International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April, 2020

# Rule Based Novel Method for Self Healing Attack Revelation for Smart Grids

**Arvind P. Kadam, S. G. Ankaliki**

***Abstract:** In this paper, we introduce a new idea for the rebuilding of measuring sensor data collected from the power grid, eliminating the impact of the attack on the integrity of confidential data. The introduced system is based on the reconstruction of Monte Carlo analysis of experimental data and the measurement of actual training data of the transfer function of the information gathered by sensor of the strong nonlinear representation data through the root is added to the sensor measurements based on quality parameters by a clever attacker. For strong, multivariate reconstruction measures against multiple attacks sensors based regulation attack detection is used. The introduced scheme is check out using a standard IEEE 34-bus and real samples were collected from a grid system. The simulation results confirm that the introduced scheme can handle the label and non-label and attacks based on the proposed rules historical measurement data decided on the basis of the received value RAE become. 5.5.*

*Self- healing recovery is possible within 10 msec of time limit if multiple attacks are detected by local system agent then feed gain of agent scheduler is adjusted to 1/4 to 1/3.*

*Finally, if the value of RAE deviates according to the complexity of the time constant increases to 20 msec to recover the original response was very close to that of the nominal case.*

***Keywords :** Cyber Security, Cyber Assaults, Deep Learning, Self-healing smart grids, State Estimation*

## I. INTRODUCTION

Smart Grid is an intellectual electricity network. It is a next generation electric power system. Smart Grid aims to fully integrate high-speed, two-way communication technology. It is the integration of information and communication (ICT) networks to monitor and control electricity production and demand [1].The future grids have the features like two way communication, distributed generation, self-monitoring, self-healing. This vision is achieved by using ICT in smart grids. We desire to obtain ICT solutions for self-healing smart grids. The principle of self-healing control is to ensure the reliability and uninterrupted power supply. In normal operation, the main purpose of self-healing control is to optimize the operation and eliminate the hidden trouble [2, 4,5].

Broad research has been reported in the literature on the detection layer of defence mechanism. Table 1 represents a brief of the research works conducted at the level of detection and mitigation. We can see that less attention has been paid by researchers to the level of mitigation. In particular, in the context of the CCDA attack mitigation through the reconstruction of sensors collect measurement data, no existing work to the best of our knowledge. In the context of self-healing [7], which is a significant characteristic of SG, there is a need to focus on mitigation layer and neutralize or reduce the effects of CCDA. [19][23]

**Table-I A summary of research on detection and Mitigation level of defense mechanism in Smart Grid**

| Defense level | Application Area |
|---|---|
| ***Detection level (Intrusion detection system (IDS) without utilizing machine learning)*** | |
| Engineering-based models and methods of game theory to security [11,12] | EMS |
| watermarking physical control inputs [13] | PCC |
| The integration of the semantic analysis with effective execution PF anticipation analysis [15] | SCAD |
| An IDS system based on a model to fight against attacks on the automatic generation of control [13] | EMS |
| Integrating IDS and host-based stations on the network [11] | SCADA |
| Generic use of phasor measurement units data (PMU) based behavioral white listing and network topology [14] | PMU |
| IDS to detect the data PMU victimized by identity theft GPS [15] | PMU |
| The attack detection on the CP network advanced metering system (AMI) on the basis of rules of behavior [17] | AMI |
| IDS alert system and early [20,21] multi-layer distributed | AMI |
| Identification stealth attacks cumulative sum and faster detection[19] | EMS/PC C |
| Abnormal detection energy consumption in smart metering using heuristics and contextual analysis of data [24-27] | Smart Meters |
| ***Detection Level (Intrusion detection system (IDS) utilizing machine learning)*** | |
| Using machine learning methods for the detection CCDA [26,27] | PCC |
| EMS function selection and detection CCDA based on supervised learning [31,32] | PCC |
| feature extraction and detection of CCDA based on unsupervised learning [12] | PC |
| C Identification CCDA using a common processing and the Kullback-Leibler distance | PC |
| C profound recognition based on learning CCDA behavioral characteristics [26] | PC |

Revised Manuscript Received on April 25, 2020.
* Correspondence Author
**Arvind P. Kadam*,** Research Scholar, Department of Electrical and Electronics Engineering, SDM College of Engineering, Dharwad-Karnataka-India, Affiliated to Visvesvaraya Technological University, Belgavi-Karnataka-India. Email: karvind1972@gmail.com
**Dr. S. G. Ankaliki,** Head & Professor, Department of Electrical and Electronics Engineering, SDM College of Engineering, Dharwad-Karnataka-India, Affiliated to Visvesvaraya Technological University, Belgavi-Karnataka-India. Email: sgasdmee@rediffmail.com

The main purpose of the control of self-healing is to restore the fault as soon as possible, can be divided into internal and external faults in the control area. In this paper self-healing feature in smart grid is shared and how the self-heals detect the attack. We present our approach to self-healing behavior in smart grids identify the attack.

## II. RULE BASED HEALING

In this work we used the concept of self-healing. Self-healing can take necessary recovery steps by self to restore specific mode of operation. As per figure 1 recovery process are rule based which are based on quality factors, the proposed system take maximum 10 msec recovery time to recover in original state[3].

### A. Requirement Elicitation

The whole set of requirements will give the desired behavior. Terms of the sequence from higher to lower level system requirements follow the requirements of a higher level. Classify the behavior of the system based on the needs of sequencing at a higher level [8].

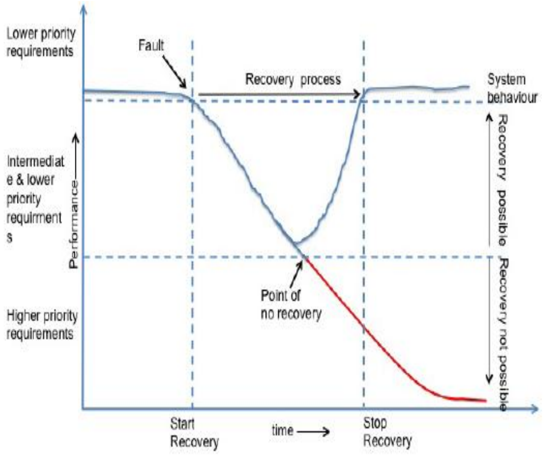


**Fig.1. Recovery Process of the system**

### B. Detection and Identification of Faults

Errors are identified and detected based on quality parameters and system behavior. The analysis provides a deviation from the intended and actual behavior. If the rules for the desired behavior is not enabled it means that the conditions are not met. We can say that the participating components involved in terms of damaged [9][16].

### C. Classification of Faults and Scope of Recovery

The criteria for the classification of error are depending on the rules that have been violated. If a higher priority rule is violated the system went into an undesirable state. It will reach no recovery. Focus on recovery procedures to bring the system back to the operating level [10].

### D. Passive Recovery

The system remains in the deviated state up to the faulty component being repaired and system enters into degraded state and performs certain time in this state. The system continues to remain in a state deviated. If the error induced due to external factors then this approach helps [13]

### E. Active Recovery

Actions taken to bring back the system to the desired behavior. The faulty device is replaced by new one. Quality based rules will be required to replace the existing 1 x 1 , 2 x 2 , 4 x 4 and more in case of software fault [19]

## III. TYPES OF SMART GRID ATTACKS

Smart grid attacks are divided into three types.

### A. Consumer End Attacks

The attack occurred at the end consumer as a smart meter or a network controller. These attacks are an attempt to steal personal current consumption profile for the user's personal information. Because of this attack, erroneous request sent to the control center and stops sending power to the damaged user requests. This denial shut down power supply of residential buildings and interrupts the quality of power delivered to hospitals, transportation. There is a threat to the user to provide personal information [21]

### B. Data Attacks

These types of attacks are targeted while data flow occurs in the communication network. In these types of attacks, including the insertion, alteration or deletion of data or control commands. One injection attacks data or load change detection is very difficult if the attacker has knowledge of the network topology information from electricity. Data protection can be very difficult because of the large amount of data collected and produced by the giant network [22][30]

### C. Direct Attacks

Power plants, substation or transmission lines are directly attack by cyber physical. The attacker can trip the components which are in normal operation. There is massive blackout by cascading failure of components. These types of attack are sending false messages to control centre, resulting in mistaken actions by control centre [24]

### D. Smart Grid Security Tools

Traditional approaches to address these security issues such as control of network security study smart and efficient trust, advanced encryption, detection of bad data. To understand the interaction between the attacker and the defender in securing the smart grid introduced many techniques such as Petri nets, clustering / partitioning, data mining. Petri nets are strong in identifying and addressing some of the events that occurred cyber physically. Data mining algorithms to collect data from the sensor network and smart grid to extract important information from the network operation of electricity [27]

## IV. MODELLING OF RESULTANT ELEMENT

This system contains electrical, magnetic and Mechanical Elements. One homogeneous models will be used by the electric analogy. Elements that are generated will be modeled by the electrical subsystems.equivalent circuit is formed to subsystem then combined using a transfer function to generate the equivalent of a whole series of elements.

*Retrieval Number: D7829049420/2020©BEIESP*
*DOI: 10.35940/ijeat.D7829.049420*
*Journal Website: www.ijeat.org*



*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication*

Figure 2 represents the flux in the system [28]

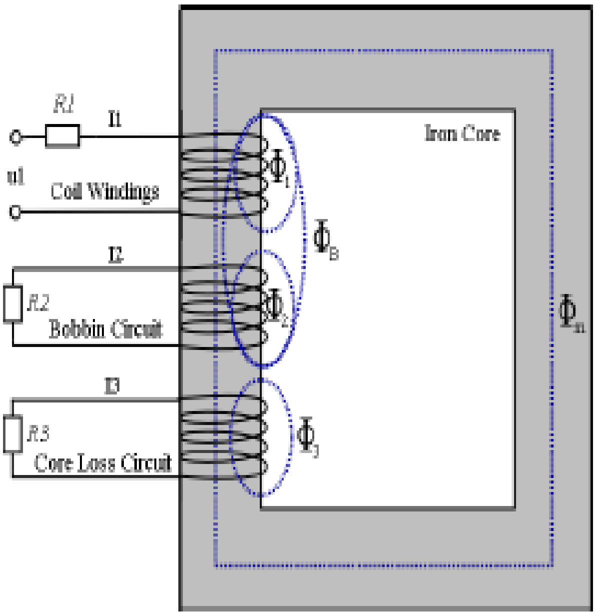


**Fig.2. Magnetic flux within the system**

The iron core is surrounded by the three coil circuits. The moving coil is with u1 voltage and R1 equivalent resistance. The second coli circuit is eddy current with resistance R2. The third coil circuit is the inductive and resistive core losses. The ϕm represents major flux flows. The flux linking coil is ϕ1. The flux flowing in eddy current is ϕ2. The flux links the coil and the eddy current is $\phi_B$. The core loss is ϕ3.

The magneto motive force (m.m.f.) that creates the flux electromotive force (e.m.f.). The emf is created across the coils by the changing flux using the following expressions [29]

$$F=\rho\Phi \quad (1)$$

$$E = N\, d\text{Ø}/dt \quad (2)$$

The circuit equations are

$$u1 = N1 d/dt ( \text{Ø}M + \text{Ø}1 + \text{Ø}B ) + R1I1 \quad (3)$$

$$0 = N2\, d/dt ( \text{Ø}M + \text{Ø}1 + \text{Ø}B ) + R2I2 \quad (4)$$

$$0 = N3\, d/dt ( \text{Ø}M + \text{Ø}3 ) + R3I3 \quad (5)$$

By m.m.f. law, Ampeere's Law $\rho\Phi$ = NI and substitute N / ρ for inductance

$$u1 = N1 (LM\, dIm/dt + L1\, dI1/dt + LB\, d/dt ( I1 +I2) ) + R1I1 \quad (6)$$

$$0 = N2 (LM\, dIm/dt + L2\, dI2/dt + LB\, d/dt ( I1 +I2) ) + R2I2 \quad (7)$$

$$0 = N3(LM\, dIm/dt + L3dI3/dt ) + R3I3 \quad (8)$$

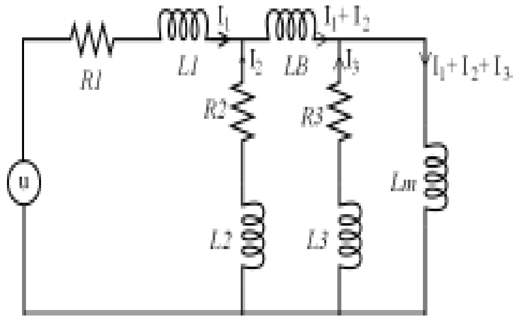


**Fig. 3. Electrical Subsystem Equivalent Circuit**

Where Im = I1 + I2 + I3., Modus represents only electrical subsystem. L2 and L3 are much smaller than Lm and LB. They can be removed with little effect on the system. The resultant equivalent circuit of the electrical subsystem shown in the Figure 3 . The transfer function derived

$$I_{R1} / u_{in} = L_BLms^2 + (L_BR_3 + LmR_5)\, s + R_2R_3 / L_BLm\, L_1s^3 + c_1s^2 + c_2s + R_1R_2R_3 \quad (9)$$

where $R_4 = ( R_1 + R_2 )$, $R_5 = (R_2 + R_3)$

$$c_1 = ( L_m ( L_B R_4 + L_1 R_5 ) + L_B L_1 R_3 )$$

$$c_2 = (R_2 ( L_m R_1 + L_1 R_3 ) + R_3 R_4 ( L_B + L_m ))$$

This is a second order system which consists of a mass moving of elements and each damping in the system with input power derived from the electrical subsystem. Mechanical subsystems can be written Newton's law

$$\ddot{x} = 1/m\, F – d/m\, \dot{x} - r/m\, x \quad (10)$$

The full model can be created using two subsystems

$$F = B\, N\, l\, I \quad (11)$$

This force moves both coil and eddy current circuit

$$F = B\, N\, l\, I_1 + B\, N\, l\, I_2 = k ( I_1 + I_2 ) \quad (12)$$

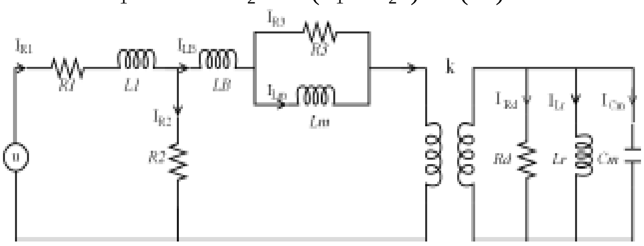


**Fig.4 Final Equivalent Circuit**

The counter e.m.f. generate due to movement of coil and bobbin

$$E = B\, N\, l\, \dot{x} = k\, \dot{x} \quad (13)$$

Capacitance $C_m$ represent the moving mass

Resistors Rd represent damping within the mechanical systemInductor Lr represent stiffness within the system

$$u1 = N1 (LM\, dIm/dt + L1\, dI1/dt + LB\, d/dt ( I1 +I2) ) + R1I1 + k\, \dot{x} \quad (14)$$

$$0 = N2 (LM\, dIm/dt + LB\, d/dt ( I1 +I2) ) + R2I2 + k\, \dot{x} \quad (15)$$

From the equivalent circuit, the following state- space expression can be formed:

$$\begin{pmatrix} i_{R1} \\ i_{LB} \\ i_{L3} \\ \ddot{x} \\ \dot{x} \end{pmatrix} = \begin{pmatrix} R_4/L_1 - R_2/L_1 & 0 & 0 & 0 & \\ R_2/L_B & -R_5/L_B & R_3/L_B & -k/L_B & 0 \\ 0 & R_3/L_m & -R_3/L_m & 0 & 0 \\ 0 & k/C_m & 0 & -k/C_m R_d & -k/C_m L_r \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} * \begin{pmatrix} I_{R1} \\ I_{LB} \\ I_{L3} \\ \dot{x} \\ x \end{pmatrix} + \begin{pmatrix} 1/L_1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} * u_{in} \quad (16)$$

**Table- II System Parameters**

| Symbol | Meaning |
|---|---|
| $R_1$ | Overall Equivalent Resistance |
| $L_1$ | Inductance |
| $R_2$ | Eddy Current Resistance |
| $R_3$ | Core loss Resistance |
| $L_B$ | Eddy Current Coil Resistance |
| $L_m$ | Mutual Inductance |
| $R_d$ | Resistor Equivalent of Resultaent factor |
| $L_r$ | Inductance Equivalent of Resultaent factor |
| Cm | Capacitance Equivalent of Resultaent factor |
| k | Constant |

## V. RULE BASED ATTACK DETECTION FOR PROPOSED RULE BASED

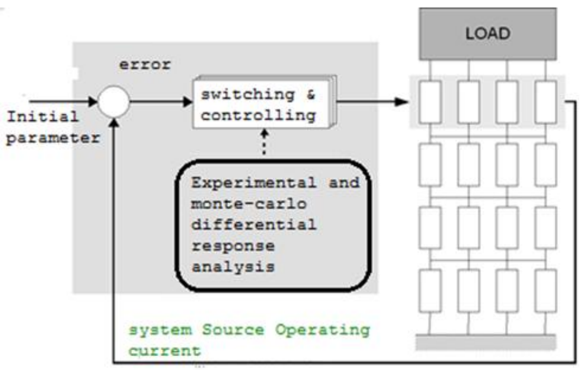


**Fig.5. Rule based attack for smart grid**

Initial parameter is compared with statistical analysis, Monte Carlo differentiation analysis and actual real time response is compared with initial parameter. The resultant error is fed to the switching and controlling system. This will control applied load appliances through the sensor. The entire distributed load monitor by quality parameter and reported beyond the limit. Depending on the quality parameter, acceptable band rule has laid down to categories attack.

### A. Attack Detection

**Symptoms:** If the item is set then the relative error is zero. Another occasion where the elements can be set, even when the elements are in the reference spectrum or has reached the travel limit.

**Diagnosis:** The first algorithm must check the response of the model.. Otherwise, check if there is an error position to determine whether it is in the experimental reference If there is an error then the relative error of the elements must be examined to determine if elements within the limits of the MSE and the input is greater than the limit MAE [31]

**Rules**: To inspect an attack, the following rules can be used

$MAE_{err} \rightarrow MSE_{min}$ r̂ $\mathbf{MAE_{err}}$

$MAE_{err}$=threshold (threshold= 5.5 for predictive SG model)

$MAE_{err1}$ :10 > threshold > $MAE_{err}$ then predicts as the **data attacks**

$MAE_{err2}$ :threshold < $MAE_{err}$ then predicts as **consumer-end attacks**

$MAE_{err1}$ : threshold > 10 then predicts as the **direct attacks** (cyber-physical)

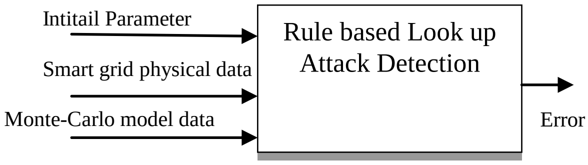


**Fig 6. Attack Detection**

## VI. RULE BASED AGENT ARCHITECTURE AND FLOW CHART

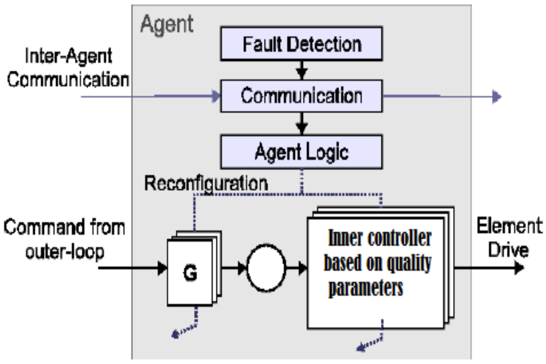


**Fig. 7a. Rule based agent architecture**

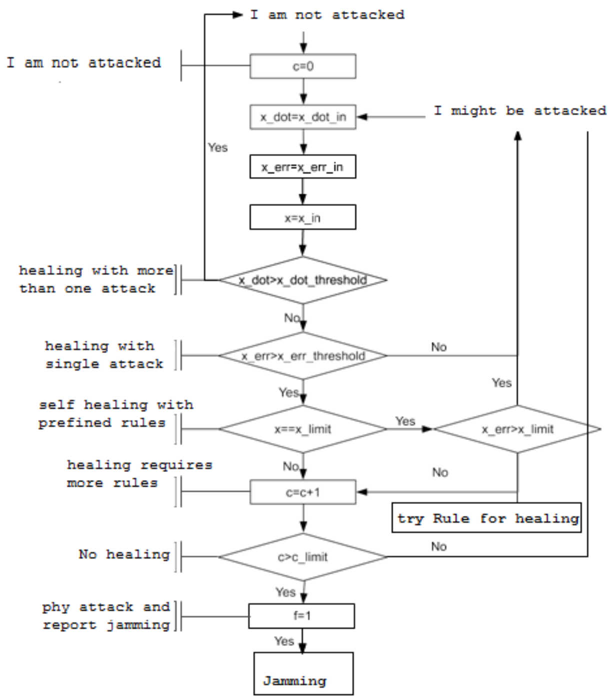


**Fig. 7b. Flow chart for Rule based Agent architecture**

Figure 7a, 7b represent the architecture of the agent. There feedforward gain command distributes between the active agent and the inner loop controller based on a model of a system error. Local agents using sensory information to detect the errors in the elements by using simple logic based rules. After detecting the error, communicated to other agents neighbor to neighbor. If the error message is received, the agent health status of updated knowledge and reconfigures control. Gain feed inputs adapted to distribute among the remaining active agent. Inner loop compensator is recharged using a loop-up table of pre-calculated parameter controller based on the number of active elements in the system temporarily to 0.07 s and the overshoot is 0.42%. A PI controller for the outer loop is then designed to match the behavior of a robust control scheme through tuning spectrum.When an error is detected, the remaining agent feed Gain from 1/4 to 1/3 and RAE basic values diverge. In a phase advance controller loop time constant, t decreased to 20 ms of the original value. This reconfiguration maintain nominal system performance. If an error is detected two feedforward gain was changed to 10 ms as the two active elements of fixed and t decreased to 50%. This reconfiguration is provided responses were very close to the nominal case [21].

## VII. ATTACK SIMULATIONS

The rules derived in the earlier section are simulated here. Sine wave input of spread spectrum provides a source of excitation. Based on the healing plants and measured values, jamming noise is added to the rule. In the detection element and simulated attack a sampling rate of 50 Hz frequency and clock are used.

**Table-III Quality parameters for Attack Detection and Isolation(ADI) using Rule based healing for smart grid**

| Sr. No. | Data Set | MSE | MAE | RAE | RRE | PSNR |
|---|---|---|---|---|---|---|
| 1 | Set1 (real) | 0.112734 | 0.101734 | 9.248587 | 0.112197 | 45.6 |
| 2 | Set2 (real) | 0.086854 | 0.075854 | 6.89581 | 0.086155 | 46.74 |
| 3 | Set3 (real) | 0.084059 | 0.073059 | 6.641772 | 0.083337 | 46.88 |
| 4 | Set4 (Markov Data) | 0.07151 | 0.06051 | 5.500942 | 0.070659 | 47.58 |

## VIII. RESULT AND DISCUSSIONS

Rule-based methods detected the location and nature of the attack quickly and accurately using the local algorithm is based on simple rules.Lower Mean Squared Error (**MSE**) suggests that correct tuned estimator for attacks and faults using proposed method for smart grid.The Mean Absolute Error (**MAE**) is used to forecast deviation in attacks and faults analysis using proposed method for smart grid.Accepted base value Relative Absolute Error (**RAE**) is quality parameter to measure the performance of a smart grid for attacks predictive model, and proposed rule based attack are decided on accepted base value i.e. 5.5.

If predicted value is less than accepted value then the error is negative and if predicted value is larger than the accepted value, the error is positive.

Lower Relative Squared Error (RRE) indicates that proposed rule based attack method reduces the error to the same dimensions as the quantity being predicted of smart grid

## IX. CONCLUSION

This proposed novel rule based self-heal attack detection and diagnosis is used to forecast deviation in attacks and faults analysis for smart grid. The level of complexity increases when the level of fault tolerance provided differs. Results obtained by using the MSE objective function. Self- healing recovery is possible within 10msec of time limit if multiple attacks are detected by local system agent then feed gain of agent scheduler is adjusted to 1/4 to 1/3. RAE value deviates accordingly. Time constant increases to 20 msec to recover the initial response were very nearer to that of the nominal case where the complexity of the diagnosis meant.

In the future, reduce the error rate for a function with low value; we intend to investigate the most objective function to promote recovery with minimal accuracy.

## REFERENCES

1. smartgrid.ieee.grid.2013 ‘ IEEE and Smart Grid
2. Fang, Xi, et al. "Smart grid—The new and improved power grid: A survey." IEEE communications surveys & tutorials 14.4 (2011): 944-980.
3. De Lemos, Rogério. "ICSE 2003 WADS panel: Fault tolerance and self-healing." Proceedings of the ICSE. Vol. 2003. 2003.
4. Salehie, Mazeiar, and Ladan Tahvildari. "Self-adaptive software: Landscape and research challenges." ACM transactions on autonomous and adaptive systems (TAAS) 4.2 (2009): 1-42.
5. Salehie, Mazeiar, and Ladan Tahvildari. "Autonomic computing: emerging trends and open problems." ACM SIGSOFT Software Engineering Notes 30.4 (2005): 1-7.
6. Ghosh, Debanjan, et al. "Self-healing systems—survey and synthesis." Decision support systems 42.4 (2007): 2164-2185.
7. Gupta, Pragya Kirti. "Self-healing Behaviour in Smart Grids."
8. Koopman, Philip. "Elements of the self-healing system problem space." Proc. workshop on architecting dependable systems. 2003.
9. Jiang, Michael, et al. "A modeling framework for self-healing software systems." Workshop “Models@ run. time” at the 10th International Conference on model Driven Engineering Languages and Systems. 2007.
10. Garlan, David, and Bradley Schmerl. "Model-based adaptation for self-healing systems." Proceedings of the first workshop on Self-healing systems. 2002.
11. Mo, Yilin, Rohan Chabukswar, and Bruno Sinopoli. "Detecting integrity attacks on SCADA systems." IEEE Transactions on Control Systems Technology 22.4 (2013): 1396-1407.
12. Vamvoudakis, Kyriakos G., et al. "Detection in adversarial environments." IEEE Transactions on Automatic Control 59.12 (2014): 3209-3223.
13. Ahmed, Saeed, et al. "Unsupervised Machine Learning-Based Detection of Covert Data Integrity Assault in Smart Grid Networks Utilizing Isolation Forest." IEEE Transactions on Information Forensics and Security 14.10 (2019): 2765-2777.
14. Lin, Hui, et al. "Runtime semantic security analysis to detect and mitigate control-related attacks in power grids." IEEE Transactions on Smart Grid 9.1 (2016): 163-178.
15. Sridhar, Siddharth, and Manimaran Govindarasu. "Model-based attack detection and mitigation for automatic generation control." IEEE Transactions on Smart Grid 5.2 (2014): 580-591.
16. Hong, Junho, Chen-Ching Liu, and Manimaran Govindarasu. "Integrated anomaly detection for cyber security of the substations." IEEE Transactions on Smart Grid 5.4 (2014): 1643-1653.
17. Yang, Yu, et al. "Intrusion detection system for network security in synchrophasor systems." (2013): 246-252.

18. Fan, Yawen, et al. "A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids." IEEE Transactions on Smart Grid 6.6 (2014): 2659-2668.
19. Mitchell, Robert, and Ray Chen. "Behavior-rule based intrusion detection systems for safety critical smart grid applications." IEEE Transactions on Smart Grid 4.3 (2013): 1254-1263.
20. Zhang, Yichi, et al. "Distributed intrusion detection system in a multi-layer network architecture of smart grids." IEEE Transactions on Smart Grid 2.4 (2011): 796-808.
21. Fadlullah, Zubair Md, et al. "An early warning system against malicious activities for smart grid communications." IEEE Network 25.5 (2011): 50-55.
22. Huang, Yi, et al. "Real-time detection of false data injection in smart grid networks: An adaptive CUSUM method and analysis." IEEE Systems Journal 10.2 (2014): 532-543.
23. Sial, Ankur, et al. "Heuristics-Based Detection of Abnormal Energy Consumption." International Conference on Smart Grid Inspired Future Technologies. Springer, Cham, 2018.
24. Sial, Ankur, Amarjeet Singh, and Aniket Mahanti. "Detecting anomalous energy consumption using contextual analysis of smart meter data." Wireless Networks (2019): 1-18.
25. Saini, Shubham, et al. "E-adivino: A novel framework for electricity consumption prediction based on historical trends." Proceedings of the 2015 ACM Sixth International Conference on Future Energy Systems. 2015.
26. Ozay, Mete, et al. "Machine learning methods for attack detection in the smart grid." IEEE transactions on neural networks and learning systems 27.8 (2015): 1773-1786.
27. Esmalifalak, Mohammad, et al. "Detecting stealthy false data injection using machine learning in smart grid." IEEE Systems Journal 11.3 (2014): 1644-1652.
28. Ahmed, Saeed, et al. "Covert cyber assault detection in smart grid networks utilizing feature selection and euclidean distance-based machine learning." Applied Sciences 8.5 (2018): 772.
29. Ahmed, Saeed, et al. "Feature selection–based detection of covert cyber deception assaults in smart grid communications networks using machine learning." IEEE Access 6 (2018): 27518-27529.
30. Singh, Sandeep Kumar, et al. "Joint-transformation-based detection of false data injection attacks in smart grid." IEEE Transactions on Industrial Informatics 14.1 (2017): 89-97.
31. He, Youbiao, Gihan J. Mendis, and Jin Wei. "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism." IEEE Transactions on Smart Grid 8.5 (2017): 2505-2516.
32. Chen, Guo, et al. "Exploring reliable strategies for defending power systems against targeted attacks." IEEE Transactions on Power Systems 26.3 (2010): 1000-1009.


## AUTHORS PROFILE

**Arvind P. Kadam,** received his Bachelor degree and M. E. degree in Electronics Engineering, from Walchand College of Engineering, sangli, Maharashtra affiliated to Shivaji University, Kolhapur, Maharashtra in 1994 and 2001 respectively .He pursuing his PhD degree from Visvesvaraya Technological University, Belgavi-Karnataka through research center SDMCET, Dharwad-Karnataka. Currently he is working as Head of Department- Electronics & Tele. Engineering at Institute of Civil & Rural Engineering, Gargoti, Dist: Kolhapur-Maharashtra. He is having 25 years of teaching experience and he has published 8 numbers of papers in various international and national conferences and journals. His current research areas include communication security in smart grid, digital communication, attack detection, spectrum sensing intelligence. He is a life member of ISTE.

**Shekhappa G. Ankaliki**, received his B.E. degree in Electrical and Electronics Engineering, M.Tech degree in Power System Engineering from Visvesvaraya Technological University, Belagavi, Karnataka, India. He received his Ph.D. degree in 2012 from Visvesvaraya Technological University, Belagavi, Karnataka, India. He was with faculty of Electrical and Electronics engineering department at Hirasugar Institute of Technology, Nidasoshi, Karnataka. Currently, he working as professor and head in department of Electrical and Electronics Engineering in SDM College of Engineering, Dharwad, Karnataka. He is having 26 years of teaching experience and he was published more than 30 numbers of papers in various international and national conferences and journals. He is a member of IEEE and also he is a member in Institution of Engineers (India). His current research areas include intelligent techniques for power system operations, power system security, distribution system service restoration, distribution system automation and distributed generation resources for power system.