Journal of Electrical Engineering and Automation (EEA) (2020)
Vol.02/ No. 03
Pages: 118-122
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2020.3.002

IoT based Smart Grid Attack Resistance in AC and DC State Estimation

Vivekanadam B
Professor,
Lincoln University,
Malaysia.
vivekanandam@lincoln.edu.my

Abstract- Use of automation and intelligence in smart grids has led to implementation in a number of applications. When internet of things is incorporated it will result in the significant improvement a number of factors such as fault recovery, energy delivery efficiency, demand response and reliability. However, the collaboration of internet of things and smart grid gives rise to a number of security issues and threats. This is especially the case when using internet based protocols and public communication infrastructure. To address these issues we should ensure that the data stored is secure and critical information from the data is extracted in a careful manner. If any threat to its security is detective an early blackout warning should be issued immediately. In this paper we have proposed a geometric view point for big data attacks which is capable of bypassing bad data detection. We have created an environment where replay scheme is used launch blind energy big data attack. The defence mechanism of our proposed work is studied and found to be efficient. Experimental evidence supports our theory and we have found our methodology to efficiently improve error detection rate.

Keywords: Big Data; Smart Grid; Power Generation; IoT-based; Replay Attack;

1. Introduction

As our everyday life keeps changing with the increase in technological development with IoT as the key centre, there is also some serious security threats and issues faced. Using Internet of Things (IoT) physical objects can be connected to the internet and made to operate by collecting and exchanging data in a seamless manner. Without the need for actual presence the IoT enables control over the devices present over a network. This results in improved economic and social benefits. Another important implementation of IoT is in Smart Grid (SG). Using IoT, smart grids can be extensively used to establish two-way communication, electricity consumption and generation as well as control of power grid remotely. Since the integration of IoT into SG, it is exposed to a number of threats such as Denial of Service [1], Data Theft and Data Manipulation. Such attacks on communication technology will result in irreversible damage in equipment resulting in loss and might also result in real-time imbalance in energy generation and consumption [2]. If these errors are not detected at an early stage, it will lead to a complete breakdown of the grid that is triggered by vulnerabilities of the system. Hence it is vital to develop power grids that are safe, reliable and secure. Moreover, these smart grids should also be built with awareness on real-time threats possible in the power grids [3-4].

The IoT-based smart metering in SG [5] will result in the use of large amount of big data. There are three main types of grid business data namely:

1. Internal grid data for managing electric power data
2. Marketing data for elasticity sales data and transaction price
3. Data for equipment testing and grid operation like SCADA data

Within a fixed time period, it is essential to extract critical information that will help in decision making and data should be processed in a parallel manner accordingly [6]. The management of structured data will prove to be useful in distributed storage system and there is need to address the challenges [7] faced along the way. In this proposed work we have used a replay mechanism of big data attack on energy to examine its effect, without prior knowledge on transmission line admittances and power grid topology [8-9]. We have identified that the proposed methodology is able to bypass bad data detection through both alternating and direct current.

The contributions made can be summarised as below:

- Recent Issues faced by IoT-based SGs are surveyed. The possible applications of the novel methodology is also introduced.

ISSN: 2582-3051 (online)
Submitted: 16.12.2020
Accepted: 12.01.2021
Published: 19.01.2021

Journal of Electrical Engineering and Automation (EEA) (2020)
Vol.02/ No. 03
Pages: 118-122
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2020.3.002

- We have used a replay approach in analysing the sustainability of the SGs in AC and DC estimations.
- Using simulations, we have verified the impact of the proposed methodology.

2. Smart-Grid Big-Data Issues

2.1 Smart-Grid Energy Big Data Issues

When the grids of electricity are upgraded, there is need for more data to be stored and processed. In order to address this issue, we will require utilities that are built with event-processing abilities such as:

- Tight cyber-physical coupling [10] that can be used to ensure a clear distinction between the information and grid is necessary for coupling infrastructural security.
- The many security measures that are available are not framed specifically for the purpose of big data issues. Hence attacks might lead to misleading BDD with fake data. It might also lead to pattern attacks when such data that holds private and sensitive information is accessible by the attackers.
- Artificial intelligence theories and Big data analytics knowledge is necessary to adapt and learn this new mechanism. But this proves to be difficult due to the heavy data present.
- It is necessary to use real-time measures to determine pricing and processing tasks of previous and current data [11]. Taking this into consideration, it will prove to be difficult to design algorithms that are equipment with intelligence to process the vast data.
- Energy cannot be contained easy and will require a largely distributed system for data saving, collecting means and also for distribution of the energy stored. Hence it becomes difficult to process, share and store such a large variety, velocity and volume of data with the other parties that are using it.

2.2 Smart-Grid Security Issues

There are a number of factors involved in security issues of a utility infrastructure such as security management, computing, networking, smart meters, intelligent electronic devices, SCADA, facilities and plants [12]. The security threats that have a crucial impact on the IoT based SG are as listed below:

- Access and Authorization: It is possible to remotely access and control the distributed devices. However any data loss due to malicious software codes will result in a compromise in meters and other devices.
- Manipulation of data: Corruption of energy data, compromise of service and denial of service are some of the service impairment threats caused by data manipulation.
- Eavesdropping and impersonating: Interception of information is a common attack commonly prevalent when using public communication networks. Similarly, attackers might also attempt to impersonate a request as a legitimate request, trying to spoof information. However, such attacks have recently been addressed and overcome.
- Accessibility: IoT based SGs that are attacked based on IP will result in the entire system becoming totally unavailable or partially unavailable.

3. Proposed Work

3.1 System Model

A typical smart grid infrastructure will comprise of a number of equipment like ICTs, measurement technologies, advanced sensing and decision-making technologies. Based on its distribution level, the control network and management of the SGs are represented in Fig.1.

ISSN: 2582-3051 (online)
Submitted: 16.12.2020
Accepted: 12.01.2021
Published: 19.01.2021

Journal of Electrical Engineering and Automation (EEA) (2020)
Vol.02/ No. 03
Pages: 118-122
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2020.3.002

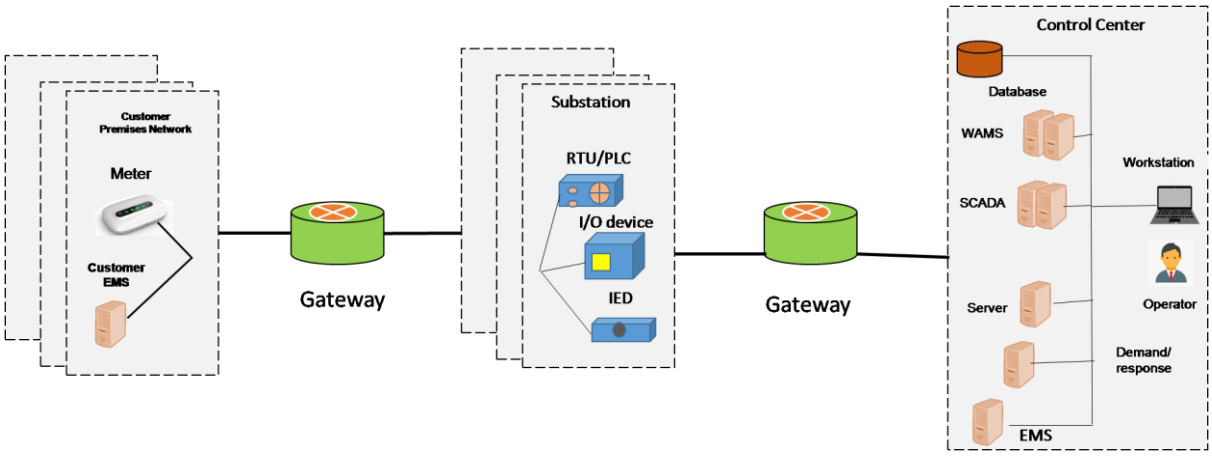

Fig.1. System Model of a Smart Grid

At the centre of the smart grid is an energy management system (EMS) incorporated with a pool of computer aided tools that are used to optimise, control and monitor the performance of distribution, transmission and generation of electricity. These actions are controlled and monitored by the grid under the hawk-eyed surveillance of SCADA system. They are also responsible for monitoring power system in a large scaled area and wide area monitoring with novel data acquisition technology. The database inside the smart grid stores system state, topology information, transmission admittance and metre data. The EMS also gives consumers a role to play in SG wherein they will be able to reduce the use of electricity at peak load hours resulting in economic benefits. Without the master computer it is possible to control all the devices using remote terminal units and programmable logic controllers. The amount of energy generated and dissipated is tracked by the customers with the help of hand-held devices or computers, remotely.

3.2 Replay Attack

As progress in technology continues, there is simultaneous advancement in security breaches and attacks. A simple malware might lead to coveting big data han and hackers who can eavesdrop on the distributed network will be able to intercept metering data. In general the parameters of the grid are kept as a secret and critically protected. However when such attacks occur it will result in heavy loss of utilities and might even tip off the balance in power supply for energy generation. In the proposed approach we use a big data replay attack that can be used on AC and DC estimations.

An energy big data in replay attack can either be detected by BDD or it can cheat the BDD erasing the trace of fabricated data. The AC state estimation is said to be e highly reliable and also processes the ability to resist against attacks imposed. Hence non linear AC status commission is also used along with DC state estimation. This indicates that any attack should possess the ability to to pass the BDD either AC state estimation. We are using a blind attack such that the attacker is unaware of transmission line admittance and power grid topology. For a perfect attack against AC state estimation the vector should be as shown in the equation below:

$$y = h(x_y) - h(x) \tag{1}$$

Where x and x_y are original and targeted state vectors and $h(\cdot)$ represents general AC power flow. If m_d is the measurement vector, the compromised measurement can be expressed as:

$$s_d = s + x = h(x) + y = h(x_y) \tag{2}$$

where s_d is the measurement vector under attack, x is the attack vector and s is the original measurement. According to eq (2) it is found that the vector under attack is inherently linear and must lie on the DC power grid surface. Based on the values measured for the vector set, we can use the replay attack for the difference between original and measured values. It is seen that there is a using the proposed methodology, it is possible to place s_d in on the grid's surface. The distance between the original and compromised value will determine the choice of the measurement vector set in order to result in a large impact of change in the system. On the other hand, the minimal distance that can be used to determine to bring in a minor change will result in decreasing the possibility of detection using better techniques.

ISSN: 2582-3051 (online)
Submitted: 16.12.2020
Accepted: 12.01.2021
Published: 19.01.2021

Journal of Electrical Engineering and Automation (EEA) (2020)
Vol.02/ No. 03
Pages: 118-122
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2020.3.002

4. Results and Discussion

In order to analyse the performance of the attacks that are imposed and benchmarked such as conventional DC attack, Random attack and big data attack, Monte Carlo simulation are experimented and the results are recorded. In the measurement, simulation results are recorded for reactive and active power that passes through all the nodes of the system. About 200 measurement vectors and 500 simulations have been diagnosed and its impact on noise distribution is observed. In Fig.2. the missed detection of the attack with respect to BDD threshold is determined. Similarly, Fig.3 shows that the survival rate is not stealthy while measuring without the use of Jacobian matrix.

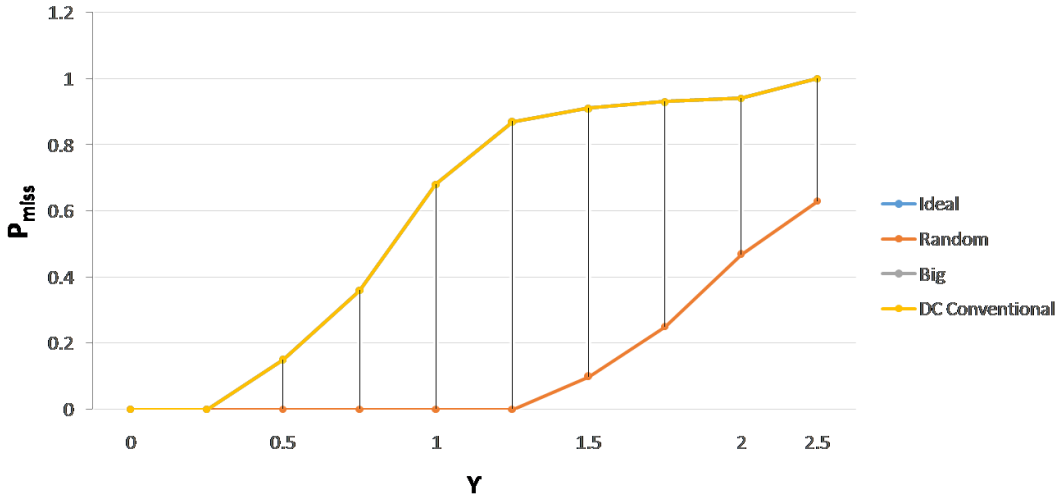

Fig.2. DC- State Estimation- Evaluation of Missed Detection Vs BDD Threshold Value

As observed in Fig.3, it is found that the miss is lowest when the models used have the wrong power flow. In AC state estimation, it is said to be in a stealthy mode because the performance of the proposed work remains typically the same. Based on the observations made, it is proved that our work needs only measurement data and the AC DC estimations resulting in favourable response rates.

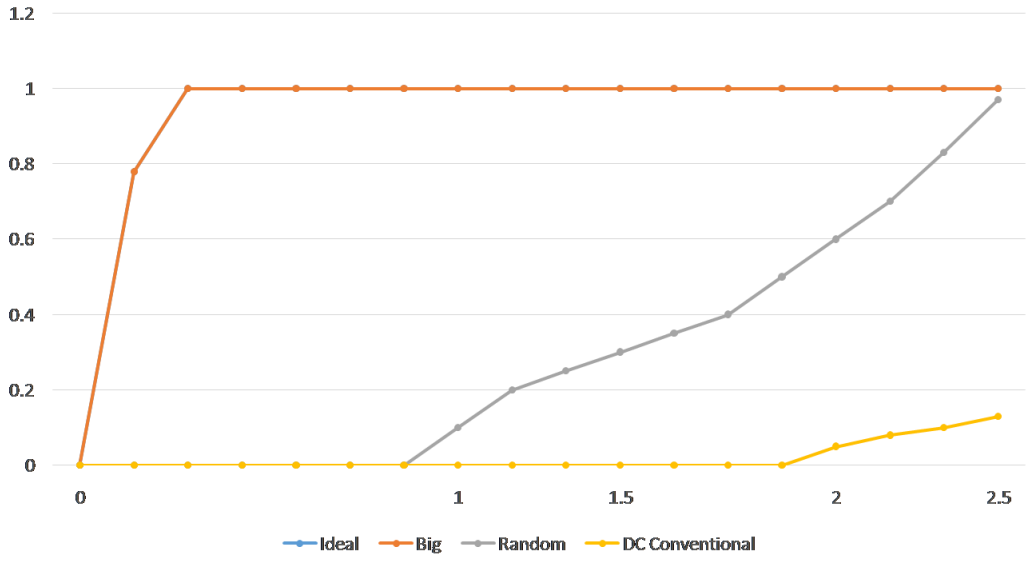

Fig.3. AC- State Estimation- Evaluation of Missed Detection Vs BDD Threshold Value

ISSN: 2582-3051 (online)
Submitted: 16.12.2020
Accepted: 12.01.2021
Published: 19.01.2021

Journal of Electrical Engineering and Automation (EEA) (2020)
Vol.02/ No. 03
Pages: 118-122
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2020.3.002

Big data attacks might lead to some challenges in the near future such as:

- If the proposed work results in significantly affecting the direction of a new research from the attacker's point of view, subsequent mechanisms of defence need to be developed to deal with its effect in an efficient manner.
- Apart from the proposed work which is based on the Euclidean distance, there are a number of powerful metrics that can be used along with the work done in this paper.
- In this method where compromised measurements play a significant part, sophisticated selection rules will further affect the working of it. A good example is random selection approach methodology.

5. Conclusion

A Smart Grid interfaced with Internet of Things will prove to be an important asset to managing energy. The biggest concern of using smart grids to manage energy is security and this paper proposes a positive solution to address the issue. We have provided big data attack model that is found to be flexible and can be used in AC and DC state determination. Keeping the data intact and preventing privacy intrusion issues, one can enjoy the various benefits SGs have to offer. The proposed paper also addresses the major challenges and issues faced by smart grid systems.

References

[1] Momoh, J. A. (2012). *Smart grid: fundamentals of design and analysis* (Vol. 63). John Wiley & Sons.
[2] McDaniel, P., & McLaughlin, S. (2009). Security and privacy challenges in the smart grid. *IEEE Security & Privacy*, *7*(3), 75-77.
[3] Sood, V. K., Fischer, D., Eklund, J. M., & Brown, T. (2009, October). Developing a communication infrastructure for the smart grid. In *2009 IEEE Electrical power & energy conference (EPEC)* (pp. 1-7). IEEE.
[4] Dugan, R. C., & McDermott, T. E. (2011, July). An open source platform for collaborating on smart grid research. In *2011 IEEE Power and Energy Society General Meeting* (pp. 1-7). IEEE.
[5] Dugan, R. C., & McDermott, T. E. (2011, July). An open source platform for collaborating on smart grid research. In 2011 IEEE Power and Energy Society General Meeting (pp. 1-7). IEEE.
[6] Santacana, E., Rackliffe, G., Tang, L., & Feng, X. (2010). Getting smart. *IEEE power and energy magazine*, *8*(2), 41-48.
[7] Parikh, P. P., Kanabar, M. G., & Sidhu, T. S. (2010, July). Opportunities and challenges of wireless communication technologies for smart grid applications. In *IEEE PES General Meeting* (pp. 1-7). IEEE.
[8] Ipakchi, A., & Albuyeh, F. (2009). Grid of the future. *IEEE power and energy magazine*, *7*(2), 52-62.
[9] Faheem, M., Shah, S. B. H., Butt, R. A., Raza, B., Anwar, M., Ashraf, M. W., ... & Gungor, V. C. (2018). Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges. *Computer Science Review*, *30*, 1-30.
[10] Shirley, D. R. A., Ranjani, K., Arunachalam, G., & Janeera, D. A. (2020). Automatic Distributed Gardening System Using Object Recognition and Visual Servoing. In *Inventive Communication and Computational Technologies* (pp. 359-369). Springer, Singapore.
[11] Mugunthan, S., & Vijayakumar, T. (2019). Review on IoT based smart grid architecture implementations. *j Electric Eng Autom*, *1*(1), 12-20.
[12] Haoxiang, W., & Smys, S. (2020). Secure and Optimized Cloud-Based Cyber-Physical Systems with Memory-Aware Scheduling Scheme. *Journal of trends in Computer Science and Smart technology (TCSST)*, *2*(03), 141-147.

ISSN: 2582-3051 (online)
Submitted: 16.12.2020
Accepted: 12.01.2021
Published: 19.01.2021