Hindawi
Journal of Sensors
Volume 2017, Article ID 8782131, 15 pages
https://doi.org/10.1155/2017/8782131

*Research Article*

# Anomaly Detection in Smart Metering Infrastructure with the Use of Time Series Analysis

**Tomasz Andrysiak, Łukasz Saganowski, and Piotr Kiedrowski**

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

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

Received 10 March 2017; Revised 31 May 2017; Accepted 13 June 2017; Published 18 July 2017

Academic Editor: José R. Villar



The article presents solutions to anomaly detection in network traffic for critical smart metering infrastructure, realized with the use of radio sensory network. The structure of the examined smart meter network and the key security aspects which have influence on the correct performance of an advanced metering infrastructure (possibility of passive and active cyberattacks) are described. An effective and quick anomaly detection method is proposed. At its initial stage, Cook's distance was used for detection and elimination of outlier observations. So prepared data was used to estimate standard statistical models based on exponential smoothing, that is, Brown's, Holt's, and Winters' models. To estimate possible fluctuations in forecasts of the implemented models, properly parameterized Bollinger Bands was used. Next, statistical relations between the estimated traffic model and its real variability were examined to detect abnormal behavior, which could indicate a cyberattack attempt. An update procedure of standard models in case there were significant real network traffic fluctuations was also proposed. The choice of optimal parameter values of statistical models was realized as forecast error minimization. The results confirmed efficiency of the presented method and accuracy of choice of the proper statistical model for the analyzed time series.

## 1. Introduction

Smart Metering Communications Networks (SMCN) are one of the most important parts of the Smart Grid system [1]. With smart metering, not only the remote, automatic electricity meters' reading but also the customer's switching on/off is possible. The reading process can be done very often, for example, every 15 minutes per every meter. Frequent reading allows for more accurate energy consumption forecasting because of having large statistic material based on individual electricity consumption profiles (the more accurate we forecast, the more money we save).

Smart Metering Communications Network consists of last-mile networks, access networks, and a backbone network. Both backbone and access networks are realized using typical methods, that is, using IP network as a backbone and mostly GPRS technology to access it. It should be noted that these typical solutions are not the only ones. There can be other very original solutions, for example, the one described in [2]. Last-mile smart metering networks use PLC (Power Line Communications), RF (radio frequency), or a hybrid of these technologies. In this article, like in [3], the RF technology is considered. Using RF technology based on short-range devices makes the last-mile smart metering network similar to WSN (wireless sensor network). Moreover, they also use the multihop technique to expand communication range. The value of bit rates used in these networks, which is between a few to a few hundred of kbit/s, is probably the last similarity of these networks. There are two main differences between WSNs and last-mile smart metering communication networks, namely, energy issues and memory deficit. In last-mile smart metering communication network, dedicated for automatic electricity meter reading, energy issues do not exist, which is opposite to WSNs [4]. The result of the first diversity is the difference in the applied routing protocols. In WSNs, routing protocols are oriented on the balanced involvement of intermediary nodes in the process of data transferring, while in smart metering, they are oriented on reliability of data distribution and acquisition. Memory deficit in communication nodes of the smart meters is caused

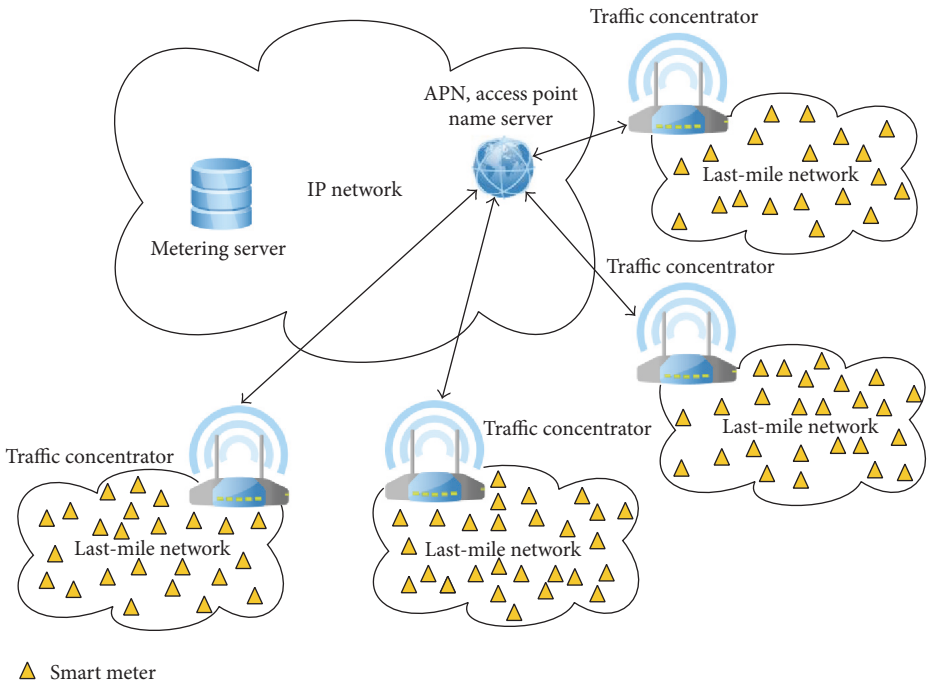


Figure 1: Smart metering critical infrastructure management system: an overview.

by using it mostly to implement sophisticated encryption algorithms, because smart metering systems, being part of the Smart Grid (which is classified as the critical infrastructure), must meet high security requirements. The result of this memory deficit forces other approaches to solve typical problems of the network maintenance. One of such problems is anomaly detection in last-mile network. It is impossible to implement even simplest anomaly detection algorithms, even though there is a spare memory, because this spare memory is reserved for the future for new more sophisticated encryption algorithms. Independent from the memory insufficiency, the second reason of difficulties with anomaly detection in smart meters is that the throughput of the last-mile network is too small to report detected anomalies in the right time. Moreover, most of the anomalies would also be detected by the neighbouring nodes, which multiplexes data traffic in the network. In smart metering, the last-mile networks operate at nearly maximum traffic load. The typical number of smart meters in a single last-mile network is around 250. Every smart meter must be read out every 15 min and it takes a few seconds (from 1 sec. to 4 sec. typically). There is only a small margin of bandwidth to support the maintenance and management or to enable the reading process during degraded propagation conditions. The above reasons induced us to carry out detection of anomalies in the data traffic concentrator. The data traffic concentrator (TC) is a thick node similar to the sink in WSNs. The construction of it is mostly based on the single-board computers which have enough RAM and ROM memory and also have a fast processor. The data traffic concentrator is connected to both last-mile and access networks. It is easy to update when there is access to network database of anomalies or the detection methods.

Bearing in mind the above, we have chosen to detect network anomalies by means of exponential smoothing of statistical models and outliers detection. The purpose of the proposed operations is to examine differences between real network traffic parameters and the same traffic's estimated statistical models. A two-stage anomaly detection method was used for the process mentioned above. Its first part consisted in seeking and elimination of any outliers in traffic parameters of the advanced metering infrastructure (AMI). This step was based on Cook's distance, which is a simple and efficient method. Consequently, in the second part of the process, the data which remained served as a base for creation of statistical models by means of exponential smoothing. In result, the operation showed differences in the tested AMI parameters.

In our solution, three types of anomalies were tested: (i) energy theft by bypassing electricity meter and energy meters shielding, (ii) electromagnetic distortion caused by Radio Frequency Interferences (RFI) and conducted interferences through power mains, and (iii) interference of communication caused by coordinated attacks.

General overview of Smart Grid advanced metering infrastructure (AMI) is presented in Figure 1. A last-mile network consists of AMI network realized by means of wireless sensor network (WSN). Power meters have built-in wireless sensors, working in industrial, scientific, and medical (ISM) bands. Traffic from power meters is received by a traffic concentrator, which plays a role of communication gateway between a WSN network and other communication links realized by, for example, IP network, General Packet Radio Service (GPRS), or Long-Term Evolution (LTE). Every traffic concentrator communicates through access point name

(APN) server (see Figure 1) which represents a link realized by packet communication network. In higher energy operator, the level application installed on the metering server is responsible for maintenance and billings.

The article is organized as follows: after Introduction, Section 2 describes communication scheme used in the last-mile test-bed network. Next, Section 3 presents related work on existing anomaly detection systems for Smart Metering Communications Network. Section 4 discusses the categories and nature of AMI security questions. Section 5 presents the structure and functioning of the research system. In Section 6, the real-life experimental setup as well as experimental results is presented. Finally, Section 7 concludes our work.

## 2. Communication Scheme Used in the Last-Mile Test-Bed Network

Communication scheme used in the examined last-mile network was designed by one of the coauthors in 2010 and published in 2011 in [5] as EGQF (Energy Greedy Quasi-Flooding) protocol. This paper presents only necessary information about the scheme for better understanding of the methods of anomaly detection. The EGQF protocol is independent from communication media types and may be used in networks using RF, PLC, or even RF/PLC [6] hybrid technologies. It uses the multihop technique for an extending transmission range and also the multipath technique to improve reliability of data transfer. The architecture of the presented network is very simple because it can operate having only two types of nodes: a traffic concentrator and electricity meters. The traffic is forced and coordinated by the traffic concentrator. At the same time, only one electricity meter is queried. All the other nodes, which are not queried at the moment, can act as transfer nodes relaying packets to or from the destination node. Due to the lack of memory, terminals do not know the network topology and even do not know the addresses of neighbouring nodes.

The EGQF protocol uses a reduced 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 querying the electricity meter. The response from the electricity meter is transported over the response packet. The ACK/Cancel packet is a packet which acts as the ACK for the destination node and as the reading process canceller for the other nodes. The ACK/Cancel packet can be sent only by the traffic concentrator to confirm the reception of the response and to put out the flooding of remaining response copies. The relaying process in nodes, which are neither destination nor source nodes, depends on transmitting the copy of the packet after random time in the condition of a not detected carrier. The difference between the typical flooding protocol and the EGQF protocol is that using a typical flooding protocol nodes sends a copy of packet always once during the transferring process, while when using the EGQF protocol, copies are sent as often as needed, for example, once, twice, or not at all. The decision whether a copy of the packet should be sent is made when the transfer discriminator (TD) value of a packet is greater than the previous stored one. 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 the least three significant bits of the control field of the packet, while the packet type code occupied two more significant bits in the same field, so that the transfer process of command packet is always canceled after receiving a response packet. It is the same with response packet transfer after receiving ACK/Cancel.

These two cases show us a situation when the copy is not sent, which is different with regard to the typical flooding protocol. This solution reduces the risk of collision. Using the same solution, it is possible to send the 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 but with smaller value of TTL. This situation does not occur very often (i.e., when a packet with a greater number of hops came earlier than a packet with a smaller number of hops), and it increases reliability [6, 7].

Only the response and command packets can have payload field. Payload field is encrypted by the application layer, whereas the rest, like overhead, is transmitted in open unencrypted mode. So it is impossible to change readouts (attack the application layer), but it is possible to generate extra traffic by the extra node which has the same address as the existing, in last-mile, smart meter. Such an attack on confidentiality causes deterioration in network performance and can even make the real smart meter unreachable, for example, by sending copies of the response packets with small value of TTL.

## 3. Related Work

In most cases, anomaly detection in LV network depends on energy theft detection. The oldest method depends on finding irregularities from the customer billing centre [8]. This centralized method does not allow reacting quickly because of having historical long-term consumption records. Therefore, in [8], the new decentralized method based on short periods customers' consumption profiles is proposed. In [9], the authors used a variety of sophisticated techniques also for theft detection. There are a lot of works which focus on communication security by means of encryption or key distribution, for example, [10, 11].

This work focuses on anomaly detection in last-mile RF Smart Grid communication network, which is not only the result of the energy theft but also the result of deliberate, malicious customers' behavior or simply unconscious disturbing actions coming from other systems. There is a similar work [12], in which anomaly detection is realized neither in the central point nor in electricity meters but in a simple way. The proposed methods of anomaly detection presented in [12] are mostly dedicated for thefts detecting, while we focused on any anomaly detection in communication.

Anomalies in communication may be caused by various factors, for example, a human or independent of human activity and unintentional or intentional actions, such as theft, for instance. There are quite a lot of works dedicated

to anomaly detection in communication networks, also in Smart Grid communications systems [13–16], including the last-mile area of their communication networks. However, in these works, the authors focus on anomaly detection in an IP network, where also for smart metering last-mile network the data is carried over IP if PLC PRIME or G3 interface was implemented [17]. We used RF technology for last-mile network, where IP technology implementation was not possible, because it would lengthen the radio frames and make the radio transmission unreliable.

In literature, most anomaly detection systems are focused on anomalies in power distribution systems such as transmission line outages, unusual power consumption, and momentary and sustained outages [18]. In our work, we proposed anomaly/attack detection system in last-mile RF Smart Grid network (not in IP network). We proposed the two-step method of anomaly detection dedicated for last-mile RF communication network consisting of nodes, which are based on short-distance devices with the memory deficit and reduced protocol stack, that is, one protocol both for the data link layer and for the network layer.

## 4. Security in Smart Metering Communications Network

Ensuring security and protection of data collected by the smart metering systems is an exceptionally essential element of the SMCN solutions. It is obvious that data gathered by smart meters say much about private aspects of the recipients' lives. Moreover, having additional information such as sequences of readings, types of devices, or the number of inmates, it is easy to create a precise profile of daily living activities of the observed recipients, which in consequence may lead to serious abuses [19, 20].

The threats coming from the recipients themselves who have the smart metering infrastructure are not a less important security problem. The recipients can perform destructive activities on AMI, which consist in disturbing data saved in the meter, reconfiguration of settings and parameters of the counter, disruption of data transmission, or replacement of the internal counter's software so that it conveys understated values of consumed energy [9, 12, 21].

However, what appears to be a more serious problem is protection against cyberattacks [22]. A large-scale application of smart metering creates new entering possibilities for an unauthorized use by information systems. Joining of smart meters with information networks of energy companies, energy sellers, and companies managing distributed generation is essential for proper functioning of smart power networks. Thus, every meter becomes a potential entering point for a cyberattack [23]. Protection of smart networks against such attacks seems to be a more complex task and much more difficult to solve in comparison with ensuring security to data collected by smart meters or prevention from the users' abuses.

Cyberattacks onto the SMCN security may be divided into two elementary groups: passive and active attacks. The passive ones are all the attempts of an unauthorized access to data or the SMCN infrastructure, in which the attacker does not use emission of signals which may disturb or even disenable correct work of the system. Active attacks, on the other hand, are all the attempts of an unauthorized access by the attacker to data or the SMCN system's infrastructure with the use of emission of any signals or activities that can be detected [24–26].

While performing a passive attack onto the SMCN, the attacker disguises their presence and tries to obtain access to the transmitted data by passive monitoring of the network. For protection against such incidents, different cryptographic mechanisms are often used. Another passive form of attack onto the SMCN is activities aiming at obtaining an analysis of the traffic within the network. In this case, the attacker's intention is not acknowledging the content of transmitted data packets but is gaining knowledge about topology of the wireless sensor network. Due to the above, collecting information on the basis of traffic analysis in the SMCN gives the intruder knowledge about the network's critical nodes which ensure its proper work [25].

Contrary to the above presented passive methods of attack onto the SMCN, by using active attack forms, the intruder directly or indirectly influences the content of the sent data and/or the network's operational capabilities [26]. Attacks of this kind are easier to detect in comparison to the passive ones because they have direct impact onto the SMCN performance quality. An effect of an active attack may be, for example, degradation of services, or, in extreme cases, lack of access to particular services, or even a complete loss of control over the SMCN network.

Active attacks can be divided into three groups [25, 26]: (i) physical attacks, destruction of a node, a node manipulation, and electromagnetic pulse (EMP); (ii) attacks onto integrity, confidentiality, or privacy of data (including unauthorized access to data); (iii) attacks on services (Denial of Service (DoS) or Distributed Denial of Service (DDoS)) and attacks directed at each SMCN network layer.

The physical attacks are direct destructive operations that aim to physically destroy or damage the AMI infrastructure. A similar role can be performed by attacks using short-term high-energy electromagnetic pulse (EPM) or high pulse distortion in the supply network [27, 28].

The attacks directed at integrity or confidentiality of data are exceptionally dangerous because they enable the attacker to gain an unauthorized access to the AMI and to data transmitted by it. One of possible forms of such activity is the Sybil attack. It consists in compromising the network's legal node and the takeover of its identifier together with access to the AMI infrastructure [29].

Another type of attacks is a Wormhole attack [30]. In this case, the attacker creates additional links and transmits packets to an unauthorized node in WSN network. This type of attack may have serious impact on routing process and can be an introduction to other more serious attacks such as "man into the middle" attack. Overall network performance can also be downgraded because of inefficient resource utilization.

The DoS/DDoS attacks in the SMCN lead to an overload of the attacked nodes and thereby they disenable acquiring data from the attacked nodes or they preclude using the

services offered by the attacked network. Attacks of this kind are usually realized by introducing network traffic which is bigger than it is possible to service. They can have different characters; for example, they may appear in the physical layer and take the form of jamming, and in the data link layer they may flood the network with packets, simultaneously leading to data colliding and necessity to retransmit it. Appearance of the DoS attack in a network layer, on the other hand, may consist in sending packets in the wrong direction [24, 31].

To protect against the above-mentioned threats, in particular different kinds of active and passive attacks, it is necessary to ensure a high level of security to the SMCN infrastructure by application of the following rules concerning sending information and the used functionalities [32, 33].

*Confidentiality*. Data sent by means of the chosen communication standard, and in particular sensitive data, should be inaccessible to outsiders. It means that no person from outside can obtain access permissions of the consumer or service supplier and that the information recipients themselves do not have access to the sensitive data allowing performing unauthorized profiling, for example, do not have access to information about performance of particular devices but only to aggregated power consumption.

*Integrity*. This requirement must ensure that the received message has not been changed during transmission. In case of last-mile networks, integrity has impact on proper and not delayed data transmission. Change in the information content, as a result of interference or a hacker's attack, could cause rupture in communication and activation of the wrong device.

*Authorization*. This operation is used for identification of devices and nodes and verification of the source or origin of the data in the network. Authorization is essential at the level of administrative task realization in the network. What is exceptionally important is proper authorization of numerators of the AMI and particular network's devices, because it conditions correct performance of the system as a whole.

*Accessibility*. This concerns access to the network, even in cases of attacks and possible damage to the devices. The infrastructure should be designed in such a way that its resources, for example, computational capabilities and memory, would enable full functionality with maximum process involvement of its elements.

*Time Sensitivity*. Every sent piece of information, offset by a particular fixed time window, may become useless. The network must retain the ability to communicate with certain time delays. In case of home metering infrastructure, time sensitivity is connected to response time, that is, time counted from the service claim to proper receiver's response. Assurance of appropriate response time conditions proper realization of the claimed service.

The problem of advanced metering infrastructure's digital security is a complex and difficult task to realize in practice. It requires designing and introducing high efficiency mechanisms of safety and security in order to provide confidentiality and integrity of data, preventing abuse caused by recipients, as well as detection and neutralization of attacks. One of the possible solutions to so-stated issue is implementation of abnormal behavior detection system for particular SMCN parameters, which points at a possibility of a given abuse appearance.

The above-mentioned solution is the main focus of the present paper.

## 5. Methodology of Anomaly Detection System: The Proposed Solution

In order to ensure appropriate level of security to critical infrastructures such as Smart Metering Communications Networks, in particular AMI last-mile network, it is necessary to monitor and control those infrastructures simultaneously. Only this type of activities enables detecting and minimizing the results of different kinds of abuses, coming from the inside (unauthorized and/or destructive actions of the recipient) as well as the outside (attacks realized by cybercriminals) of the protected infrastructure [19].

The most often implemented solutions, realizing so-stated aim, are the IDS/IPS systems *(Intrusion Detection System/Intrusion Prevention System)*, that is, mechanisms of detection (IDS) and preventing intrusions (IPS), operating in real time [34]. In the hierarchy of critical infrastructure, they should be placed just after security elements, such as firewalls. IDS systems are used for monitoring threats and incidents of safety violation and for informing about their occurrence. The IPS systems, on the other hand, additionally take actions to prevent an attack, minimize its effects, or actively respond to security violation. Thus, the mentioned solutions allow for an increase in the level of protection of the AMI infrastructure by means of strengthening communication control between its different elements.

The IDS systems may be classified as belonging to one of two groups using different techniques of threat identification. The first one is based on detection of known attacks by means of defined, specific (for them) features, called signatures. The second, on the other hand, is based on an idea of monitoring the system's normal operation in order to detect anomalies, which may proclaim an intrusion [34, 35].

The basic advantage of methods based on anomaly detection is the ability to recognize unknown attacks (abuses). These methods use knowledge of not how a particular attack looks like but of what does not correspond to defined norms of the network traffic. Therefore, the IDS/IPS systems founded on the use of anomalies are more efficient and effective than systems using signatures in the process of detecting unknown, new types of attacks (abuses) [36].

Bearing in mind the above, for the purpose of this research paper, we decided to detect anomalies by means of performing an analysis of deviations from the real AMI last-mile traffic parameters with regard to the estimated statistical models (Figure 2). In our method, detecting anomalies is performed in two steps. In the first stage, three exponential smoothing models are formed as a basis for the AMI network traffic parameters. For this reason, prior to creating

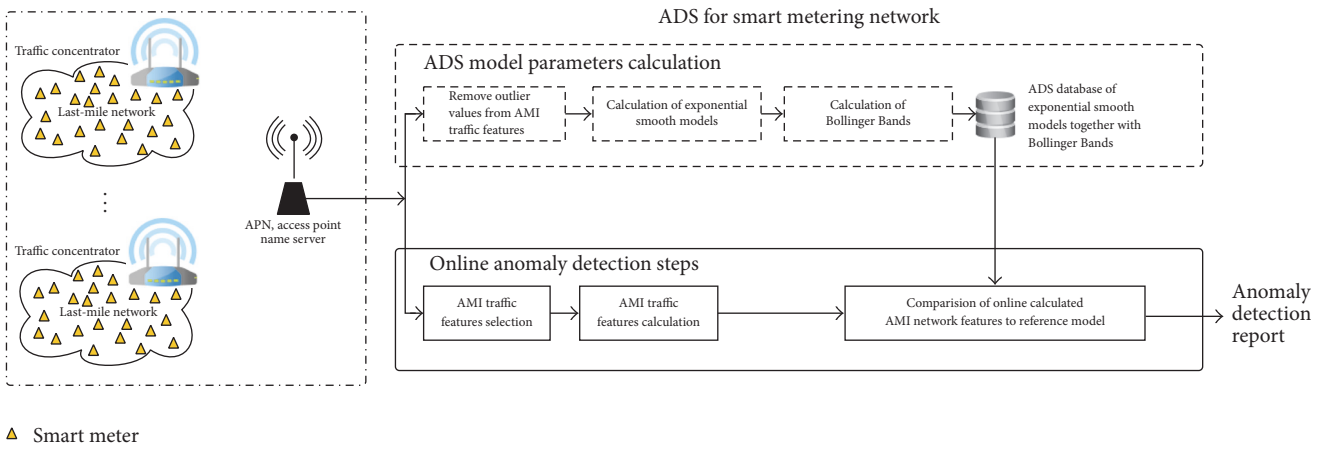


Figure 2: General overview of the proposed anomaly/attack detection method for AMI smart metering network.

the models, features of the network traffic are chosen and calculated by means of outliers detection and their exclusion. Next, the exponential smoothing models of parameters are estimated (on the basis of features of the analyzed AMI network traffic). In consequence, we obtain statistical models which serve as a basis for anomaly detection method. In the second stage, anomaly detection systems choose and estimate appropriate features of the network traffic, after which they compare the differences between the real network traffic and the calculated statistical models to perform AMI network parameters assessment.

In Figure 2, we can see a block scheme of the proposed anomaly detection method. Traffic from AMI last-mile network is captured by means of APN gateway. The proposed method is divided into two main steps. First step consists of calculation of model reference parameters (the elimination procedure of outliers' observations is realized at this stage) from extracted AMI network traffic features. Models for AMI network traffic features can be updated when the model is not up to date because of different reasons, for example, network architecture changes. Model parameters are calculated based on three different exponential smoothing models and Bollinger Bands calculation (see Sections 5.2 and 5.3). Reference models are used for comparing online the extracted AMI network traffic features in the second step of the proposed method. When calculated online, values of AMI network exceed parameters stored in the ADS reference model. The database anomaly report is detected for a given traffic feature (more explanation is presented in Section 6).

*5.1. Outliers Detection and Elimination: Cook's Distance.* Due to the nature of the Smart Metering Communications Networks' infrastructure (which is similar in many ways to WSN), there is a real threat of significant fluctuations of the analyzed traffic parameters in a network, that is, high likelihood of occurrence of outliers. Origin of the mentioned fluctuations may vary, for example, radio wave propagation (environmental source), changes to the infrastructure (technical source), hardware damage, an aftermath of a network attack, and intended deceit of users. Construction of a statistical model on a set of such data may lead to many unfavorable consequences. It is then highly likely that inference, predication, and decision-making process based on such a model will be burdened with big errors, and the created model will not reflect the main mechanisms regulating behavior of the analyzed phenomenon. Therefore, evaluation of influence of particular observations onto the final result should be an essential element of initial data analysis. It would allow detecting outliers and eliminating them from the data set.

In our approach, identification of outliers in the analyzed SMCN traffic parameters is performed by means of a method using Cook's Distance [37]. The essence of this method is estimation of the distance which states the level of data matching for two models: (i) a complete model, which includes all observations from the learning set, and (ii) a model built on a set of data, from which one $i$ observation was omitted.

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

where $\widehat{Y}_j$ is the forecasted value of $x$ variable for observations number $j$ in the complete model, that is, built on the whole learning set; $\widehat{Y}_{j(i)}$ is the forecasted value of $x$ variable for observations number $j$ in the model built on the set $Y_{j(i)}$, where $i$ is number of observations that were temporarily deactivated, MSE is the mean-model error, and $m$ is the number of parameters used in the analyzed model.

For Cook's distance $D_i$ threshold value, above which the given observation should be treated as an outlier, in compliance with criterion (1), 1 is accepted, or alternatively

$$\frac{4}{n - m - 2}, \tag{2}$$

where $n$ is the number of observations in the learning set.

*5.2. The Exponential Smoothing Models for Estimation of AMI Traffic Features Value.* The exponential smoothing methods

are a wide range of statistical models with different assumptions and complexity levels, which emerge from a common idea of creating forecasts by means of weighted moving averages. The common denominator of those methods is assigning (exponentially) weight decreasing with distance in time to past observations in the process of setting new forecast of a future observation [38].

It is easy to notice that exponential smoothing models are based on a sensible assumption that the future value depends on not only the last observed value but also their whole series of the past values. At the same time, the influence of old values (previous) is smaller than the influence of the new values [39].

Great practical importance of exponential smoothing models is based on the fact that they are suitable for forecast construction not only in conditions of stabilized development of phenomena to our interest but also when this development is irregular, characterized by trend's fluctuations. In these models, solid analytic trends are not accepted. To the contrary, it is assumed that, for every period, assessment of the trend's level and possible periodical fluctuations are built as some average from these kinds of evaluations made in previous periods [38, 40]. Among many representations known in literature, in this paper, the following models will be used: Davies and Brown [41], Holt's linear [42], and Winters' [43] models. It is due to a different representation of the compositional models of the analyzed time series and willingness to determine possibly the best model for the presented method of anomaly detection.

*5.2.1. Brown's Model.* A simple model of exponential smoothing, otherwise called Brown's model [41], is one of the methods most often used in case of a time series with fixed or very weak trend, when the series does not show developmental trend and fluctuations of its values result from random factors. This method consists in smoothing the time series of the forecasted variable by means of weighted moving average; however, the weights are defined according to exponential rule.

This model can be described by means of the following recurrent formula:

$$F_1 = x_1, \tag{3}$$

$$F_t = \alpha F_{t-1} + (1-\alpha) F_{t-1}, \tag{4}$$

where $x_1, x_2, \ldots, x_n$ are values of the forecasted series, $F_t$ is the value of the forecast in time $t$, and $\alpha$ is a parameter of the model, so-called smoothing constant, with the value of $\alpha \in [0, 1]$.

The conclusion from (4) is that the value of forecast in time $t$ depends, in recurrent manner, on the value of the time series and forecasts for times $t-1, t-2, \ldots, 1$. As the value of forecast $F_1$, necessary for construction of the model, we most often accept the initial value of the variable forecasted in the time series, that is, $x_1$, or arithmetic average of few first values of the variable $x$ from the time series.

The value of coefficient $\alpha$ influences the degree of a time series smoothing, so if $\alpha \approx 1$, then the constructed forecast will highly count the ex post errors of the previous forecasts. However, in the opposite case, when $\alpha \approx 0$, the built forecast will employ those errors to a small extent. Brown assumed that the parameter $\alpha$ should equal $2/(n+1)$, where $n$ is the number of observations [44].

Because the size of coefficient $\alpha$ has impact on the quality of the predictive model and the size of forecasts' errors, it is impossible to point arbitrarily the best value of that coefficient for every data. Therefore, this problem can be defined as an optimization task; that is, we are looking for such an $\widehat{\alpha}$, for which

$$s(\widehat{\alpha}) = \min_{\alpha \in [0,1]} s(\alpha), \tag{5}$$

where $s(\alpha)$ denotes an objective function, which characterizes the standard forecast error.

The often used objective function is

$$s(\alpha) = \frac{1}{n} \sum_{t=1}^{n} \left| F_t - x_t \right|, \tag{6}$$

which describes mean absolute forecast error. Its form is essential, because minimization of the objective function (5) is minimization of the sum of absolute deviations. This problem is easy to check for computationally simpler linear programming problem.

*5.2.2. Holt's Linear Model.* For smoothing and forecasting a time series, in which developmental model and trend of random fluctuations may be present, Holt's model [42] is most often used. It is described by means of two parameters, $\alpha$ and $\beta$, and it then takes the following form:

$$\begin{aligned} F_1 &= x_1, \\ S_1 &= x_1 - x_0, \\ F_t &= \alpha x_1 + (1-\alpha)\left(F_{t-1} + S_{t-1}\right), \\ S_t &= \beta\left(F_t - F_{t-1}\right) + (1-\beta) S_{t-1}, \end{aligned} \tag{7}$$

where $x_1, x_2, \ldots, x_n$ are the values of the forecasted series, $F_t$ is the smoothed value of the time series, $S_t$ describes the smoothed trend's growth value in the moment of time $t$, variables $\alpha$ and $\beta$ are the model's parameters, and $t$ indexes the consecutive time moments.

The values of $F_t$ and $S_t$ are calculated in recurrent manner. The forecasts of the future time series' values, however, are determined in the following way:

$$x^*_{n+k-1} = F_{n-1} + k \cdot S_{n-1}, \quad k = 1, 2, 3, \ldots. \tag{8}$$

Holt's model's parameters $\alpha$ and $\beta$ are chosen in such a way that they minimize possible errors of the expired forecasts. For this reason, specific values of these parameters are taken and determined, in compliance with dependency (8), with the assumption that $n = t$ and $k = 1$ are the expired forecasts.

$$x^*_t = F_{t-1} + S_{t-1}, \tag{9}$$

for time moments $t$, where $t = 2, 3, \ldots, n-1$ on the basis of series values from the previous period $\{x_1, x_2, \ldots, x_{t-1}\}$. These forecasts can be compared to factual values of the series $x_t$. The obtained differences are errors of the expired forecasts which are given by a model for the taken parameters $\alpha$ and $\beta$. As a measurement of the method's quality, the average of errors of the expired forecasts should be acknowledged. It may be a linear average,

$$J_1 = \frac{1}{n-2}\sum_{t=2}^{n-1}\left\lceil F_{t-1} + S_{t-1} - x_t \right\rceil, \tag{10}$$

or root mean square,

$$J_2 = \sqrt{\frac{1}{n-2}\sum_{t=2}^{n-1}\left(F_{t-1} + S_{t-1} - x_t\right)^2}. \tag{11}$$

Finally, it is necessary to choose from all possible $\alpha$ and $\beta$ parameter values such data that provides the lowest error value $J_1$ or $J_2$. By doing so, optimal parameters values and a measure of the forecast error are determined for the taken model. It is commonly accepted that $\alpha \in [0, 1]$ and $\beta \in [0, 1]$.

*5.2.3. Winters' Model.* Winters' model is a generalized Holt's model form. It is used for forecasting and smoothing a time series, in which a seasonal component, development trend, and random fluctuations may occur. There are two most often used types of Winters' model: (i) multiplicative model, when the level of seasonal fluctuations around the trend increases or decreases (more precisely when the relative level of seasonal fluctuations is approximately constant), and (ii) additive model, when the level of seasonal fluctuations around a weak trend or a constant level does not change, that is, when the absolute level of seasonal fluctuations is approximately constant. For the purpose of the presented solution, only the additive model will be described and used.

Winters' [43] model is described by means of three parameters, $\alpha$, $\beta$, and $\gamma$, representing, respectively, the smoothing constant for the trend's level, the change in the trend's level, and seasonal fluctuations. For so-described parameters, it then takes the following form:

$$\begin{aligned} F_{t-1} &= \alpha\left(x_{t-1} - C_{t-1-r}\right) + (1-\alpha)\left(F_{t-2} + S_{t-2}\right), \\ S_{t-1} &= \beta\left(F_{t-1} - F_{t-2}\right) + \left(1-\beta\right)S_{t-2}, \\ C_{t-1} &= \gamma\left(x_{t-1} - F_{t-1}\right) + \left(1-\gamma\right)C_{t-1-r}, \end{aligned} \tag{12}$$

where $x_1, x_2, \ldots, x_{n-1}$ are values of the forecasted series, $F_{t-1}$ is the smoothed value of the forecast variable in moment $t-1$ after elimination of the seasonal values, $S_{t-1}$ describes with evaluation the increment trend in the moment of time $t-1$, $C_{t-1}$ is evaluation of the seasonal index in the moment $t-1$, $r$ is the length of the seasonal cycle (the number of phases in the cycle, where $1 \le r \le n$), variables $\alpha$, $\beta$, and $\gamma$ are the model's parameters with values from the range [0, 1], and $t$ is an index of the following moments of time.

The forecast $x_t^*$ in the moment of time $t$ is given by the following dependency:

$$x_t^* = F_n + S_n\left(t-n\right) + C_{t-r}, \quad t > n. \tag{13}$$

Parameters $\alpha$, $\beta$, and $\gamma$ are chosen similarly as in Holt's model, minimizing the mean square error of the expired forecasts; or values close to 1 are chosen when the components of the time series change quickly; or values close to 0 are chosen when the series' components do not show quick changes.

As values of $F_1$, $S_1$, and $C_1$, we take, respectively, the value from the time series corresponding to the first phase of the second cycle (or the average value from the first cycle), the difference of the average values from the second and first cycles, and the quotient value of the variable in the first cycle in relation to the average value in the first cycle.

*5.3. Estimation of the Forecast Variability: Bollinger Bands.* Bollinger Bands is a tool of technical analysis invented by Bollinger at the beginning of the 80s of the 20th century [45]. It was created on the basis of observation of financial instruments volatility. It is composed of three elements: (i) the middle band (core), which is $n$ periodic moving average; (ii) the upper band, being $k$ times of $n$ periodic standard deviation above the middle band; and (iii) the bottom band, being $k$ times of $n$ periodic standard deviation below the middle band. The main idea of this tool is the rule that when data variability is low (their standard deviation decreases), then the bands shrink. However, in case the data variability increases, the bands expand. Thus, this tool shows dynamics of data variability. It usually defaults to the values of parameters $k = 2$ and $n = 20$ [46]. Such approach is based on the assumption that, in data of normal distribution, the area of two standard deviation widths includes 95 percent of all observations.

In the presented solution, we used Bollinger Bands to estimate forecasts variability of the exploited statistical models. As the middle band (the core), we adopted the values of statistical models' forecasts, $k$ was the double standard deviation, and $n = 15$ (due to the 15-minute analysis windows). Figure 3 presents an exemplary PPM signal and Bollinger Bands created on its base (for Holt's model).

*5.4. The Condition of Model's Parameters Update.* It is possible that data in the analyzed time series will fluctuate due to the nature of the AMI network traffic parameters. The reasons for such a phenomenon are to be found in possible changes of the AMI network infrastructure (ageing of devices and replacement with new/other models) or emergence of permanent obstacles, which have significant impact on the transmitted radio signal. These factors should cause adapting of the proposed anomaly detection method to the changing conditions (which are not an aftermath of any abuses). One of the possible solutions to so-stated problem can be an update procedure of the reference statistical models, realized on new data sets which contain the subject fluctuations.

The condition for creation of a new reference model should be detection of a significant and possibly permanent statistical variability in the analyzed data set (elements of a time series). Assuming a close-to-normal data distribution, we can deduce that in the range of width of six standard deviations there is over 99 percent of data. Thus, if we define

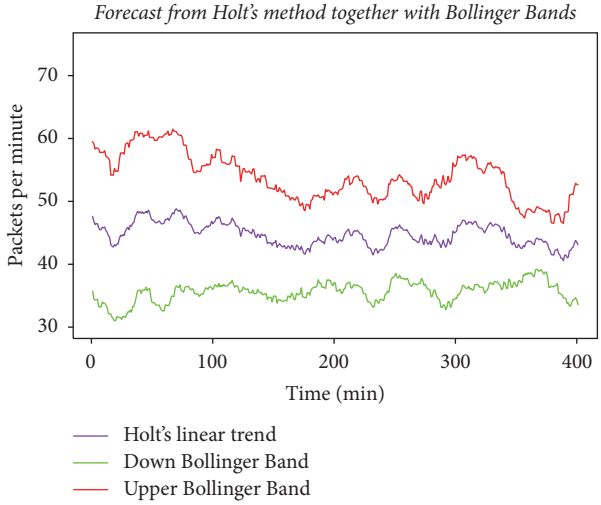


Figure 3: Exemplary Bollinger Bands for packets per minute (PPM) network feature.

the average on the basis of the forecast set of the given exponential smoothing model, and the standard deviation is estimated for the real values of the analyzed data, then a great degree of not fulfilling the above stated condition may proclaim that the statistical nature of the analyzed data has changed.

Due to the above, the following condition can be formulated. If it is not satisfied, the reference model should be updated.

$$x_i \in (\mu - 3\sigma, \mu - 3\sigma) \quad i = 1, 2, \ldots, n, \tag{14}$$

where $\{x_1, x_2, \ldots, x_n\}$ is a time series limited by $n$-elements analysis window, $\mu$ is the average calculated on the forecasts of the given reference model in the analysis window, and $\sigma$ is the variance of the tested time series elements in relation to such an average.

In result of conducting many experiments in the presented solution, we adopted the size of analysis window $n = 15$ and an assumption that only not satisfying condition (14) in over 30% of analysis windows in a time period of a week causes an effect in the form of reference model update.

## 6. Experimental Installation and Results

Figure 2 presents general overview of the proposed anomaly detection method. Traffic from 70 power meters distributed across eight buildings is captured by APN gateway through an IP link. The proposed method is divided into two mains steps: calculation of ADS model parameters and online anomaly detection. In both steps, we have to extract AMI traffic features proposed in Table 1. After that, we calculate initial reference models for every traffic feature. Models are calculated for a period of one week and time is divided into 15 minutes' analysis windows. Every traffic feature is organized as one-dimensional time series. First substep in model parameters calculating removes outlier values (see Section 5.1) from every traffic feature in order to remove

Table 1: AMI network traffic features captured from sensor network gateway.

| Network feature | AMI network traffic feature description |
|---|---|
| $NF_1$ | RSSI: received signal strength indication for AMI power meter [dBm] |
| $NF_2$ | LQI: link quality indicator value (values: 0–127) |
| $NF_3$ | PER: packet error rate per minute [%] |
| $NF_4$ | PPM: number of packets per minute |
| $NF_5$ | TTL: packet time to live value |

suspicious values from the model calculation. After that, we calculate exponential smooth models with the use of three exponential smooth models: Brown, Winters, and Holt (see Section 5.2).

In the next step, we compute Bollinger Bands (see Section 5.3) for achieving network traffic features variability intervals. In the end, we save models parameters together with associated Bollinger bands to database of reference models. In the second step of the proposed method, we compare values of online extracted AMI network features to reference models stored in the ADS database. ADS model gives us variability interval/variability canal for a given traffic feature. When the online calculated AMI traffic features values do not exceed interval set by the reference model, we assume that there is no anomaly/attack for a given traffic feature. When network traffic exceeds values set by the reference model, an anomaly detection report is generated for a given traffic feature.

The method proposed so far would not be resistant to AMI network changes, like increasing number of sensors or topology changes. In these cases, the reference models will not be updated and the number of FP indicators would increase in time. That is why we propose a trigger condition which is responsible for initiation of model parameters recalculation (see (14)). When the proposed condition is not satisfied in 30% of 15 minutes' analysis windows (30% of analysis windows in a period of one week), we recalculate traffic profiles for a period of one week (network traffic values are always stored for a period of one week which is why we can always recalculate traffic profiles when condition from (14) is not satisfied). New ADS network profiles are always active since the beginning of a new week.

*6.1. Experimental Setup and Results.* In this section, we showed experiments and results obtained in real-world test of the AMI power meter network. We proposed four different scenarios that trigger anomaly/attack in our test network. We proved that the proposed anomaly/attack detection method can be useful in detection of unwanted situations in the AMI measurement network.

The anomaly detection method presented in the article was evaluated by means of real-world installation of AMI network. The AMI network traffic was captured from installation placed in our university building [47]. The network consisted of 70 sensor nodes installed within energy power meters (see Figure 4). Sensors were installed on four floors (see Figure 6),

Table 2: DR [%] and FP [%] for anomalies/attacks performed on AMI network with Scenario 1.

| Feature | Holt | | Winters | | Brown | | Description |
|---|---|---|---|---|---|---|---|
| | DR [%] | FP [%] | DR [%] | FP [%] | DR [%] | FP [%] | |
| $NF_1$ | 92.40 | 8.80 | 90.20 | 9.80 | 88.10 | 10.40 | Significant impact on $NF_1$ in Scenario 1 |
| $NF_2$ | 96.00 | 5.60 | 94.10 | 7.50 | 90.20 | 9.80 | Significant impact on $NF_2$ in Scenario 1 |
| $NF_3$ | 91.00 | 9.40 | 88.40 | 11.30 | 86.30 | 12.70 | — |
| $NF_4$ | 81.40 | 9.20 | 89.10 | 11.10 | 86.20 | 12.60 | — |
| $NF_5$ | 72.20 | 10.20 | 70.10 | 12.60 | 68.20 | 12.80 | — |

Figure 4: Opened power meter with signed WSN communication radio module.

Figure 5: Cluster of electricity power meters in building 2.3.

located in eight separate buildings. In Figure 5, we can see a cluster of electricity meters installed in building 2.3 (see Figure 6). A traffic concentrator was placed on the second floor. Traffic from the AMI network was captured from IP connection of the traffic concentrator signed by red octagon located in building number 2.4 (see Figure 6). In the next step, we extract five traffic features $NF_1$–$NF_5$ (Table 1), where every traffic feature is represented by one-dimensional time series values.

We used these traffic features for anomaly/attack detection by means of the proposed statistical algorithm.

First two features describe the quality of the radio link: $NF_1$ RSSI [dBm] (higher value stands for better signal's strength) and $NF_2$ LQI value (values change from 0 to 127; lower values indicate higher link quality). LQI characterizes strength and quality of the received packet (in other words, how easily the received signal can be demodulated), contrary to RSSI, which gives us information about the received signal strength (it is not the measure of ability to decode signal), where radio frequency power can originate from arbitrary source such as Gaussian Frequency Shift Keying (GFSK), other ISM systems, Wi-Fi, Bluetooth, or background radiation. $NF_3$ and $NF_4$ features give us two values in a period of one minute: packet error rate (PER) per minute (number of corrupted packets received by concentrator)/(number of all packets received by the concentrator) in time interval (in our case, it was one minute) and PPM, number of packets per minute. $NF_5$ carries information about TTL value of packets received by a traffic concentrator. The proposed anomaly detection method was designed especially for data link and network layers. Because of security restrictions, we do not have access to the application layer payload. Application layer data is, in our case, available only for the energy supplier. We focused on detection of anomalies/attacks in layer 2 and layer 3, because there are not many anomaly detection solutions that work in last-mile AMI network. Additionally, predictable amounts of traffic made it a great candidate for anomaly detection, and we use this feature. Traffic is actually small taking into account computing power of the traffic concentrator processor but it is also large enough not to implement anomaly detection in smart meter.

We created different anomaly and attack scenarios for anomaly detection in the AMI network, and we selected four of them to evaluate the proposed method:

*Scenario 1.* Radio Frequency Interferences (RFI) and conducted interferences through power mains and Electromagnetic Interferences (EMI).

*Scenario 2.* Existence of natural and human-made obstacles,

*Scenario 3.* Power meter intentional damages,

*Scenario 4.* Coordinated attacks on power meter AMI network.

Scenarios used for anomaly/attack detection have various impacts on AMI network traffic features proposed in Table 1. In Scenario 1, we consider distortions caused by, for example, different radio ISM systems, and conducted EMI distortions carried by physical power line. A conducted EMI distortion may come from devices connected to power mains like electric engines, switching power supply, welding machines, or any industrial environment. Parts of conducted EMI distortions are presented in IEC standard 61000-4-4 [48]. We simulated some distortions that belong to both groups.

Distortions from Scenario 1 have biggest impact on network features $NF_1$ (RSSI) and $NF_2$ (LQI). Detection rate and false positive partial results for Scenario 1 are presented in Table 2.

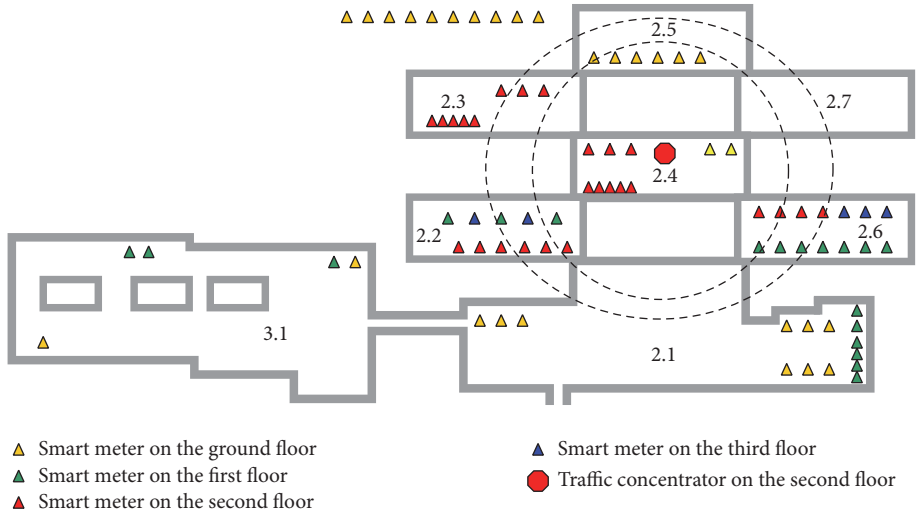


Figure 6: Physical layout of power meters of AMI network in the university building [5].

Table 3: DR [%] and FP [%] for anomalies/attacks performed on AMI network with Scenario 2.

| Feature | Holt | | Winters | | Brown | | Description |
|---|---|---|---|---|---|---|---|
| | DR [%] | FP [%] | DR [%] | FP [%] | DR [%] | FP [%] | |
| $NF_1$ | 88.20 | 8.20 | 86.10 | 10.10 | 83.20 | 11.80 | Significant impact on $NF_1$ in Scenario 2 |
| $NF_2$ | 92.40 | 5.20 | 90.30 | 7.30 | 87.50 | 9.40 | Significant impact on $NF_2$ in Scenario 2 |
| $NF_3$ | 82.20 | 9.60 | 80.20 | 11.20 | 76.40 | 12.40 | — |
| $NF_4$ | 80.20 | 10.10 | 78.10 | 12.10 | 76.30 | 12.60 | — |
| $NF_5$ | 85.60 | 12.20 | 82.40 | 12.60 | 79.40 | 12.80 | — |

An attack, according to Scenario 1, is easy to carry out, for example, by using amateur shortwave radio set to the same frequency as the working channel; modulation type does not matter. The best results in attacking give the transmitter localized close to the traffic concentrator or a cluster of electricity power meters.

Scenario 2 was simulated by locating groups of power meter sensors on different floors and distant buildings (see Figure 6). Temporarily placed obstacles, like a big truck, can also have an impact on WSN network transmission. Localization and distance between the AMI power meter sensors have impact on every captured network traffic feature. Partial results for Scenario 2 can be observed in Table 3.

The easiest way to carry out the attack according to Scenario 2 is grounding the concentrator antenna or slightly unscrewing it. In our experiments, we achieved this effect by reducing transmitting power and increasing the receiver's sensitivity simultaneously.

Intentional damage from Scenario 3 is caused by power meter users who want to avoid/delay paying electricity bills or want to bypass power meter or disturb AMI network operation. Electromagnetic metallic shielding and bypassing of power meter are exemplary methods for disturbing of the AMI sensor operation. Partial results for this scenario are presented in Table 4. Intentional damage can be seen especially for $NF_3$, where PER for a given power meter increases.

In our experiments, we simply turned smart meters off from mains or remotely changed the radio channel frequency just to make communication impossible. In real situation, instead of power meter intentional damaging, the easiest way to achieve the same effect is forcing the fuse protection (before input connector) to act.

Scenario 4 takes into account coordinated attacks/anomalies performed on power meters Smart Grid infrastructure. We simulate WSN flooding attack [49] and after that we add some intermediate sensor in order to perform additional links (Wormhole-type attack [30]). This type of attack/anomaly has the biggest impact on $NF_4$ PPM (number of packets per minute) and $NF_5$ TTL (packet time to live) value. Subsequent partial result can be seen in Table 5. In this scenario, traffic features ($NF_1$–$NF_3$) did not give us usable information for anomalies detection, so they can be omitted in this case.

Attacks, according to Scenario 2, were emulated by us with the use of smart meter service terminal, which is a mobile, specific kind of the traffic concentrator. We sent from service terminal to all power meters a "set date & time" command in broadcast flooding mode every 5 seconds.

Attacks described in Scenarios 1–3 require physical access, for example, in case of EMI distortions conducted through power mains or enough proximity to a selected part of physical infrastructure and in case of EMI distortions conducted through radio. Power meter shielding also requires

Table 4: DR [%] and FP [%] for anomalies/attacks performed on the AMI network with Scenario 3.

| Feature | Holt | | Winters | | Brown | | Description |
|---|---|---|---|---|---|---|---|
| | DR [%] | FP [%] | DR [%] | FP [%] | DR [%] | FP [%] | |
| $NF_1$ | 86.40 | 8.60 | 84.10 | 10.30 | 80.70 | 12.60 | — |
| $NF_2$ | 88.40 | 8.40 | 85.20 | 9.80 | 83.10 | 11.70 | Significant impact on $NF_2$ in Scenario 3 |
| $NF_3$ | 90.50 | 6.40 | 87.20 | 8.80 | 85.60 | 10.90 | Significant impact on $NF_3$ in Scenario 3 |
| $NF_4$ | 82.30 | 11.50 | 79.50 | 12.40 | 76.40 | 12.80 | — |
| $NF_5$ | 86.20 | 12.40 | 83.40 | 12.50 | 80.80 | 12.80 | — |

Table 5: DR [%] and FP [%] for anomalies/attacks performed on AMI network with Scenario 4.

| Feature | Holt | | Winters | | Brown | | Description |
|---|---|---|---|---|---|---|---|
| | DR [%] | FP [%] | DR [%] | FP [%] | DR [%] | FP [%] | |
| $NF_1$ | — | — | — | — | — | — | Insignificant/negligible for Scenario 4 |
| $NF_2$ | — | — | — | — | — | — | Insignificant/negligible for Scenario 4 |
| $NF_3$ | — | — | — | — | — | — | Insignificant/negligible for Scenario 4 |
| $NF_4$ | 92.40 | 6.50 | 90.20 | 8.60 | 87.10 | 10.40 | — |
| $NF_5$ | 90.50 | 7.60 | 87.30 | 9.80 | 85.50 | 11.70 | — |

physical access to power meter. In case of Scenario 4, for example, flooding attacks on last-mile network can be performed remotely by a GPRS/IP gateway.

The anomaly detection method based on network profiles has a weakness coming from the fact that profiles are aging. This can cause an increase in the false positive (FP) values. To alleviate this effect, we propose in Section 5.4 a condition that triggers recalculation of WSN network profiles. However, there can still be situations when temporary detection rates and false positive values can be a little bit worse between the profiles' update processes. These situations may appear when we rapidly change the network structure, for example, by adding entire streets with large number of new power meters. The proposed trigger will indicate the need to recalculate new profiles, but it will happen with a programmed delay.

In order to decrease effectiveness of the proposed anomaly detection solution, the attacker needs knowledge about anomaly detection algorithms used for profiles calculation, when the system recalculates profiles, and what kinds of traffic features are extracted from the network traffic. The attacker armed with such knowledge can temporarily disturb AMI network operation between recalculations of new profiles. If the attacker has information about traffic features used by anomaly detection algorithm, he can perform an attack that would not have an impact on the proposed traffic features.

Taking into account all four scenarios, the overall performance of the proposed anomaly/attack method for five AMI network features is presented in Table 6. Most simulated attacks and anomalies were detected. In case of DR [%], values change from 68.20 to 92.26%, while FP varies between 6.40 and 12.80%. The best results for three simulated scenarios (Scenarios 1–3) were obtained for features $NF_1$ and $NF_2$. For these scenarios, features $NF_1$ and $NF_2$ were the most universal. For Scenario 4, $NF_4$ and $NF_5$ features fit better to the characteristic of simulated anomalous events. From the three evaluated models, we achieved the best results for Holt's exponential smoothing model, where not only exponential smoothing but also forecasting for time series with trend is possible.

Table 6: Overall DR [%] and FP [%] for anomalies/attacks performed on AMI Smart Grid network.

| Feature | Holt | | Winters | | Brown | |
|---|---|---|---|---|---|---|
| | DR [%] | FP [%] | DR [%] | FP [%] | DR [%] | FP [%] |
| $NF_1$ | 89.00 | 8.53 | 86.80 | 10.07 | 84.00 | 11.60 |
| $NF_2$ | 92.26 | 6.40 | 89.87 | 8.20 | 86.93 | 10.30 |
| $NF_3$ | 87.90 | 8.47 | 85.27 | 10.43 | 82.77 | 12.00 |
| $NF_4$ | 84.07 | 9.32 | 84.23 | 11.05 | 81.50 | 12.10 |
| $NF_5$ | 83.62 | 10.60 | 80.80 | 11.88 | 78.48 | 12.53 |

Anomaly detection prediction based on Holt's exponential smoothing model gives us DR [%] values within 83.62–92.26% interval and FP [%] values changing from 6.40 to 10.60%. We were able to detect all performed anomalies/attacks described in the proposed scenarios taking into account all extracted traffic features (it was not possible to detect all anomalies/attacks by means of one traffic feature). In literature, there are many various anomaly detection methods using different algorithms [36, 50, 51] applied to WSN networks. On the basis of literature analysis, we can state that in general for WSN anomaly detection solutions FP [%] values are generally less than 10% [36, 50, 51]. Taking into account Holt's exponential smoothing model, we achieve FP values changing from 6.40 to 10.60%, so we can state that this interval is acceptable for anomaly detection class security systems.

## 7. Conclusions

Providing an adequate security and protection level of data sourced by intelligent measuring systems is currently an intensively examined and developed question for the world's

leading seats of learning. It is obvious that the AMI networks, due to their nature, are exposed to a significant number of threats originating from both outside and inside of their own infrastructure. Data collected recurrently by intelligent meters contain much information about private aspects of recipients' lives, which may be used for realization of serious abuse. Other, but not less important, problems of security within the AMI infrastructure are dangers coming from the recipients themselves. In some cases, they may perform actions which are destructive for the AMI. Such activities may consist in disturbing data saved in the meter or hampering their transmission. However, the key security problem is providing an adequate level of protection against external abuse, that is, safety from cyberattacks. In this case, every element of the SMCN infrastructure, AMI in particular, may become a potential attack point.

Growing level of complexity, globalization of range, and dynamically increasing number and nature of new attacks impose a change in approach towards realization of network security systems. Currently, most often implemented mechanisms are the methods of detection and classification of abnormal behaviors reflected in the analyzed network traffic parameters. An advantage of such solutions is protection against attacks unknown so far, often directed towards defined resources of critical infrastructures, or simply being the so-called zero-day exploits. Anomaly detection systems, in those cases, may play the key role. Their task is then detection (for the purposes of automatic response) of not typical behaviors in the network traffic which constitute symptoms of diverse abuse, originating both inside and outside the secured infrastructure.

The article presents an effective solution to the problem of anomaly detection in the network traffic for the critical measurement infrastructure. The structure of the AMI network, built for the purpose of the experiment, is presented and described. Crucial security problems which have a direct impact on proper operation of the advanced measurement infrastructure are discussed. A two-stage method was proposed for anomaly detection in the examined sensory network traffic, represented by proper time series. In the first stage, any possible outlying observations in the analyzed time series were detected and eliminated. The purpose of such operation was to prepare correct data for creation of standard statistical models based on exponential smoothing. Estimation of possible fluctuations of models' forecasts was realized by means of suitably parameterized Bollinger Bands. An update procedure was also proposed for the standard models in case serious fluctuations appear in the real network traffic. The second stage consisted in examining statistical relations between the standard traffic model and its real variability in order to detect abnormal behavior, which could signify an attempt of some abuse, for example, a network attack.

In the article, we proposed a method for anomaly/attack detection in data link and network layers. We did not analyze application layer, because in our case the application layer payload is only available for energy supplier. We focused on layer 2 and layer 3 because there are not many anomaly detection solutions in this area.

The proposed method of anomaly detection was evaluated with the use of real AMI network, which consists of 70 power meter nodes, located in eight distant buildings. After network traffic features extraction, we checked three different statistical models based on exponential smoothing together with Bollinger Bands. On the basis of four practical scenarios, we can conclude that the most promising results were achieved for Holt's exponential smoothing model. The proposed model fits to the characteristic of the network traffic features extracted from the AMI network. In case of Holt's model, not only is exponential smoothing possible, but also we can forecast time series with trend. We also propose a solution for aging reference models. We propose a condition (see (14)) for triggering recalculation of model parameters.

For future work, we are planning to examine usability of statistical models for anomaly detection in AMI power meter network using Power Line Communication (PLC) module instead of radio communication. In the next step, we would like to propose anomaly detection solution for hybrid AMI power meter network using at the same time radio communication and PLC communication modules.

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

## References

[1] S. Finster and I. Baumgart, "Privacy-aware smart metering: a survey," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 2, pp. 1088–1101, 2015.

[2] B. E. Bilgin, S. Baktir, and V. C. Gungor, "Collecting smart meter data via public transportation buses," *IET Intelligent Transport Systems*, vol. 10, no. 8, pp. 515–523, 2016.

[3] P. Kulkarni, S. Gormus, Z. Fan, and B. Motz, "A mesh-radio-based solution for smart metering networks," *IEEE Communications Magazine*, vol. 50, no. 7, pp. 86–95, 2012.

[4] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 6–28, 2004.

[5] 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.

[6] P. Kiedrowski, "Toward more efficient and more secure last mile smart metering and smart lighting communication systems

with the use of plc/rf hybrid technology," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 675926, 9 pages, 2015.

[7] 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.

[8] 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.

[9] S. Amin, G. A. Schwartz, A. A. Cardenas, and S. S. Sastry, "Game-theoretic models of electricity theft detection in smart utility networks: providing new capabilities with advanced metering infrastructure," *IEEE Control Systems*, vol. 35, no. 1, pp. 66–81, 2015.

[10] X. D. Wang and P. Yi, "Security framework for wireless communications in smart distribution grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 809–818, 2011.

[11] J.-L. Tsai and N.-W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 906–914, 2016.

[12] A. K. Marnerides, P. Smith, A. Schaeffer-Filho, and A. Mauthe, "Power consumption profiling using energy time-frequency distributions in smart grids," *IEEE Communications Letters*, vol. 19, no. 1, pp. 46–49, 2015.

[13] Y. Guo, C.-W. Ten, S. Hu, and W. W. Weaver, "Preventive maintenance for advanced metering infrastructure against malware propagation," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1314–1328, 2016.

[14] R. Berthier, D. I. Urbina, A. A. Cárdenas et al., "On the practicality of detecting anomalies with encrypted traffic in AMI," in *Proceedings of the 2014 IEEE International Conference on Smart Grid Communications, SmartGridComm 2014*, pp. 890–895, Venice, Italy, November 2014.

[15] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 667–674, 2011.

[16] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1244–1253, 2013.

[17] ITU-T Recommendation G.9904 (10/2012): Narrowband orthogonal frequency division multiplexing power line communication transceivers for PRIME networks, 2013.

[18] R. Moghaddass and J. Wang, "A hierarchical framework for smart grid anomaly detection using large-scale smart meter data," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–11, 2017.

[19] V. Aravinthan, V. Namboodiri, S. Sunku, and W. Jewell, "Wireless AMI application and security for controlled home area networks," in *Proceedings of the 2011 IEEE PES General Meeting: The Electrification of Transportation and the Grid of the Future*, Detroit, Mi, USA, July 2011.

[20] Trilliant, White Papers, The Home Area Network: Architectural Considerations for Rapid Innovation, pp. 1–7, 2010.

[21] M. Balakrishnan, *Security in Smart Meters, Document number: SEC s. MTMTRWP REV0*, Free scale Semiconductor, Arizona, Ariz, USA, 2012.

[22] B. J. Murrill, E. C. Liu, and R. M. Thompson, "Smart meter data: Privacy and cybersecurity," *Smart Meters and the Smart Grid: Privacy and Cybersecurity Considerations*, pp. 1–45, 2012.

[23] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," in *Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM'07)*, pp. 2526–2530, Barcelona, Spain, May 2007.

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

[25] E. Cayirci and C. Rong, *Security in Wireless Ad Hoc and Sensor Networks*, John Wiley and Sons, Ltd, 2009.

[26] H. K. D. Sarma and A. Kar, *Security Threats in Wireless Sensor Networks*, Elsevier, October 2006.

[27] M. Tyndall, R. Marshall, E. K. Armstrong, and C. Marshman, "Potential EMC implementation problems of smart metering, display and communications," in *Proceedings of the 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, ISGT Europe 2011*, Manchester, UK, December 2011.

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

[29] A. V. Pramo, M. Abdul Azeem, and O. M. Prakash, "Detecting the sybil attack in wireless sensor network," *International Journal of Computers & Technology*, vol. 3, no. 1, 2012.

[30] S. Ji, T. Chen, and S. Zhong, "Wormhole attack detection algorithms in wireless network coding systems," *IEEE Transactions on Mobile Computing*, vol. 14, no. 3, pp. 660–674, 2015.

[31] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[32] K. Billewicz, *Smart Metering Inteligentny System Pomiarowy*, Wydawnictwo Naukowe PWN, 2011.

[33] A. Lee and T. Brewer, "Guidelines for smart grid cyber security, 1, smart grid cyber security strategy, architecture and high-level requirements," NISTIR 7628, 2010.

[34] 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, May 2005.

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

[36] 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.

[37] R. D. Cook, "Detection of influential observation in linear regression," *Technometrics. A Journal of Statistics for the Physical, Chemical and Engineering Sciences*, vol. 19, no. 1, pp. 15–18, 1977.

[38] 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.

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

[40] C. C. Pegels, "Exponential forecasting: some new variations," *Management Science*, vol. 12, pp. 311–315, 1969.

[41] O. L. Davies and R. G. Brown, "Statistical forecasting for inventory control," *Journal of the Royal Statistical Society. Series A (General)*, vol. 123, no. 3, p. 348, 1960.

[42] C. C. Holt, *Forecasting Seasonals and Trends by Exponentially Weighted Moving Averages, ONR Memorandum*, vol. 52,

Carnegie Institute of Technology. Available from the Engineering Library, University of Texas at Austin, Pittsburgh, PA, USA, 1957.

[43] P. R. Winters, "Forecasting sales by exponentially weighted moving averages," *Management Science. Journal of the Institute of Management Science. Application and Theory Series*, vol. 6, pp. 324–342, 1960.

[44] R. G. Brown, *Smoothing, Forecasting and Prediction of Discrete Time Series*, Prentice-Hall, Englewood Cliffs, NJ, USA, 1963.

[45] J. Bollinger, *Bollinger on Bollinger Bands*, McGraw Hill, 2002.

[46] S. Vervoort, "Smoothing the bollinger bands," *Technical Analysis of Stocks & Commodities*, vol. 28, no. 6, pp. 40–44, 2010.

[47] UTP University of Science and Technology in Bydgoszcz, Poland, http://wyszukaj.utp.edu.pl/mapa.

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

[49] Y. Guo, C.-W. Ten, S. Hu, and W. W. Weaver, "Modeling distributed denial of service attack in advanced metering infrastructure," in *Proceedings of the 2015 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference (ISGT'15)*, February 2015.

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

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