Residential Microgrid cyber-attack identification using Highly Secure framework based on Machine Learning

SivaNagiReddy Kalli[1], Cheeti Harshini[2], Kasani Aparna[3], Chavali Bhavitha[4]

[1] Professor, Department of Electronics and Communication Engineering,

Sridevi Women's Engineering College, Hyderabad, India

[2, 3, 4] U.G Student, Department of Electronics and Communication Engineering,

Sridevi Women's Engineering College, Hyderabad, India

[1]sivanagireddykalli@gmail.com

ABSTRACT:

Economy and people life can be great impacted by using highly secure and best infrastructure. There are many domains such as water supply domain, communication domain, energy generation and transmission systems which require a highly secure and best infrastructure as it is two-way communication. Even these types of systems need stability, reliability and improved efficiency than existing state of art techniques. Many cyber-attack frames are designed in recent year which has high impact and frequency of use with higher publicity. Power system can be secured using different cyber-attack detection systems. Real time detection of issues in data integrity, attacks and sensor failure can be achieved by proposed model. For residential microgrid the proposed model can be used with higher satisfactory performance and high accuracy with practical data operation.

Keywords—*machine learning, Highly secure framework, cyber-attack, impact of infrastructure, residential microgrid.*

Number: 10.14704/nq.2022.20.7.NQ33268 **Neuro Quantology 2022; 20(7):2105-2109**

Introduction

Machine Learning is branch of artificial intelligence in which the study the computer science, use of data and algorithm. WSN is the study of infrastructure less wireless network is used to monitor, physical or environmental condition. Micro grid is a local energy grid with control capability disconnect from grid to enable it to operate in both grids connected Island. Micro grid is used to development of energy sources such as wind turbine and solar panel. From micro grid technology we get the benefit for electric grid but it is limited for the higher voltage profile, power losses and lower costs. The communication between Consumers and micro grid the smart meters use as a decision-making unit. In micro grid smart meter plays significant role. According to US Department of Homeland Security in electric power companies 224 malicious cyber-attacks reported. For local consumers it is impossible to reach all points for comparison because of high complexity and non-Linearity of micro grid. The paper is proposed with data integrity attacks and defends them. The proposed work can detect the cyber-attack by measuring the features and learning of microgrid. In Micro grid cyber security band cyber-attack, the Micro grid is a small size system consumption sides and it operate on 2 models ; 1) grid connected, 2) islanded, Microgrid dealing with data transmission and decision making on data that are interconnected. AMI is the charge of data gathering, data communication and energy consumer. AMI makes a decision in generation and consumption Smart meters is used for collecting and analyzing the situation of microgrid. As seen above there are two layers found as physical layer and cyber layer. Physical layer includes utility grid, storage and AMI while cyber layer includes analog and digital output, microgrid controls and analog and digital input. The role of AMI in typical micro grid to gather the load consumption data transfer to decision making unit. In any situation the healthy micro grid satisfies generation and demand balance equation. According to consumer demand the AMI can reduce the total micro grid cost by providing data. The cyber

security in grid connected mode the AMI can Increase the cost of micro grid. The cyber security in is landed mode serves result such as loss generation and demand balance. In these we have seen two types of micro grid of cyber-attack. a) Microgrid damage highly done by malicious attacks by instantaneous and strong attacks. b) Long term but gradual with smooth effect. The existing system developed with Euclidean and Cos-Sim framework-based algorithm. Those frameworks have lowered accurate and more detection delay.

a) Euclidean Classifier

This is minimum distance classifier used for identification of different attacks without machine learning. The distance between Cartesian coordinates of point is used for calculation of Euclidean distance as shown below,

$$(p, q) = \sqrt{((q1 - p1)2 + (q2 - p2)2 \ldots..(1)}$$

A Line segment in given points also show Euclidian space. Smallest distance or smallest difference among two points or two types of data is calculated using Euclidean distance.

b) Cosine Similarity (Cos-Sim)

Irrespective of size how the data is matching with each other can be calculated using cosine similarity (Cos-Sim). The input data is considered as vector and classification is done using given formula to find similarity between two vectors. The basic formula can be as given below,

$$\text{Cos}\ (x, y) = x.\ y\ /||X|| * ||y|| \ldots\ (2)$$

Where '.' mentions dot product '*' is used for cross product, ||x|| represents length of a vector x. The frameworks are very basic frameworks having lower accuracy with more detection delay. So these frameworks can't be used for residential microgrid as its very complex system and there are many possibilities of cyber-attacks as there is huge number of operators. So to avoid the drawbacks we are going to use machine learning based framework which gives better accuracy as well as delay in detection is very less with more compatibility.

II. LITERATURE SURVEY

Author [1] seen that detection of simple approach for fake news used the naive Bayer classifier. Here we get 74% accuracy. Feragut et al [2] is work on a neutral network based on mechanism performed voltage and modern reading ensuring from hug range of load condition of power system. On the Observation use of neutral network mechanism are good. The team finding the conclusion that while using the addition of features first and build a detector use infer and exploit for signal machine learning is better. Here we get 97% accuracy. Fangyu el at [3] on cyber-attack proposed a high dimension detection and identification. In the distribution of power grids are analyzed by cyber and physical attack with after that steam with a high dimension matrix of different sensor is constructed. The detection and identification power electronics using the raw electrical waveform of cyber-attack for distribution of power grids with photovoltaic. The Machine Learning is best on anomaly detection that is developed for load forecasting. To construct a benchmark 1 st used the load data and k-mean clustering done by using scaling. To calculate occurrence and parameter the dynamic programming is used. On the compassion of methods seen that the symbolic aggregator approximation and robustness and effective ness method is verify from the numeric simulations [4].

III. Secured Frame Work for the Microgrid Cyber Attacks

The framework of model-free reinforcement learning (RL) designed for **Moderately Visible Markov Decision Method** (MVMDM) is for detection of online anomaly/attacks which overcomes drawbacks of state of art techniques. The use of reinforcement learning (RL) model used for proposed method which is even used for online cyber-attacks. Residential smart-grid is analyzed for detection of accurate and timely RL-based method for understanding its effectiveness. Detection of cyber-attacks based on given algorithm which is model-free RL with MVMDM is used for universal purpose. There is no need of multiple attack must get train as this model is machine learning model. Even with proposed model new unknown attacks can be identified. Using trial and error method direct mapping is possible as we are using model free RL approach. Under given operating condition

data can be generated or obtained is used for training phase.

It's mostly a difficult task to obtain real attack data for training phase. So, for training we are going to follow detection approach which is robust and training is done with attacks having low magnitude with worst case scenario by observing detection difficulty. Compare to normal observation this proposed model has more sensitivity even there is slight deviation.

Low magnitude attacks are not much interested as there is very low performance change on our system. So, to find online cyber-attack detection system using RL is proposed in this system.

The learning and online detection phases make up the RL-based detection system under consideration. In the literature, it was numerically demonstrated that SARSA, a model-free RL control algorithm [12], outperformed the model-free MVMDM settings. The defender is therefore trained with numerous episodes of experience utilizing the SARSA algorithm throughout the learning phase. The defense learns from SARSA. A simulation environment is established for training, and during the training process, at each time, the defense acts in response to what it has observed, incurring a cost as a result from the simulation. The environment has given bellow.

1: Input: Q-table learned in Algorithm 1.

2: Choose an initial o based on the pre-attack state and choose the initial a = continue.

3: t ←0

4: while x ≠ stop do

5: t ←t + 1

6: Collect the measurements yt.

7: Determine the new o ←Q(o; x) Q(o; x) + α (r + Q(o′; x′) - Q(o; x)) [From SARSA Algorithm]

8: x ← arg $\min_a$Q(o; x).

9: end while

10: Declare an attack and terminate the procedure

Proposed model has following components as shown in above figure, a) Smart Meter b) AMI communication system c) Anomaly detection model d) Microgrid central control unit. The suggested solution approach can be used in a distributed smart grid system, where the metre readings are received in a distributed fashion but the learning and detection duties are still carried out at a single centre.

IV.RESULTS

The calculation of the average detection delay and the probability of false alarm for the proposed detector, the Euclidean detector [13], and the cosine-similarity metric based detector [14] using Monte Carlo simulations over 10000 trials. We change the benchmark test thresholds and change "a" for the suggested algorithm to produce the performance curves. We employ Algorithm 2, which applies the Q-tables discovered in SARSA [12] for a = 0.01 and a = 0.1, to assess the suggested algorithm. We also provide precision, recall, and F-score information for each simulation case. To impose of an upper bound on the detection latency because computing these measurements necessitates computing the number of detected and missed trials (that corresponds to the maximum acceptable detection delay). So that, if the attack is discovered inside this bound, we believe it has been discovered; otherwise, it would have been overlooked. We choose this constraint to be 10 time units as an illustration. Then, we determine the Out of 10,000 trials, the following were the precision, recall, and F-score for false data injection (FDI), jamming, and Denial of Service (DoS) attacks are analyzed for proposed system. And following results are obtained.

Formulas used for calculation of precision, recall and F-score.

$$\text{Precision} = \frac{\#\text{ trials } (\tau \le \text{Stop Time} \le \tau + 10)}{\#\text{ trials } (\tau \le \text{Stop Time} \le \tau + 10) + \#\text{ trials } (\text{Stop Time} < \tau)} \quad (3)$$

$$\text{Recall} = \frac{\#\text{ trials } (\tau \le \text{Stop Time} \le \tau + 10)}{\#\text{ trials } (\tau \le \text{Stop Time} \le \tau + 10) + \#\text{ trials}(\text{Stop Time} > \tau + 10)} \quad (4)$$

$$\text{F} - \text{score} = \frac{2\,\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (5)$$

Where "# trials" means "the number of trials with".

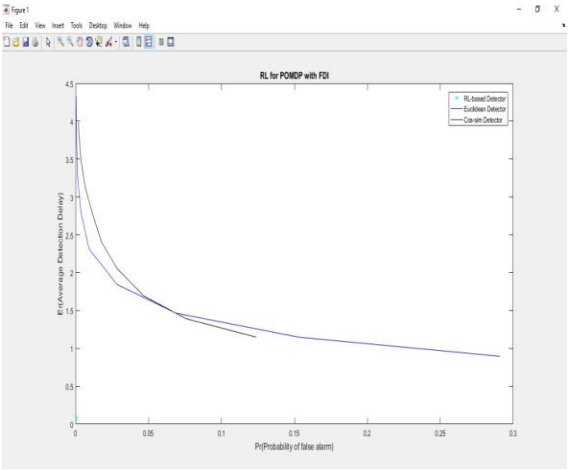

Fig.1 probability is plotted w.r.t average detection delay for proposed method for attack from FDI

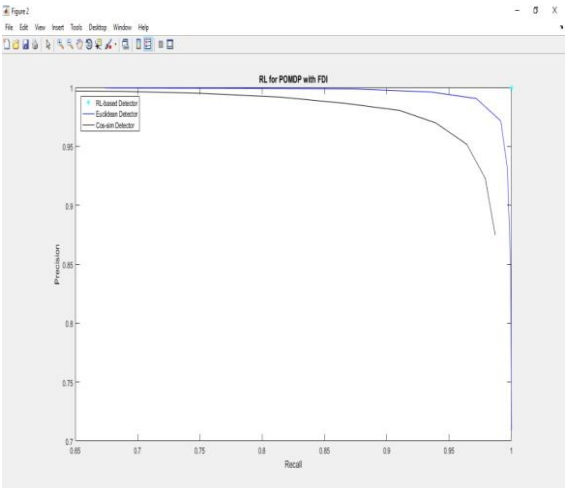

Fig.2: Precision vs. recall for the proposed and the benchmark detectors against a random FDI attack.

TABLE 1: For proposed work calculated Precision, recall, and F-score (a=0.1)

Measure	FDI	Jamming	DoS
Precision	0.9976	0.9973	0.9975
Recall	1	1	1
F-score	0.9989	0.9986	0.9989

TABLE 2: proposed method parameters area calculated as Precision, recall, and F- score (a=0.01)

Measure	FDI	Jamming	DoS
Precision	0.9999	0.9995	0.9996
Recall	1	1	1
F-score	0.9999	0.9998	0.9999

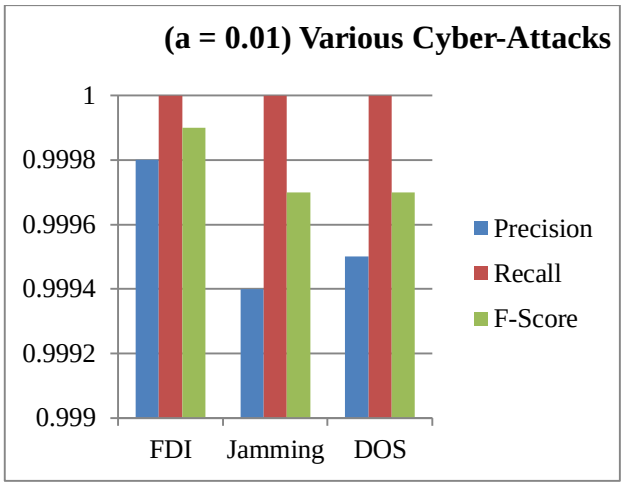

Figure 3: Comparison attacks for Precision, recall, and F-score (a=0.02)

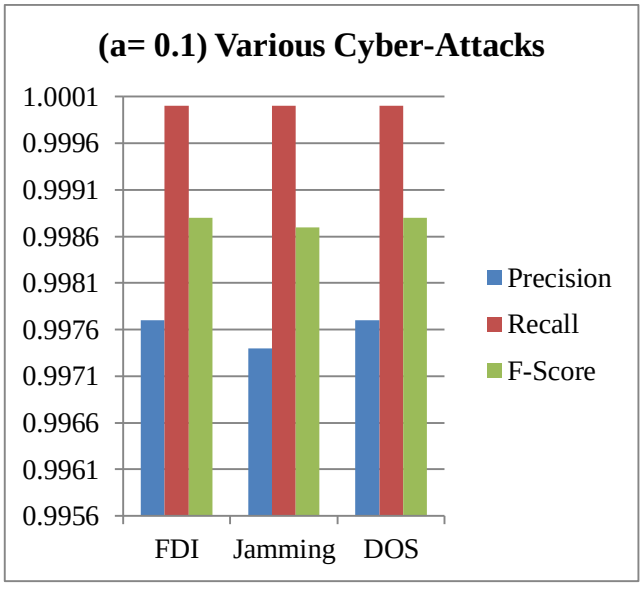

Figure 4: Comparison attacks for Precision, recall, and F-score (a=0.2)

V. CONCLUSION

Central unit which has huge demand in microgrid can be attacked by online attackers which may be used for misleading and causing harm to management. So, there is need of higher data integrity for complete operations of microgrid. There may cause mismatch between demand and supply. So, in this we designed a model which has very high data integrity over cyber-attacks for residential microgrid providing intelligent and accurate solution. In proposed system architecture and flow chart are explained in detail for innovative model which can help to cure residential microgrid. Smart meter readings with 342 houses are used for recorded dataset. Performance parameter shows the superior performance of proposed model. Parameters such as precision, recall and F1-score are used for system analysis. Proposed model with following features can be considered for future enhancement, best sophisticated memory technique can be used, Advance structure of NN can be used for calculation of Q value, and Even Deep RL can be used for better performance.

REFERENCES:

1. Naive Bayes Classifier-Mykhailo Granik, Volodymyr Mesyura. Published inthe year in 2017 in Vinnytsia, Ukraine. "Areview of false data injection attacksagainst modern power systems," IEEE Transactions on Smart Grid, vol. PP, no. 99,pp. 1–1, 2016.
2. Fangyu et al "Cyber security in the smart grid: Survey and challenges," Computer Networks, vol. 57, no. 5, pp. 1344–1371, 2013.
3. Ferragut et al "A survey on cyber security for smart grid communications," IEEE Communications Surveys&Tutorials, 2012.
4. Naive Bayes "False data injection attacks in electricity markets," in 2010 First IEEE International Conference on Smart Grid Communications, Oct 2010, pp. 226–231.
5. Yaokai Feng et al, "False data injection attacks against state estimation in electric power grids," in Proceedings of the 16th ACM Conference on Computer and Communications Security, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 21–32.
6. H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010, 2010.
7. Patric Nader, "Quickest detection of false data injection attack in wide-area smart grids," IEEE Transactions on Smart Grid, vol. 6, no. 6, pp. 2725–2735, Nov 2015.
8. W. Moon IEEE Transactions on Power Electronics, vol. 36, no. 4, pp. 4105-4115, Apr. 2021.
9. G. W. Moon IEEE Transactions on Power Electronics, vol. 36, no. 1, pp. 401-408, Jan. 2021.
10. SivaNagiReddy Kalli "An effective motion object detection using adaptive background modeling mechanism in video surveillance system". Journal of Intelligent & Fuzzy Systems, vol. 41, no. 1, pp. 1777-1789, 2021,11 August 2021, **DOI:** 10.3233/JIFS-210563
11. SivaNagiReddy Kalli & Bhanu Murthy Bhaskara, "Efficient Field Programmable Gate Array Implementation for Moving Object Segmentation using BMFCM", Indian Journal of Science and Technology, Vol 10(1), DOI: 10.17485/ijst/2017/v10i1/109393, January 2017.
12. R. S. Sutton and A. G. Barto, *Reinforcement learning: An introduction*. MIT press Cambridge, 1998, vol. 1, no. 1.
13. K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," *IEEE Transactions on Control of Network Systems*, vol. 1, no. 4, pp. 370–379, Dec 2014.
14. D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Processing Letters*, vol. 22, no. 10, pp. 1652–1656, Oct 2015.