A Review on False Data Injection in Smart Grids and the Techniques to Resolve Them

P. Asha, K. Deepika, J. Keerthana, and B. Ankayarkanni

1 Introduction

Smart grid alludes to an enhanced electricity supplying from major power plant to the end inside our home. There are many power plants that produce electricity using a wide variety of resources such as wind energy, nuclear energy, coal, natural gas etc. Smart grid constitutes monitoring, analyzing, controlling and communication capabilities to the delivery system to increase the rate of production of the system in the meantime it reduces the energy intake. It forms on several mechanics. It deals with global warming, energy independence scenarios. Smart grid uses smart net meters to overcome the instability of conventional smart grid. Smart grid utilizes two-way communication to build up on efficiency and reliability. It transmits information to enable the operators, users and electrical devices. The system keeps a track on energy consumption at all locations. The system repairs on its own, grants the electricity markets to grow and make business. It opposes the power leakages. Smart grid includes load handling, demand response support, decentralization of power generation. Load handling reduces the energy intake. Demand response support guides to use low priority electronic devices when rates are low to minimize electricity bills. Decentralization of power generation grants the user to produce onsite power. Smart grid is the next generation of power grid [1]. Power grid is a network that transfers electricity from power plants to consumers. Power grid and smart grid are under several risks [2]. The rise in computerization advances the new projects of malicious attacks [3]. The attackers interfere the security by injecting the

P. Asha (✉) · B. Ankayarkanni
Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India

K. Deepika · J. Keerthana
Sathyabama Institute of Science and Technology, Chennai, India

S. Smys et al. (eds.), *New Trends in Computational Vision and Bio-inspired Computing*, https://doi.org/10.1007/978-3-030-41862-5_153

errors [4]. Since there are more number of access points the smart grids are more vulnerable to such cyber-attacks. Cyber-attacks can be classified into:

- ATA-Availability targeted attacks
- ITA-Integrity targeted attacks
- CTA-Confidentiality targeted attacks

ATAs attempts at delaying or corrupting/disrupting the communications where in, ITAs makes adversary attempts in order to insert some unauthorized information against the operator's will. The CTA attacker neither disrupt nor hinder the communication but it has illegal ingress to the confidential information that may perturb electricity markets [5]. If the adversary has comprehensive knowledge about the power systems then the attack which he/she creates can be neglected that it goes unnoticed. These attacks can easily pass bad data test and is utilized for power system state estimation [6]. The attacks become feasible if the attackers possess insufficient knowledge in the intrusion of false information with respect to power system grids. They are mainly caused by circuit breakers, transformer tap changers and switches as well as due to the attacker's minimal physical access towards grid failure and improper grid topology. The malicious attacks could damage the whole grid system.

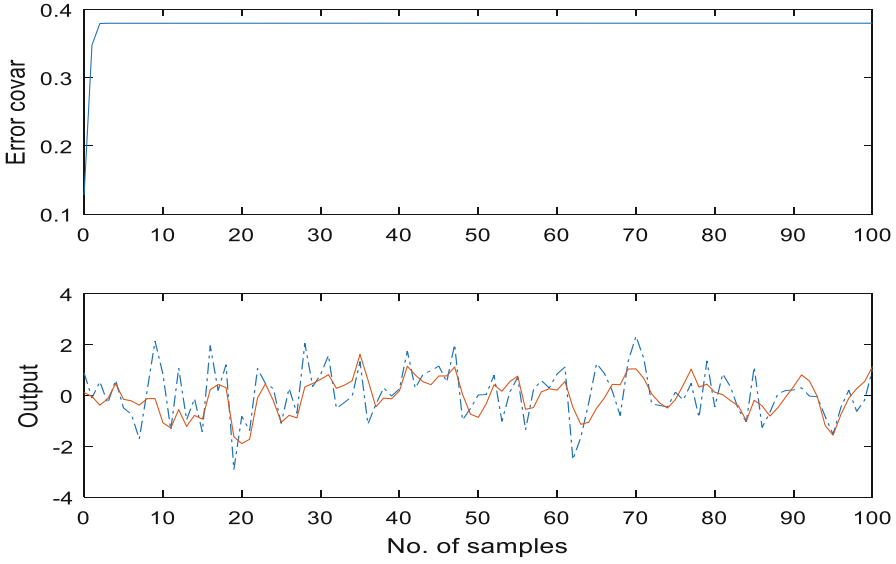
2 False Data Injection Attacks

In smart grid, units are connected to local networks. As the collector node comprises the most receptive data it could be easily targeted. The intruder can easily inject the false information by attacking the node. The more is the access points, the more prone are the smart grids to cyber-attacks. Among those attacks, the most severe attack is false data injection attacks. False data injection attacks occur due to undersigned measurement irregularities, errors. The attacks are classified as linear and non-linear attacks. Linear attacks occur only in DC supplies where the attacker's attacks are hidden. Non-linear attacks occur only in AC supplies where the attacks are easily detected. Smart meters play an essential role in smart grid, as it enhances the susceptibilities. There are two different meters. They are critical and redundant meters. Critical meters are easily removable. If removed the system becomes unbearable and easily attacks are prone to occur. Redundant meters are not critical but it identifies the attack easily. If the meters are removed then the attack is perfect but to it efficiency of the attacker should be high.

2.1 Kalman Filter

Kalman filter is one of the most implemented methods in system representing with continuous data gathering. It wraps many fields spanning the control systems,

communication, computer science etc. It provides many specific in-depth methods for state estimation and prediction. The algorithm works in two step process in appraisal of current state variables along with their ambiguities. Kalman filter runs in real time analysis by making use of only the present input and previously calculated state and eliminates additional past information. Kalman filter is a recursive filter and neglects the Gaussian errors. Kalman filter is something were the noise and other errors are easily detected, this is done by three ways of estimations, it is not only dynamically estimated, and previous estimation values are taken into consideration, but still it has another way where it uses the measurements through the meters like PMU and then estimated by dynamic state estimators to detect and eliminate the noise signals, false data and other gross errors. At first kalman filter was linearly extended. Here the noise modulations and the load changes were very high which slowly started declining the efficiency of the filter. In order to overcome this problem unscented kalman filter was used which was nonlinear. Little efforts were taken to handle the inefficiency of the kalman filter especially in cyber-attacks like false data injections. The kalman filter works so efficiently in carefully detecting the false data. Due to which its efficiency gets reduced. This can be managed by improving the unscented kalman filter (UKF) or by temporal based detection (UKF) improvement functions efficiently than temporal based detection as it can easily detect the replacement of meters.



The above figure is a graph that represents the Kalman filter. The final output is represented as above. The x axis represents the sample ratio and the y axis represents the voltages.

Table 1 Comparison of various techniques

Techniques	Filtering capacity	Time complexity	Robustness
EKF	High	High	Common
UKF	Highest	Highest	Weaker
Enhanced EKF	Higher	Higher	Stronger

2.1.1 Techniques used in Kalman Filter

Various techniques used in Kalman Filter are stated below (Table 1).

Extended Kalman Filter

Extended kalman filter considers two things one is the predicted false data and the other one is the intrusion of false data. Therefore producing the optimal state estimation values of the system. It is effective and used in linear system. It ignores the nonlinear measurements; whenever the load is high the accuracy of the system will have fluctuations [7].

Enhanced Extended Kalman Filter

It is used in nonlinear measurements of the systems. It has two conditions where it predicts and filters the false data injected in the smart grids. It is even more efficient than EKF. Even when the load is large and nonlinear it predicts and minimizes the false data by filtering process. It will linearize the non-linearized data. Thus it maintains the efficiency of the filter.

Unscented Kalman Filter

It does not linearize the non-linearized values, instead it propagates through the nonlinear functions only it filter high but the robustness value is very low.

2.2 Bad Data Detection

It is an error correction method which is developed and estimated for the distribution grid. Bad data detection is classified as single or multiple bad data its main function is to recognize and remove the error. Injecting bad data in smart grids will lead to severe risks such as creating problems in power distribution process or will lead to device breakdown. Traditional bad data detection is easily bypassed. Distribution

state estimation is now newly developed method which can detect the bad data. The harmful user will result in the grid which cannot be predicted in the systems. The hackers can easily cause price hike by just changing the meters reading. The bad data directly attacks the control center and misleads it and becomes highly dangerous. Bad data detection test is mainly useful to perceive the bad data. As it is the most hazardous cyber-attack, data cannot be perceived by the conventional state estimation method and only detected by bad data detection method. Distributed state estimated method may be used to detect bad data detection. It can also be detected by chi-squares test. It is derived from sum of squared errors. It eliminates null hypothesis and data becomes independent. It compares the distribution of plaintext and decrypted cipher text. It is used for solving modern cryptographic problems. Minimum chi square estimation is used to detect unobserved quantities based on observed data [8–11]. Even under conventional operating circumstances, the measurements found varied due to random errors [12]. The mechanism of apperceiving exceptional errors is termed to be BDD. Conventional BDD attempts to perceive measurement errors employing the statistical properties of the weighted measurement residual. Note that the measurement dismissal may be acting as a key issue regarding the BDD characterization and performance. It seems mandatory to have a large number of measurements than the preset minimal threshold value. However, prevailing measurement ordonnances may not always haul such coveted level of sacking which draws up the BDD useless. Techniques involved in the bad data injection technique are:

- In cyber side
- In physical side

2.2.1 Cyber Side

It is where the variations are made in the communication levels or in the measuring meters. The basic way is to make the meters fail since the connections in the home area networks are only limited, easily these devices can be made out of their services by the attackers. So that it paves way for them to use artificial meters to intrude their false data easily [13–16], thus these smart meters of the attackers help them to transfer the false data packages to the control centers. The other way is where the IP address or the password of the regularly used meters can be altered, since the smart meter's passwords are not highly complex [17–19]. It can be easily cracked. In case if the smart meters are secured with complex passwords then he attackers can seize it by identifying the authentication of the smart grids. They monitor the traffic flow and get to know the critical operations so that they could delay the operation by slowing it down exclusively. The other method is where they inject worm to the smart grids. This would easily deploy the data of the meters, by sending update commands to the meters thus slowly the injected worm spreads in large scale to the entire system or network.

2.2.2 Physical Side

If an adversary possess maximal knowledge regarding the power grid topology and the transmission-line values, then he can regulate the false data injection attack vector so that, the attack resides undetected and productively clears the bad data detection tests, which is habitually used for power system state estimation [20]. A pragmatic false data injection attack is substantially an attack with deficient information because of the attacker's dearth of real-time knowledge in regard to disparate grid parameters such as, the location of circuit breaker switches, transformer tap changers as well as the attacker's restricted physical ingress to most grid facilities. Other way is by collapsing the time synchronization mechanism in smart grids.

Here they would send the bad data on the GPS systems. This is such an easy way through which the hackers execute their attack externally even without entering into the communication networks.

These are the physical and cyber side where the attackers not only steal the private information but also cause energy theft system failures and dispatches.

2.3 Phasor Measurement Unit (PMU)

PMU measures the electrical waves on the grid. The real time measurements can be done by protective delay device. PMU measures the Analog AC waveforms digitized by an analog to digital converter. PMU takes both global positioning system (GPS) and non-GPS references while they are adjusted with standard and working synchronously. PMU measures the electrical waves on an electrical grid. Main principle of PMU is measuring its power flow, power injection and sends the measured data to the control center that appraises the status of the system in real time. PMU uses digital signal processing components to quantify the AC waveforms and transfigures them into phasors based on requirements of system frequency and under the control of GPS. Many widely distributed PMU in the power system are designed for,

- Real time governance and monitoring
- Network congestion management and State estimation
- Fortification and govern distributed generation
- Angular, voltage state surveillance

3 Results and Discussion

The work concentrates on the continuous monitoring of the activities of the attackers. The attacker's activity will reveal the type of the attack they try to attempt. The work analyses the attack and redirects them to the honey pot which

exactly looks like a real (original) server there by providing fake information for the intruder and at the same time it accumulates the information about the hacker. There are four modules in the proposed system. They are Client module, Authentication Server module, Back-end server module and Honey pot server module. It has been implemented using Java 1.4 with back end as MS-Access.

Initially, provide the username and password to trigger the server. Triggering the main server happens by invoking the server source code. If both the username and password is correct server starts successfully. The server window displays whole login information of registered user when the user tries to login. Provide username and password to trigger the honeypot server. For the process to proceed, after logging in, the server should trigger the honeypot server. Information will be displayed in the honeypot server window when the fake user tries to enter into the account and also provide the information which of the file user tries to access. Clicking on Sign up to proceed with the registration process (Fig. 1). For the process to continue one should sign up by providing the secret code so that server generates the access rights and user id (Fig. 2).

Firstly the user should registration with the certain details to proceed for the login (Fig. 3). It contains Username, Password and Machine IP. Select the file which is generated during registration time. Selecting the checkbox that is not the rights given by the server, then the client is redirected to the honeypot server. Message box pops up if the access rights given by the client is valid.

After logging in with the exact information client window will be displayed so that original data can be downloaded. Client window will be opened so that one can search the required document and download it. Downloaded information is displayed and can also edit the downloaded information but the backend will

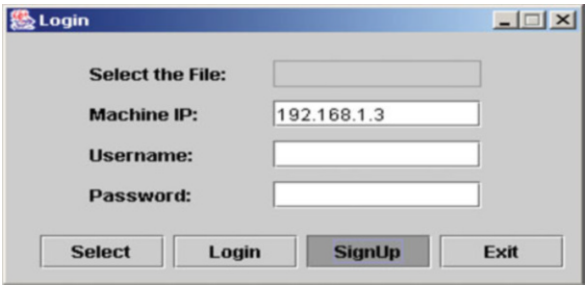


Fig. 1 Login

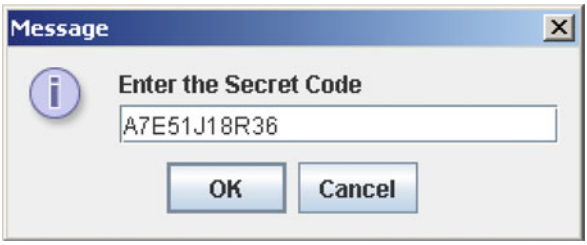


Fig. 2 Secret code for access rights

Fig. 3 Registration

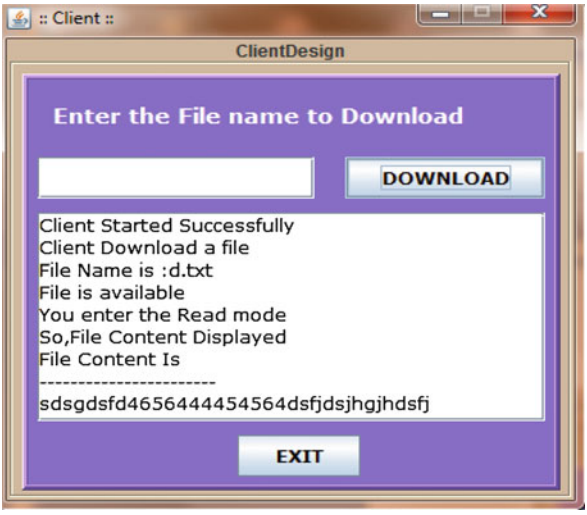


Fig. 4 File downloaded (client side)

not be effected (Fig. 4). Server window records the user behavior and displays the information that which file the client accessed. After which, finally the Honey pot server window displays the information that which file the client accessed (Fig. 5).

3.1 Defending Methods

3.1.1 Strict Analysis

This is highly essential to prevent the bad data to intrude easily, here the critical meters should be authenticated and should be defined to take up only the necessary information, if only the desired information are taken by the system then there will be no such spaces given for the unauthorized data to get into the system. Moreover

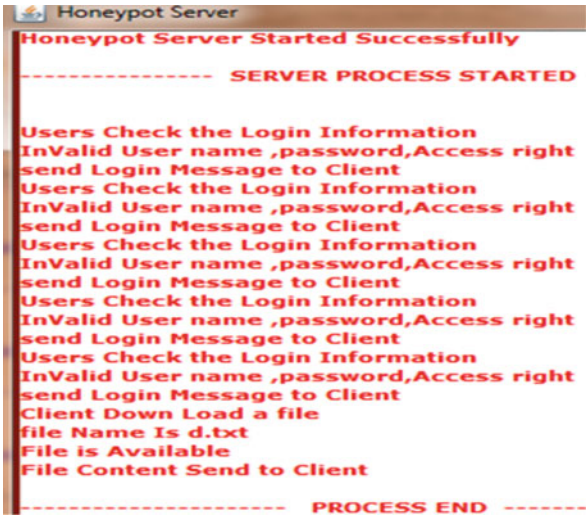


Fig. 5 Suspicious behavior

there are many developed ways such as Transport layer security protocol (TLS), Secure socket layer (SSL), HMAC, SHA etc. which removes invalid entries and forged data to intrude into the system.

3.1.2 Wireless Network in Smart Grids

Wireless network in smart grid is widely adapted nowadays. Since the route for bad data injection has started from the constructional flaw or in the topology of the transmission line.

If it becomes wireless the structural error can be minimized and hence the bad data can be easily reduced from intruding and disturbing the proper transmission of information through the smart grids.

3.1.3 Introducing Modules

The smart grids are used for storage of historical data, so that the changes in the new entry of information can be easily detected. In addition to it if we embed the analyzing modules at each and every level of the smart grids, then easily we can detect the malicious data and can reduce the attacks from penetrating and spreading fast throughout all the areas in the smart grids.

4 Conclusion

In this paper, we have discussed about Kalman filter, Bad data detection test and Phasor measurement unit to reduce the false data injection attacks. In Kalman filter, we use few techniques like extended, unscented, enhanced extended Kalman filter as it is one of the most implemented methods in system representing with continuous data gathering. In bad data detection test, we consider single or multiple bad data as its main function to identify and remove the error. In Phasor measurement unit, it can be utilized for the protection and control for distributed generation.

References

1. S. A. Foroutan and F. R. Salmasi, "Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method," in *IET Cyber-Physical Systems: Theory & Applications*, vol. 2, no. 4, pp. 161–171, 12 2017.
2. H. Karimipour and V. Dinavahi, "On false data injection attack against dynamic state estimation on smart power grids," *2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE)*, Oshawa, ON, 2017, pp. 388–393.
3. M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks against nonlinear state estimation in smart power grids," *2013 IEEE Power & Energy Society General Meeting*, Vancouver, BC, 2013, pp. 1–5.
4. T. Lan, W. Wang and G. M. Huang, "False data injection attack in smart grid topology control: Vulnerability and countermeasure," *2017 IEEE Power & Energy Society General Meeting*, Chicago, IL, 2017, pp. 1–5.
5. K. Khanna, S. K. Singh, B. K. Panigrahi, R. Bose and A. Joshi, "On detecting false data injection with limited network information using transformation based statistical techniques," *2017 IEEE Power & Energy Society General Meeting*, Chicago, IL, 2017, pp. 1–5.
6. H. Karimipour and V. Dinavahi, "Robust Massively Parallel Dynamic State Estimation of Power Systems Against Cyber-Attack," in *IEEE Access*, vol. 6, pp. 2984–2995, 2018.
7. Y. Jiang and Q. Hui, "Kalman filter with diffusion strategies for detecting power grid false data injection attacks," *2017 IEEE International Conference on Electro Information Technology (EIT)*, Lincoln, NE, 2017, pp. 254–259.
8. R. Xu, R. Wang, Z. Guan, L. Wu, J. Wu and X. Du, "Achieving Efficient Detection Against False Data Injection Attacks in Smart Grid," in *IEEE Access*, vol. 5, pp. 13787–13798, 2017.
9. Q. Yang, D. An, R. Min, W. Yu, X. Yang and W. Zhao, "On Optimal PMU Placement-Based Defense Against Data Integrity Attacks in Smart Grid," in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1735–1750, July 2017.
10. K. Khanna, B. K. Panigrahi and A. Joshi, "Bid Modification Attack in Smart Grid for Monetary Benefits," *2016 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, Gwalior, 2016, pp. 224–229.
11. K. Khanna, B. K. Panigrahi and A. Joshi, "Feasibility and mitigation of false data injection attacks in smart grid," *2016 IEEE 6th International Conference on Power Systems (ICPS)*, New Delhi, 2016, pp. 1–6.
12. R. H. Etemad and F. Lahouti, "Resilient decentralized consensus-based state estimation for smart grid in presence of false data," *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Shanghai, 2016, pp. 3466–3470.
13. M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," *2012 IEEE Global Communications Conference (GLOBECOM)*, Anaheim, CA, 2012, pp. 3153–3158.

14. P. Asha, Roshni Sridhar and Rinnu Rose P. Jose, "Click Jacking Prevention in Websites using Iframe Detection and IP Scan Techniques ", ARPN Journal of Engineering and Applied Sciences, VOL. 11, NO. 15, pp. 9166–9170, August 2016.
15. D. Wang, X. Guan, T. Liu, Y. Gu, Y. Sun and Y. Liu, "A survey on bad data injection attack in smart grid," *2013 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, Kowloon, 2013, pp. 1–6.
16. Asha P, Architha K, Madhavi Latha N, "Design And Implementation Of IOT Based Security Aware Architecture Using IDS", Research Journal of Pharmaceutical, Biological and Chemical Sciences, 8(2),pp.2293–2300, 2017.
17. B. Tang, Jun Yan, S. Kay and H. He, "Detection of false data injection attacks in smart grid under colored Gaussian noise," *2016 IEEE Conference on Communications and Network Security (CNS)*, Philadelphia, PA, 2016, pp. 172–179.
18. C. Liu, A. Stefanov, J. Hong and P. Panciatici, "Intruders in the Grid," in *IEEE Power and Energy Magazine*, vol. 10, no. 1, pp. 58–66, Jan.-Feb. 2012.
19. Asha P., Lahari T., Kavya B. (2018) Comprehensive Behaviour of Malware Detection Using the Machine Learning Classifier. In: Zelinka I., Senkerik R., Panda G., Lekshmi Kanthan P. (eds) Soft Computing Systems. ICSCS 2018. Communications in Computer and Information Science, vol 837. Springer, Singapore
20. O. Kosut, L. Jia, R. J. Thomas and L. Tong, "Malicious Data Attacks on the Smart Grid," in *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.