An efficient Intrusion Detection System against cyber-physical attacks in the smart grid

Mohamed Attia, Sidi Mohammed Senouci, Hichem Sedjelmaci, El-Hassane Aglzim, Daniela Chrenko

An efficient Intrusion Detection System against cyber-physical attacks in the smart grid☆

Mohamed Attia[a,*], Sidi Mohammed Senouci[a], Hichem Sedjelmaci[b], El-Hassane Aglzim[a], Daniela Chrenko[c]

[a] DRIVE EA1859, University of Bourgogne Franche-Comté, Nevers F58000, France
[b] IRT SystemX, Paris-Saclay, France
[c] University of Technology at Belfort-Montbéliard, Belfort 90010, France

Without robust security mechanisms, the smart grid remains vulnerable to many attacks that can cause serious damages. Since state estimation is a critical entity to monitor and control electricity production and distribution, intruders are more attracted by this entity in order to disrupt the smart grid reliability. In this context, we propose an Intrusion Detection System (IDS) archi-tecture to detect lethal attacks with a focus on two smart grid security issues: (i) Firstly, against integrity issue with price manipulation attack, we propose a Cumulative Sum (CUSUM) algo-rithm that detects this attack even with granular price changes; (ii) Secondly, the availability issue with Denial of Service (DoS) attack against which we develop an efficient method to monitor and detect any misbehaving node. Performance evaluations show the robustness of the proposed IDS system compared to existing mechanisms. The achieved detection rate is above 95% and the false positive rate is below 5%.

1. Introduction

Today, electric power distribution is made possible by the power distribution grid; a system of transmission mediums that allows electricity to be transferred from the point of generation to consumers like homes, offices or industries. The electrical grid is expected to evolve to a new grid paradigm: the smart grid that uses two-way flows of electricity and information to create an automated and distributed advanced energy delivery network. A smart grid is an electricity network that can intelligently integrate the actions of all users connected to it – generators, consumers, and those that do both – in order to optimize the production, supply as well as the consumption of electricity and provide several features to its customers [1]. This smartness comes from the usage of Information and Communication Technologies (ICT) [2], where data is exchanged between three main levels, as described with more details in the proposed architecture in Section 3. The first level is Home Area Network (HAN), which is composed by consumer's appliances like smart meters and connected devices. The second level, known as Neighborhood Area Network (NAN), is the aggregator where consumers' information is aggregated to be transmitted to the upper level. Finally, the last level is the control center where all data are analyzed.

Though, all smart grid features and advantages will be useless if this system is highly vulnerable to different kinds of attacks that

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. N. K. Yadhav.

* Corresponding author.
E-mail addresses: mohamed.attia@u-bourgogne.fr (M. Attia), Sidi-Mohammed.Senouci@u-bourgogne.fr (S.M. Senouci), hichem.sedjelmaci@irt-systemx.fr (H. Sedjelmaci), el-hassane.aglzim@u-bourgogne.fr (E.-H. Aglzim), daniela.chrenko@utbm.fr (D. Chrenko).

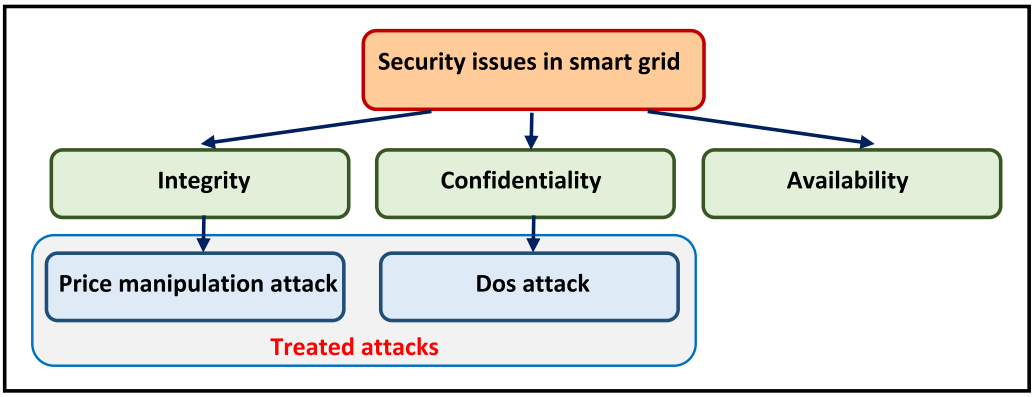

Fig. 1. Security issues in smart grid and classification of treated attacks.

can turn those features to catastrophic results beginning by non-satisfying consumers' needs, disrupting the electricity grid and in some cases causing serious physical damages to the utility grid or even intermediate stakeholders and end consumers' equipment [3].

As shown in Fig. 1, three main security objectives should be addressed in the smart grid: availability, integrity and confidentiality [4,5]. Among lethal attacks targeting availability in smart grid, there are *traffic flooding*, where the attacker aims to delay message transmission [6], *buffer flooding*, in which the intruder sends many false events in order to flood the aggregator's buffer [7] and *jamming attack,* where the attacker jams the power price for a period to make a great change in consumers' behavior [8]. All those attacks are categorized as *Denial-of-Service (DoS) attacks* where intruders aim to degrade the communication performance and prevent different stakeholders from useful information [9]. Besides, the control center will be unable to extract proper estimation of the electricity consumed and then will be pushed to take wrong decisions to produce energy and supply it to the appropriate regions.

Concerning confidentiality issue, there are many attacks presented in literature like eavesdropping communication channels in power networks to intercept useful data using traffic analyzers [10] or wiretappers (i.e. equipment used to eavesdrop channels) [11]. For the integrity issue, *false data injection (FDI) attacks* are heavily threatening the smart grid and can be introduced at different levels. For example, we mention *load redistribution attack* where the attacker compromises critical nodes to alter the load distribution and make serious damages [12]. Furthermore, *price manipulation attack* is one of the stealthy attacks that can occur and threat the smart grid information integrity and has a dangerous effect on the demand response equilibrium. This attack can cause huge changes in the demanded and/or consumed power, which may disorder the smart grid stability [13]. This kind of attack is known under different names in the literature like price information falsification [13], fabrication of price messages and false price injection [14].

With these kinds of attacks, the attacker may act in three levels: first, the attacker may target the control center or pretend that he is the control center and send a fake pricing. However, this task is not easy to the attacker since the control center is strongly robust against attacks because of its paramount role to collect information and make decisions. Furthermore, it has a huge computation capacity and can therefore integrate sophisticated security algorithms. That is why, it is fair to consider that this entity is trustful and cannot be threatened. Second, the attacker can target the aggregator node where he can alter the price information or block access to this node and thereafter create a fake access point. Third, the attacker can act at the level of the customer site by modifying the pricing information in the smart meter. This disturbance can be made by either the modification of *price information* or a *jamming attack* where the intruder can prevent the customer from receiving the right price information [9]. These kinds of attacks can cause many problems like lines failure [14] or financial losses [15].

The state estimation is a paramount entity that enhances the efficiency and reliability of the smart grid. It provides the estimation of the electricity production and consumption states in real time based on meter measurements. For this reason, we focus our work to deal with attacks that target especially the state estimation since they are lethal and can make greater damages compared to other attacks [16]. Hence, this paper focuses on *price manipulation attack* and develops a detection model based on Cumulative Sum (CUSUM: a sequential analysis technique used for monitoring change detection) algorithm. Moreover, an abnormal behavior detection algorithm is proposed to identify *DoS attacks*. Our added value draws its strength from the fine selection of the algorithm parameters obtaining a high accuracy rate. Furthermore, the proposed models rely on a lightweight detection algorithm since it is based on simple but efficient rules and equations to fit with all nodes especially those with restricted computation capacity like smart meters.

The main contributions in this paper are summarized as follows:

- A taxonomy is constructed to classify attacks targeting integrity and availability in smart grid.
- A new smart gird architecture with hierarchical IDS agents deployment is proposed.
- A *price manipulation attack* detection algorithm is developed based on CUSUM algorithm. It can detect this attack even with granular price change, which is not possible using traditional security mechanisms.
- An efficient method is developed to monitor and detect any misbehaving node to counter *DoS attacks*.

The remainder of this paper is organized as follows: an overview of the related works is presented in Section 2. Section 3

Table 1
Attacks taxonomy.

Reference	Attack naming	Attack description	Targeted issue	Impact on	Detection mechanism	Reaction
[16]	False data injection	Injecting false data	Integrity	Power grid operation system	CUSUM algorithm	N.C
[9]	Jamming attack	Jamming Signal channels	Availability	Electricity price	Multiact dynamic game	N.C
[17]	Time delay attack	Introducing delays in the telemetered control signals	Availability	Dynamics of power system	N.C	N.C
[18]	Blind false data injection	Injecting false data	Integrity	State estimation	N.C	N.C
[19]	False data injection	Injecting false information	Integrity	Pricing signals	Non-parametric CUSUM detection	Control algorithm
[20]	False data injection	Sending bogus measurements	Integrity	State estimation	N.C	N.C
[14]	Rate alteration attack	Fabricating price messages	Integrity	Consumers load profile	N.C	N.C
[13]	DoS and price information attack	Making power price unavailable or falsified	Availability integrity	Real time pricing	N.C	N.C
[21]	Jamming attack	Broadcast interference to disrupt messages	Availability	Network traffic load	N.C	Generating camouflage traffic

*N.C : Not Concerned.

introduces the proposed architecture with the placement of IDS agents. Then, attack models, their impacts and countermeasures are described in Section 4. Numerical results are introduced in Section 5. Finally, we conclude this paper in Section 6.

2. Related work

In this section, some related works on smart grid security mechanisms against lethal attacks are summarized. These attacks mainly target to disturb the state estimation and make damages to the smart grid.

Table 1 conducts a taxonomy to categorize the main security issues and solutions exposed in literature, including attack naming and description, targeted issue, impacts on the targeted entities and finally the proposed detection and reaction mechanisms. Hereafter, main contributions are detailed.

In [16], Yang et al. developed an algorithm to identify the optimal number of smart meters to manipulate in order to find the optimal attack strategy, which aims to perturb the state estimation of the grid system and bother its stability. Then, to defend against this attack, they proposed a rule-based detection to identify the stealthy false data injection in the network using *CUSUM* technique [16]. The drawback of this work is that this algorithm is embedded in a centralized way in the control center unit, which makes the detection of distributed attackers difficult. In addition, the control center cannot monitor the entire network, especially when a huge number of connected devices, like smart meters and sensors, are connected. A centralized monitoring system generates also a high overhead since it has to collect and analyze all received packets.

Ma et al. [9] proposed a multiact dynamic game between the attacker and defender, in which the optimal strategies are taken by the two sides to maximize their own profits. Here, the attacker would proceed to jam a certain number of signal channels carrying measurement information. The goal is to manipulate the electricity price in order to create an opportunity for gaining profit. In this paper, the authors do not evaluate their approach in terms of detection as well as false positive rates to test the performance and robustness of their model.

Recently, Sargolzaei et al. [17] modeled a *Time Delay Switch (TDS) attack*. This attack consists in putting a random delay on the power Load Frequency Control (LFC) system. They proved the impact of this attack and demonstrated the risks and damages that it can leave on the power system. Besides, they do not propose any countermeasure to prevent the intrusion caused by this attack.

Yu et al. [18] aimed to generate a new *blind false data injection attack* by using the Principal Component Analysis (PCA) approach. The drawback of this work is that the authors suppose that malicious attackers have knowledge of the grid topology. This assumption is not evident especially with the extreme extension and complexity of the smart grid. Moreover, like the previous work, there is no defensive mechanism to detect those stealthy attacks and ensure the protection of the state estimation.

Giraldo et al. [19] developed an attack model where the intruder compromises a device or a communication channel to inject an arbitrary time signal in the price information. To detect this attack, they developed a non-parametric CUSUM detection statistic. Moreover, they proposed a control algorithm to mitigate the negative impacts of the treated attacks. The drawback of this work is that the attacker launches random attacks that can be very small so negligible or very high and so easily detectable. Furthermore, the detection time is high and can degrade the smart grid performance.

Bi and Zhang [20] formulated a *false data injection attack* where the intruder firstly starts fabricating biased transmission congestion pattern, then injects false electricity price. To do so, a simple algorithm is proposed to find the most appropriate congestion pattern with lower possible change in the normal system operators. Moreover, the impact of this *load redistribution attack* on the future market is discussed.

Mishra et al. [14] dealt with the *rate alteration attack* by fabricating price messages. This leads to a major alteration in the electricity consumption profile and disorder the smart grid. They treat also the problem of cascading failure where the attacker chooses the best lines to make greater failures.

Dong et al. [13] investigated the impact of *DoS* and *price information attacks* targeting the real-time pricing in order to mislead the demand response program in the smart grid and push it to make wrong decisions. This wrong decision is caused by the inability of getting the correct actual electricity price. They proposed a Constrained Markov Decision Process (CMDP) to analyze the loss that can be generated from these attacks.

Lu et al. [21] developed a generic *jamming attack* model, then investigate its impact in terms of generated delays on the network traffic load. They proved that the delay performance for practical smart grid applications is highly sensitive to the network traffic load under this attack. Moreover, they proposed a distributed model named TACT (Transmitted Adaptive Camouflage Traffic) that helps to mitigate the negative effect of *jamming attack*. Nevertheless, there is no countermeasure proposed to defend against these attacks in the last cited works.

Based on Table 1, it can be noticed that there is no detection model that is both robust and lightweight able to defend the smart grid against *price manipulation attacks* especially with granular price changes, which are generally undetectable by traditional security mechanisms. Using the same statement for *DoS attack* for which most proposed defensive models are not lightweight and therefore cannot be embedded in low resource capacity devices such as smart meters. In this context, we develop lightweight algorithms (since rely on rule-based-detection) that can detect even minor alteration attacks in electricity price as well as misbehaving nodes launching *DoS attacks*.

3. Proposed smart grid architecture with IDS agents deployment

In this section, the hierarchical architecture of the proposed Intrusion Detection System (IDS) including the placement of the IDS modules to protect the smart grid from attackers is presented.

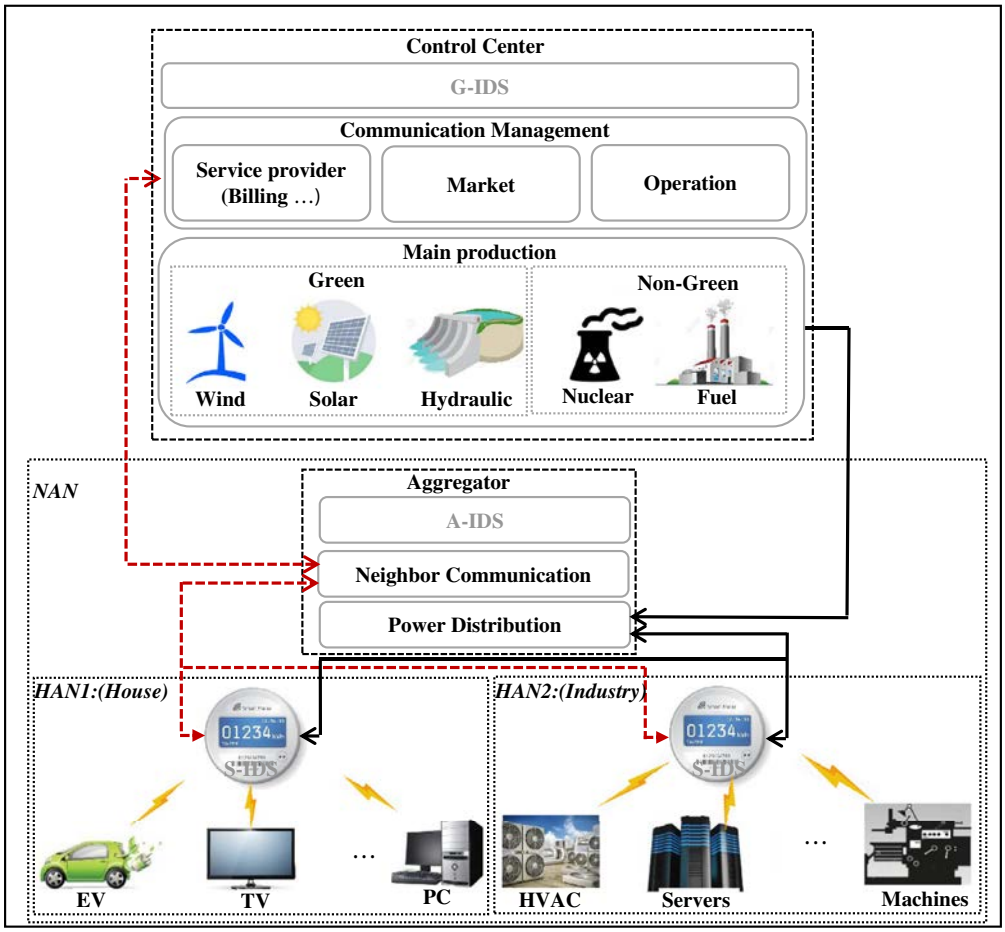

Fig. 2. HAN & NAN architecture with IDS agents' deployment hierarchy.

As shown in Fig. 2, the architecture integrates all smart grid levels, starting from the lowest level, known as Home Area Network (HAN) [22]. Then, by expanding the scope, the Neighborhood Area Network (NAN) [22] is formed. Finally, the head-ends and the communication management construct the top level. All these entities are monitored by the control center [16].

At the HAN level, we differentiate between two kinds of consumers: the first ones are characterized by low electricity consumption, namely the houses. They do not need specific equipment or sophisticated devices to control or manage their used power. The second ones are those consuming a huge amount of electricity like industries, hospitals, companies, etc. These kinds of consumers require dedicated infrastructure with high monitoring mechanism. An IDS agent (noted S-IDS (SmartMeter-IDS) in Fig. 2) is embedded at each smart meter node to monitor appliances like TV, laptop, industrial machine, HVAC, etc. A wireless network like Zigbee or Bluetooth carries the communication. Composed by several HANs, the NAN is featured also by a neighbor communication block to ensure the control of messages interconnection between control center and HAN via WiFi or Zigbee technology. According to the power network, a power distribution block supplies the electricity from head ends to end consumers. These two latest blocks constitute the aggregator (called also actuator or collector) [22] in which we introduce an IDS agent (noted A-IDS (Aggregator-IDS) in Fig. 2) to supervise the HANs data and control messages in a semi-centralized manner. The main role of the actuator is to aggregate data, remove redundant information [15] and send them to the control center afterwards.

At the centralized level, the control center guides the whole communication and management aspect of the smart grid, namely billing, marketing and operation as well as power production from renewable or non-renewable sources. An IDS agent (noted G-IDS (Global-IDS) in Fig. 2) is deployed also in the control center to monitor the lower levels (i.e. Aggregators and smart meters) and to reduce the risk of attacking this critical node, which is responsible of collecting all information and make the adequate decision to balance between electricity supply and demand. The dashed red arrows represent the communication interconnections between the different equipment. These connections can be either wired or wireless like ZigBee, Bluetooth or Wi-Fi. The black full line arrows represent the power interconnection between different electricity network components, which is insured by the traditional power lines.

The IDS agents' distribution architecture takes advantages from the distributed aspect by deploying these agents at the smart meters' level, then with more centralized manner at the aggregator level and finally with pure centralized manner in the control center level. Following this distribution, we gain the features of the hierarchical distribution. The added value of this architecture

compared to those proposed in literature like in [16] remains in the fact that, in one side, even if the attack is bypassed and not detected in such level (i.e. smart meter or aggregator), it will be detected at the upper level which has by definition more computation capacity to detect intruders. In the other side, if the attack is identified in lower level, it will reduce the monitoring load and overhead of the upper level.

4. Attacks models, impacts and countermeasures

This section first describes the attacks models to launch *price manipulation* then *DoS attacks*, followed by their impacts and countermeasures. As discussed before, we consider that the control center is a trustful entity since it incorporates a great computation capacity and hence robust detection policies. Therefore, the attacker can launch his attack at either the smart meter or the aggregator level. Any detected attack will be forwarded to the control center to take the convenient decision towards this node.

4.1. Attacks model

In this subsection, the attacker's strategy to launch price or *DoS attack* is introduced.

4.1.1. Price manipulation attack

The purpose of the intruder here is to alter the real electricity price information which aims to induce the end-user electricity consumption behavior. To do so, the attacker starts with identifying the actual price in the network, then calculates the change to make in order to reach his goal and overheat the cables until their braking [14] or at least make financial loss to the utility [13], limiting the variation and hence avoids being detected. Based on price elasticity of demand (i.e. the rate linking between the change in electricity demanded and the change in its price), the attacker computes the change that he should make in the current price to obtain the desired variation of electricity to be consumed. The *price elasticity of demand* measures the impact of small variation in price on the demand. It is calculated as follows:

$$\begin{aligned} \varepsilon &= \frac{\%\,Change\ in\ Quantity\ Demanded}{\%\,Change\ in\ Price} \\ &= \frac{\Delta q/q}{\Delta p/p} \end{aligned} \tag{1}$$

where q, Δq, p, Δp are consumed electricity (in MWh), variation on consumed electricity, electricity price (per MWh) and variation on electricity price, respectively.

There are two kinds of price elasticity of demand: a high elasticity where a low change in price implies a high change in demand; and a low elasticity where a low change in price implies a low change in demand. In electricity price case, the elasticity of demand is high. Therefore, the attacker has to make a little change in electricity price to create a huge difference in electricity demand and consumption since the latter is very sensitive to any price change.

Two main actions of the attacker can be distinguished with the aim to cause damages in the smart grid or make it unstable and pushed to financial loss. The first can be done by increasing the electricity price when it is cheap in order to discourage customers to consume energy. In this case, an important difference between electricity produced and consumed is made (i.e. more electricity produced than consumed). This will lead to financial loss because of electricity overproduction, then the remaining load will be lost and dissipated by Joule effect. The other case is reducing the electricity price during peak times (i.e. when the electricity demand is high) where the price is supposed to be high in order to meet this demand and reduce energy consumption. Hence, the electricity generator will exhaust its resources to provide the demanded power. Moreover, the load will increase and exceed the lines' capacities resulting on lines failure.

4.1.2. DoS attack

The attacker's goal here is to disturb the state estimation by preventing it useful information. For example, an intruder can jam the signal and hence prevent the system from sending or receiving useful information like electricity price, amount of electricity consumed or even the needed amount to be produced. Several attacks can lead to this goal like *blackhole attack* [23], which consists in dropping messages sent or received from one node to another (i.e. delete them or do not send them). This attack is characterized by the fluctuation of the Packet Delivery Ratio (PDR) [23]. Therefore, the number of sent packets will no longer follow normal distribution like in the case of natural situation. This kind of attack prevents the state estimation from having accurate information of the consumed energy or the future demand load. Therefore, this will lead it to take wrong decisions in terms of electricity consumption prevision as well as false energy command production.

Another attack can be envisaged, *time delay attack* [17], where the attacker makes some delays in sent packets and so, the Jitter (i.e. the delay between exchanged packets) will deviate from normal distribution. This can lead also, in its turn to a wrong decision at the wrong time. This kind of attacks can lead to critical problems like infrastructure damages, service interruption or financial loss due to the existence of malicious users [22]. The financial loss may affect not only the utility company, but involves also the premise owner. These attacks can be performed through the smart meter's communication module or the aggregator.

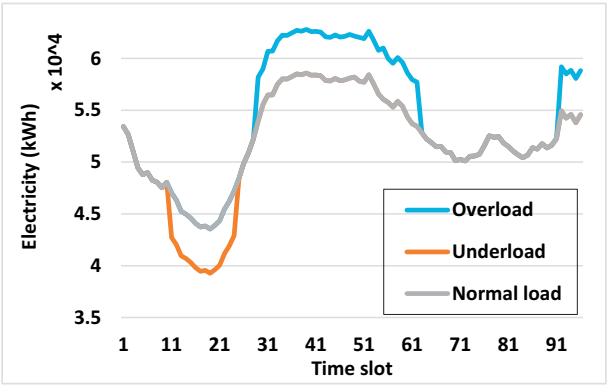

Fig. 3. Electricity demand evolution under attack.

4.2. Attacks impact

In this subsection, the impacts and damages that *DoS* and *price manipulation attacks* can leave are discussed. The main negative impacts are twofold: the first is the financial loss that can affect both the utility provider and the consumer. The second is lines failure. The attacks impacts are obtained considering a statistical analysis of how such attacks can induce the hole electricity consumption profile, and hence how this can cause financial losses and lines failure. For simplicity purposes and to have more accurate values, we apply this analysis on only smart meters. However, it is obvious that the impact of these attacks is more serious when targeting aggregators, depending on the number of connected smart meters to this node.

As shown in Fig. 3, the attacker has more interest to launch his attack in specific time slots, namely when the electricity is very expensive or very cheap. He attempts to be opportunistic and attack in periods that guarantee to reach his goal and disrupt the smart grid. That is why he avoids random attacks that risk to be not effective. As introduced before, among the goals of the attacker, there is pushing the utility provider to financial loss by jamming or increasing the electricity price when the demand and so the price is low. This case is illustrated in Fig. 3 by the orange line (noted underload). He may choose also the period of the highest demand to launch this attack (represented by blue line in the figure and noted by overload). Consequently, he can make heavy damages in the smart grid where generators risk to be harmed and electricity lines risk to be overloaded and broken.

These actions can be achieved by either altering the pricing information or jamming the signal carrying the pricing data (DoS attack). Therefore, the consumer will either receive a wrong electricity price or be deprived of the new electricity pricing and then he may consider the old pricing information. As consequence, these attacks will make a huge change in the hole electricity consumption profile. This will create a great disturbance on the state estimation and may make several damages to the smart grid.

The impact of the attack is always more serious for the utility provider compared to the consumer because it follows the electricity profile reduction or saturation of all consumers. As shown in Fig. 4, the financial loss is estimated to be 184 Euros per day when the attacker is compromising only 100 smart meters and can reach 256 Euros in the case of attacks spread among 200 smart meters. The financial loss will be catastrophic if the attacker succeeds to launch his attack to a large number of nodes. This loss is obviously heavy when it is calculated for a whole year and can exceed billions of Euros when the attacker succeeds to compromise several smart meters deployed in the whole country. For instance, in France there is a prevision to deploy more than 35 million smart meters by 2021. By attacking all of them, the financial loss can exceed 40 million Euros per day.

The issue of lines failure can lead to entire regions deprived of electricity. Moreover, in this case, the utility provider will have to

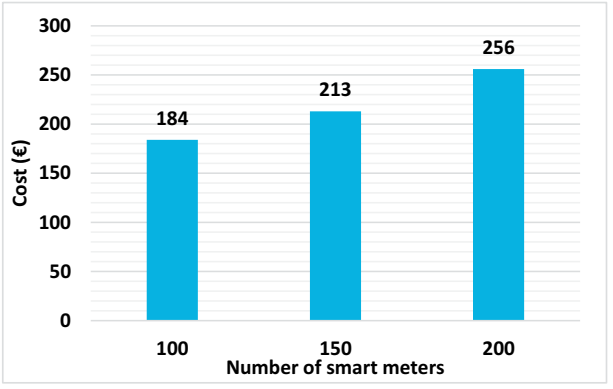

Fig. 4. Financial loss per day for a restricted number of smart meters.

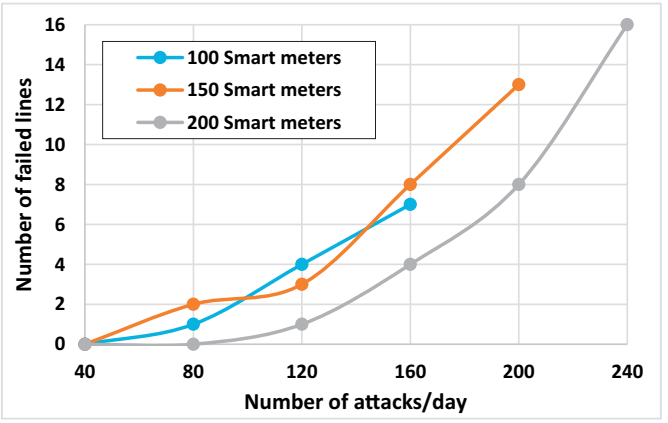

Fig. 5. Lines failure due to attacks.

invest in additional material to fix this failure, which is very heavy in terms of money and time. Fig. 5 depicts the evolution of lines failure in function of the number of launched attacks. For 100 smart meters, the number of failed lines can reach 7 for 160 launched attacks. The lines failure will highly increase when the falsified electricity price reaches larger number of smart meters. In the case of 200 smart meters, the number of broken lines is increasing to 16 when the attacker succeeds to introduce 240 attacks. Another catastrophic impact can be produced in this context: the cascading failure [24]. When one concerned line is overloaded until its heating, this line will be broken. After that, the entire load of this line will be switched to other lines. If those lines cannot support this additional and accumulated load, they will be overloaded and heated, which will eventually cause their failure.

4.3. Attacks countermeasures

This subsection introduces the proposed countermeasure models against *price manipulation* and *DoS attacks*, respectively.

4.3.1. Price manipulation attack

Here, we suppose that the price is updated by the utility each $k = 15$ min [19]. To detect this attack, Cumulative Sum (CUSUM) approach is used because of its accuracy to monitor and detect any small deviation. The detection rules and equations are as follows:

$$S(0) = 0 \tag{2}$$

$$S(k+1) = S(k) + p(k) - w(k) \tag{3}$$

$$\text{Take action if} |S(k+1)| > \alpha_1 \,\&\, |S(k+1) - S(k)| > \alpha_2 \tag{4}$$

where *S(k), p(k), w(k),* α_1 and α_2 are CUSUM algorithm parameters: the accumulated impact of the disturbance, electricity price, mean value, CUSUM and additional thresholds respectively. The mean value is calculated based on the price estimation. It depends on the previous announced prices and the prevision of the future price depending on the electricity demand evolution.

The effectiveness of this algorithm relies heavily on *w(k)* which should be selected carefully since the CUSUM sensitivity measurement comes essentially from the subtraction $p(k) - w(k)$. Note that the price variation is finely moderated over time and cannot be increased or decreased abruptly. Otherwise, the pricing policy is under attack. The second important parameter in the algorithm is the CUSUM threshold, α_1. This parameter value should be also precise to obtain high accuracy rate. The second condition (i.e. $|S(k+1) - S(k)| > \alpha_2$) does not belong to the standard CUSUM algorithm. It is added to enhance the accuracy of our detection

Algorithm 1
Price manipulation attack detection.

For each time slot k
  //**Inputs :**
  Electricity price $p(k)$
  accumulated impact of the disturbance $S(k)$
  //**Compute:**
  mean value $w(k)$
  thresholds α_1 and α_2
  $S(k+1)$
  If $|S(k+1)| > \alpha_1$ and $|S(k+1) - S(k)| > \alpha_2$ **then**
    Send alert for attack detection with the node Id and the type of attack to the control center
  End if
End for

system. This condition tackles the fact that the attacker always launches a small price change attack to stay undetectable. Hence, by applying only the first condition, we may fall in bad detection rate when using a high threshold (i.e. high value of α_1). However, when minimizing the first threshold, high false alarms rate may occur where some normal nodes will be declared as malicious. The two thresholds α_1 and α_2 are computed based on the reaction of the system in normal conditions and under attack. Algorithm 1 summarizes the steps followed by our Intrusion Detection System to identify *price manipulation attack*.

4.3.2. DoS attack

Here, the model to detect any abnormal behavior of the node (i.e. smart meter, aggregator) is developed. When a node behavior does not follow normal distribution, it will be suspected and classified as malicious node.

$$\begin{array}{c} \\ Node1 \\ Node2 \\ Node3 \\ \vdots \\ Noden \end{array} \begin{bmatrix} \boldsymbol{t1} & \boldsymbol{t2} & \boldsymbol{t3} & \cdots & \boldsymbol{tk} \\ y1(t1) & y1(t2) & y1(t3) & \cdots & y1(tk) \\ y2(t1) & y2(t2) & y2(t3) & \cdots & y2(tk) \\ y3(t1) & y3(t2) & y3(t3) & \cdots & y3(tk) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ yn(t1) & yn(t2) & yn(t3) & \cdots & yn(tk) \end{bmatrix}$$

Matrix M (5)

We note by $V_{Nj} = \{y_j(t_1), y_j(t_2), y_j(t), \ldots y_j(t_k)\}$ the node j's vector where t_k represents the time (k is the number of time slots). $y_j(t_k)$ denotes the PDR (Packet Delivery Ratio) or the Jitter (i.e. the delay between exchanged packets). The parameter n represents the number of nodes to be monitored (i.e. $j = 1 \ldots n$). Having n nodes where each one possesses k values, we form the matrix M with size $n*k$ as shown in Eq. (5).

To have a normal behavior, each node should have a PDR/Jitter flow that follows normal distribution characterized by $(\mu_1(j), \sigma_1(j))$. $\mu_1(j)$ represents the mean value and $\sigma_1(j)$ represents the standard deviation. $\mu_1(j)$ and $\sigma_1(j)$ are calculated as follows:

$$\mu_1(j) = \frac{\sum_{i=1}^{k} y_j(t_i)}{k} \tag{6}$$

$$\sigma_1(j) = \sqrt{\frac{\sum_{i=1}^{k} (y_j(t_i) - \mu_1(j))^2}{k}} \tag{7}$$

When $y_j(t_k)$ is outside the interval $[\mu_1(j) - 3*\sigma_1(j), \mu_1(j) + 3*\sigma_1(j)]$, the node is no longer following normal distribution. Therefore, this node will be classified as suspect. Applying this algorithm at each line (i.e. each node) of matrix M, we monitor the node behavior over time. For each time slot, the couple $(\mu_1(j), \sigma_1(j))$ is calculated to check if the node behavior follows normal distribution or not and hence if the node is normal or not. To enhance our algorithm performance and obtain better detection accuracy, we monitor also the node behavior among its neighbors (nodes on the same geographical zone having similar characteristics like smart meters for the same neighborhood). To do so, the algorithm is applied to each column of the matrix M. We note by $C_{Ni} = \{x_i(N_1), x_i(N_2), x_i(N_3), \ldots x_i(N_n)\}$ the i^{th} column (representing the i^{th} time slot) of the matrix M where N_j is the j^{th} node ($j = 1 \ldots n$). In normal situation, the number of exchanged packets at each node as well as the Jitter between those packets follow a normal distribution [23]. To have a normal behavior, the average number of sent packets/Jitter should be within an interval of $[\mu_2(i) - 3*\sigma_2(i), \mu_2(i) + 3*\sigma_2(i)]$, where:

$$\mu_2(i) = \frac{\sum_{j=1}^{n} x_i(N_j)}{n} \tag{8}$$

$$\sigma_2(i) = \sqrt{\frac{\sum_{j=1}^{n} (x_i(N_j) - \mu_2(i))^2}{n}} \tag{9}$$

In other words, at each time slot t_j, the behavior of each node is checked to identify if it follows normal distribution compared to its neighbors during the same time slot. Otherwise, it will be classified as suspect. Consequently, if the $y_j(t_k)$ value of the j^{th} node does not follow normal distribution over time and compared to its neighbors, it will be declared as malicious. In this case, an alert message will be sent to the control center to take appropriate action against this node. This double monitoring of the node (over time and by comparison to its neighbors) allows us to enhance the detection rate and reduce the false positive rate to counter this kind of attack. Furthermore, this technique reduces false alarms in case of network congestion or overload. Algorithm 2 introduced below provides the instructions of our Intrusion Detection System to identify *DoS attacks*.

As detailed in the proposed architecture in Section 3, both proposed countermeasures are embedded in hierarchical fashion in the IDS agents to detect more efficiently price manipulation and DoS attacks. In fact, the developed algorithms are embedded in a distributed manner at the smart meter level, then, with more centralized way in the aggregator, finally, with pure centralized manner in the control center. As mentioned before, the strong point of this architecture is, in one side, even if the attack is bypassed and not detected in such level (i.e. smart meter or aggregator), it will be detected at the upper level since it has more computation capacity to detect intruders. In the other side, if the attack is identified in lower level, it will reduce the detection load and overhead of the upper level.

Algorithm 2
DoS attack detection.

For each node j and time slot i
  //Inputs:
  j^{th} node vector of PDR/Jitter:
  $V_j = \{y_j(t_1), y_j(t_2), y_j(t_3), \ldots y_j(t_k)\}$
  i^{th} column of the matrix M of PDR/Jitter (corresponding to the time slot t_i):
  $C_{N_i} = \{x_i(N_1), x_i(N_2), x_i(N_3), \ldots x_i(N_n)\}$
  //Compute:
  Mean values and standard deviations:
  $\mu_1(j)$, $\mu_2(i)$, $\sigma_1(j)$ and $\sigma_2(i)$
  For each time slot t_i
    If $y_j(t_i) \notin [\mu_1(j) - 3^* \sigma_1(j)\ \mu_1(j) + 3^* \sigma_1(j)]$ and $x_i(N_j) \notin [\mu_2(i) - 3^*\sigma_2(i), \mu_2(i) + 3^*\sigma_2(i)]$ **then**
    Send alert for attack detection with the node Id and the type of attack to the control center
    End if
  End for
End for

5. Experimental results

In this section, the proposed models are evaluated to show their performance and robustness against the most lethal attacks, namely *price manipulation* and *DoS attacks*. Matlab tool is used to implement the approaches. Like in most security mechanisms models, we test the robustness of our models in terms of: (i) Detection Rate (DR), which is the ratio of correctly identified malicious nodes over total number of attackers, (ii) False Positive Rate (FPR), which is the ratio of normal nodes that are classified as malicious over total number of normal nodes and (iii) the Accuracy Rate (AR), which is the subtraction of FPR from the DR (i.e. AR = DR − FPR). As specified previously, the attack can be launched at either smart meter or aggregator level. Hereafter, the obtained results according to the two treated attacks and their countermeasures are discussed.

5.1. Simulation of price manipulation attack countermeasure

This subsection deals with the attack where the intruder attempts to modify the electricity price announced by the utility and diffused in the network. Table 2 summarizes the main simulation parameters.

In this part, we evaluate our countermeasure model in function of the number of attacks per day (i.e. 24 h). Each node receives the new price information every 15 min. Hence, in the case of 100 nodes, we have 100*96 data that can be attacked and falsified per day.

To obtain the best thresholds couple (α_1, α_2) that exhibits the greatest performances, a set of simulations were conducted and applied to 200 nodes under 250 attacks which refers to the worst case in our experiment. We vary α_1 from 0,0037 to 0,0049 and α_2 from 0,005 to 0,015. These chosen intervals for each threshold are obtained after a set of tests to find the bounds of each threshold to give accepted results. For each couple (α_1, α_2), the Accuracy Rate (AR) were measured. As shown in Table 3, the best thresholds couple is (α_1 = 0,0043, α_2 = 0,01) where the AR reaches 93,3%.

We compare the proposed algorithm with the CUSUM approach developed in [19] to detect price manipulation attack in terms of AR. The algorithm proposed in [19] is characterized by the usage of only the first condition and threshold to detect attacks (i.e. if $|S(k+1)| > \alpha$, the algorithm announces that there is an attack). α is computed with the same principle used previously to compute α_1 and α_2 (*the best* value *is* $\alpha = 0.006$). To conduct this comparison, we consider 200 nodes susceptive to be attacked. The obtained results exposed in Fig. 6 show that the algorithm outperforms the existing CUSUM algorithm.

It is clear that the margin gap between the two algorithms accuracy rate is significant and ranges from 17% under 60 attacks to 27% under 250 attacks. This result can be explained by the fact that, due to the granular price change attack, the standard CUSUM falls into low DR if α is very small and into high FPR if α is high. In the proposed model, this issue is overcome thanks to the proposition of the second condition and threshold in parallel with the first ones (i.e. if $|S(k+1)| > \alpha_1$ *and* $|S(k+1) - S(k)| > \alpha_2$, the proposed algorithm announces that there is an attack). In one side, Fig. 6 shows that the algorithm proposed in [19] fails to detect accurately the price manipulation attack. Such algorithm is considered non-reliable in security domain where its AR is around 67% against 250 launched attacks. In the other side, this figure affirms that using both conditions provide better AR (above 94% against 250 launched attacks) where false alarms will be reduced and DR will be enhanced at the same time.

Hereafter, more detailed results are introduced to show the reaction of the proposed algorithm depending on the number of compromised nodes.

Table 2
Simulation parameters.

Number of nodes (smart meters, aggregators)	100, 150 and 200
Number of lines	12, 18 and 24
Node's data rate	30 Mbps
Transmission frequency	15 min
Number of time slots	96
Electricity price (Euros/MWh)	From 117,6 to 159,4

Table 3
Algorithm's thresholds selection.

α_1 \ α_2	0,005	0,0075	0,01	0,0125	0,015
0,0037	40,6	50,2	80,1	70,6	65,1
0,0040	45,3	55,7	88	71,5	70,8
0,0043	55	61,3	93,3	85,4	72,2
0,0046	30,9	53,6	78,7	49,6	37,5
0,0049	29,8	48,4	71,3	51	44,9

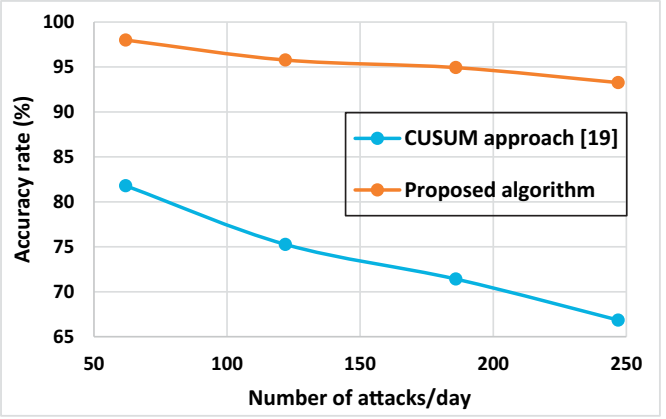

Fig. 6. Detection rate of price manipulation attack.

Fig. 7 depicts the obtained detection rate when we use our algorithm. It is obvious that in the case of a small number of considered nodes (i.e. 100 nodes), we obtain highest detection rate which slowly decreases when the number of attacks increases. However, even when the number of nodes increases, our system remains robust against the increasing number of attacks. The detection rate is always above 97.5% even with 200 nodes under 250 attacks launched in different time slots during 24 hours. Although the number of attacks is exceeding the number of nodes, the system detects almost all intrusions. This underlines the high capacity of the developed algorithm to capture any abnormal change in electricity pricing over time.

Fig. 8 shows that the False Positive Rate (FPR) is decreasing when we have larger number of nodes under the same number of

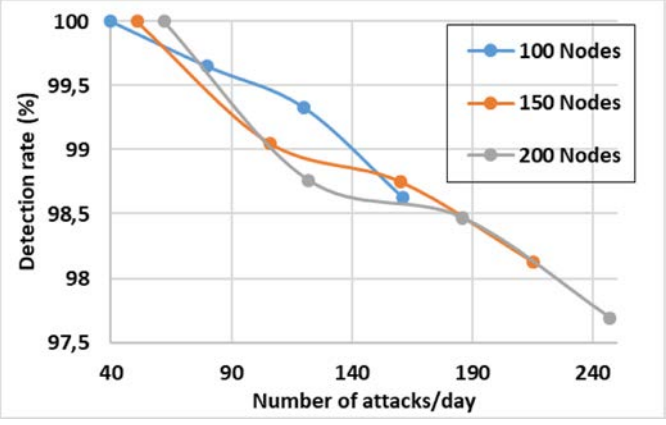

Fig. 7. Detection rate of price manipulation attack according to nodes number.

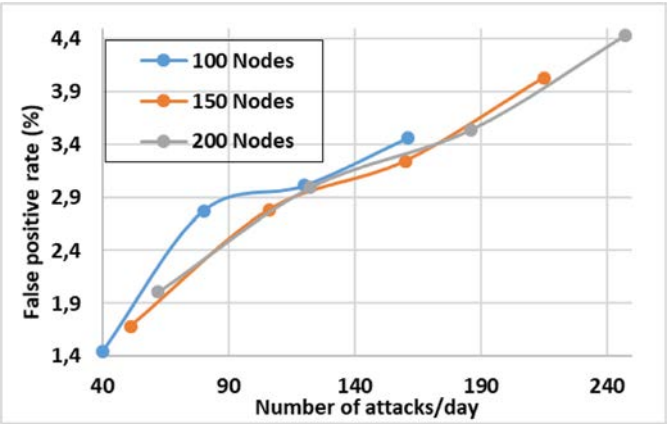

Fig. 8. False positive rate of price manipulation attack according to nodes number.

attacks. For example, when the number of attacks is equal to 160, the FPR with 100 nodes is equal to 3.5% against 3% for 150 nodes. The FPR slightly increases when the number of nodes and so the number of attacks rises. But it remains under 4.5% for 250 attacks.

5.2. Simulation of DoS attack countermeasure

In this subsection, we deal with the attacks where the intruder attempts to delay or delete useful information to mislead the state estimation and push it to take wrong decisions in the wrong time. This can make the smart grid unstable and highly perturbed. Table 4 summarizes the main simulation parameters.

The proposed algorithm is compared to a solution based on SVM (Support Vector Machines), a temporal detection (referred to the detection over time) and neighborhood detection (referred to the detection compared to neighbor nodes). Table 5 illustrates the DR reaction of each model. Obviously, SVM is the best one for any percentage of malicious nodes but its drawback is that is computationally expensive and cannot be deployed in appliances with low resources capacity like smart meters. After SVM, our model shows the best DR with a huge difference in results compared to others. 95% of attacks are detected by our model when there is less than 30% of malicious nodes compared to approximately 88% obtained by the other two models.

Table 6 shows that other models are less resistant against false alarms (i.e. FPR) where our model remains the best even compared

Table 4
Simulation parameters.

Number of nodes (smart meters, aggregators)	100
Node's data rate	30 Mbps
Meter Reading Payload of the node	512 Bytes
Transmission frequency	15 min
Number of time slots	18

Table 5
Detection rate of DoS attack.

Malicious nodes (%)	SVM-based (%)	Temporal detection-based (%)	Neighborhood detection-based (%)	Our model (%)
5	100	100	100	100
10	100	99.5	99	99.8
15	99	97.8	97	98.2
20	98	91.8	91	96
30	96	88.2	86	95

Table 6
False positive rate of DoS attack.

Malicious nodes (%)	SVM-based (%)	Temporal detection-based (%)	Neighborhood detection-based (%)	Our model (%)
5	0	0	0	0
10	1	0	0	0
15	2	0	5	0
20	3	15	12	1
30	7	17	15	5

to SVM. As shown in Table 6, our model remains robust with no false alarms until 15% of malicious nodes and with 5% of false alarms at the worst case when the percentage of malicious nodes is 30%. However, other models show their weakness against FPR with 17% of false alarms from the temporal algorithm in case of 30% of malicious nodes.

6. Conclusion

State estimation is a critical entity in the smart grid that can be the target of attackers to make great cyber and physical damages in the power network. Therefore, it is mandatory to develop security mechanisms in order to strengthen the smart grid reliability and protect it from lethal attacks. In this paper, we deal with the most lethal attacks that can occur in the smart grid. The first is *price manipulation attack* where the attacker will use the price elasticity of demand to predict the falsified price to inject in the network and then make physical or financial loss to the utility grid. The second is *DoS attack* that aims to disturb the state estimation and deprive it as well as end-users of useful information. Both of those attacks can break down the entire power system and cause heavy financial losses and catastrophic physical damages. To counter these attacks, new detection policies using CUSUM algorithm and abnormal behavior detection are proposed. Numerical results show that our proposed models insure high accuracy rate with above 95% and under 5% in terms of detection and false positive rates, respectively. As perspective, we aim to study the impact of a coalition between these two attacks, namely *price manipulation and DoS attacks.* This coalition is supposed to be more lethal and more difficult to be detected. Then, we aim to propose an efficient countermeasure against this coalition. Moreover, further lethal attacks targeting the power grid will be addressed, namely load redistribution and jamming attacks.

Acknowledgment

This work has been funded by the European project ITEA FUSE-IT [25].

References

[1] Cecilia AA, Sudarsanan K. A survey on smart grid. International conference on emerging trends in engineering, technology and science (ICETETS). 2016. p. 1–7.
[2] He H, Yan J. Cyber-physical attacks and defences in the smart grid: a survey. IET J Mag 2016;1(1):13–27.
[3] Patel A, Alhussian H, Pedersen JM, Bounabat B, Júnior JC, Katsikas S. A nifty collaborative intrusion detection and prevention architecture for smart grid ecosystems. Comput Secur 2017;64:92–109.
[4] Wang W, Lu Z. Cyber security in the smart grid: survey and challenges. Comput Netw 2013;57(5):1344–71.
[5] Komninos N, Philippou E, Pitsillides A. Survey in smart grid and smart home security: issues, challenges and countermeasures. IEEE Commun Surv Tutorials 2014;16(4):1933–54.
[6] Lu Z, Lu X, Wang W, Wang C. Review and evaluation of security threats on the communication networks in the smart grid. Proc. of military communications conference (MILCOM' 10. 2010.
[7] Jin D, Nicol DM, Yan G. An event buffer flooding attack in DNP3 controlled SCADA systems. Proceedings of the 2011 winter simulation conference. 2011.
[8] Li H, Han Z. Manipulating the electricity power market via jamming the price signaling in smart grid. GLOBECOM workshops. 2011. p. 1168–72.
[9] Ma J, Liu Y, Song L, Han Z. Multiact dynamic game strategy for jamming attack in electricity market. IEEE Trans Smart Grid 2015;PP(99).
[10] Wright CV, Coull SE, Monrose F. Traffic morphing: an efficient defense against statistical traffic analysis. Proc. of ISOC network and distributed system security symposium (NDSS). 2009.
[11] Jain K. Security based on network topology against the wiretapping attack. IEEE Wirel Commun 2004;11(1):68–71.
[12] Xiang Y, Wang L, Yu D, Liu N. Coordinated attacks against power grids: load redistribution attack coordinating with generator and line attacks. IEEE power & energy society general meeting. 2015.
[13] Dong Q, Niyato D, Wang P, Han Z. Deferrable load scheduling optimization under power price information attacks in smart grid. WCNC. 2013. p. 4683–8.
[14] Mishra S, Li X, Kuhnle A, Thai MT, Seo J. Rate alteration attacks in smart grid. INFOCOM. 2015. p. 2353–61.
[15] Yussof S, Rusli ME, Yusoff Y, Ismail R, Ghapar AA. Financial impacts of smart meter security and privacy breach. International Conference on information technology and multimedia (ICIMU). 2014. p. 11–4.
[16] Yang Q, Yang J, Yu W, An D, Zhang N, Zhao W. On false data-injection attacks against power system state estimation: modeling and countermeasures. IEEE Trans Parallel Distrib Syst 2014;25(3):717–29.
[17] Sargolzaei A, Yen K, Abdelghani MN. Delayed inputs attack on load frequency control in smart grid. ISGT. 2014. p. 1–5.
[18] Yu ZH, Chin WL. Blind false data injection attack using PCA approximation method in smart grid. IEEE Trans Smart Grid 2015;6(3):1219–26.
[19] Giraldo J, Cardenas A, Quijano N. Integrity attacks on real-time pricing in smart grids: impact and countermeasures. IEEE Trans Smart Grid 2016:99.
[20] Bi S, Zhang YJ. False-data injection attack to control real-time price in electricity market. IEEE global communications conference (GLOBECOM). 2013.
[21] Lu Z, Wang W, Wang C. Camouflage traffic: minimizing message delay for smart grid applications under jamming. IEEE Trans Dependable Secure Comput 2015;12(1):31–44.
[22] Mitchell R, Chen IR. Behavior-rule based intrusion detection systems for safety critical smart grid applications. IEEE Trans Smart Grid 2013;4(3):1254–63.
[23] Zaidi SAR, Ghogho M. Stochastic geometric analysis of blackhole attack on smart grid communication networks. SmartGridComm. 2012. p. 716–21.
[24] Mishra S, Li X, Pan T, Kuhnle A, Thai MT, Seo J. Price modification attack and protection scheme in smart grid. IEEE Trans Smart Grid 2016;PP(99):1–12.
[25] Fuse-It project. http://www.itea2-fuse-it.com/; 2014-2017.