HAL open science

A New Intrusion Detection Approach Against Lethal Attacks in the Smart Grid: Temporal and Spatial Based Detections

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

To cite this version:

Mohamed Attia, Hichem Sedjelmaci, Sidi Mohammed Senouci, El-Hassane Aglzim. A New Intrusion Detection Approach Against Lethal Attacks in the Smart Grid: Temporal and Spatial Based Detections. REVE2016, Mar 2016, Compiègne, France. 10.1109/GIIS.2015.7347186 . hal-03327555

HAL Id: hal-03327555

https://hal.science/hal-03327555v1

Submitted on 13 Feb 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution - NonCommercial 4.0 International License

A New Intrusion Detection Approach Against Lethal Attacks in the Smart Grid: Temporal and Spatial Based Detections

Mohamed Attia, Hichem Sedjelmaci, Sidi Mohammed Senouci and El-Hassane Aglzim DRIVE EA1859, Univ. Bourgogne Franche Comté, F58000, Nevers France
Contact authors: {mohamed.attia, Sid-Ahmed-Hichem.Sedjelmaci, Sidi-Mohammed.Senouci, el-hassane.aglzim}@u-bourgogne.fr

***Abstract*—The smart grid is the new vision of the traditional power grid, which is characterized by the integration of communication network between all its components beginning from the producers, going through the transmission and distribution units and finishing by the consumers and end users. The heterogeneity of its components imposes a sophisticated security architecture to protect the smart grid from any attack's attempt. In this paper, we propose an architecture in which Intrusion Detection System (IDS) agents are implemented with a distributed manner to monitor the consumer side, building appliances and smart meters. Those IDSs rely on rule-based detection policy, which consists in the combination of temporal and spatial detection rules. Simulation results prove that this combination enhances attack's detection rate and reduces false positive rate.**

***Index Terms*— Intrusion Detection System (IDS), rules-based detection, smart grid, smart meter**

I. Introduction

THE smart grid, known as next-generation power system, has the ambition to greatly enhance efficiency and reliability of future power systems with renewable energy resources. Nowadays, the entire world relies on the smart grid's new features to deliver the electricity with a high performance. Besides, as far as the smart grid has more features, as more it will be vulnerable to several lethal attacks. This is due especially to the millions of electronic devices inter-connected via communication networks throughout critical power facilities. That is why it is mandatory to set up a serious detection policy to protect all the smart grid stakeholders. To overcome this problem, many researchers propose a multitude of security solutions in different levels and with different loads and impacts. As mentioned in [1] and [2], availability, integrity and confidentiality are the main security objectives in the smart grid. In this paper, we are dealing with the attacks targeting the integrity issue in the smart grid since they can cause great damages, perturbations and losses. We focus especially on the ones that attempt to alter or delete the state estimation's information, namely the prevision of electricity consumed or which should be produced. Taking into account these major security issues, we propose a rules-based detection algorithm to detect this kind of attacks with a focus on *blackhole* attack, which consists in dropping messages exchanged between nodes. We accord also importance to the *time delay* attack, which is characterized by adding delays before sending packets. This algorithm relies on monitoring the node's behavior (i.e. appliances or smart meters) either *temporarily* by supervising exchanged information over time or *spatially* by comparing its behavior with its neighbors. To the best of our knowledge, we are the first using hybrid detection model (i.e. *combining between special and temporal detections)* to detect those lethal attacks. Simulation results prove the efficiency of this hybrid algorithm in terms of detection and false positive rate compared with the algorithms based on learning, temporal or spatial-based detection techniques.

The remainder of this paper is organized as follows: an overview of some related works is presented in Section II. Section III introduces the proposed architecture with the placement of the IDS agents. Then, the attack model and its countermeasures are defined in Section IV. Simulation results are discussed in section V. And finally, we conclude this paper in Section VI.

II. Attacks Model and Countermeasures

This section contains a description of the attacks model then the countermeasures to deal with these attacks.

A. Attack model

In our work, we focus specifically on attacks that have as goal the state estimation and aims to perturb or even break down the utility system. There is a multitude of attacks that can lead to this goal, for example, *blackhole* attack [4] 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 number of sent packets [4]. Therefore, this number of sent packets will no longer follow a normal distribution like in the case of natural situation. Another attack will be envisaged, the *time delay* attack [5], where the attacker makes some delays to sent packets and so, the Jitter (i.e. the delay between exchanged packets) will deviate from normal distribution. Those attacks can lead to a wrong decisions and cause critical problems like

infrastructure damage, service interruption or financial loss due to the existence of malicious users[3].The proposed detection policy is designed to detect this kind of attacks, with a special focus on *blackhole* and *time delay* attacks. To detect the *blackhole* and *time delay* attacks, we monitor respectively the Number of Sent Packets (NSP) and Jitter (i.e. the delay between the packets). Here, the NSP and Jitter are monitored temporally over time and spatially compared to the neighborhood nodes.

B. Temporal and spatial-based detections

Our proposed model is based on rules-based approach to take advantages from its benefits namely the low complexity requirements with the least false positive rate compared to the anomaly based detection algorithm [6]. Moreover, we added some features to enhance the accuracy of our model in order to be as near as possible to the learning algorithm's performance namely in term of detection rate.

In this section, we describe our proposed countermeasures to defend the smart grid from attacks targeting especially the state estimation. Our countermeasures algorithm relies on temporal and spatial attack detection, by monitoring the NSP and Jitter. Our model follows the behavior of each node and detects any abnormal or unexpected behavior. A node here represents the smart meter, the actuator or even the control center. We note by $l_{Ni} = \{x_i(T_1), x_i(T_2), x_i(T_3), \ldots x_i(T_k)\}$ the node *i*'s vector where *k* represents the number of Time slots T. *x(T)* denotes either the NSP or the Jitter. We note *n* the number of nodes to be monitored (i.e. *i*=1…*n*). Therefore, we obtain a $n*k$ matrix size. The matrix is equal to: $M = \{l_{N1}, l_{N2}, l_{N3}, \ldots l_{Nn}\}$. l_{Ni} denotes the ith line of the matrix M. In normal situation, each node follows normal distribution characterized by the couple (μ1(i),σ1(i)) where $\mu_1(i)$ is the mean vector of the node *i* and $\sigma_1(i)$ is the standard deviation. $\mu_1(i)$ and $\sigma_1(i)$ are calculated as follows:

$$\mu_1(i) = \frac{\sum_{j=1}^{n} x_i(T_j)}{n} \quad (1)$$

$$\sigma_1(i) = \sqrt{\frac{\sum_{j=1}^{n}(x_i(T_j) - \mu_1(i))^2}{n}} \quad (2)$$

In normal behavior, each value of the l_{Ni} should follow a normal distribution and should be within an interval of $[\mu_1(i) - 3*\sigma_1(i), \mu_1(i) + 3*\sigma_1(i)]$. When *x* is out of the interval, the node is suspected as abnormal node. According to the spatial detection, it is based on detecting any abnormal node's behavior compared to its neighbors to detect attempts of any node to attack. To do so, we treat the matrix M vertically. We note by $c_{Ni} = \{x_i(N_1), x_i(N_2), x_i(N_3), \ldots x_i(N_n)\}$ the ith column of the matrix *M* where *Nj* is the jth node. In normal situation, the number of exchanged packets at each node as well as the Jitter between those packets follow a normal distribution [4]. To have a normal behavior, the average number of sent packets should vary within an interval of $[\mu_2(i) - 3*\sigma_2(i), \mu_2(i) + 3*\sigma_2(i)]$, where:

$$\mu_2(i) = \frac{\sum_{j=1}^{n} x_i(N_j)}{n} \quad (3)$$

$$\sigma_2(i) = \sqrt{\frac{\sum_{j=1}^{n}(x_i(N_j) - \mu_2(i))^2}{n}} \quad (4)$$

So, like in temporal-based detection, if the value *x* doesn't follow a normal distribution, the node is classified as abnormal node. In this way, when the two approaches declare such node as abnormal, this node is announced as malicious node. By monitoring the NSP, we can detect if there is an intruder who aims to drop or delete some packets. So with this mechanism we can detect one of the most lethal attacks, namely the *blackhole* attack. Our algorithm is applicable also to monitor the Jitter to detect *time delay* attack. We need just to fill the matrix *M* with the Jitter between the packets and follow the same steps defined before. Combining between temporal and spatial detection can enhance the smart grid performance by increasing attack detection rate and minimizing the false positive rate. The algorithm summarizing the principle of the *blackhole* and *time delay* attacks detection is illustrated in Algo. 1 below:

1: IDS monitors the Features (*F*) NSP or/and JITTER of the Node (i.e. smart meter, actuator, control center)
2:*// Temporal detection:*
3:Monitor*F*' distribution of a $Node_i$ over time
4:***if***$(F_T)_i \in [(mean_{F_T} - 3*\sigma_{F_T})$ && $(mean_{F_T} + 3*\sigma_{F_T})]$***then***
5:*// $Node_i$ is suspected as an attacker*
6:*//Spatial detection:*
7:Compares the NSP' distribution of a $smartmeter_i$ with its neighbors
8:***if***$(F_S)_i \in [(mean_{F_S} - 3*\sigma_{F_S})$ && $(mean_{F_S} + 3*\sigma_{F_S})]$***then***
9:*// $Node_i$ is detected as a black hole/time delay attack that target estimation energy*
10:*//Response:*
11:Send an ***Alert message (Attack's id, NSP or/and JITTER, and detection time)***to Control Center

Algo. 1. Attack detection rules for *blackhole* and *time delay* attacks

III. Experiment Results

In this section, we show the evaluation of our proposed detection model, which is a combination between spatial-based and temporal-based detections, using Matlab tool. We compare its performances with a temporal-based detection, a spatial-based detection, and one of the most popular learning algorithms SVM (Support Vector Machines). We check the robustness of each algorithm in term of Detection Rate (DR) and False Positive Rate (FPR) defined as follows:

- *Detection Rate (DR):*the ratio of correctly identified malicious nodes over total number of attackers,
- *False Positive Rate (FPR):*the ratio of normal nodes that are classified as malicious over total number of normal nodes.

Table I summarizes the main simulation parameters.

TABLE I
Simulation parameters

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

As illustrated in Fig. 3, in term of detection rate, the learning algorithm is the best since it relies on a sophisticated technique that results in more time and computing requirements[6].Its DR is always above 96% when the malicious node is under 30%. Compared to this algorithm, our proposed model called hybrid detection model has a good performance with less complexity and with low energy consumption. This proposed algorithm is still robust with more than 95% of DR when the malicious nodes do not exceed 25%.It remains more advantageous compared to temporal or spatial-based detection when scheduled separately where their DR decreases to less than 90% when the malicious nodesexceed27%.

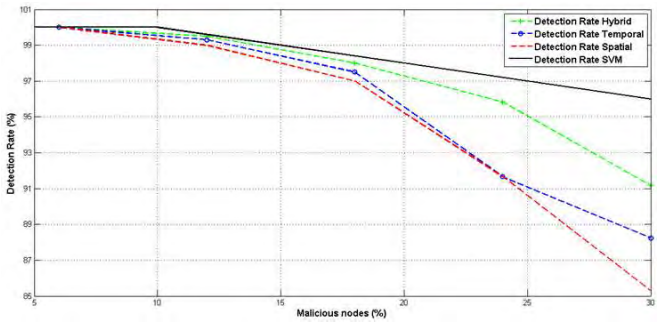

Fig. 3. Detection rate

According to Fig. 4, we show that our proposed algorithm has the lowest FPR (False Positive Rate) among all the other algorithms, namely: temporal, spatial-based detection or learning algorithm. Especially when the malicious nodes rate exceeds 18%, the FPR of all other algorithms is approximately high compared to our algorithm. For example, the FPR of the temporal or spatial-based detection algorithm is higher than 10% when the malicious node exceeds 22%. As shown in Fig. 4, using only temporal or spatial-based detection policy can result in a high percentage of FPR, more than 12% when the number of malicious node is over 24% and can reach 16% when the malicious node rate reach 30%. According to the learning algorithm, it has lower FPR (less than 7% with 30% of malicious nodes), but it is still higher than our proposed algorithm. This remains the major drawback of the learning algorithm (i.e. high FPR) besides its highest accuracy rate. Moreover, it is more consuming in term of energy and requires a high computing processor. Our proposed model has the best FPR statistics over all the others since the FPR is less than 6% at the worst case when we have 30% of malicious nodes and under 2% when the malicious node doesn't exceed 21%.

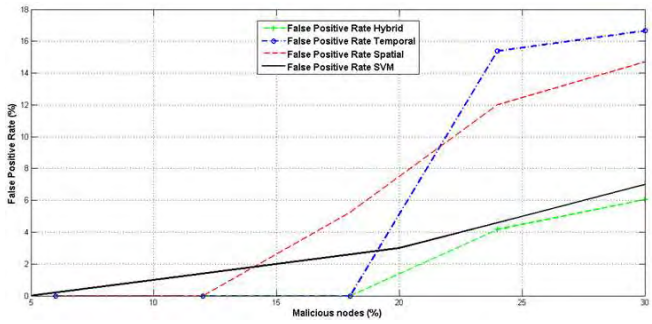

Fig. 4. False positive rate

As proved in Fig.3 and 4, by combing between the two lightweight detection policies, namely spatial and temporal-based detection, we prove that the *blackhole* and *time delay* attacks are detected with a high accuracy, i.e. high detection and low false positive rates.

IV. Conclusion

In this paper, we focus on detecting the most lethal attacks that aim to disturb the state estimation of the smart grid, break down the entire power system and cause heavy financial losses and catastrophic damages; we can cite for instance blackhole, time delay or false data injection attacks. We propose a new detection policy that aims to combine the advantages of spatial and temporal-based detection techniques to detect these attacks with a high accuracy. Simulation results prove that our detection policy exhibits a high detection and low false positive rate compared to learning and spatial (or temporal)-based detection techniques. This result is achieved even when the number of attackers is higher. As perspective of this work, we will propose some techniques to ensure and protect the privacy of the exchanged data between the smart meter and the control center.

Acknowledgment

This publication is a result from FUSE-IT Project, labeled by ITEA2 in2013 (Project Nr 13023), funded in France by DGE – Direction Générale des Entreprises.

References

[1] W. Wang, Z. Lu, "Cyber security in the Smart Grid: Survey and challenges". Computer Networks, 57(5), pp. 1344-1371, 2013.

[2] N.Komninos, E.Philippou,A.Pitsillides, ,"Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures", IEEE Communications Surveys & Tutorials, 16(4), pp. 1933-1954, 2014.

[3] R. Mitchell, I.R. Chen,"Behavior-Rule Based Intrusion Detection Systems for Safety Critical Smart Grid Applications", IEEE Trans. Smart Grid, 4(3), pp 1254-1263, 2013.

[4] S.A.R. Zaidi, M.Ghogho: "Stochastic geometric analysis of blackhole attack on smart grid communication networks",SmartGridComm, pp. 716-721, 2012.

[5] A.Sargolzaei, K. Yen, M.N. Abdelghani, "Delayed inputs attack on load frequency control in smart grid", ISGT, pp. 1-5, 2014.

[6] T.H Hai,E.N Huh, M. Jo, "A lightweight intrusion detection framework for wireless sensor networks", Wireless Communications and Mobile Computing, 10(4), pp. 559-572, 2010.