Hindawi
Security and Communication Networks
Volume 2017, Article ID 7892182, 19 pages
https://doi.org/10.1155/2017/7892182

Research Article

Predictive Abuse Detection for a PLC Smart Lighting Network Based on Automatically Created Models of Exponential Smoothing

Tomasz Andrysiak, Łukasz Saganowski, and Piotr Kiedrowski

Institute of Telecommunications and Computer Science, Faculty of Telecommunications, Computer Science and Electrical Engineering, University of Technology and Life Sciences in Bydgoszcz (UTP), Ul. Kaliskiego 7, 85-789 Bydgoszcz, Poland

Correspondence should be addressed to Tomasz Andrysiak; andrys@utp.edu.pl

Received 23 July 2017; Accepted 19 September 2017; Published 25 October 2017

Academic Editor: Steffen Wendzel

One of the basic elements of a Smart City is the urban infrastructure management system, in particular, systems of intelligent street lighting control. However, for their reliable operation, they require special care for the safety of their critical communication infrastructure. This article presents solutions for the detection of different kinds of abuses in network traffic of Smart Lighting infrastructure, realized by Power Line Communication technology. Both the structure of the examined Smart Lighting network and its elements are described. The article discusses the key security problems which have a direct impact on the correct performance of the Smart Lighting critical infrastructure. In order to detect an anomaly/attack, we proposed the usage of a statistical model to obtain forecasting intervals. Then, we calculated the value of the differences between the forecast in the estimated traffic model and its real variability so as to detect abnormal behavior (which may be symptomatic of an abuse attempt). Due to the possibility of appearance of significant fluctuations in the real network traffic, we proposed a procedure of statistical models update which is based on the criterion of interquartile spacing. The results obtained during the experiments confirmed the effectiveness of the presented misuse detection method.

1. Introduction

In the last decade, digital technologies started to cover cities, creating a skeleton of immense intelligent infrastructure based on information and communication technologies (ITC). The aim of building such a ubiquitous system is to create Smart Cities (SC), which have the ability to manage their resources in a better way to enhance the quality of life and safety of their citizens.

One of the key elements of a Smart City is a system of management, monitoring, and smart steering of street lights. This system allows for optimal use of the lighting infrastructure and facilitates reduction of lighting operating costs. It mostly involves prolonged operation of light sources and, as a result, a less often need to exchange them, which is costly. A decrease in the consumption of electric energy also causes limitation of CO_2 emission. Data presented in [1, 2] show that, in the recent decade, approximately 20 per cent of the received electricity is consumed by lighting, where the biggest share concerns roads and streets. Reduction of energy consumption thanks to the use of energy-saving light sources and introduction of Smart Lighting (SL) is performed in numerous ways, of which the most important are (i) reduction of the intensity of light in a given time and space, (ii) switching on and off the lamps precisely in time, and (iii) taking into account the variable capacity of light sources in long-term operation. Utilization of such type of activities ensures optimization of light management costs and limits the electricity consumption costs even up to 40 per cent.

Usually, the Smart Lighting system is an extension of already existing traditional lighting systems. Its implementation is based on installing controllers/drivers in every lamp. The controllers communicate with the steering server via an existing energetic network with the use of LonWorks protocol

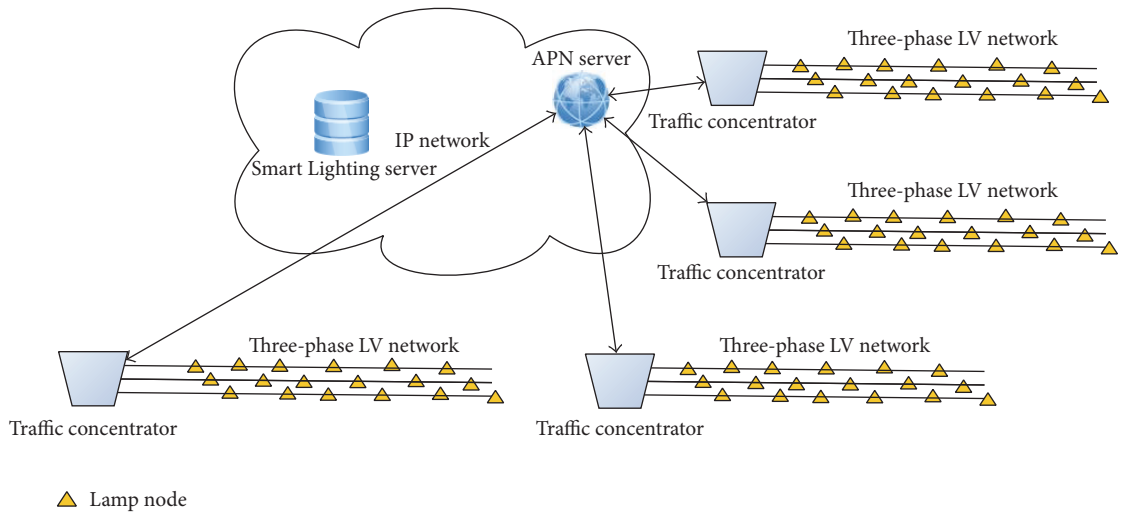


Figure 1: Smart Lighting critical infrastructure.

and Power Line Communication (PLC) technology. The steering server safely communicates through a data transmission network with a central management and control system. The central management system facilitates full control over all of the supervised lamps. This allows for configuration of parameters such as scenarios of switching on/off the lamps and time for initiation of the energy-saving function. It also supplies us with information concerning the current performance of the infrastructure, and it reports failures and provides data about lamps which work defectively [3].

In Figure 1, we can see the general block scheme of a Smart Lighting Communication Network (SLCN). The network consists of lamp nodes (yellow triangles) connected by three-phase low-voltage (LV) power mains by means of PLC modems. Traffic from the lamp nodes is received by a traffic concentrator (TC). The traffic concentrator also plays a role of a gateway between the PLC network and the Internet Protocol (IP) network. The Access Point Name Server (APN) allows us to make a connection by means of packet communication (e.g., Long-Term Evolution (LTE)) to the PLC lighting network.

Smart Lighting systems can be classified in two ways. The first way treats them as a subset of Smart City systems, which are further understood as a subset called the Internet of Things. Such classification does not include the whole area of SL application (e.g., it does not contain Road Lighting systems, which in fact are identical to the street lighting systems in terms of communication solutions). Therefore, the authors believe that a better way of classification is to define the Smart Lighting as a part of the Smart Grid (SG) system. This is a result of the fact that the Smart Lighting communication systems, next to Smart Metering (SM), are the biggest communication systems in Smart Grid when it comes to the number of nodes and the size of the geographic area where they operate. The second key similarity is the technologies used in the fields of the last-mile area of those communication systems. In SL, four technologies are applied, namely, PLC, Radio Frequency (RF), General Packet Radio Service (GPRS), and Meter-Bus (M-BUS), while in Smart Metering there are only two: PLC and RF. As far as RF technologies are concerned, in Smart Lighting and Smart Metering, the used solutions are identical. However, in case of PLC, the differences are significant, of which the most important are the following: (i) in terms of SM, the standard PLC interfaces are applied [4], while in case of SL they are not (the existing Digital Addressable Lighting Interface (DALI) [5] has only local use, e.g., steering a few lamps located on the same pole, not to control hundreds of lamps in a lighting course/string); (ii) the SM devices must communicate in Band A according to CENELEC [6], and SL devices must communicate in Band A if the system's operator is an energy supplier, or in Band B, C, or D if it is the receiver of energy; (iii) there is a requirement to encrypt the transmitted information in case of SM, while for SL there is no such obligation.

Even though, on the market, there are PLC chips equipped with encryption modules (mostly AES-128), this function is seldom used. There are numerous reasons for this fact, for instance, (i) bothersome distribution of encryption keys, (ii) extending the transmission frames and thus improving the unreliability and transmission time, and (iii) finally the cost of implementation.

Actions connected with violating the safety rules in Smart Lighting Communication Networks (especially in the last-mile area) may be deliberate or unaware. Unaware interference usually happens when the LV network powers both streets and households, in which there are connected loads that do not meet the standards of electromagnetic compatibility. On the other hand, the deliberate interference in a communication system consists in intentional switching into not only loads not being able to fulfil the norms, but also elements such as capacitors, interfering generators, or terminals emulating a hub. Switching such devices even into the LV networks dedicated only to lighting is not difficult; therefore, an intruder may use them imperceptibly for a longer period of time.

There are different reasons why the smart lights operator needs anomaly and intrusion detection for the PLC smart lights network. In case of attacks, the smart light operator is responsible for proper operation of the PLC smart lights network. The smart lights network operator is also responsible to the customer in case of improper network operation and may be exposed to penalties. Intentional and unintentional damage cause additional costs to the operator when the attacker changes smart lights to ones instantly on with maximum luminosity. Reaction on anomalies in the smart lights network is also important for public transport safety (especially in intersections) when the attacker might switch off entire segments of the PLC smart lights network. Switching lights off may also be responsible for decreasing public safety in areas where smart lights are off by an attacker. Due to similar reasons, energy suppliers use anomaly and intrusion detection systems in Smart Grid networks especially for detecting energy thefts. Energy operators detect abuses in, for example, WSN (Wireless Sensor Network) smart meter infrastructures [7].

In our system, we propose a solution concerning detection of different types of abuses in the network traffic for the SL infrastructure, which is based on automatically created models of exponential smoothing. To detect abnormal behavior that may be a symptom of possible malpractice, we counted the values of variance between the forecast in the estimated model of traffic and its real variability. In the abovementioned process, we used a two-step method of abuse detection. In the first step of the proposed solution, we identified and then eliminated outliers using the criterion based on Mahalanobis's distance. In the second step, however, we estimated proper statistical models smoothed exponentially for the analyzed network traffic parameters. As a result, the respective operations presented differences in the tested SLCN parameters, which point at possible occurrence of malpractice.

The article is organized as follows. After the Introduction, Section 2 describes the communication protocol used in the last-mile testbed network. Next, Section 3 presents related work on existing abuse detection solutions for Smart Lighting Communications Networks. Section 4 focuses on the main security risks related to the PLC network. Section 5 presents the structure and operation of the proposed solution. In Section 6, a real-life experimental setup and experimental results are presented and discussed. Finally, Section 7 concludes our work.

2. Communication Protocol Used in the Considered Solution

A communication protocol in last-mile Smart Lighting networks was proposed in 2010 and published in 2011 in [8] as EGQF protocol (Energy Greedy Quasi-Flooding) by one of the coauthors. In the same year, this protocol was implemented in Smart Metering networks, which used a low-power RF technology for communication. The EGQF protocol is independent of communication media types and may be applied in networks using RF, PLC, or even RF/PLC hybrid technologies. This protocol is dedicated to tiny communication nodes based on short distance devices connected to shared communication mediums. It uses the multihop technique for transmission range extension and also uses the multipath technique to improve reliability of data transfer. The multipath scheme is useful for delivering data in unreliable environments, such as PLC. The retransmission mechanism is used only by the destination node, without any extra RAM memory occupation, because the RESPONSE packet is already kept in the transmission buffer of a transceiver. The decision to launch the retransmission is as follows: after sending the RESPONSE, the destination node starts a retransmission timer. After the timer expires, the destination node sends RESPONSE again and stops the timer. This timer can also be stopped if a copy of RESPONSE or ACK/Cancel is received during the period of the timer's operation. The number of retransmissions is reduced by a protocol parameter, RC (Retransmission Counter). In our experiments, RC was set to 1. The architecture of the presented network is very simple because it can operate with only two types of nodes, that is, a traffic concentrator and a terminal (a lamp). All the traffic is forced and coordinated by the traffic concentrator. Due to the lack of memory, terminals do not know the network topology and even do not know the addresses of neighboring nodes.

The EGQF protocol uses a small set of packet types, that is, command packets, response packets, and ACK/Cancel packets. Command packets, in most cases, are used by the traffic concentrator for controlling or querying the lamp or the pole. The answer or acknowledgement from the lamp is transported over the response packet. The ACK/Cancel packet is a packet which acts as the low layer ACK for the destination node and as the relaying process canceler for the other nodes. The ACK/Cancel packet is sent only by the traffic concentrator to confirm the reception of the response and to cancel the flooding process of response, or even command copies. The relaying process in nodes, which are neither destination nor source nodes, depends on transmitting the copy of the packet after the sum of constant short time (60 ms) and random time in the condition of an undetected carrier. The difference between the typical flooding protocol and the EGQF protocol is that while using a typical flooding protocol, the nodes always send a copy of the packet once, whereas while using the EGQF protocol, copies are sent as often as needed, for instance, once, twice, or never. The decision of whether a copy of the packet should be sent is made when the transfer discriminator value of the packet is greater than the previously stored one. The initial (or set at the end of the process) transfer discriminator value is zero. The transfer discriminator consists of two fields organized in the following order: the packet type code and the time-to-live (TTL) counter. The TTL occupied three least significant bits of the control field of the packet, while the packet type code occupied two more significant bits in the same field. Commands are coded as 00, responses as 01, and ACK/Cancel as 11, so that the transfer process of the command packet is always canceled after receiving a response packet. This is the same as response packet propagation after receiving ACK/Cancel. The above cases show us a situation where the

relaying process was canceled, which is a difference with regard to the typical flooding protocol. The solution adopted in EGQF reduces the risk of collision. Using the same schema, it is possible to send a copy of the same packet type more than once. Such situation occurs when, after sending the copy of the packet, the same packet is received again with a greater value of TTL than the already copied packet. This situation occurs very seldom (e.g., when a packet with a greater number of hops comes earlier than a packet with a smaller number of hops), and it increases reliability [9].

3. Related Work

Every administrator of a Smart Lightning network or a safety specialist would like to be timely informed about any nontypical behaviors in the infrastructure that he is in control of (whether they are connected to attacks, abuses, or improper performance of devices or applications) [10]. The most important issue is to aim for the detection of new threats and such hazards that would break through the traditional defense mechanisms. One of the possible solutions is the use of systems based on Network Behavior Anomaly Detection (NBAD) [11]. These solutions do not utilize knowledge about the attacks'/abuses' signatures [12] but they are based on behavioral analysis [13]. Such an approach allows for the detection of numerous threats, which "manifest" their presence with nontypical behaviors in the network [14].

Generally, NBAD systems use statistical profiles or behavioral models to detect potential threats/anomalies. Most often, the model approaches are autoregressive ones, for example, AutoRegressive Moving Average (ARMA) or AutoRegressive Fractional Integrated Moving Average (AFIMA) [15], or mixed models composed of autoregressive and exponential smoothing ones [16] (combined to improve the forecasting process). There can also be found solutions applied to anomaly detection in the network traffic, which are based only on traditional, exponential smoothing models [17]. However, all those approaches do not use the processes of optimization to find defined exponential smoothing models, best matching the input data. In the subject literature, there can also be found other works (theoretical ones in particular), that is, Gardner [39, 40], Ord and Lowe [20], or Archibald [41], describing procedures of automatic prediction of future time series' values, based though on defined exponential smoothing models. In the solution proposed by us, we use a mathematical methodology presented by Hyndman [38, 43] which depends on seeking an optimal model (in the process of nonlinear optimization) and automatic procedure of prediction to find the future values of the analyzed time series. Then, detection of anomalies consists in comparing the variability of the real, time series' values with the estimated model of that traffic. Such a solution has not been yet used for anomaly/abuse detection in the Smart Lightning network traffic.

However, exhaustive description of methods and techniques of detection of anomalies and/or outlier observations can be found in review articles [14, 24]. They describe diverse approaches to anomaly detection, starting with machine learning methods, through data mining and information theory, and finishing on spectral solutions. Nevertheless, analysis of those solutions should be conveyed in close connection with their application.

Extensive research has been conducted on security in Smart Grids; most of them are done for anomaly detection in backbone networks and/or all areas of networks based on TCP/IP or UDP/IP protocol stack [25]. Not only does anomaly detection in LV network concern Smart mMtering systems, but also data transmitted over the LV network must be encrypted. In Smart Lighting systems, there are no security requirements for the transmitted data. Most works focus on data transfer reliability [26] in Smart Lighting last-mile communication networks, which is realized by using two independent technologies, for instance, PLC and wireless. In this work, the authors proposed a decentralized method of anomaly detection, similar to the one in [27], but the difference is that our method is proposed for Smart Lighting systems, not for Smart Metering.

In spite of that, we did not find anomaly/attack detection publications for Smart Lighting PLC based networks; there are different methods of anomaly detection used in Wireless Sensor Networks (WSN) or Smart Metering networks. In general, the anomaly detection methods used so far for sensor networks (especially for WSN) were divided into [18, 19] statistical methods (e.g., statistical chi-square test, kernel density estimator), signal processing methods (e.g., based on frequency analysis like Discrete Wavelet Transformation (DWT)), data mining (e.g., clustering methods like K-means, Support Vector Machines (SVM)), computational intelligence (e.g., Self-Organizing Maps (SOM)), rule-based methods, graph based methods (e.g., tree construction), and hybrid methods [18, 19, 21]. Part of the anomaly/attack detection methods work in lower protocol layers (e.g., data link layer or network layer) while others are focused on the application layer (especially for the Advanced Metering Infrastructure (AMI) used by energy operators).

4. Security Risks in PLC Smart Lighting Communication Networks

In Smart Cities, security of critical infrastructures is essential for providing confidentiality, accessibility, integrity, and stability of the transmitted data. The use of advanced digital technologies (ITC), which connect more and more complicated urban infrastructures, is risky because there may appear different types of abuses which may hamper or completely disenable proper functioning of a Smart City. Undoubtedly, one of the biggest frailties of a Smart City is the Smart Lighting system when taking into account the size of the area where it functions, potentially big number of the system's devices, and the generated operational costs. Therefore, providing a proper level of security and protection becomes a crucial element of the SLCN solutions [28].

The task of a Smart Lighting system is not only to light the streets. Depending on the kind of pavement, it must control the brightness of the lighting, its dimming, homogeneity, and reflectivity, providing drivers and pedestrians with maximum safe visibility. Therefore, lighting installations with

luminaires, which are used as light sources, must be easily controllable. Such controlling may include whole groups or even individual lamps, which may be turned on or off according to a specified schedule or dimmed up to any degree at specified times, and the state of individual devices must be easy to control. In comparison to a traditional autonomic lighting system, Smart Lighting solutions are characterized by much bigger functionality and flexibility; however, due to their intelligent nature, they may be liable to different types of abuses (attacks). Such actions may be realized by both the sole receiver of the service and intruders wanting to enforce a specific state of infrastructure [29].

The receiver most often causes destructive actions to the SLCN, which interfere with the transmission of control signals (by active or passive influence) to achieve a change in period and/or intensity of the light. Increasing the intensity of lighting in front of the receiver's property allows for switching off the light on his land, which may result in significant economic benefits. However, a much bigger problem seems to be protection against intended attacks. There are numerous reasons for performing such attacks, the main one being to disturb the controlling system in order to set a different value of lighting than the one established by the operator. Switching off the light or reduction of its intensity in some area may facilitate criminal proceedings. Another reason is malicious activity consisting in hindering the lives of neighbors or local authorities by forcing a change in the schedule of lighting (e.g., switching off the light at night or turning it on during the day). However, a much more serious challenge seems to be protection against attacks realized for criminal purposes. Then, every potential Smart Lighting lamp may become a point by means of which an attack on SLCN may be performed [10].

Such actions, in particular in the area of the last mile, may have a conscious or unconscious nature. The unconscious interference most often happens when the LV network feeds both the streets and the users' households, where the included loads do not meet electromagnetic compatibility standards. The conscious form of interference in the communication system is related to deliberate activity that consists in switching into the SLCN infrastructure such elements as capacitors, interfering generators, or terminals emulating a hub. Loading such devices, even in LV networks dedicated only to lighting, is not difficult, and using them by an intruder may remain unnoticed for a longer time.

Smart Lighting network security and protection from such attacks seems to be a harder task to solve than the prevention of possible abuses (to achieve quantifiable but limited economic benefits) from the receivers' side.

Attacks on Smart Lighting Communication Networks can be divided into two basic categories: passive and active. Passive attacks are any activities aiming to gain unauthorized access to the data or SLCN infrastructure, for which the attacker does not use emission of signals that may disturb and/or disenable correct performance of the signal. Active attacks, on the other hand, are all the attempts of illegal access to the data or the SLCN system's infrastructure by means of any signals or realization of any actions which may be detected [30].

Realizing a passive attack on the SLCN, the intruder camouflages one's presence and attempts to gain access to the transmitted data by passively listening to such a network. It is most often realized by switching into the network additional node which has similar functionalities to the original one. In such situation, we can distinguish three cases: (i) pretending to be a hub, (ii) pretending to be a particular lamp, (iii) or participating only in transferring frames in the transmission process.

To provide protection from such events, appropriate cryptographic mechanisms are most often used. Another kind of passive attack on the SLCM is activities for analyzing the traffic inside the network. In this case, the intruder's intention is not to know the content of the transmitted packets of data, but to get topological knowledge enabling the learning of the structure of the attacked network.

Contrary to the above presented passive forms of attacks on the SLCN infrastructure, in case of realization of an active attack, the intruder influences indirectly or directly the contents of the sent information and/or functionality of the system. Attacks of this kind are much easier to detect in comparison to the passive ones, because they cause visible disturbances in the SLCN performance. An effect of conducting an active attack may be degradation of a specific service or, in extreme cases, complete loss of control over the whole or some part of the SLCN infrastructure.

Due to the form, purpose, and manner of realization, active attacks can be divided into three types: (i) physical attacks aiming at destroying and/or disturbing correctness of the SLCN's node operation by means of an electromagnetic pulse (EMP), (ii) attacks on integrity and confidentiality of the transmitted data, and (iii) and attacks oriented onto particular layers of the SLCN (especially for the provided services).

Physical attacks are all kinds of destructive activities whose aim is to completely destroy or damage the SLCN infrastructure. One of their forms may be activities performed by means of an electromagnetic pulse (EPM) or injecting high pulse distortion into the power supply network [31].

Attacks directed onto the integrity or confidentiality of data, however, are especially dangerous, because they enable the attacker to gain unauthorized access to the information transmitted via the SLCN. This type of attack was presented in [32].

Another kind of attack in the SLCN consists in overloading the attacked network infrastructure, which is visible in the lack of correct data transmission or disenabling access to specific services. Such actions are usually realized by introducing to the network bigger traffic than can be served. They can also have other forms; for instance, they can occur in the physical layer performing jamming activities, and in the layer of data link they can flood the network with packets, causing as a result a collision of data and a necessity to retransmit them. The simplest way to perform such an attack is to connect an additional capacitor to the power circuit. This will cause suppression of the PLC modem carrier signal. Another method is to load into the SLCN a generator broadcasting in the transmission band of the system, which

causes reduction of the signal/noise gap more, rendering a higher level of interfering signal. Reduction of the gap causes then an increase in the number of transmission errors. Another solution is to add any PLC modem, transmitting in the same band that is used by the Smart Lighting system. This solution is a bit more advanced than the use of a generator and causes the modems remaining within the intruder's reach to stay in the "receive" state without the ability to switch to the "broadcast" mode in the period when it transmits, for instance, when it broadcasts without a break or with short breaks [9].

To ensure protection against the above presented threats, especially different kinds of active and passive attacks, it is necessary to provide a high level of security to the critical SLCN infrastructure by continuous monitoring and control of the network traffic. One of the possible solutions to the so-stated problem can be to implement a detection system of anomalies reflected in defined SLCN traffic parameters. In consequence, the detected nonstandard behaviors of specific parameters may indicate a possibility of a given abuse or any other form of attack. The present paper focuses on the above stated question.

5. The Proposed Solution: Predictive Abuse Detection System

For ensuring a high level of security to Smart Lighting Communication Network systems, it is required that they are properly protected by means of passive actions (network monitoring, storing incidents, and reporting) and active actions (constant supervision to enforce the adopted security policy). Realization of the so-stated tasks ensures connection between technologies: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). In the hierarchy of network infrastructure protection, these systems are located just after security elements, such as a firewall.

The aim of the IPS systems is to undertake actions to prevent an attack, minimize its results, or actively respond to violation of security rules. From the technical side, IPS, in big simplification, is an IDS connected with a firewall. As far as topology is concerned, IPS systems can be divided into network solutions based on (i) a passive probe connected to the monitoring port of the switch analyzing all packets in a given network segment (ii) or a probe placed between two network segments operating in a transparent bridge mode that transmits all packets in the network. The basic aim of such solution is to compare between the real network traffic and the remembered attack signatures [12].

However, IDS systems are used to increase the security of the protected network both from the inside and from the outside. Their advantage is that they can be used for network traffic analysis and use diverse threat identification techniques. One of them consists in the detection of known attacks with the use of specified features (signatures), which describe changes in the network traffic. The second, on the other hand, is based on monitoring normal network's performance in order to find deviations from the norms (anomalies), which may indicate a break-in to the protected network infrastructure.

Anomaly detection (abuses) consists in recognition of nonstandard patterns of behaviors reflected in the network traffic parameters. All incidents deviating from those patterns (which are profiles that describe normal behavior of the network traffic) are classified as potentially dangerous and might signify an attempt of an attack or abuse. High efficiency and effectiveness of methods based on anomaly detection are closely related to the ability of recognition of unknown attacks (abuses). These methods operate on the basis of knowledge of not how a given attack runs (what is its signature), but what exceeds the defined network traffic pattern. Therefore, systems based on anomaly detection work better than those using signatures while detecting new, unknown types of attacks (abuses) [14].

In the present article, we propose a predictive abuse detection system for PLC Smart Lighting Networks based on automatically created models of exponential smoothing. Assuming that the correctness of the created statistical model directly depends on the quality of data used for designing it, at the initial stage, we identified and eliminated outlying data by means of Mahalanobis's distance (see Section 5.1). For the so-prepared data, statistical models were created (which constituted patterns) for particular network traffic parameters. This process was realized by means of exponential smoothing methods which, in turn, assume that the future forecasted value depends not only on the last observed value, but also on the whole set of the past values. Simultaneously, the influence of past values (former ones) is weaker than the influence of the newer values, that is, earlier ones (this methodology is further developed in Section 5.2). It should be noticed that the presented assumption agrees with the generally accepted rules of prediction. Bearing in mind the possibility of occurrence of essential real network traffic fluctuations (triggered by natural factors), a procedure of the pattern models' update was proposed on the basis of the interquartile spread criterion (see Section 5.3).

In Figure 2, we presented a block scheme of the proposed anomaly/attack solution for smart lights Power Line Communication networks. The presented solution is spread out across two physical localizations. On the right part of Figure 2, we can see the analyzed smart light PLC network with smart light marked as a yellow triangle connected to different phases of low-voltage power mains. The PLC traffic from different localizations of smart light PLC networks (in our case, we used 3 localizations on different streets) is gathered by the traffic concentrator and repacked into IP packets in order to send PLC network traffic by means of standard IP WAN network to distant locations where we perform anomaly/attack detection steps. We used two routers equipped with different WAN (Wide Area Network) ports or LTE (Long-Term Evolution) modems in order to connect these two localizations by means of dedicated safe connection through VPN (Virtual Private Network).

On the left of Figure 2, we can see the second part of our anomaly/attack detection solution placed on a distant location (in our case, the university building). The proposed solution is divided into two branches. The first branch is responsible for calculation of reference models for PLC anomaly/attack detection purposes. The second branch

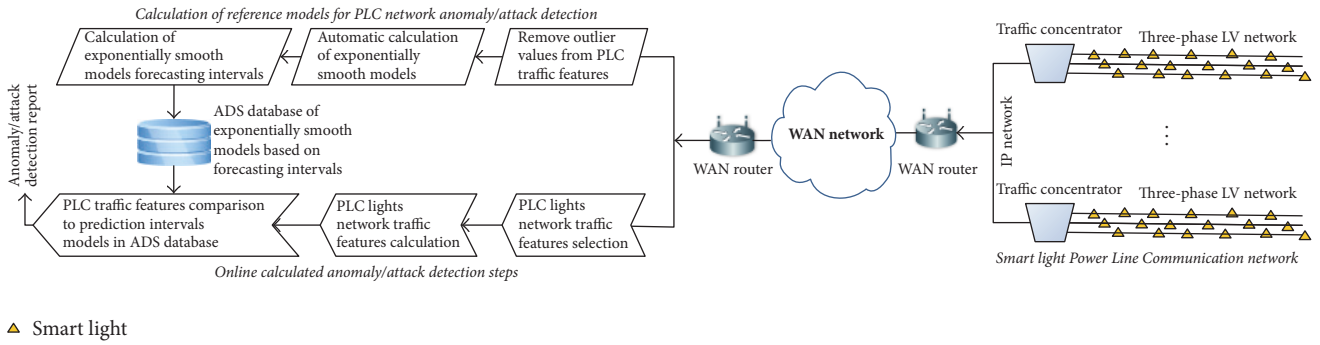


Figure 2: Block scheme of the proposed anomaly/attack solution for smart lights Power Line Communication network.

consists of steps performed online during anomaly/attack detection steps. In order to achieve reference models for PLC network traffic, we extracted traffic features from the PLC network traffic (more details are presented in Section 6.2). After removing outlier values for every traffic feature, we performed automatic calculation of exponential smoothing models and, in the end, forecasting intervals based on these models (details are presented in Section 5.2). Connection between the two branches of the proposed model is realized by means of ADS database where forecasting intervals based on exponential smoothing models are stored separately for every extracted PLC network traffic feature. Additionally, the reference models are updated when necessary to prevent the models from aging in case of changes in, for example, traffic characteristics or physical architecture (by providing additional segments of PLC smart light network). Recalculation of the model is controlled by a trigger condition presented in more detail in Section 5.3.

The second branch of the proposed model also consists of selection and calculation of the PLC network traffic features (see Section 6.2). PLC network traffic features are sampled and calculated with fixed time intervals, appropriate for smart light networks. In order to detect anomalies, we compare online calculated traffic features to prediction intervals read from the ADS database where the prediction intervals based on exponential smoothing models are stored. When the online calculated traffic features are outside the prediction intervals estimated by the model, we generate an anomaly detection report for a given traffic feature (more details are provided in Section 6).

5.1. Outliers Detection and Elimination Based on the Mahalanobis's Distance. The quality of a statistical model directly depends on the quality of data used to design it. The values of variables describing observations in actual datasets are often outlying (not typical). This is due to the specifics of the examined phenomenon or different kinds of errors. The outlier observations may have a very strong influence on the results of analysis and therefore they require special attention.

The notion of outliers is not directly defined in the literature. In the present work, a general definition, taken from Hawkins's work [33], is used. An outlier is such an observation that deviates from the remaining observations to such an extent that it generates an assumption that it was created by another mechanism; for instance, it comes from a different distribution in the dataset. It is worth noticing that, according to the above definition, such emergence indicates not fulfilling one of the most basic assumptions concerning the analyzed dataset, namely, that it is an i.i.d. set (independent and identically distributed). In that case, occurrence of an outlier means that it comes from a different distribution and should not be analyzed with other elements of the examined set of data.

Analyzing particular elements and the operational environment of Smart Lighting Communication Networks, it becomes obvious that there may appear real possibilities of considerable fluctuations of the analyzed network traffic parameters (and, as a consequence, emergence of outliers). These fluctuations may have diverse sources, for instance, (i) environmental, connected with interruptions caused by high-energy electromagnetic pulse; (ii) technical, related to changes in the infrastructure; (iii) devices' damage; (iv) as a consequence of a network attack; or (v) intentional, unfair interference in the SLCN infrastructure. Thus, an important element of the preliminary analysis of data should be the evaluation of the impact that particular observations may have on the final result, and in case of detection of outliers they should be deleted from the set of data.

In our approach, identification of outliers in the analyzed SLCN traffic parameters is performed by means of a method utilizing Mahalanobis's distance. The essence of this method lies in the estimation of the distance between the analyzed observation vector x and the average value in the examined dataset based on the calculated matrix of variance and covariance [34]:

$$MD^2(x) = (x - \hat{\mu})\,\hat{\Sigma}\,(x - \hat{\mu}), \tag{1}$$

$$\hat{\Sigma} = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \hat{\mu})(x_i - \hat{\mu}), \tag{2}$$

where $\hat{\mu}$ is the average value from the analyzed dataset and $\hat{\Sigma}$ is the matrix of variance and covariance.

To underline the generality of our method, we left the original Mahalanobis's measure matrix record (the case of multiple regression); however, with time series, we have a one-dimensional case. Identification of outliers is performed by comparing Mahalanobis's square distance for each of the

observations with critical values taken from χ^2 distribution. If there are significant differences (at an accepted level of importance), the given observation is treated as an outlier. This approach has one drawback though; namely, the value of the criterion (1) itself directly depends on statistics which are very sensitive to the occurrence of distant values. To eliminate this disadvantage, modifications were proposed for calculating the meter (1) by exchanging the average $\widehat{\mu}$ with a resistant positional parameter. One of the proposals is the use of Minimum Volume Ellipsoid Estimator (MVE) [35]. In this case, $\widehat{\mu}$ takes the value of the center of gravity of the ellipsoid with a minimum volume containing at least h observations of a given set, where $h = (n/2) + 1$, and n is the complete set of elements of the analyzed dataset. The second proposal is to designate a positional parameter $\widehat{\mu}$ in formula (1) according to the following rule [35]: $\widehat{\mu}$ is an average from these h observations of the given set, for which the determinant of covariance matrix is the smallest. Such a resistant positional estimator is called Minimum Covariance Determinant (MCD) estimator. The third approach suggested in the paper [36] uses the analysis of main components and identifies the distant observations just after transformation of all observations in space of main components by determining in this space Mahalanobis's square distance. The authors of this approach propose, at the stage of preparing analytical data, to standardize the variables by means of a median as a positional parameter and MAD, that is, median absolute deviation, as a dispersion parameter. After using such standardization, calculation of Euclidean distance in space of main components is equivalent to the calculation of the resistant variant of Mahalanobis's distance.

In summary, it is necessary to state that the MD measure modifications presented above are trying to eliminate the basic drawback of the described method, that is, not always reliable inference on the basis of classical statistics, which are very sensitive to the occurrence of nontypical observations. Therefore, to make an optimal choice, numerous experiments were performed on datasets containing the subject parameters of SLCN traffic, for both the original Mahalanobis's method and its presented modifications. As a result of the analysis of the obtained results, that is, the size, location, and number of outliers, for further consideration, we chose the approach proposed by Filzmoser et al. This method uses analysis of main components for identification of outliers and it is further developed in [36].

5.2. The SLCN Traffic Features' Forecasting Using Exponential Smoothing Models. Forecasting is still one of the main tasks of the time series analysis. Construction of those predictions is usually a multistage process, including matching the adequate model on the basis of historical data and evaluation of the quality of this matching (diagnostics). Correct conduct of such analysis requires appropriate knowledge and experience. It is usually also time-consuming, which may become an obstacle when it is necessary to collect forecasts for numerous time series simultaneously. Thus, in practice, there is a natural need to automate this forecasting.

In case of some stages connected to matching the optimal model for data, complete automatization is not possible. Particularly, finding an appropriate compromise between the complexity of the model and the quality of its matching to the data often requires interpretation of the results by an analyst. Automation of the optimal model's choice usually requires adopting some assumptions simplifying the whole process (e.g., defining the statistical criterion, which will be used as a measure of matching quality of the model or the possible ranges of variation of model parameters) [37].

Algorithms allowing for automatic construction of forecasts should realize all the stages of the analysis, that is, (i) the choice of the optimal model for data, (ii) parameters' estimation, and (iii) the forecasts' construction (point and/or interval). While searching for an optimal model, it is important to use proper criteria which will protect from too good matching of the model to the learning data, which in turn may lead to bad quality of forecasts for the new periods. The algorithms should also be resistant in case of occurrence (in the analyzed time series) of outlier observations, or they should be equipped with mechanisms of their detection and elimination. Additionally, the algorithms should be easily used for a big number of diverse time series without the necessity of an analyst's interference, and they should be characterized by acceptable computational complexity [20].

One of the possible solutions to the so-stated problem of automatic forecasting is the ExponenTialSmoothing or ErrorTrendSeason (ETS) models, which constitute a family of adaptive models developed by Hyndman et al. [38], which uses generalized algorithms of exponential smoothing. Their crucial advantages are simplicity, relatively quick adaptive matching algorithm, and ease of understanding and interpretation of the results. The common denominator of these methods is assigning (exponentially) the weights, decreasing with distance in time, to the past observations during the process of designating a new forecast for a future observation. This is due to the fact that the classical assumptions of the quantitative prediction come down to the postulate of the relative invariability of the development mechanism of the studied phenomena and events. In methods based on ETS, exponential smoothing may be realized by means of different models, properly adjusted to the analyzed data.

When the time series' character and variability are analyzed, it is easy to notice that they are optionally composed of four elements: a trend, seasonal fluctuations, periodical fluctuations, and random disturbances. The seasonal fluctuations usually have an approximately constant period of time, whereas the time of the complete cycle of cyclical fluctuations is usually changeable. Optionally, the components of the analyzed time series may be connected in two ways: additively and multiplicatively [39]. In the exponential smoothing models, the trend is a combination of level c and increment g values. These two components may be connected in four different ways, including the attenuation parameter $\phi \in [0, 1]$. We then obtain diverse types of trends, such as the following [40]:

$$\text{No trend: } V_h = c, \tag{3a}$$

$$\text{Additive: } V_h = c + gh, \tag{3b}$$

$$\text{Multiplicative: } V_h = cg^h, \tag{3c}$$

$$\text{Attenuated: } V_h = cg^{(\phi+\phi^2+\cdots+\phi^h)}, \tag{3d}$$

where V_h describes the character of the trend and h parameter describes the forecast's horizon.

If we take into consideration three possible combinations of the seasonal component with a trend, that is, lack of seasonality, the additive variant, and multiplicative variant, then we obtain twelve exponential smoothing models, which can be written as

$$l_t = \alpha P_t + (1-\alpha) Q_t, \tag{4a}$$

$$b_t = \beta R_t + (\phi - \beta) b_{t-1}, \tag{4b}$$

$$s_t = \gamma T_t + (1-\gamma) s_{t-m}, \tag{4c}$$

where l_t denotes the series level at time t, b_t denotes the slope at time t, s_t denotes the seasonal component of the series at time t, and m denotes the number of seasons in a given period; the values of P_t, Q_t, R_t, and T_t vary according to which of the cells the method belongs to, and $\alpha, \beta, \gamma, \phi \in [0, 1]$ are constants denoting model parameters [38].

The method with fixed level (constant over time) is obtained by setting $\alpha = 0$, the method with fixed trend (drift) is obtained by setting $\beta = 0$, and the method with fixed seasonal pattern is obtained by setting $\gamma = 0$. Note also that the additive trend methods are obtained by letting $\varphi = 1$ in the damped trend methods [41].

The works [42] discuss specific cases of state space models with a single source of error, which may be a basis for some methods of exponential smoothing. Including the possible character of these errors, we may present the state space models for all twelve types of exponential smoothing as follows:

$$Y_t = w(z_{t-1}) + r(z_{t-1})\epsilon_t, \tag{5a}$$

$$z_t = f(z_{t-1}) + g(z_{t-1})\epsilon_t, \tag{5b}$$

where $z_t = [l_t, b_t, s_t, s_{t-1}, \ldots, s_{t-m+1}]^T$ denotes the state vector, $w(x), r(x)$, $f(x)$, and $g(x)$ are continuous functions with continuous derivatives, and $\{\epsilon_t\}$ is a Gaussian white noise process with mean zero and variance σ^2, and $\mu_t = w(z_{t-1})$ [42]. The error ϵ_t may be included in the model in an additive or multiplicative way. The model with additive errors has $r(z_{t-1}) = 1$, so that $Y_t = \mu_t + \epsilon_t$. The model with multiplicative errors has $r(z_{t-1}) = \mu_t$, so that $Y_t = \mu_t(1 + \epsilon_t)$. Thus, $\epsilon_t = (Y_t - \mu_t)/\mu_t$ is the relative error for the multiplicative model. The models are not unique. Apparently, any value of $r(z_{t-1})$ will lead to identical point forecasts for Y_t [38].

From the twelve exponential smoothing models described by dependency (4a), (4b), and (4c) after including the additive and multiplicative error ϵ_t, we obtain 24 adaptive models in the states' space. The choice of an adequate exponential smoothing model in a particular prognostic task requires the selection of the best form of the model as well as initialization of the z_0 vector's components and parameters estimation $\Theta = [\alpha, \beta, \gamma, \phi]^T$.

It is necessary to calculate the values of z_0 and Θ parameters; otherwise, the models will not be useful for the prognostic process. It is not difficult to compute the likelihood of the innovations state space model (LISSM*) (see (6)); achieving the maximum likelihood estimates (MLE) is similarly easy [38].

$$\text{LISSM}^*(\Theta; z_0) = n \log\left(\sum_{t=1}^{n} \frac{\epsilon_t^2}{z_{t-1}}\right) + 2\sum_{t=1}^{n} \log\left|r(z_{t-1})\right|, \tag{6}$$

where n is the observations' number.

Calculating the above is not difficult when recursive equations are used [43]. Minimizing LISSM* is a procedure used to calculate the parameter Θ and the initial state z_0.

The present model was selected by means of the Akaike Information Criterion (AIC):

$$\text{AIC} = \text{LISSM}^*\left(\widehat{\Theta}; \widehat{z}_0\right) + 2k, \tag{7}$$

where k is the number of parameters in Θ plus the number of free states in z_0 and $\widehat{\Theta}$ and z_0 define the estimates of Θ and z_0. From all the models applicable to the data, we selected the one which minimizes the AIC [44].

The AIC is also a method which enables us to choose between the additive and multiplicative error models. However, there is no difference between the point forecasts of the two models, to make it impossible for the standard accuracy measures, like the mean squared error (MSE) or mean absolute percentage error (MAPE), to differentiate between the error types.

The presented methodology, connected to optimal searching for proper models of exponential smoothing, requires providing some initial values. Usually, the values of parameters α, β, and γ are included in the range $(0, 1)$. However, to avoid the problem with instability, we use a narrower range of parameters, that is, $0.1 \le \alpha \le 0.9$, $0.1 \le \beta \le 0.9$, $0.1 \le \gamma \le 0.9$, and $\beta \le \phi \le 1$. We also limit the values of the initial states z_t of the vector's elements. This is done in such a way that the seasonality indexes were summed up do zero for the additive model and added to m for the multiplicative model. As the initial values in the nonlinear optimization, we use $\alpha = \beta = \gamma = 0.5$ and $\phi = 0.9$.

When we summarize the above ideas, we obtain an automatic forecasting algorithm. It operates in compliance with the following three-stage formula: (i) all proper models are applied to each of the series to optimize the parameters (smoothing the variable's initial stage), (ii) selection of the best matching model according to AIC, and (iii) creation of point forecasts on the grounds of the most effective model (with optimized parameters) for a necessary number of future stages [38].

All the above described kinds of exponential smoothing models are created in compliance with the prediction theory's assumptions, including the ongoing degradation processes (i.e., possible lack of stability in the variable correctness in time). Big flexibility of those models and their adaptive ability in case of irregular changes of the direction of speed of the trend, or deformations and shifts in seasonal fluctuations, make them a comfortable tool for short-term forecasting

and prediction. Hyndman et al. [38, 43] provide a detailed description of the proposed algorithm.

5.3. The Condition of Statistical Model's Update. The process of statistical models' designation on the basis of experimental data is usually a complex task which depends on the knowledge about the object and attributes of the measuring results (observations). The quality of the designated statistical model directly depends on the quality of data used for its estimation.

In the present work, the experimental object is network traffic of an SLCN infrastructure and data characterizing the state of the Smart Lighting system. Both datasets are represented by defined time series. While analyzing the character of the examined dependencies, in particular the SLCN traffic parameters, it is necessary to notice the possibility of occurrence of significant fluctuation of data. The reasons of this phenomenon are to be sought in possible changes in the SLCN infrastructure, that is, aging of devices, replacement with new/other models, or modifications in the topology of the network. Obviously, when the nature of the analyzed data changes, there should be made a new estimation and creation of an updated statistical model on the basis of datasets composed of the subject fluctuations. As a result, this should cause adaptation of the proposed method of anomaly detection to the changing conditions (which are not an aftermath of any attack or abuse).

For the initial data selection, that is, checking if we are dealing with significant fluctuations in the analyzed time series, we use the one-dimensional quartile criterion [45]. For every analyzed set of data, we calculate the first (Q1) and third (Q3) quartiles and the interquartile range (IRQ) IRQ = Q3 − Q1. As influential observations, we accept those whose values exceed the range (Q1 − 1,5IRQ, Q3 + 1,5IRQ). As extremely influential observations, however, we understand those exceeding the range (Q1 − 3IRQ, Q3 + 3IRQ).

In the next step, for every detected influential observation, we check fulfilling the condition of whether it fits the range of forecasts of the appropriate reference model, that is, the following condition:

$$x_i \in \left(\mu_f - \sigma_f, \mu_f + \sigma_f\right) \quad i = 1, 2, \ldots, n, \tag{8}$$

where $\{x_1, x_2, \ldots, x_n\}$ is a time series limited by n-element analysis window, μ_f is the average forecast of the given reference model in the analysis window, and σ_f is the standard deviation of appropriate prognosis.

The estimation condition of the new standard model should be an ability to detect (in the analyzed time series) significant and possibly stable statistic changeability. Therefore, updating the statistical model will be realized when in the analyzed time series over 30 per cent of analysis windows in a weekly period contain observations not fitting the acceptable prognosis range of the appropriate reference model. The above condition is a consequence of the observed dependency that the value of the false positive (FP) parameter of the presented anomaly detection system increases exponentially when in over 30 per cent analysis windows in a weekly period we note significant changeability in data.

Table 1: PLC data link and network layer traffic features extracted from the traffic concentrators.

Network feature	PLC smart lights network traffic feature description
DLN_1	RSSI: received signal strength indication for PLC lamps [dBm]
DLN_2	SNR: signal-to-noise ratio [dBu]
DLN_3	PER: packet error rate per time interval [%]
DLN_4	PPTM: number of packets per time interval
DLN_5	TTL: packet time-to-live value

Table 2: PLC application layer traffic features extracted from the traffic concentrators.

Network feature	PLC smart lights network traffic feature description
APL_1	ENE: power consumption by PLC lamp [Wh]
APL_2	TEMP: lamp temperature [°C]
APL_3	LUL: lamp luminosity level in % (value: 0–100%)
APL_4	NR: number of lamp resets per time interval
APL_5	PS: power supply value [V]

6. Experimental Installation and the Anomaly/Attack Detection Method and Results

In Figure 2, we presented a block scheme which consists of the main steps in the proposed anomaly/attack detection method. In the first step, we extracted the PLC traffic features from two experimental PLC smart lights networks (additional explanation can be found in Section 6.1). There are two main branches in the proposed method: calculation of reference models for PLC network anomaly detection and the second branch consisting of online steps for extraction of traffic features, comparison of traffic features for reference model in ADS reference models database, and generation of an anomaly/attack detection report for a given traffic feature.

Values of the PLC traffic features can be captured in an arbitrary time interval but usually a 15-minute time interval is sufficient for the PLC smart light network. The extracted PLC network traffic features (see Tables 1 and 2) are represented as a one-dimensional time series. In case of a reference model generation, we have to remove suspicious values first by removing outlier values from network traffic features (see Section 5.1). After that step, we can start to calculate exponential smoothing models (see Section 5.2) and in the end exponential smoothing models forecasting intervals. We calculate a separate model for every PLC traffic feature and store them in a database of reference models. The reference models are calculated for a one-week period with a 15-minute resolution window. An example of the calculated forecasting intervals for traffic features can be seen in Figure 3. We can see two prediction intervals for signal-to-noise ratio (SNR) PLC traffic feature. When the online calculated network traffic feature is within boundaries set by two prediction intervals (see Figure 3), we assume that there is no anomaly/attack in

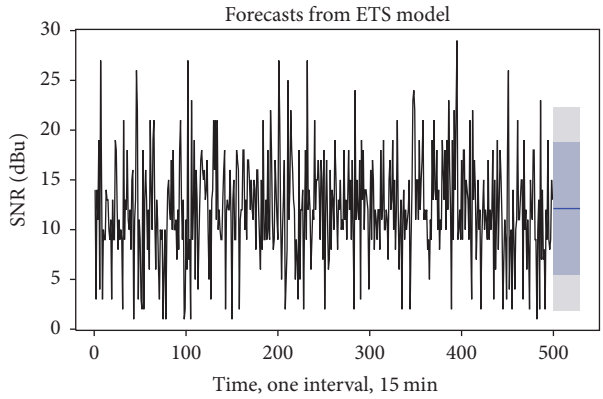


Figure 3: Two prediction forecast intervals (80% narrower, 95% wider) and 30-sample prediction interval calculated with the use of exponential smoothing model (PLC traffic feature, signal-to-noise ratio (SNR) [dBu]).

this case. We expect that 80 or 95% of the values for a given PLC traffic feature will lie inside these intervals (see Figure 3).

The second branch in our anomaly/attack detection method consists of steps calculated online during normal work of the PLC network anomaly/attack detection method. In the first two steps, we extract and calculate PLC lights network traffic features from Tables 1 and 2. Next, for every traffic feature, we check if the online calculated traffic feature values are within the intervals designated by reference models stored in ADS reference database models. When the online calculated traffic features are outside reference intervals, we generate a detection report about possible anomaly/attack triggered by the given PLC traffic feature.

The main issue of the so far proposed anomaly/attack detection conception is the problem of reference models' aging. This phenomenon comes from the fact that the PLC lights network has a dynamic structure. Connecting additional segments of PLC smart lights networks will result in changing of network traffic characteristics and, as a consequence, the necessity of changing reference models. Nonupdated reference models will cause as a result a constant increase of false positive values (FP [%]). To alleviate this drawback, we propose a trigger condition responsible for the recalculation process of the reference models (see Section 5.3 for more details). Reference models are calculated in a one-week period with the use of 15-minute windows. Based on empirical experiments, we recalculate all reference models when trigger conditions (see (8)) are not satisfied in 30% of the 15-minute analysis windows during the one-week period. We started to use new recalculated models at the beginning of the new week (the new model is valid for a minimum of one-week period).

6.1. Experimental Testbed. The analyzed data were captured in two locations: Nieszawska Street in Toruń City (Poland) and University of Technology and Life Sciences (UTP) campus in Bydgoszcz City (Poland). We also used an additional separate Smart Lighting low-voltage LV PLC network testbed constructed during studies in GEKON project [46].

The first PLC network, located in Nieszawska Street, which was dedicated to a Smart Lighting low-voltage LV network, has a length of 3 km (see Figure 4), divided by a traffic concentrator located in the middle of the street. The PLC smart lights network contains 108 lamps (only one lamp is located on every electric pole). Old gas-discharge lamps were gradually replaced by smart LED lights. We used this network for testing traffic concentrators and experiments for detecting anomalies/attacks in PLC traffic.

The second network was placed at the University of Technology and Life Sciences (UTP) campus (see Figure 4). In this case, it was not a dedicated network with a separate power supply (offices, classrooms, and labs were powered by the same power supply network). The testbed in UTP campus consisted of 36 lamps.

Tests were performed in the laboratory (located in UTP campus) with different types and numbers of lamps (gas-discharge lamps and LED lamps). The PLC traffic from both locations was captured from the WAN (from Nieszawska Street) and local network placed in the university laboratory.

6.2. Experimental Setup and Results. In this section, we present the methodology and results achieved for the proposed anomaly/attack detection with the use of exponential smoothing based models. We propose a set of different scenarios for evaluating the usability of the proposed method.

All experiments were carried out by means of two real-world PLC lights networks (see Section 6.1). A part of the testbed located in the university campus can be seen in Figure 5. The picture presents different types of smart lights used in the experiments. Connections between the 36 lamps for the testbed partially presented in Figure 5 are presented in Figure 7. We can see connection schemes between lamps assigned to three-phase power mains with signed possible high-quality and low-quality links. The entire traffic as mentioned earlier is accessible by the traffic concentrator (red rectangle in Figure 7).

Every lamp consists of a PLC modem used for communication, a lamp microprocessor controller, and a power supply. An opened LED lamp with signed internal elements is presented in Figure 6.

The first step in our method requires capturing the PLC traffic from smart lights networks presented in Section 6.1.

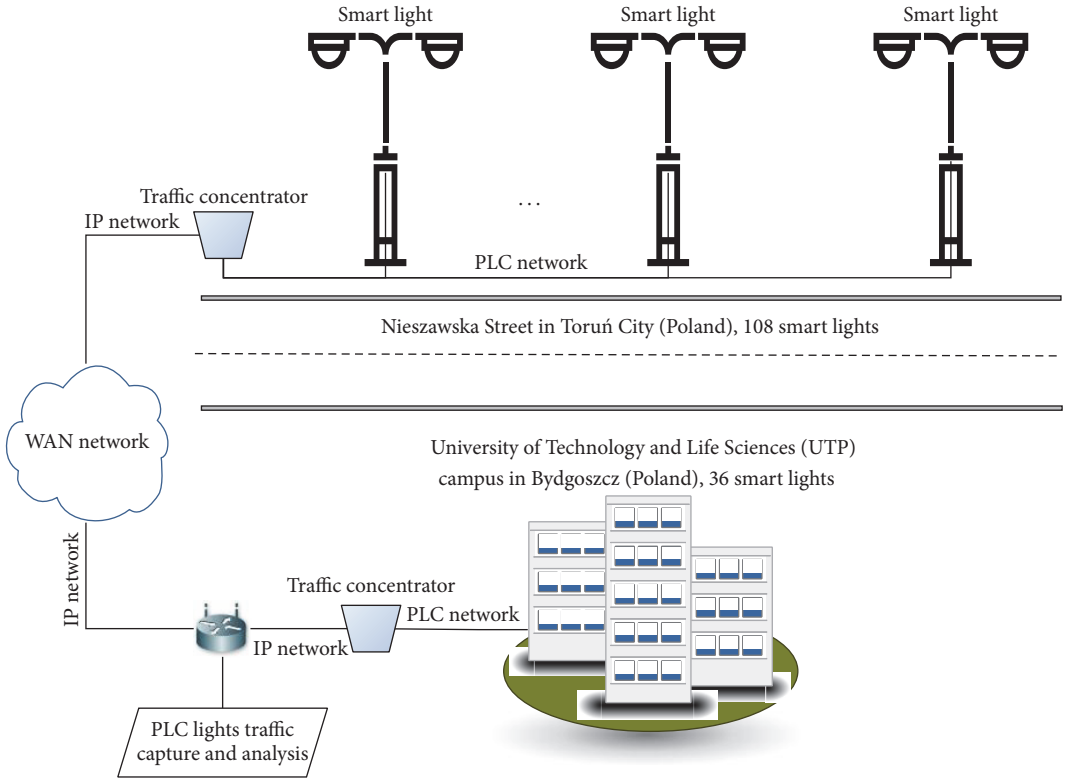


Figure 4: Experimental testbed used for evaluation of the proposed anomaly/attack detection method.

Figure 5: Part of the testbed used for achieving experimental results, located in the university campus.

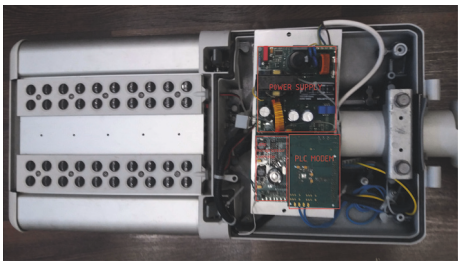


Figure 6: Opened LED smart light used in experiments.

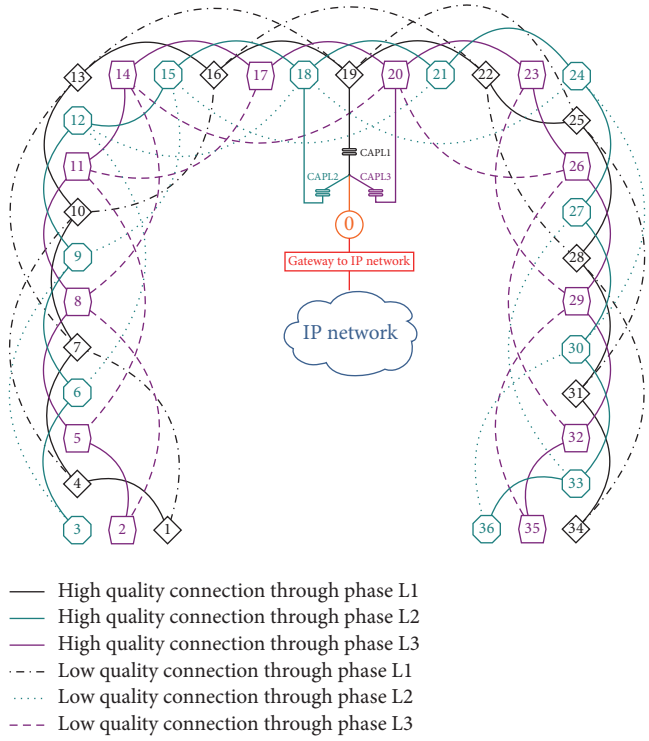


Figure 7: Schematic connection between 36 smart lamps for the testbed located in the university campus.

We collect PLC traffic from traffic concentrators which are responsible for translating the PLC network packets into IP packets. In the next step, we extract the PLC traffic features in order to analyze these features for anomaly/attack detection.

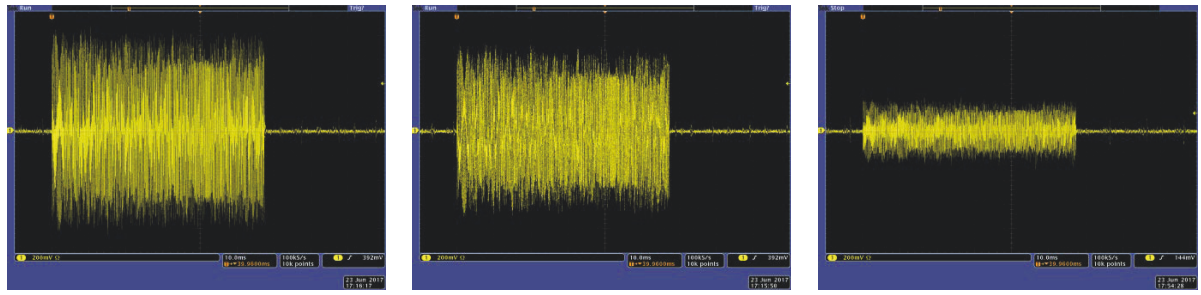
In our experiments, we extracted features that belong to every layer of a PLC protocol stack. In Tables 1 and 2, we can see the extracted PLC traffic features together with explanations.

Traffic features from Table 1 are extracted based on data link and network layers of PLC communication stack. DLN_1 and DLN_2 features give us information about the quality of the received signals transmitted through the power mains. RSSI gives us information about the received signal strength where the signal power may come from any sources (e.g., different modulations, background radiation). RSSI does not give us information about the possibility of signal decoding. SNR [dBu] measure gives us information about the relation between the desired signal and the noise level. DLN_3 traffic feature stands for Packet Error Rate (PER) per time interval. In our case, we used a 15-minute time interval. PER is calculated as a quotient between the number of destroyed packets received by the traffic concentrator and the number of all packets received by the traffic concentrator for a given period of time. DLN_4 feature PPTM stands for the number of packets per time interval. The last feature from layer 2/layer 3 DLN_5 gives us TTL information connected to packets received by the PLC concentrator. In Table 2, there are traffic features extracted from the data payload (application layer) of the PLC packets. The application layer traffic features are connected with parameters used by the energy supplier/operator management staff. APL_1 feature gives us information about power consumption for a given period of time separately for a given lamp. APL_2 carries information about the temperature read from smart lights. LUL (lamp luminosity level, in [%]) feature has values of luminosity sent by the lamp to the traffic concentrator. APL_4 carries the number of lamp resets per time interval (the value is stored in the Static Random Access Memory (SRAM) with backup power provided by a supercapacitor). The last value extracted from the data payload is PS (power supply) in volts [V] which is useful information for maintenance systems.

After PLC network features extraction, we can analyze subsequent traffic features in order to detect possible anomalies/attacks. We propose scenarios (as realistic as possible) in order to evaluate the efficiency of the proposed anomaly detection methodology.

There are different purposes of attacking smart lights PLC networks. First of all, the attacker would like to disturb the control system of a smart light operator in order to change the settings of the lamps parameters. Switching lamps off or lights' intensity reduction for a given area may cause an increase in crime or can be dangerous for car traffic (highest possibility of car accidents especially at intersections). Intentional damage or setting lamps instantly on near selected attacker possessions causes additional financial losses to the operator.

Detecting anomalies is also an important thing for the smart lights operator. The operator will be able to react faster



(a) (b) (c)

Figure 8: Impact (on signal received by the smart light) of 470 nF capacitance connected to the power line: (a) without capacitor, (b) capacitor connected close to the traffic concentrator, and (c) capacitor connected inside the lamp pole.

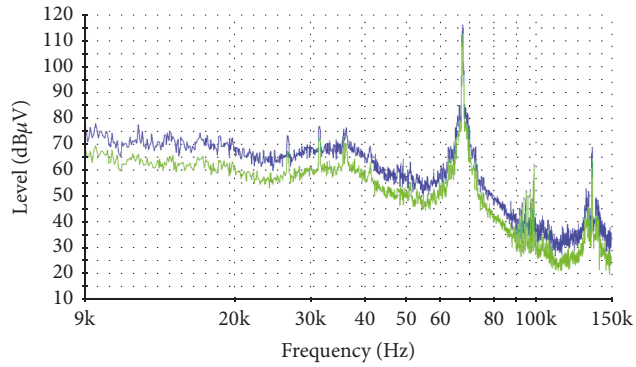


Figure 9: Characteristics of the interference signal generated by damaged notebook switching supply.

on damage, intentional damage, and network attacks, so it will be possible to limit the negative economic and social consequences.

We can divide the proposed scenarios into two main groups: (i) the first type of scenario requires physical access to the PLC network infrastructure in case of attacks on the physical infrastructure of a PLC smart lights network and (ii) the second type of attack requires knowledge about devices used in the PLC network and protocols used in the smart lights network.

Scenario 1. The first type of attack belongs to Group I of attacks. It is an attack on the physical layer and requires connection of a capacitor to the power line. The bigger the value of capacitor we connect, the higher the attenuation of PLC signal we achieve. In our case, we connected a 470 nF capacitor to the power line. In Figure 8, we can see oscillograms: Figure 8(a) without connected capacitor, Figure 8(b) with the same value capacitor connected near the traffic concentrator, and Figure 8(c) with capacitor 470 nF connected directly inside the lighting pole. In the presented oscillogram, we can see decreasing values of modulated PLC signals. When we connect a capacitor with higher values, for example, 4.7 uF, close to the PLC, the transmitter' modem would not be able to transmit any packet because of the too low current efficiency of power supply or line amplifier.

A different method of attack on the physical layer is connection of a signal generator to the power line. The connected generator has to transmit the signal with values that belong to the PLC frequency band used by the attacked network. The higher the level of the injected signal, the bigger the values of PER (DLN_3 feature) and the lower values of the SNR traffic feature. We performed such an attack by means of a damaged/prepared switching power supply which comes from a notebook computer. This is an easy and cheap way to perform such attack. We transmitted a narrow bandwidth signal with 90 dBuV power close to the disturbed device. In Figure 9, we can see the characteristics of the interference signal that comes from the damaged laptop power supply.

We also disturbed PLC power mains by a professional Electrical Fast Transient (EFT)/Burst generator [22] that is used during electromagnetic compatibility (EMC) tests and capacitive coupling clamp (in this case, there is no need for a galvanic connection to the power mains) according to the IEC 61000-4-4 [47] recommendation.

In our experiments, the capacitors and generator were connected constantly but the attacker can arbitrarily connect these elements by a microcontroller controlled device and take into consideration, for example, sunrise and sunset.

Attacks from Scenario 1 have an impact mainly on data link and the network layer from Table 1. In Table 3, we can see the results of the proposed anomaly/attack detection method.

Table 3: DR [%] and FP [%] for anomalies/attacks performed on the SLCN in Scenario 1.

Network feature	DR [%]	FP [%]	Description
DLN_1	90.80	4.80	—
DLN_2	98.00	3.60	The biggest impact on DLN_2 in Scenario 1
DLN_3	97.00	3.20	The biggest impact on DLN_3 in Scenario 1
DLN_4	81.40	5.20	—
DLN_5	75.40	7.40	—

Table 4: DR [%] and FP [%] for anomalies/attacks performed on the SLCN in Scenario 2.

Network feature	DR [%]	FP [%]	Description
DLN_1	91.40	4.30	—
DLN_2	98.80	3.80	The biggest impact on DLN_2 in Scenario 2
DLN_3	97.60	3.10	The biggest impact on DLN_3 in Scenario 2
DLN_4	82.60	6.40	—
DLN_5	78.60	7.80	—

Table 5: DR [%] and FP [%] for anomalies/attacks performed on the SLCN in Scenario 2.

Network feature	DR [%]	FP [%]	Description
APL_1	98.40	2.80	—
APL_2	91.20	5.20	—
APL_3	96.80	3.80	—
APL_4	—	—	Not important in this scenario
APL_5	—	—	Not important in this scenario

Scenario 2. In the second scenario, the attacker would like to generate random packets by means of a connected unauthorized smart lamp or a PLC modem. This is a more sophisticated attack than in case of using a generator (see Scenario 1). Constantly generated packets by the attacker's PLC modem cause modems which are within the impact of this transmission to be constantly in the receiving mode and to be unable to transmit or receive any packets. The attacker transmits packets with the use of carrier frequency/frequencies used in the attacked network one by one with the shortest delays as possible between consecutive packets. Packets transmitted by the attacker may be understandable or not from the smart lights network's point of view. Results of DR [%] and FP [%] for anomaly detection in case of Scenario 2 are presented in Tables 4 and 5.

Indirectly, this type of attack can also be seen in application layer parameters because part of the lamps will switch to maximum luminosity after three connection attempts to the traffic concentrator (we set 900 seconds between attempts). In this case, energy consumption will increase and other parameters that depend on energy consumption also will change (e.g., the lamp's temperature).

Scenario 3. The attack performed in Scenario 3 belongs to Group II of attacks. This type of attack requires knowledge about the PLC smart lights network topology, devices used in the smart lights network, communication protocols used for every layer of PLC communication stack, and so forth.

The attacker, in the presented scenario, connected an additional traffic concentrator (with the same MAC address as the valid traffic concentrator). The attacker's traffic concentrator pretends to be a valid communication device and takes part in packet exchange between lamps. The attacker is placed near lamps and wants to change the lamps' settings. In this case, the attacker is far from the concentrator and the valid concentrator does not receive the command (or a command copy) sent by the fake concentrator. In order to prevent the command from reaching the valid concentrator, it is best to send a command with TTL = 0.

We also performed a similar attack when the attacker was close to the valid concentrator. In this case, anomaly is revealed by the registration command packet with TTL = TTLmax. The valid concentrator will never hear packets' copy with TTLmax. In a proper situation, the packet should have TTL < TTLmax. In this case, the attacker does not care that packets will not arrive to the valid concentrator. Results for the presented scenario are presented in Table 6.

Scenario 4. In the presented scenario, the attacker connected an additional device with a PLC modem and tried to change and retransmit packets with destroyed bits. This action causes an increasing number of corrupted packets with wrong Cyclic Redundancy Check (CRC) bytes. In this case, we can see an increasing value of Packet Error Rate (PER) (DLN_3) network feature. For example, if we send a command to lamps with new luminosity settings, some lamps may not get this information. When a lamp does not receive any command after three connection attempts to the concentrator (number of attempts' parameter NA and time between attempts are protocol parameters in our experiments set to NA = 3

Table 6: DR [%] and FP [%] for anomalies/attacks performed on the SLCN in Scenario 3.

Network feature	DR [%]	FP [%]	Description
DLN_1	—	—	Not important in this scenario
DLN_2	—	—	Not important in this scenario
DLN_3	—	—	Not important in this scenario
DLN_4	90.60	4.60	—
DLN_5	98.60	3.40	—

Table 7: DR [%] and FP [%] for anomalies/attacks performed on the SLCN in Scenario 4.

Network feature	DR [%]	FP [%]	Description
DLN_1	—	—	Not important in this scenario
DLN_2	—	—	Not important in this scenario
DLN_3	98.40	3.40	—
DLN_4	85.40	7.24	—
DLN_5	92.60	6.60	—

Table 8: DR [%] and FP [%] for anomalies/attacks performed on the SLCN in Scenario 4.

Network feature	DR [%]	FP [%]	Description
APL_1	98.80	2.40	—
APL_2	90.30	4.80	—
APL_3	96.50	3.60	—
APL_4	—	—	Not important in this scenario
APL_5	—	—	Not important in this scenario

and time 900 seconds), then they will switch to maximum luminosity. This situation causes additional costs to the installation's operator. This type of attack can be especially seen in application layer network features, such as APL_1 (ENE, power consumption by PLC lamp [Wh]), APL_3 (LUL, lamp luminosity level received from the lamp), and, indirectly, the lamp's temperature (APL_2). Detection rate DR [%] and false positive FP [%] results for Scenario 4 are presented in Tables 7 and 8.

Scenario 5. In the next scenario, the attacker would like to prevent receiving the broadcast command (e.g., a command that wants to set a group of lamps to certain luminosity) by lamps. When the attacker's PLC modem detects a broadcast command sent by a traffic concentrator, it transmits an arbitrary command (i.e., no operation command (NOP)) in the unicast mode. Transmission in the unicast mode has a higher priority and lower delay, which is why this transmission will reach first the lamp. The lamp will respond to this packet by switching to the acknowledge ACK/awaiting state. Broadcast command receiving is only possible for lamps in IDLE state. Results for this scenario are presented in Tables 9 and 10.

Additional explanation requires application network features APL_4 (number of lamp resets per time interval (NR)) and APL_5 (power supply (PS) value). These parameters are mainly important for the smart lights network operator and were not affected by the attack simulated in our experiments. Such parameters are important for smart lights network management and may indirectly have an impact on the transmission parameter, but we did not have the chance to observe the impact of these parameters during our experiments.

Taking into account all scenarios, the detection rate (DR) values change from 75.40 to 98.80%, while the false positive ranged from 7.80 to 2.40%. We can see that, depending on the attack scenario, only part of the network traffic features selected from the PLC traffic give us meaningful information from the anomaly/attack detection's point of view. For example, in Scenario 4, we can see a direct impact on data link and network layer features and indirect influence on application layer features extracted from the data payload.

Results achieved by the proposed anomaly/attack detection proved the usefulness of the proposed method. Anomaly detection systems are characterized by higher values of false positive in comparison to classic intrusion detection systems (IDS), which are based on the database of already known attacks.

We verified the achieved results by comparing the proposed solution to methods available in the literature. Although we did not find anomaly and intrusion detection for smart lights PLC network operating in data link, network layer, and application layer, there are anomaly and intrusion detection systems applied to WSN smart meter networks in Smart Grid AMI (Advanced Metering Infrastructure). Such solutions are mainly designed for energy theft detection and for failure and maintenance purposes and operate usually in network and application layers. Anomaly and intrusion detection systems for energy theft detection use, for example,

Table 9: DR [%] and FP [%] for anomalies/attacks performed on the SLCN in Scenario 5.

Network feature	DR [%]	FP [%]	Description
DLN_1	—	—	Not important in this scenario
DLN_2	—	—	Not important in this scenario
DLN_3	—	—	Not important in this scenario
DLN_4	92.40	7.74	—
DLN_5	90.20	7.70	—

Table 10: DR [%] and FP [%] for anomalies/attacks performed on the SLCN in Scenario 4.

Network feature	DR [%]	FP [%]	Description
APL_1	94.20	2.60	—
APL_2	88.40	4.40	—
APL_3	98.40	2.40	—
APL_4	—	—	Not important in this scenario
APL_5	—	—	Not important in this scenario

the HMM (Hidden Markov Models) [48], rule-based solutions [13], and statistical methods by means of, for example, Bollinger Bands [49]. Different kinds of methods are for estimation of metering errors in AMI infrastructure with the use of, for example, DTW (Dynamic Time Warping) [23]. In general, anomaly detection systems are very diverse and so a straightforward comparison is not easy, though it can be stated, bearing in mind the available literature [7, 11, 13, 15, 16, 23, 48–50], that false positive values for anomaly detection type systems are generally less than 10% [18, 19, 21]. This level of false positive parameter is acceptable for the proposed class of systems, especially for anomaly detection systems.

We also proposed a mechanism that prevents the aging of exponential smoothing models (see Section 5.3). Such an installation like smart lights networks or Wireless Sensor Networks (WSN) changes over time, so it is important to predict such a situation and update anomaly detection reference profiles in order to prevent the increase of false positive values.

7. Conclusions

The number of potential threats in dynamically created Smart Cities, and in particular in their critical communication infrastructures, is very big and is increasing every day. Thus, protection from constantly newer vectors of attacks is becoming more complicated and requires the use of highly specific solutions. Currently, the most often used mechanisms ensuring an adequate level of security in such infrastructures are the methods of detection and classification of abuses (attacks) unknown so far, often directed onto defined sources of critical communication infrastructures. The basic aims of such solutions are the early detection and reaction to the symptoms of nontypical behavior of network traffic which may indicate various abuses originating both outside and inside the protected infrastructure.

The article presents effective solutions concerning the detection of different types of abuses in network traffic for the critical infrastructure of Smart Lighting. It proposes and describes the structure of the SLCN created for the purposes of the experiment. The structure was built with the use of Power Line Communication technology. The key security problems are also discussed, which have a direct impact on proper operation of the Smart Lighting critical infrastructure; that is, the authors described the possibilities of emergence of both external factors and active forms of attacks aiming at gaining influence on the informational contents of the transmitted data. The article proposes an efficient and effective method of abuse detection in the analyzed Smart Lighting network traffic. At the initial stage of the solution, there is identification and elimination of outliers, which is performed by means of Mahalanobis's distance. The objective of such an activity was correction of data for automatic creation of statistic models (standards) based on exponential smoothing methods. The choice of optimal values of the estimated statistical models was realized as minimization of their forecast error. The article also presents a procedure of recalculation (update) of the standard models in case there are permanent changes in the character of the SLCN traffic. The next step is the calculation of the difference value between the forecast in the estimated traffic model and its real variability in order to detect abnormal behavior, which may indicate an attempt of an abuse, for example, a network attack or unauthorized interference in the SLCN infrastructure.

The proposed anomaly/attack detection system based on predictive analysis with the use of exponential smoothing method was evaluated by five attack scenarios. The proposed scenarios have an impact on every layer of PLC communication stack. In order to detect an anomaly/attack, we extracted 10 network features from the PLC traffic network. For all scenarios, we achieved detection rate (DR) values changes from 75.40 to 98.80%, while the false positive ranged from 7.80 to 2.40%. In order to prevent ADS reference models' aging, we added a trigger condition used for reference profiles recalculation. The achieved results are promising and proved that statistical analysis of traffic features with

the use of exponential smoothing models can be useful for anomaly/attack detection and maintenance purposes for smart lights operators.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This research was supported by the National Centre for Research and Development and also by the National Fund for Environmental Protection and Water Management under the realized GEKON program (Project no. 214093), and it also was supported by the Polish Ministry of Science and High Education and Apator S.A. Company under Contract 04409/C.ZR6-6/2009.

References

[1] IEEE Standards Association, *IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads*, The Institute of Electrical and Electronics Engineers, 2011.

[2] M. Górczewska, S. Mroczkowska, and P. Skrzypczak, "Badanie wplywu barwy swiatla w oswietleniu drogowym na rozpoznawalnosc przeszkód (light color influence on obstacle recognition," *Electrical Engineering*, vol. 73, pp. 165–172, 2013.

[3] H. Schaffers, "Landscape and Roadmap of Future Internet and Smart Cities," 2012.

[4] S. Sun, B. Rong, and Y. Qian, "Artificial frequency selective channel for covert cyclic delay diversity orthogonal frequency division multiplexing transmission," *Security and Communication Networks*, vol. 8, no. 9, pp. 1707–1716, 2015.

[5] IEC 62386-102:2014, Digital addressable lighting interface - Part 102: General requirements - Control gear, 2014.

[6] EN 50065-1:2011, Signalling on low-voltage electrical installations in the frequency range 3 kHz to 148.5 kHz, General requirements, frequency bands and electromagnetic disturbances, 2011.

[7] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, "Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: a feasibility study," *IEEE Systems Journal*, vol. 9, no. 1, pp. 31–44, 2015.

[8] P. Kiedrowski, B. Dubalski, T. Marciniak, T. Riaz, and J. Gutierrez, "Energy greedy protocol suite for smart grid communication systems based on short range devices," in *Image Processing and Communications Challenges 3*, vol. 102 of *Advances in Intelligent and Soft Computing*, pp. 493–502, Springer, Berlin, Germany, 2011.

[9] P. Kiedrowski, "Errors nature of the narrowband plc transmission in smart lighting LV network," *International Journal of Distributed Sensor Networks*, vol. 2016, Article ID 9592679, 9 pages, 2016.

[10] A. S. Elmaghraby and M. M. Losavio, "Cyber security challenges in smart cities: Safety, security and privacy," *Journal of Advanced Research*, vol. 5, no. 4, pp. 491–497, 2014.

[11] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: methods, systems and tools," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 303–336, 2014.

[12] M. Esposito, C. Mazzariello, F. Oliviero, S. P. Romano, and C. Sansone, "Evaluating pattern recognition techniques in intrusion detection systems," in *Proceedings of the 5th International Workshop on Pattern Recognition in Information Systems (PRIS'05), in Conjunction with ICEIS 2005*, pp. 144–153, Miami, FL, USA, May 2005.

[13] R. Mitchell and I.-R. Chen, "Behavior-rule based intrusion detection systems for safety critical smart grid applications," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1254–1263, 2013.

[14] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: a survey," *ACM Computing Surveys*, vol. 41, no. 3, article 15, 2009.

[15] T. Andrysiak and Ł. Saganowski, *Network Anomaly Detection Basedon ARFIMA Model, Image Processing & Communications Challenges 6, Advances in Intelligent Systems and Computing*, vol. 313, Springer, 2015.

[16] E. H. M. Pena, M. V. O. De Assis, and M. L. Proença, "Anomaly detection using forecasting methods ARIMA and HWDS," in *Proceedings of the 32nd International Conference of the Chilean Computer Science Society, SCCC 2013*, pp. 63–66, November 2013.

[17] G. Galvas, "Time series forecasting used for real-time anomaly detection on websites," 2016, https://beta.vu.nl/nl/Images/stageverslag-galvas_tcm235-801861.pdf.

[18] M. Xie, S. Han, B. Tian, and S. Parvin, "Anomaly detection in wireless sensor networks: a survey," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1302–1325, 2011.

[19] P. Cheng and M. Zhu, "Lightweight anomaly detection for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 653232, 2015.

[20] K. Ord and S. Lowe, "Automatic forecasting," *The American Statistician*, vol. 50, no. 1, pp. 88–94, 1996.

[21] V. Garcia-Font, C. Garrigues, and H. Rifà-Pous, "A comparative study of anomaly detection techniques for smart city wireless sensor networks," *Sensors*, vol. 16, no. 6, article 868, 2016.

[22] EFT/Burst generator Teseq, http://www.teseq.com/products/NSG-3060.php.

[23] N. Zhou, J. Wang, and Q. Wang, "A novel estimation method of metering errors of electric energy based on membership cloud and dynamic time warping," *IEEE Transactions on Smart Grid*, vol. 8, no. 3, pp. 1318–1329, 2017.

[24] V. J. Hodge and J. Austin, "A survey of outlier detection methodologies," *Artificial Intelligence Review*, vol. 22, no. 2, pp. 85–126, 2004.

[25] Y. Wang, T. T. Gamage, and C. H. Hauser, "Security Implications of Transport Layer Protocols in Power Grid Synchrophasor Data Communication," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 807–816, 2016.

[26] M. Mahoor, F. R. Salmasi, and T. A. Najafabadi, "A hierarchical smart street lighting system with brute-force energy optimization," *IEEE Sensors Journal*, vol. 17, no. 9, pp. 2871–2879, 2017.

[27] C. Liao, C.-W. Ten, and S. Hu, "Strategic FRTU deployment considering cybersecurity in secondary distribution network," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1264–1274, 2013.

[28] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems Magazine*, vol. 21, no. 6, pp. 11–25, 2001.

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

[30] T. Macaulay and B. L. Singer, *ICS vulnerabilities. In: Cybersecurity industrial control systems SCADA, DCS, PLC, HMI, SIS [Internet]*, CRC PRESS: Taylor & Francis Group, 2012, https://www.crcpress.com/Cybersecurity-for-Industrial-Control-Systems-SCADA-DCS-PLC-HMI-and/Macaulay-Singer/9781439801963 [Google Scholar].

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

[32] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 981–997, 2012.

[33] D. M. Hawkins, *Identification of Outliers*, Chapman and Hall, London, UK, 1980.

[34] M. J. Healy, "Multivariate Normal Plotting," *Journal of Applied Statistics*, vol. 17, no. 2, p. 157, 1968.

[35] P. J. Rousseeuw, "Least median of squares regression," *Journal of the American Statistical Association*, vol. 79, no. 388, pp. 871–880, 1984.

[36] P. Filzmoser, R. Maronna, and M. Werner, "Outlier identification in high dimensions," *Computational Statistics & Data Analysis*, vol. 52, no. 3, pp. 1694–1711, 2008.

[37] R. L. Goodrich, "The Forecast Pro methodology," *International Journal of Forecasting*, vol. 16, no. 4, pp. 533–535, 2000.

[38] R. J. Hyndman, A. B. Koehler, R. D. Snyder, and S. Grose, "A state space framework for automatic forecasting using exponential smoothing methods," *International Journal of Forecasting*, vol. 18, no. 3, pp. 439–454, 2002.

[39] E. S. Gardner, "Exponential smoothing: the state of the art," *Journal of Forecasting*, vol. 4, no. 1, pp. 1–28, 1985.

[40] E. S. Gardner Jr., "Exponential smoothing: the state of the art-part II," *International Journal of Forecasting*, vol. 22, no. 4, pp. 637–666, 2006.

[41] B. C. Archibald, "Parameter space of the holt-winters' model," *International Journal of Forecasting*, vol. 6, no. 2, pp. 199–209, 1990.

[42] J. Durbin and S. J. Koopman, *Time series analysis by state space methods*, vol. 24, Oxford University Press, Oxford, UK, 2001.

[43] R. J. Hyndman and Y. Khandakar, "Automatic time series forecasting: the forecast package for R," *Journal of Statistical Software* , vol. 27, no. 3, pp. 1–22, 2008.

[44] H. Bozdogan, "Model selection and Akaike's information criterion (AIC): the general theory and its analytical extensions," *Psychometrika*, vol. 52, no. 3, pp. 345–370, 1987.

[45] J. Ramsey and D. Wiley, "Book Reviews : exploratory data analysis John W. Tukey Reading, Mass: Addison-Wesley, 1977, Pps. xvi +688. $17.95," *Applied Psychological Measurement*, vol. 2, no. 1, pp. 151–155, 1978.

[46] National Fund for Environmental Protection and Water Management under the realized GEKON program (project no. 214093).

[47] IEC 61000-4-4, http://www.iec.ch/emc/basic_emc/basic_emc_immunity.htm.

[48] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, "A multi-sensor energy theft detection framework for advanced metering infrastructures," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1319–1330, 2013.

[49] Y. Liu, S. Hu, and T.-Y. Ho, "Leveraging strategic detection techniques for smart home pricing cyberattacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 2, pp. 220–235, 2016.

[50] C.-H. Lo and N. Ansari, "CONSUMER: a novel hybrid intrusion detection system for distribution networks in smart grid," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 1, pp. 33–44, 2013.