Detection and Trust Evaluation of the SGN Malicious node

Faisal Al Yahmadi[1†] and Muhammad R Ahmed[1†],
1606002@mtc.edu.om Muhammad.ahmed@mtc.edu.om
Military Technological College, Muscat, Oman

Summary
Smart Grid Network (SGN) is a next generation electrical power network which digitizes the power distribution grid and achieves smart, efficient, safe and secure operations of the electricity. The backbone of the SGN is information communication technology that enables the SGN to get full control of network station monitoring and analysis. In any network where communication is involved security is essential. It has been observed from several recent incidents that an adversary causes an interruption to the operation of the networks which lead to the electricity theft. In order to reduce the number of electricity theft cases, companies need to develop preventive and protective methods to minimize the losses from this issue. In this paper, we have introduced a machine learning based SVM method that detects malicious nodes in a smart grid network. The algorithm collects data (electricity consumption/electric bill) from the nodes and compares it with previously obtained data. Support Vector Machine (SVM) classifies nodes into Normal or malicious nodes giving the statues of 1 for normal nodes and status of -1 for malicious –abnormal- nodes. Once the malicious nodes have been detected, we have done a trust evaluation based on the nodes history and recorded data. In the simulation, we have observed that our detection rate is almost 98% where the false alarm rate is only 2%. Moreover, a Trust value of 50 was achieved. As a future work, countermeasures based on the trust value will be developed to solve the problem remotely.

Key words:
Smart Grid Networks, Security, Malicious, Attacks, Support Vector Machine, turst evaluation.

1. Introduction

Smart Grid Network (SGN) is an electrical grid network that uses information and communications technology (ICT). This collects and action autonomously on information data collected from the network, such as behaviors of suppliers and consumers, this improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity. Moreover this work on the advanced new technologies and developed infrastructure to prepare the world to overcome the arising challenges expected to be faced in the coming decades. New implementations such as integration of alternative energy sources and decentralized generation will help overcome the growing global power demand expected with the adaptation of Electric vehicles AVs and other smart household appliances. SGN implementation of new technologies allows for two-way stream of both power and data [1]. These implementations will grant the network a greater ability to detect, react and pro-act towards power usage or other businesses. Suspicions power usage patterns by consumers will also be recognised and responded to with the new technology implementation. SGN enables service providers to monitor the behaviour of all stockholders of the electricity. SGN has the capability of enabling the consumer to become an active participant in the network. In order to ensure network economic feasibility and a high quality service with minimum losses, security and safety of supply is prioritised. Some of the benefits that SGN grants beneficiaries are as follows:

- Integration of alternative energy sources
- Decentralized generation
- Reliably electrical supply
- Greener power production
- Active consumer participation
- Better resilience towards grid blackouts

SGN implementation of information and communication technologies (ICT) allowed the new network to monitor, operate and control the system with added features. These control manners were only available for service providers at the generation phase. However, ICT helped to extend these manners across all SGN phases reaching transmission and distribution phases [2]. Two-way communication enables both service providers and companies to utilize the developed infrastructure for a more efficient grid. Two-way communication also allows consumers to be true active participants with ability to choose new power usage patterns that were not possible with the conventional grid. Moreover, to standardize the new SGN operation, National Institute of Standards and Technology (NIST) proposed an SGN model standardizing SGN architecture as shown in Fig. 1. The proposed model lists seven domains, which are:

- Generation
- Transmission
- Distribution
- Operations
- Service providers
- Markets
- Consumer.

Manuscript received June 5, 2021
Manuscript revised June 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.6.13

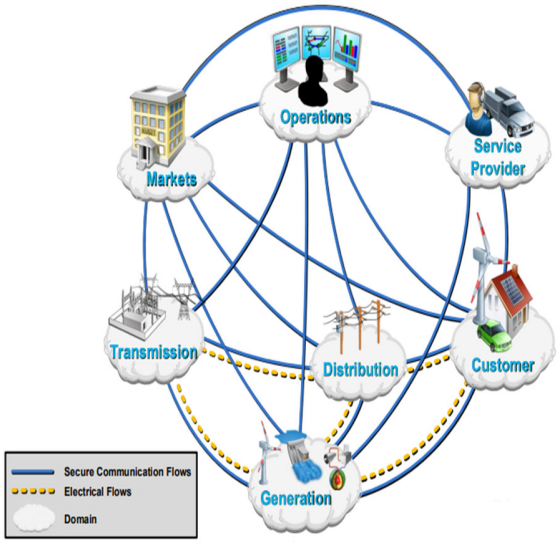

Fig. 1. Smart grid architecture model (SGAM) by [NIST] [3]

These above mentioned domains use secure communication in order to operate SGN efficiently. The proposed model also illustrates the electricity path between different domains, which are transmission, distribution, customer and generation, while communication flows across all seven domains.

Security provisioning is a critical necessity for any wired and wireless communication network [4]. Therefore, a machine-learning model will be adopted to detect attacks on SGN. Machine learning technology uses machines learning algorithms to artificially improve their performance as more data is being trained [5]. Machine learning has different techniques and models developed for various applications; one of the uses is solving classification problems. Support Vector Machine (SVM) is a classic machine learning technique which has the ability to classify high dimensional data [6]. This paper aims to develop an algorithm using one of the machine learning techniques, an SVM based model is used and simulated by MATLAB. The simulation platform was chosen as MATLAB has the ability to classify attacked nodes by comparing collected data with average data collected from the same consumer/household. Attack detection revolves around two pillars, which are average electrical power consumption of the consumer monthly and average monthly electrical bill of the consumer. Besides we have calculated the trust value of the node date. SGN is basically developed based on the wireless sensor network (WSN) concept. The data collecting process starts with nodes representing consumers sending data to a central node and back to the supplier (the app/ algorithm) as shown in Fig. 2.

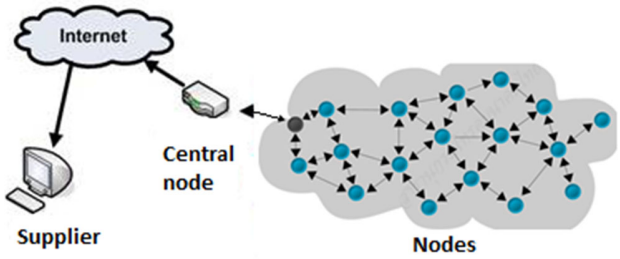

Fig. 2. A conceptual illustration of a generic WSN [7]

SGN security is a critical necessity. Some algorithm was developed based on the WSN concept to provide the security measure for SGN nut it is not fulfilling the targeted security by the researcher.

2. Smart grid networks security requirements

In the Smart grid, the security has the utmost importance when it comes to sharing our data with multiple parties. Security is vital across all SGN and systems. Moreover, to explain the security requirements for all types of networks, the following requirements will be discussed [1].

- Confidentiality: or privacy, which means data can be only accessed by authorized parties
- Authentication: means the ability of the service or host to differentiate between users identity
- Integrity: data can only be modified by authorized parties
- Availability: data are available to authorized parties when requested
- Nonrepudiation: receiver must have the ability to identify the received message sender or source
- Data Freshness: the data received should be the current and new data.
- Secure management: in the network management levels the security should be dealt is an efficient way.

3. Vulnerabilities of SGN

Security is an essential need for smart grid networks, especially cyber security. Smart grid will digitalize the grid by implementing new technologies. The backbone of a smart grid is the information and communication technologies (ICT) which will be sending and receiving data that needs to be delivered safely and on time in order to properly operate grid functions. Different data will have different security levels and different functions. Digitalizing the grid with new technologies made the grid more complexes, which exposed it to a wider range of

attacks. Any attack that delays, manipulates or views data can affect thousands of households and consumers. The vital security concern of SGN network security is connecting the private dwellings to the internet exposing consumer's privacy to many risks. There are many external/physical and software/internal vulnerabilities in SGN [2]. Hence, if attacks happen in SGN that could compromise the privacy of the dwellings. Both External and Internal vulnerabilities will be discussed below:

3.1 Physical/External vulnerabilities:

Physical security has to do with physically existing devices and equipment that operates the grid. Some of the vulnerabilities are as follows:

a. Vital power electronics located in unguarded areas
b. Outdated power electronics made without security in mind
c. Outdated power electronics might be fully or partially incompatible with new technologies

3.2 Software vulnerabilities:

Software security has to do with designed systems and software that has been fabricated to operate grid functions and protect its security. Some of the vulnerabilities are as follows:

a. Customer information security.
b. Greater number of intelligent devices.
c. Implicit trust between traditional power devices.
d. Using Internet Protocol (IP) and commercial off-the shelf hardware and software.
e. Modbus security selected.

4. SGN attackers

The attackers of SGN normally try several methods to attack the network. In order to discuss the attacks, we have to understand the source and motive behind it. There are several types of attackers exists [3], it is easier to classify network attackers to two main divisions depending on the attacks types which are external and internal attackers explained as follows:

4.1 External attackers:

External attackers are the one who execute attacks against SGN without having access to the grid internal security. Some of the attackers who commits these attacks are [4]:

a. Non-Malicious attackers: who view the security and operation of the system as a puzzle to be cracked. Those attackers are normally driven by intellectual challenge and curiosity.
b. Terrorists: who view the smart grid as an attractive target as it affects millions of people making the terrorists draw more attention at a large scale.
c. Competitors: attacking each other for the sake of financial gain.

4.2 Internal attackers:

Internal attackers are the one who execute attacks while having access or knowledge to the network security [5]. These attacks can be harder to detect and have a higher success rate because of the valuable resources attached to the attacks. These attacks can be correlated with the following attackers [4]:

a. Consumers: driven by vengeance and vindictiveness towards other consumers making them figure out ways to shut down their home's power.
b. Employees: disgruntled on the utility/customers or ill-trained employees causing unintentional errors.

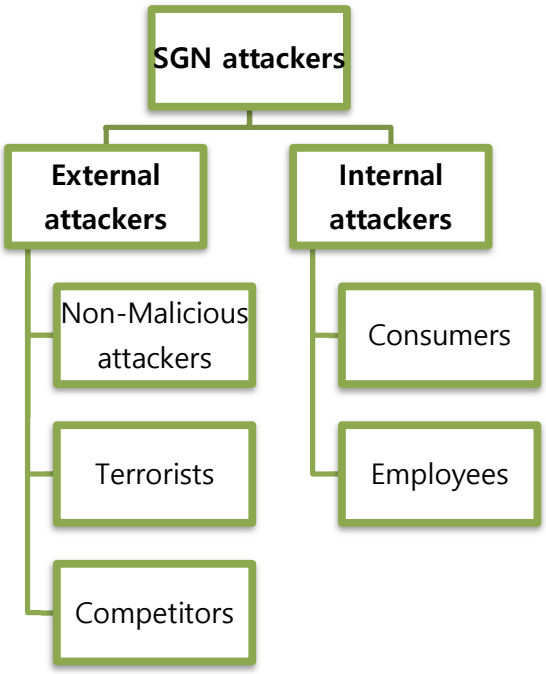

Fig. 3. SGN attackers types units,

5. SGN types of attacks

SGN is a large scale network and usually across thousands of miles. The bigger the network the higher chance it will encounter attacks. To insure both company and consumer security, all attacks must be studied before

happening to prevent anyone taking advantage of weak links in the systems and to put the right measures to encounter them. SGN attacks can be classified into External and Internal attacks and will be discussed as follows.

External attacks can be defined as the attacks that are executed directly through the grid infrastructure or grid physical components rather than through ICT of the grid. These attacks can cause destruction In other words; it can be defined as physical attacks.

On the other hand, internal attacks can be defined as attacks targeting network nodes or other components connected to the grid ICT, which leads to abnormal or malicious behavior of the target casing distribution or malfunction to the network.

In SGN, there are several external and internal attacks found in the literature [6]. We have outlined a few attacks in Fig. 4 below.

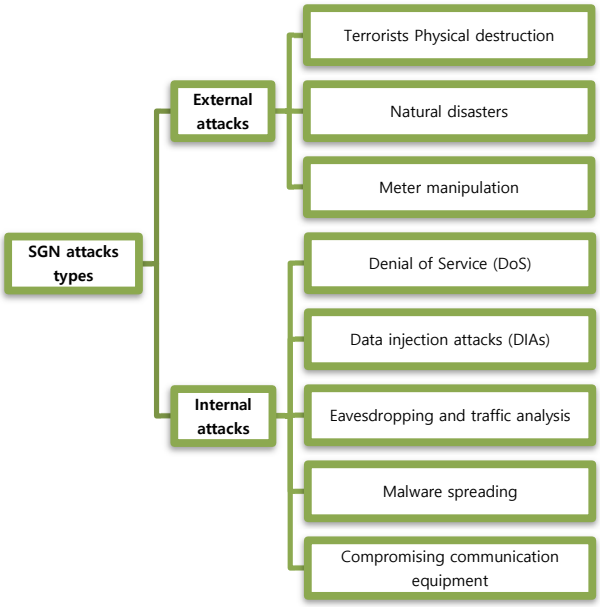

Fig. 4. SGN Types of Attacks

6. Vital challenges for attack detection

Detection of attacks can be a difficult task, because some attacks are not trying to alter the system operation and the reason might be to steal or view data. Considering these, preventive measures must be applied and checked regularly. In this process, researchers found some challenges when detecting malicious attacks as listed below [7].

- Old power electronics devices and equipment was designed in the early days without cyber security in mind. This causes the power electronics to serve as a weak point in network security.
- Smart grid is a massive network that has digital components all across the nation and most of the devices are located out of companies' guarded facilities. These components can be reached and used as multiple entry points to access the network from anywhere.
- Smart grid implements different technologies together increasing the network complexity. The more complex the system is, the more exposure the network to a wider range of attacks. This will ultimately increase the need to regularly supervise the network for any up normal activity.
- Lack of expertise. Since smart grid network have not been around for a long time, engineers have to think ahead to prevent weak links in the security chain of the system. Implementing new technologies can have flaws and will need a regular risk assessment and development to perform in the best manner possible.
- Different standards. Different regions have their own standards and policies making it difficult to settle on one universal security architecture. Integration of systems and technologies can have various difficulties as systems can be in different locations. Which make the attackers in their attention. As a result, that can be hacked or might be weaken the systems. Developing the security mechanism for these older systems is infeasible. Therefore, having universal standards will speed the development process and will eliminate possible threats faster and more efficient.

7. Related works

Smart grid network introduces enhancements and improved capabilities to the conventional power network making it more complex and vulnerable to different types of malicious attacks. Till today, several

works have been done by many researchers to find the best way to detect malicious attacks but very few were focusing on the smart grid malicious attacks. Moreover, no significant importance has been given to finding the malicious attack based on the misbehaviour or abnormal behaviour of the node. Even though some researchers worked based on the misbehavior, but their main focus was to prevent or protect the routing. In the following section, related researchers work will be discussed:

Takiddin et al. in [7] provided answers to three major questions pertaining to the performance of electricity theft detectors in the presence of data poisoning attacks. By proposing a sequential ensemble detector based on a deep autoencoder with attention (AEA), gated recurrent units (GRUs), and feed forward neural networks. The proposed robust detector retains a stable detection performance that is deteriorated only by 1−3% in the presence of strong data poisoning attacks. However, in this method it is normally ensemble performs multiple learners, as a result computation get complicated, which reduce the speed and memory requirements rise.

Zhang et al. in [8] proposed a time series anomaly detection model based on the periodic extraction method of discrete Fourier transform. The detection model determines the sequence position of each element in the period by periodic overlapping mapping, thereby accurately describing the timing relationship between each network message. The experiments demonstrate that the model has the ability to detect cyber attacks such as man-in-the-middle, malicious injection, and Dos in a highly periodic network. The detection model also has a good anomaly detection capability. This model focus on the DoS attacks.

Jiang and Qian in [9] discussed defense mechanisms to either protect the system from attackers in advance or detect the existence of data injection attacks to improve the smart grid security. Focusing on signal processing techniques, this article introduces an adaptive scheme on detection of injected bad data at the control center. Jiang and Qian presented a detection scheme that can self-adaptively detect both non-stealthy and stealthy attacks. The scheme comprises determining two estimates of the state of the monitored system using the state measurement data provided by the remote sensing system at two sequential data collection slots, and determining bad data injection attacks by monitoring the measurement variations and state changes between the two slots. Analysis and simulation results shows that the proposed scheme is efficient in terms of data attack classification and detection accuracy. The research is good to detect data injection attacks.

Zhe et al. in [10] proposed a model based on machine learning to detect smart grid DoS attacks. The model collects network data, then selects features and uses PCA for data dimensionality reduction, and finally uses SVM algorithm for abnormality detection. By testing the SVM, Decision Tree and Naive Bayesian Network classification algorithms on the KDD99 dataset, it is found that the SVM model works best. This method has higher classification detection rate and accuracy, which can effectively improve the security of the smart grid DoS intrusion detection system. This method the data need to go thorough standardization process and in PCA we need to select the principle components otherwise it may miss data features.

Xia et al. in [11] suggest a method to identify all malicious users in a neighbourhood area network. The method uses Group Testing based Heuristic Inspection (GTHI) algorithm, which can estimate the ratio of malicious users on-line, mainly by collecting the information that how many malicious users have been identified during the inspection process. Based upon the ratio of malicious users, the GTHI algorithm adaptively adjusts inspection strategies between an individual inspection strategy and a group testing strategy. The GTHI algorithm outperforms existing methods in some aspects: compared with the BCGI algorithm, it has a wider range of applications; compared with the ATI algorithm, it can locate malicious users within much shorter detection time, regardless of the ratio of malicious users. However, this method does not include the user estimation in the testing phase.

Nandanoori et al. in [12] proposed a Koopman mode decomposition (KMD) based algorithm to detect and identify false data attacks in realtime. The Koopman modes (KMs) are capable of capturing the nonlinear modes of oscillation in the transient dynamics of the power networks and reveal the spatial embedding of both natural and anomalous modes of oscillations in the sensor measurements. The Koopman-based spatio-temporal nonlinear modal analysis is used to filter out the false data injected by

an attacker. This algorithm detects the induced attack within 1 second of attack initiation in the presence of load changes in the network. This method normally works only work based on the false data injection.

Drayer and Routtenberg in [13] a method is developed to addresses Classical residual-based methods for bad data detection of false data injection (FDI) by using graph structure of the grid and the AC power flow model. Drayer and Routtenberg derived an attack detection method that has the ability to detect previously undetectable FDI attacks. This method is based on concepts originating from graph signal processing (GSP). The proposed detection scheme calculates the graph Fourier transform of an estimated grid state and filters the graph's high-frequency components. By comparing the maximum norm of this outcome with a threshold, the method can detect the presence of FDI attacks. Extensive case studies show that the graph signals originating from power systems exhibit the required decaying behavior in their Fourier components. This concentration within the low-frequency components is destroyed for grid states affected by FDI attacks. This facilitates the detection of previously undetectable attacks based on the high-frequency content. In this method sampling is necessary but sampling may cause loss of information.

Patil and Sankpal in [14] proposes an enhanced grid sensor placement (EGSP) algorithm to place grid sensors in the distribution network to monitor and control the smart meters installed in the field. The algorithm provides a simple and efficient way to place grid sensors in the distribution network for monitoring and controlling the smart meters deployed in the distribution network. A simulation model of distribution network has been developed for the analysis of the proposed algorithm. The analytical computation and simulation result shows that the number of grid sensors needed to track all the smart meters connected in the distribution network varies between half the number of SM nodes to equal number of SM nodes depending on how many SM nodes are connected to each EP node. In this method the computation is higher.

Xia et al. in [15] proposed an adaptive binary splitting inspection (ABSI) algorithm which adopts a group testing method to locate and identify all malicious users in a neighbourhood area in a smart grid within the shortest detection time. The paper proposed two inspection strategies, which are a scanning method in which users will be inspected individually, and a binary search method by which a specific number of users will be examined as a whole. During the inspection process of the proposed scheme, the inspection strategy as well as the number of users in the groups to be inspected are adaptively adjusted. Simulation results show that the ABSI algorithm outperforms existing methods in some aspects. Specifically, the ABSI algorithms surpasses the ATI algorithm in terms of the inspection speed. Compared to the BCGI algorithm, the ABSI algorithm is a more general approach. This method requires storage capacity.

Kaygusuz et al. in [16] propose a machine learning and convolution-based classification framework to detect misbehaving malicious smart grid devices. The framework specifically utilizes system and library call lists at the kernel level of the operating system on both resource-limited and resource-rich smart grid devices such as RTUs, PLCs, PMUs, and IEDs. Focusing on the types and other valuable features extracted from the system calls, the framework can successfully identify malicious smart-grid devices. The performance of the proposed framework on a realistic smart grid testbed conforming to the IEC-61850 protocol suite was evaluated on 5 different realistic cases. The test cases specified how behaviour of authentic and compromised devices could differ in the smart grid. The evaluation results demonstrated that the proposed framework could perform with very high accuracy (average 91%) on the detection of compromised smart grid devices. This method has high computational cost and need extensive training data .

Pu et al. in [17] proposed attack recognition mechanism based on Deep Belief Network to extract attack features. The work aims to study the FDI attack behavior and accurately extract the relevant features of the behavior, and provide an effective criterion for the accurate identification of attack behavior in the smart grid. At the same time, through the optimization of the number of nerve cells and the number of layers in each layer of the deep neural network to ensure the real-time detection, the security defense system of the power grid is further enhanced. Simulation results showed that the proposed Deep Belief network could effectively increase the accuracy of feature extraction. The method does not perform well for two-dimensional structure of input data.

Ten et al. in [18] revealed the intrinsic relations between data integrity attacks and real-time electrical market operations, and explicitly characterize their complex interactions as a process simulator. The paper also proposed a simulation-based global optimization problem formulated from which attackers could maximize financial incentives through constructed data integrity attacks. Moreover, a systematic online attack construction strategy is proposed, such that attackers can launch the desired attacks only by the real-time data streams of meter measurements and no power network topology or parameter information is needed. A corresponding online defense strategy is also presented to detect and identify the malicious measurements without extra meter hardware investments. Exploring the properties of the measurement time series in state estimation gives a new perspective of security analytics for Smart Grid system. This method has high computational time as it is doing global optimization.

He et al. in [19] exploits a deep learning techniques to recognize the behavior features of FDI attacks with the historical measurement data and employ the captured features to detect the FDI attacks in real-time. The proposed detection mechanism effectively relaxes the assumptions on the potential attack scenarios and achieves high accuracy. Furthermore, an optimization model is proposed to characterize the behavior of one type of FDI attack that compromises the limited number of state measurements of the power system for electricity theft. Method simulation results showed that the detection method can achieve high detection accuracy in the presence of the occasional operation faults. This work well only to predict the potential attack can happen.

The existing literature depicts that the vast majority of present methodologies to find the malicious in smart grid exists are in a general sense based on cryptographic primitives. Typically, in cryptographic solutions, the source uses cryptographic information to create and send additional authentication. As a results the extra information needed and the malicious can be detected based on the additional information data. The other introduced strategies are typically relying upon calculations and high level of training data. However, these methods have high computational overhead, because of every validation requires an immense number of checking to come up with the final decision about the malicious. Therefore, it is essential to develop an effective method to detect the malicious in the smart grid networks.

8. Methodology

Machine learning has many techniques, Support Vector Machines (SVM) based algorithm is used because of the model ability to classify unreliable data [20]. Which is suitable for high-dimensional data collected from across SGN. Therefore, SVM has been chosen for the proposed solution in this paper.

SVM model categorize the collected data by finding the optimal hyperplane shown in Figure 5 below, which will consist of the largest distance between the two different classes and that distance is called margin [21]. Margin is calculated from the nearest vector to the hyperplane and it must be without interior point as shown in Figure 5 below.

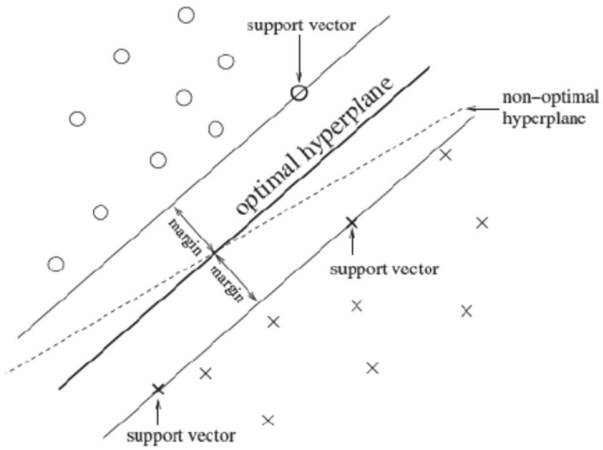

Fig. 5. SVM with its Optimal and non-optimal Hyperplane [22]

The closest point to the hyperplane which will be in contact with the margin parallel lines are called support vectors. Support vectors sets the hyperplane boundary [23]. Figure 5 also shows the two types of data, which are ×'s defining points of a value of 1 and O's defining points of a value of -1. The desired algorithm, a training phase to the system must be conducted offline using a resourceful information source. The training phase uses three Open System Intercommunication9 (OSI) layers, which are a

physical layer followed by medium accessed control layer (MAC) ending with a network layer. After training then collecting the desired data, a data trimming procedure will be implemented on these data sets. Data trimming is a vital step in order to reduce data size which will ultimately allow SVM to process it further. After completing data training and having training sets ready, classification can be done by a linear plane as illustrated in Fig. 6 below.

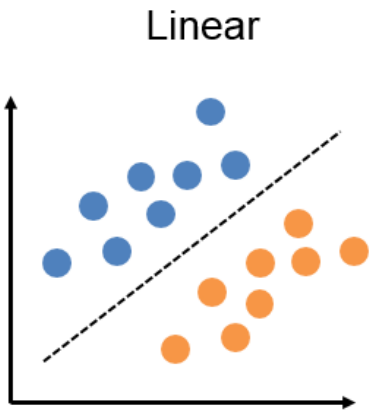

Fig. 6. Linear classification [24]

However, linear classification has limitations when it comes to classifying unreliable data [25]. Therefore, moving the data to a higher dimensional space will allow more functions that were not possible to be applicable such as mapping training sets.

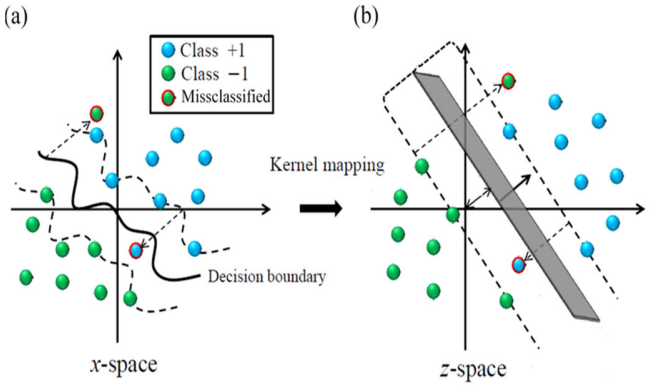

Fig. 7. A problem solved by mapping the training set [26]

As figure 7 shows, a problem that was unsolvable by using linear classification can be classified if training set data moved to a higher dimensional space. After understanding the theoretical part, it is now possible to explain the mathematical calculations behind the SVM method.

Assume that linear separability sample set is (x_i, y_i) with training data sets of:

$$i = 1, \dots, n, x \in R^d, y \in \{+1, -1\}$$

During this research, it's assumed that {1} is the normal and {-1} is the attacked or abnormal. Which leads to the equation of hyperplane classification as follows:

$$w.x + b = 0 \quad \text{---------- (1)}$$

In equation (1), the vector w is a normal vector while b is offset value. The best classifying hyperplane is supported by training data samples. While having this statement in mind, support vectors can be considered as the hyperplane training samples. Moreover, the formulation of the problem will be as follows:

$$min\emptyset\,(w) = \frac{1}{2}\|w\|^2 = \frac{1}{2}\,(w.w)$$
$$subject\ to\ y_i[(w.x_i) + b] - 1 \geq 0, i = 1,2,\dots,n \quad \text{---}$$
$$\text{---(2)}$$

Hence, a formulation of the classification function will be as follows:

$$f(x) = sgn\,\{(w^*.x) + b\} = sgn\,\{\sum_{i=1}^{n} a_i^* y_i (x_i.x) + b^*$$
$$\text{--- (3)}$$

And a formulation of the optimal classification function will be as follows:

$$f(x) = sgn\,\{\sum_{i=1}^{n} a_i^* y_i k(x_i.x) + b^* \quad \text{------- (4)}$$

The function mentioned above (. x) is kernel function while a_i are function multipliers.

Based on the SVM model we detect the malicious. After that we do a trust evaluation based on the nodes history and recorded data, it gives the model structure. Then, the calculation is done for the trust value. In this model a relay node is normally responsible to keep the historical data. The historical data (D_h) are considered as the data average that received in the recent period of time. The real time data (D_r) is the currently recorded data of the node. The trust value (T) of the received data can be calculated as in equation 5.

T=[max*(|Dr – Dh| - K)>0?0: (|Dr – Dh| - K)/K] .(5)

In equation 5, max is a maximum value and K is the is the threshold and it is defined as the upper bound of the absolute value of the difference between the real-time monitoring value and the historical value that can be set by the experts and experience on the system.

In our implementation, the nodes are connected to each other. Specifically, a node connects to a single neighbor node. When all nodes are connected, the optimal hyperplane will be calculated through the previously explained functions and all data from the nodes will be classified into either a normal node or attacked/abnormal node. This process is possible with the use of SVM because of the method ability to classify high-dimensional data.

9. SGN Assumptions and Implementation scenario

In this paper, we considered the following assumptions to implement the methodology:

1- The end used will specify the area of interest. Area of interest has been modelled as a grid Ω of Nx × Ny points scenario. The specified area is given as $A = Nx \times Ny$. Where Nx is the area length in meters (X-Axis) and Ny is the width in meters (Y-Axis) giving the product of the area A.

2- Nodes are sensors that are stationary after deployment (generation of network) and it can be said that nodes are the smart meters that are located in all consumers participating in SGN. Nodes are the communication channel between service provider and consumers and are responsible for collecting and forwarding the monitored data to the central node illustrated previously in Fig. 2.

3- Nodes communicate with Neighbour nodes in a pre-set radio range of (0.25 m2) and to the central node.

4- SVM based algorithm is responsible for classification of nodes.

5- The network is assumed to be synchronized and the monitoring is continuous.

6- The difference between real-time data and historical data is 2 and max is 100. We consider, in real time we should receive maximum 11 data in a minute which is historical data. if the trust value is 50 we will consider the trust value is fine but need further investigation which can be done manually.

Fig. 8. Simulated SGN Network

The hypothetical scenario was considered from one of the village –AFI- in Al Batinah South Governorate, sultanate of Oman as shown in figure 8 taken from google maps. The Area A in the simulation was set by default to N_x of 500 (m) and a N_y of 500 (m) and The default setting of 75 nodes represents smart meters in households in the shown area above. Average electricity consumption set by default to 30 Kwh. Data collected from electricity provider [27] in the area mention above. The monthly bill is also set to a default 250 Omani Riyals calculated using the online bill calculated provided by the service provider [28].

10. Results

The method was simulated based on the hypothetical scenario considered for the implementation. In order to create the scenario, we have obtained the data about the average electricity consumption of the inheritance of the subscribers from the electricity supplier [27] [28]. The Average electricity bill was set as a base to simulate the

network. In our simulation, the basic parameter was set are as follows:

Table 1. Parameters

Parameters (components)	Used values
Number of nodes	8 scenarios
Number of central nodes	1 node
Average electricity consumption	30 Kwh
Average monthly electric bill	250 OMR

In the evaluation process for the effectiveness of the implemented model, we have considered a set of matrices to determine the detection of the attacks.

a) Detection Rate: This is the detection percentage of the attacks based on the total number of attack was performed

b) False positive rate (false alarms): This is the ratio between the number classified as an abnormal node (which is considered as an attacked node) on the total number of normal connections.

The simulation in MATLAB gave us the attack detection accuracy of 98% and the False alarms rate as low as 2% from the total number of attacks.

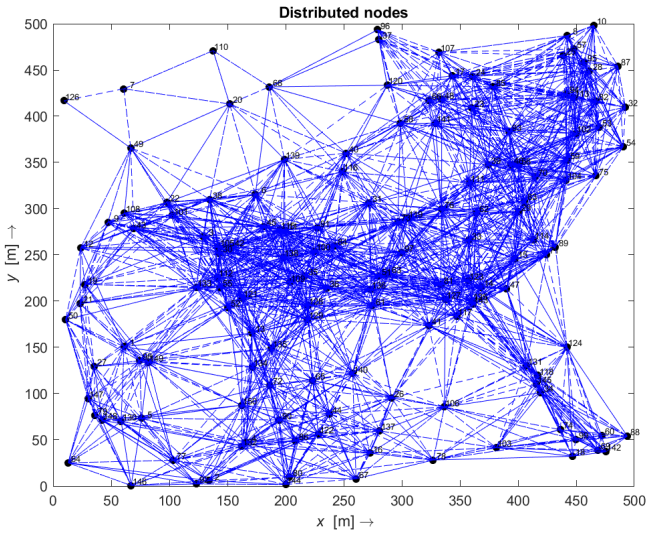

Fig. 9. Simulated SGN Network

Figure 9 illustrates a sample SGN generated through the algorithm. A network of 150 nodes is presented which correspond to an average population area as mentioned in the hypothetical scenario of AFI village.

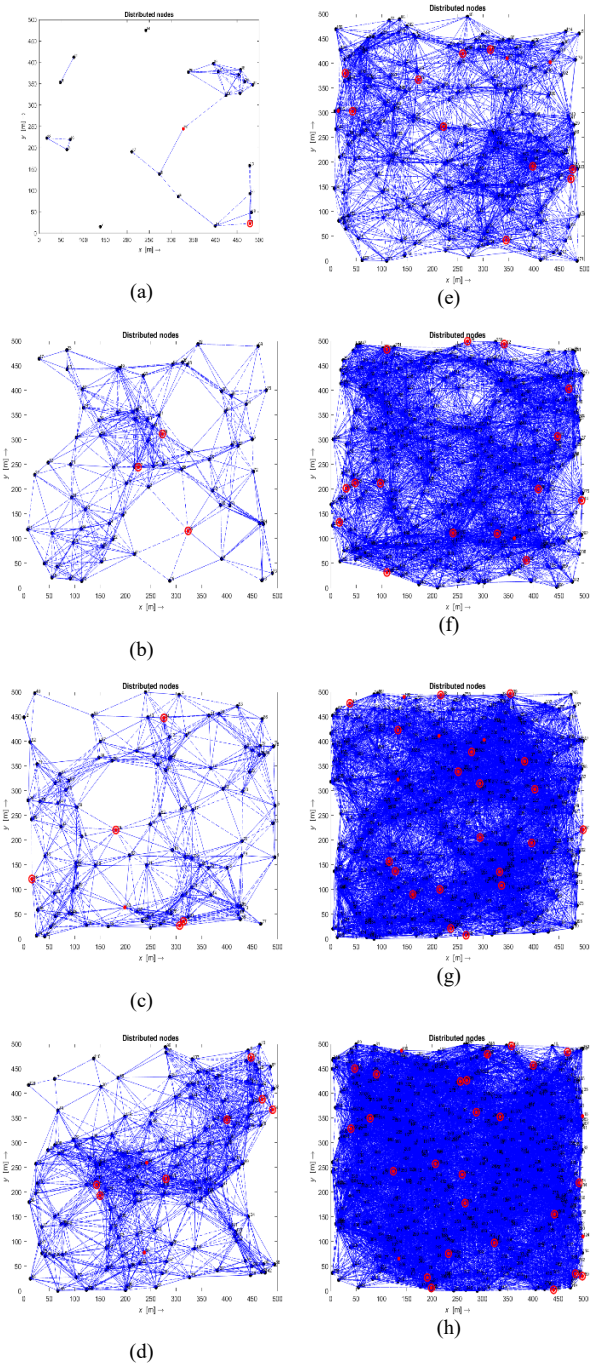

Fig. 10. Detection Malicious Nodes

Figure 10 shows eight different simulations of malicious detection in SGN. The simulations then have been applied to the developed model/algorithm and showed the detection of malicious nodes highlighted by red circles. Figure 10 shows the implementation of different scenarios ranging from light populated (a) area to highly dense area (h). Each letter from (a) to (h) represent a different number of nodes to test the model in the mentioned scenarios. Letters from (a) to (h) correspond starting from (25, 75, 100, 150, 200, 300, 400 and 500) in order. The simulation also gives vital information that is illustrated in figure 9 below.

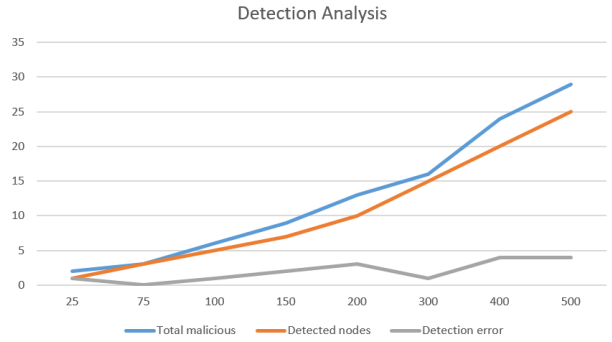

Fig. 11. Detection rate analysis

Figure 11 illustrates the detection rate pattern in different node scenarios that are mentioned previously. A high detection rate is shown as the number of nodes increases while detection error has unnoticeable/slow/minor increase, which legitimize the model effectiveness in dense population areas.

After detection of the malicious with the implemented method, based on the consideration and simulation result we have calculated the trust value. In view of the detection, we have considered D_r and D_h value as 12 and 11 respectfully. The calculated trust value based on the equation 5 is shown as follows:

$$T=[100*(|12 – 11| - 2)>0?0: (|12 – 11| - 2)/2]$$

$$T= [100*(1/2)]$$

$$T=50$$

As a result, we are getting a trust value of 50. Meaning that we will double check the node manually.

11. Conclusion

Smart Grid Network is an evaluation for a new generation of smart power networks that participate in actions approaching from all associated end users. The SGN infrastructure developed with bidirectional communications between end-users and the SGN operator. This led the networks for the attack surface against the power system. In order to protect the network in this paper, we have developed an SVM based algorithm to detect the malicious and taking nodes history and recorded data we have done the node trust evaluation. The simulation result in MATLAB gave us an effective detection outcome. The result shows us that our detection rate is about 98% and the false positive is only 2% and the node trust value is 50. In future, we would like to simulate the network on a larger scale and implement it at the hardware level.

References

[1] M. Uma and G. Padmavathi, “A Survey on Various Cyber Attacks and Their Classification,” p. 7, 2013.

[2] ETV 2 NITTTRCHD, *Cyber Security in Smart Grid: Overview Session 1 Module 15 by Janorious Rabeela*, (Jan. 04, 2019). Accessed: Feb. 16, 2021. [Online Video]. Available: https://www.youtube.com/watch?v=bvGrh7lITeE

[3] D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rohde, “Protecting Smart Grid Automation Systems Against Cyberattacks,” *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 782–795, Dec. 2011, doi: 10.1109/TSG.2011.2159999.

[4] F. Aloul, A. R. Al-Ali, R. Al-Dalky, M. Al-Mardini, and W. El-Hajj, “Smart Grid Security: Threats, Vulnerabilities and Solutions,” *SGCE*, pp. 1–6, 2012, doi: 10.12720/sgce.1.1.1-6.

[5] M. Jouini, L. B. A. Rabai, and A. B. Aissa, “Classification of Security Threats in Information Systems,” *Procedia Computer Science*, vol. 32, pp. 489–496, Jan. 2014, doi: 10.1016/j.procs.2014.05.452.

[6] A. Sanjab, W. Saad, I. Guvenc, A. Sarwat, and S. Biswas, “Smart Grid Security: Threats, Challenges, and Solutions,” *arXiv:1606.06992 [cs, math]*, Jun. 2016, Accessed: Mar. 06, 2021. [Online]. Available: http://arxiv.org/abs/1606.06992

[7] A. Takiddin, M. Ismail, U. Zafar, and E. Serpedin, “Robust Electricity Theft Detection Against Data Poisoning Attacks in Smart Grids,” *IEEE Transactions on Smart Grid*, pp. 1–1, 2020, doi: 10.1109/TSG.2020.3047864.

[8] L. Zhang, X. Shen, F. Zhang, M. Ren, B. Ge, and B. Li, “Anomaly Detection for Power Grid Based on Time Series Model,” in *2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous*

Computing (EUC), Aug. 2019, pp. 188–192. doi: 10.1109/CSE/EUC.2019.00044.

[9] J. Jiang and Y. Qian, "Defense Mechanisms against Data Injection Attacks in Smart Grid Networks," *IEEE Communications Magazine*, vol. 55, no. 10, pp. 76–82, Oct. 2017, doi: 10.1109/MCOM.2017.1700180.

[10] W. Zhe, C. Wei, and L. Chunlin, "DoS attack detection model of smart grid based on machine learning method," in *2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS)*, Jul. 2020, pp. 735–738. doi: 10.1109/ICPICS50287.2020.9202401.

[11] X. Xia, Y. Xiao, W. Liang, and M. Zheng, "GTHI: A Heuristic Algorithm to Detect Malicious Users in Smart Grids," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 805–816, Apr. 2020, doi: 10.1109/TNSE.2018.2855139.

[12] S. P. Nandanoori, S. Kundu, S. Pal, K. Agarwal, and S. Choudhury, "Model-Agnostic Algorithm for Real-Time Attack Identification in Power Grid using Koopman Modes," in *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Nov. 2020, pp. 1–6. doi: 10.1109/SmartGridComm47815.2020.9303022.

[13] E. Drayer and T. Routtenberg, "Detection of False Data Injection Attacks in Smart Grids Based on Graph Signal Processing," *IEEE Systems Journal*, vol. 14, no. 2, pp. 1886–1896, Jun. 2020, doi: 10.1109/JSYST.2019.2927469.

[14] Y. S. Patil and S. V. Sankpal, "EGSP: Enhanced Grid Sensor Placement Algorithm for Energy Theft Detection in Smart Grids," in *2019 IEEE 5th International Conference for Convergence in Technology (I2CT)*, Mar. 2019, pp. 1–5. doi: 10.1109/I2CT45611.2019.9033759.

[15] X. Xia, Y. Xiao, and W. Liang, "ABSI: An Adaptive Binary Splitting Algorithm for Malicious Meter Inspection in Smart Grid," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 445–458, Feb. 2019, doi: 10.1109/TIFS.2018.2854703.

[16] C. Kaygusuz, L. Babun, H. Aksu, and A. S. Uluagac, "Detection of Compromised Smart Grid Devices with Machine Learning and Convolution Techniques," in *2018 IEEE International Conference on Communications (ICC)*, May 2018, pp. 1–6. doi: 10.1109/ICC.2018.8423022.

[17] Q. Pu *et al.*, "Detection Mechanism of FDI Attack Feature Based on Deep Learning," in *2018 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Oct. 2018, pp. 1761–1765. doi: 10.1109/SmartWorld.2018.00297.

[18] S. Tan, W. Song, M. Stewart, J. Yang, and L. Tong, "Online Data Integrity Attacks Against Real-Time Electrical Market in Smart Grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 313–322, Jan. 2018, doi: 10.1109/TSG.2016.2550801.

[19] Y. He, G. J. Mendis, and J. Wei, "Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017, doi: 10.1109/TSG.2017.2703842.

[20] N. Cristianini, J. Shawe-Taylor, and D. of C. S. R. H. J. Shawe-Taylor, *An Introduction to Support Vector Machines and Other Kernel-based Learning Methods*. Cambridge University Press, 2000.

[21] S. S. Keerthi and C.-J. Lin, "Asymptotic Behaviors of Support Vector Machines with Gaussian Kernel," *Neural Computation*, vol. 15, no. 7, pp. 1667–1689, Jul. 2003, doi: 10.1162/089976603321891855.

[22] "Fig. 4. SVM classification with a hyperplane that maximizes the...," *ResearchGate*. https://www.researchgate.net/figure/SVM-classification-with-a-hyperplane-that-maximizes-the-separating-margin-between-the-two_fig3_221926953 (accessed Jan. 13, 2021).

[23] G. C. Calafiore and L. E. Ghaoui, *Optimization Models*. Cambridge University Press, 2014.

[24] J. Sullivan, "Neural Network from Scratch: Perceptron Linear Classifier," *John Sullivan*, Aug. 16, 2017. https://jtsulliv.github.io/perceptron/ (accessed Jan. 13, 2021).

[25] R. Grosse, "Lecture 3: Linear Classification," p. 10.

[26] "Figure 1. Graphical presentation of the support vector machine...," *ResearchGate*. https://www.researchgate.net/figure/Graphical-presentation-of-the-support-vector-machine-classifier-with-a-non-linear-kernel_fig1_299529384 (accessed Jan. 13, 2021).

[27] "Pages - Home." https://mzec.nama.om/en-us/Pages/home.aspx (accessed Mar. 19, 2021).

[28] "Bill Calculator." https://mzec.nama.om/en-us/Pages/billcalculator.aspx (accessed Mar. 19, 2021).