion. Data prepared in such manner was used for neural networks' recurrent learning in order to forecast vales of the analyzed time series. We also proposed a procedure of recurrent learning of the used neural networks in case permanent changes occur in the nature of the SLCN network traffic. To detect abnormal behavior which can be symptomatic of an abuse attempt, e.g. a network attack or unauthorized interference in SLCN infrastructure, relations between the forecasted network traffic and its real variability were examined.

As a result of research and experiments we achieved promising results of detection rate and false positive values from 97.68% for LFP2 feature to 83.43% for LFP6 while false positive values were in range from 2.41% to 5.32%. Such results cause that the proposed algorithm can be useful for Smart Lights Communication Network for anomaly detection and to shorten maintenance procedures in case of infrastructure failure. Further works can be conducted in direction of learning process improvement by automatic selection of the most representative parts of time series used for supervised learning process. There can also be investigated a possibility of hybrid algorithm usage in order to take advantage of the best features of different types of machine learning algorithms.

References

[Barford, 02] Barford, P., Kline, J., Plonka, D., Ron, A.: A signal analysis of network traffic anomalies, Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement. ACM, 71–82, 2002.

[Bengio, 94] Bengio, Y., Simard, P., Frasconi, P.: Learning long-term dependencies with gradient descent is difficult, IEEE Transactions Neural Networks, 5(2),157–166, 1994.

[Bhuyan, 14] Bhuyan, M., H., Bhattacharyya, D., K., Kalita, J., K.: Network anomaly detection: methods, systems and tools, IEEE Communications Surveys & Tutorials, 16(1), 303–336, 2014.

[Brownlee, 18] Brownlee, J.: Long Short-Term Memory Networks with Python, Develop Sequence Prediction Models With Deep Learning, Machine Learning Mastery, 2018.

[Brownlee, 19] Brownlee, J.: Deep Learning for Time Series Forecasting, Predict the Future with MLPs, CNNs and LSTMs in Python, Machine Learning Mastery, 2019.

[Castro, 13] Castro, M., Jara, A., Skarmeta, A.: Smart Lighting Solutions for Smart Cities, In Proceedings of the 2013 27th International Conference on Advanced Information Networking and Applications Workshops, 1374–1379, Barcelona, Spain, 25–28 March 2013.

[Cheng, 15] Cheng, P., Zhu, M.: Lightweight anomaly detection for wireless sensor networks, International Journal of Distributed Sensor Networks, 3, 2015.

[Chondola, 09] Chondola, V., Banerjee, A., Kumar, V.: Anomaly Detection: a Survey, ACM Computing Surveys, 41(3), 1–72, 2009.

[Elmaghraby, 14] Elmaghraby, A., S., Losavio, M.: Cyber security challenges in smart cities: Safety, security and privacy, Journal of Advanced Research, 5(4), 491–497, 2014.

[Esposito, 05] Esposito, M., Mazzariello, C., Oliviero, F., Romano, S., P., Sansone, C.: Evaluating Pattern Recognition Techniques in Intrusion Detection Systems, Proceedings of the 5th International Workshop on Pattern Recognition in Information Systems, 144–153, Miami, FL, USA, May 2005.

[Garcia-Font, 17] 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.

[Hochreiter, 97] Hochreiter, S., Schmidhuber, J.: Long short-term memory, Neural Computation, 9(8), 1735–1780, 1997.

[Jackson, 99] Jackson, K.: Intrusion Detection Systems (IDS). Product Survey, Los Alamos National Library, LA-UR-99-3883, 1999.

[Kiedrowski, 15] Kiedrowski, P.: Toward More Efficient and More Secure Last Mile Smart Metering and Smart Lighting Communication Systems with the use of PLC/RF Hybrid Technology, International Journal of Distributed Sensor Networks, 2015, 1–9, 2015.

[Lim, 08] Lim, S., Y., Jones, A.: Network Anomaly Detection System: The State of Art of Network Behavior Analysis, Proceedings of the 2008 International Conference on Convergence and Hybrid Information Technology, 459–465, 2008.

[Liu, 12] Liu, J., Xiao, Y., Li, S., Liang, W., Chen, C., L., P.: Cyber security and privacy issues in smart grids, IEEE Communications Surveys & Tutorials, 14(4), 981–997, 2012.

[Macaulay, 12] Macaulay, T., Singer, B., L.: ICS vulnerabilities. In: Cybersecurity industrial control systems SCADA, DCS, PLC, HMI, SIS, Taylor & Francis Group, 2012.

[Miao, 11] Xie, M., Han, S., Tian, B., Parvin, S.: Anomaly detection in wireless sensor networks: A survey, Journal of Network and Computer Applications, 34(4), 1302–1325, July 2011.

[Rajasegarar, 08] Rajasegarar, S., Leckie, C., Palaniswami, M.: Anomaly detection in wireless sensor networks, IEEE Wireless Communications Magazine 2008, 15(4), 34–40, 2008.

[Rinaldi, 01] Rinaldi, S., M., Peerenboom, J., P., Kelly, T., K.: Identifying, understanding, and analyzing critical infrastructure interdependencies, IEEE Control Systems Magazine, 21(6), 11–25, 2001.

[Rong, 13] Rong, J.: The design of intelligent street lighting control system, Advanced Materials Research, 671–674, 2013.

[Rossi, 16] 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, 9-12 October 2016.

[Sample, 13] Sample, Ch., Schaffer, K.: An Overview of Anomaly Detection, IT Professional, 15(1), 8–11, 2013.

[Shiavi, 07] Shiavi, R.: Introduction to Applied Statistical Signal Analysis, Elsevier, 2007.

[Smoleński, 12] Smoleński, R.: Conducted Electromagnetic Interference (EMI) in Smart Grids, Springer, London, UK, 2012.

[Tukey, 77] Tukey, J.W.: Exploratory Data Analysis, Addison-Wesley, Boston, 1977.

[Wang, 16] Wang, Y., Gamage, T., T., Hauser, C., H.: Security Implications of Transport Layer Protocols in Power Grid Synchrophasor Data Communication, IEEE Transactions on Smart Grid, 7(2), 807–816, 2016.

[Wu, 10] Wu, Y., Shi, C., Zhang, X., Yang, W.: Design of new intelligent street light control system, Proceedings of the 2010 8th IEEE International Conference on Control and Automation, 1423–1427, June 2010.

[Yau, 17] Yau, K., Chow, K., P., Yiu, SM., Chan, CF.: Detecting anomalous behavior of PLC using semi-supervised machine learning, Proceedings of the 2017 IEEE Conference on Communications and Network Security, 9-11 October 2017.