INTERNATIONAL JOURNAL OF ELECTRONICS, MECHANICAL AND MECHATRONICS ENGINEERING
Vol.9 Num.2 - 2019 (1657-1667)

Cyber Security Algorithm Development For Microgrid And Smart Grid Systems

Ahmet DURMUŞ [1] , Mehmet Emin TACER [2]

Abstract: Smart grids are advanced grids that use intelligent ways to distribute power and manage it with high level of technical and physical safety in its different components. In these types of grids, the power station and the consumer are both considered as effective power supplier. They can generate, buy, and sell power as of kWh to the other. Thus, financial channels are concerned, so that the safety and privacy for each of them are important. This paper will be concerned on developing a cybersecurity algorithm used to apply a flexible way for determining to either isolate the network, reauthorize access, or successfully accept the access for financial transactions made by normal users.

Keywords: *Renewable Energy, Smart Grids, Cyber Security.*

Introduction

Smart grid is a type of grid that applies improvement of normal grids in a way of combination between computer-based systems of information technologies and traditional electrical grid. This type of grids uses two-way communication to enhance the network behavior in generation, consumption, reliability, stability and cost effect between the generation station and the consumer demand with momently updated information. Generally smart grid is contained of other small smart partitions - called microgrids - each of them should be in connection with the other simultaneously. Smart grid has some advantages in energy savings through consumption reduction, fraud detection and technical losses, reduced balancing cost, peak reduction, and reduction of carbon emissions (Hamilton & Miller , 2010). Although it consists of some Intelligent Appliances, Smart Power Meters and AMI's, Smart Substations, Super Conducting Cables, Integrated communications, and Phasor Measurement Units (PMU) [2] [3] [4].

Despite of the advantages that smart grids have, and the role of user control which appear between of smart components, a technical awareness and countermeasures should be taken to satisfy the stable control of the network. In other words; the user role is made over smart appliances turning them ON or OFF, or by

[1] *Dept. of Electrical and Electronics Engineering, Istanbul Aydin University, Istanbul, Turkey, ah.durmus.93@gmail.com*
[2] *Dept. of Electrical and Electronics Engineering, Istanbul Aydin University, Istanbul, Turkey, emintacer@aydin.edu.tr*

generating power, so an import and export processes of KWh's are made in a channel between user and the grid. This means financial transactions are made. So that, to protect the stability of processes in the grid, and by knowing that the normal user also could be an attacker at the same time, cyber security issues are shown up for concern. In this paper, an algorithm [which is a procedure that could be used for data processing, automated reasoning and calculations; using step by step process] is developed for cybersecurity protection in smart grid systems. It is going to be discussed after taking a review of cyber security in normal grids and other works related with.

Cyber Protection of Normal Power Grid

Cyber protection requires a widely used component protection which is the SCADA systems. This because main central network keeps collecting data from other widely distributed substations using controlled systems. Thus, SCADA systems are considered as the nerve of that operation. The collected data are used by the energy management system EMS in normal grids, and this usage could be considered as a weak point when a communication down fault or delay occurs, due to the trim in control process which means a possible power outage. (Ten, Manimaran, & Liu, JULY 2010)

A SCADA Security Protection Framework called RAIM Framework introduced and it is contained from 4 steps mainly: real time monitoring, anomaly detection, impact analysis, and mitigation strategy. A simplified methodology for impact analysis of a computer network systems, called Attack Tree Modeling used for identifying the adversary objectives. It is a graph that shows the connection of more than one attack of each node in the system as shown in figure 1.

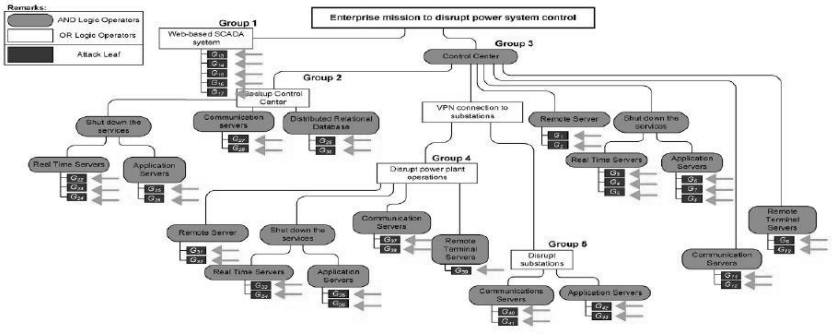


Figure 1: Normal network connection

A likelihood measure is presented to show the vulnerability level starting from 0 to 1, which means an index of vulnerability between most invulnerable to the most vulnerable one and called Vulnerability index which is determined based on evidence of intrusion attempts, existing counter measurement, and password policy enforcement. Hypothesis in this modeling presents:

- Condition 1: The system is clean and free of any intrusion attempt that is concluded from the electronic evidence in the system.
- Condition 2: 1 or more of countermeasures are implemented to protect against attack leaf.
- Condition 3: 1 or more password policies are enforced corresponding to each attack leaf.

Condition 1 is met when there is no evidence of system intrusion suggestion. Condition 2 is met such as a web server is installed which contains a firewall to prevent attacks. Condition 3 once password is implemented; taking in consideration that poor passwords result unauthorized access. (Ten, Manimaran, & Liu, JULY 2010)

After the cyber security principles in normal power grid introduced, and because of all advantages that smart grid has over the normal one (Hamilton & Miller , 2010) ; a need for examining the cyber security in smart grid systems appears. Especially that the coming future will depend over smart grid systems completely, after transferring to it from the normal grid being completed.

Cyber Protection of Smart Grid Systems

Some papers that describe the cyber protection of smart grid systems like Stefanov et al [6]; explaining that the cyber-attack could be discovered by tracking either voltage leakage or step change in frequency and another one like Diovu et al [7] which is developing a firewall scheme against DDoS attacks which mainly affect the AMI, in addition to Liu et al [8] which introduce a scheme for intrusion detection mechanism against false data injection attack over AMI; especially by exploiting the CPN [Colored Petri Nets which is a graphical oriented language for design, specification, simulation and verification of systems] of smart meters. Each of them has its own way for decrement the effect of cyber-attack over AMI units, but the common point between them is that assuming the attacker may not be one of the normal users. This point is the main difference between previous works and what is described in this paper here. This paper is proposing that control should be applied as nearest as possible to the user himself. So that more accurate security could be implemented for all other users of the smart network.

Types of cyber-attacks which could be done over the system could be divided for 3 groups, the first one concerned in DDoS attacks, second one “Man in the middle” technique, the final one is metering data falsification. DDoS attack depends on flowing and pumping extremely high traffic to the server which contains sensitive data in order to take the control over the server under cover of this traffic. The second one (man in the middle) is a technique used to track sent and received data; it may not affect them but can easily have a copy of them and edit these data such as measurements of consumed and generated power which are sent between the smart meter and the AMI unit. This type can change those values or even change transactions done in between. Finally, for metering data falsification which may be considered as cyber and physical attack at same time; for physical one it is simply changing the reading and writing values over meters. For cyber one it appears as changing in recorded values when being transmitted (such as man in the middle technique described previously). This could easily be detected and fixed by re-read of original data sent from other small fixed sensors which are spread over all parts of smart grid network and appliances. [7]

Proposed Smart Grid Cybersecurity

Proposed algorithm is highly flexible, and code could easily be injected into the framework of the microgrid systems with zero cost and can detect the vulnerability degree over the system; then to either isolate, reauthorize or to successfully access for the system as will be shown later here. Now, for proposed hypothesis in AMI modeling contains five conditions which could be presented as :

Table 1: Proposed hypothesis in AMI modeling

Proposed conditions	Occurs when
Condition 1	The system is clean and free of any intrusion attempt that is concluded from the electronic evidence in the system.
Condition 2	1 or more of countermeasures are implemented to protect against attack leaf in any of **one-way of communication way**.
Condition 3	1 or more of countermeasures are implemented to protect against attack leaf in **two way of communication at the same time**.
Condition 4	1 or more password policies are enforced corresponding to each attack leaf in any of **one-way of communication way**.
Condition 5	1 or more password policies are enforced corresponding to each attack leaf in **two way of communication at the same time.**

While the power is converted between HP to LP in order to accomplish the loads needs, small power stations are needed for feeding process [2]. In same principle the need for smaller partitions in smart grid systems appear, and those are called microgrids. These microgrids normally designed to derive the required power to loads. So that; it has a limit of power transmitted and received. While designing is processed for these microgrids; steady state conditions are also considered, and it differs according to load types. These steady state conditions considered as the norm one of the system, which represent the clear condition of the system; which is also named as condition 1 as shown in Table 1.

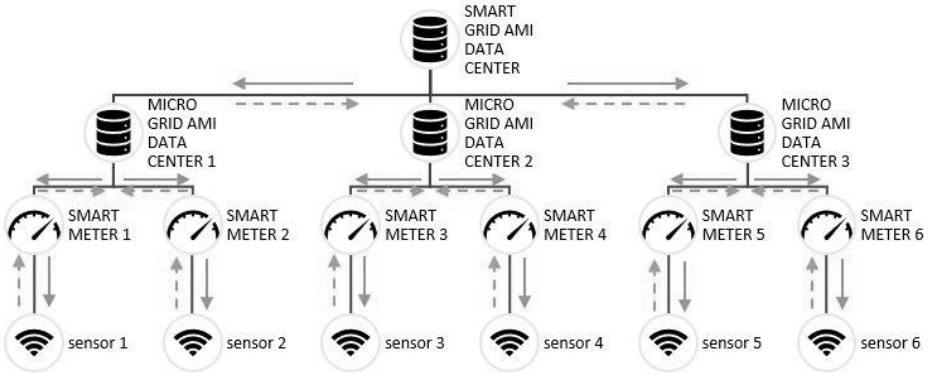


Figure 2: Proposed connection between AMI unites and Smart meters

Figure 2 shows concerned parts in this study of smart grid systems. Each part uses normally two way of communication with other components. Sensors are fastened over appliance itself and gives information

about its consumed or generated power to the smart meter as analog signals which convert it in its turn to digital one and send it to the AMI data center to store it in the memory. As known for digital systems, there is a firewall for each of them in which it can protect its digital data. As example in smart homes, digital devices are connected to sensors of microwave or freezer or oven, …. etc; those digital devices are used to monitor the system status and are maybe normally working with android system; which is also has its own firewall for protecting the digital data. Also; for AMI data centers, it consists of servers to store the data, so that firewall is also exists.

Now, while considering the firewall of the system, between data center and appliance; if data are sent from server to the consumer side; data is transmitted from server (which may has a firewall) to the appliance (which may also has a firewall); this represent a one way communication with one countermeasure applied as a firewall; then it gives us condition 2. If data are transmitted from server to the consumer side, and another data are also delivered to server from the consumer side at the same time; this give us 2 way communication at the same time; thus condition 3 is satisfied.

In same procedure and principle if password policy is applied for one way communication between server and consumer side then condition 4 is satisfied. If it is applied on both way of communication, then condition 5 is also satisfied. Knowing that instead of password policies, human related prints could be used to access the system instead of passwords, such as fingerprints, or eye scan or both of them at the same time.

The system could be attacked once it is prepared for work but not yet connected to any loads, in other words; it is in the stage of testing it before being completely connected to work in full load to the system; in this stage bugs could be inserted from a hacker in the server to steal consumer billing information or changing the read data in future. In this case condition 1 is satisfied only, because there is no countermeasure or passwords are applied to the system yet; due to it is in the stage before full connection to the load. After that if it is connected, another conditions of 2,3,4, and 5 could be considered; because the system is fully connected now, so that different conditions could be counted in after.

χ will indicate the vulnerability level over all the system or in other word the system condition whether it is vulnerable or not. It will be considered for the smallest leaf in the system between sensor and smart meter, or smart meter and microgrid data center, or microgrid data center and smart grid data center, etc… After that to calculate the system vulnerability completely; all of these χ's will be multiplied together as it will be shown later.

- If [condition 1 ∩ condition 2 ∩ condition 3 ∩ condition 4 ∩ condition 5] are satisfied will give us $\chi = 0.2$
  Here all conditions are satisfied, therefore there is no evidence that the system is subject to malicious attempts. i.e: password and countermeasures are implemented for one way and two way of communications and the system is clean from any previous intrusions.

- If any 2 of 5 conditions are satisfied, then $\chi = 2*1/5 = 0.4$

1: for condition 1, 2: for condition 2, 3: for condition 3, 4: for condition 4, 5: for condition 5. And by eliminating repeated conditions:

~~1,1~~	1,2	1,3	1,4	1,5
~~2,1~~	~~2,2~~	2,3	2,4	2,5
~~3,1~~	~~3,2~~	~~3,3~~	3,4	3,5
~~4,1~~	~~4,2~~	~~4,3~~	~~4,4~~	4,5
~~5,1~~	~~5,2~~	~~5,3~~	~~5,4~~	~~5,5~~

Thus □= 10 / 25 = 0.4
This gives indicate that the system is vulnerable by 40%.

In same principle:

- If any 3 of 5 conditions are satisfied, then: □= 0.6
- If any 4 of 5 conditions are satisfied, then □= 0.8.
- If condition 1 or condition 2 or condition 3 or condition 4 or condition 5 or none of them is met, then □ = 1. This indicates that the system is highly vulnerable.

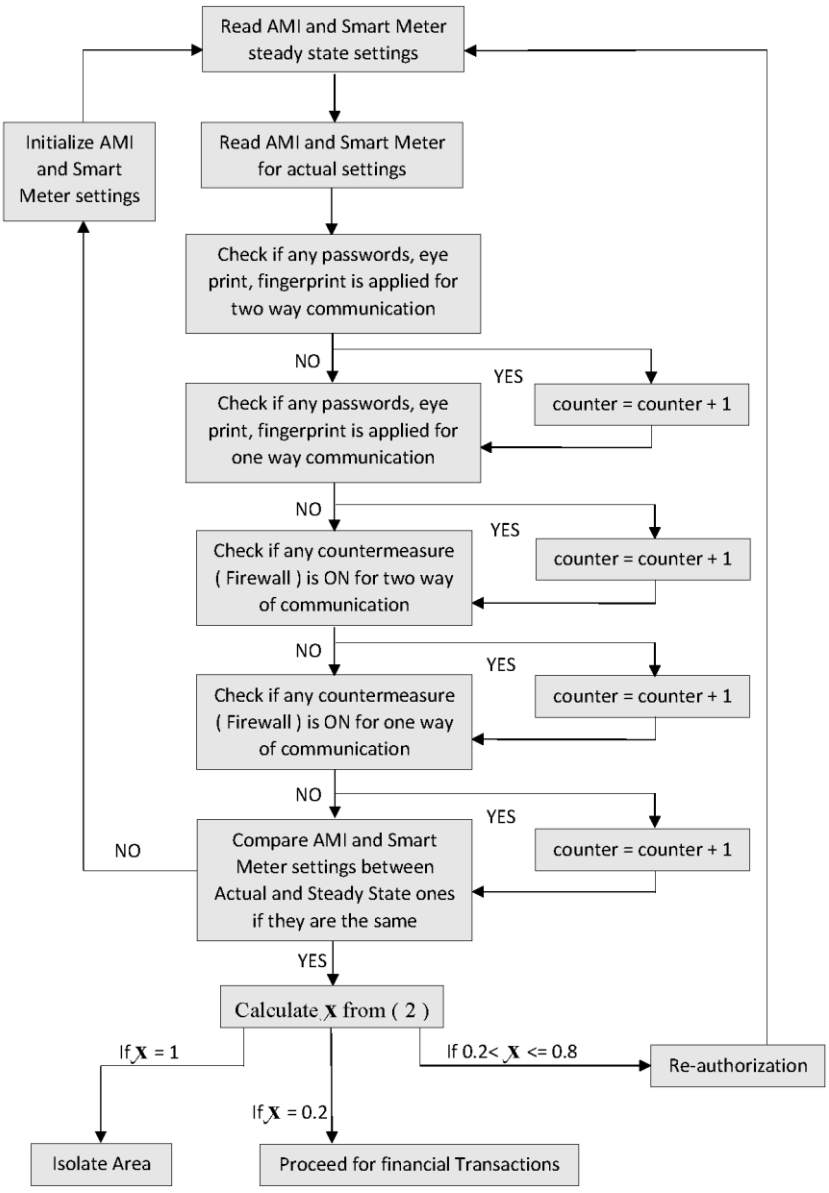
To know the overall system attack indices, and after calculating □ for every leaf (□$_i$), the overall will be:

$$\text{counter} = \text{counter} + 1 \text{ , counter: \# of countermeasures or password applied} \quad (1)$$

$$\chi_i = \begin{cases} \text{counter} * 0.2 \text{ , } 2 <= \text{counter} <= 4 \\ 1 \text{ , counter} <= 1 \\ 0.2 \text{ , counter} = 5 \end{cases} \quad (2)$$

$$\chi_{system} = \prod \chi_i \text{ , } i = 1,2,3,4, \ldots. \quad (3)$$

Proposed Smart Grid Cybersecurity Algorithm



Simulation of Proposed Smart Grid Cybersecurity Consumer Algorithm

The simulation process is tested for small leaves or microgrids only. So that; equation (1) and (2) are basically considered. Equation (3) could be easily inserted later to calculate the overall system vulnerability indices.

To prove that proposed algorithm here can be applied in programmable way, which should be implemented in AMI unites programming, 3 stage codes had been simulated. Knowing that the program is basically used

to know the internal process inside AMI unites and smart meters for how it could be applied and to display this in easier way; a display function had been used to show the internal status of code running.

First of all, the code started by clearing any previous value and initialize the simulation program for starting. After that, AMI control unites are directed to read the steady state conditions of its internal settings from internal physical memory and also for smart meters. Then actual readings of those settings are also gathered in order to compare the match between steady state and real readings.

Then the program will send a signal code to the framework of server or system to test if any countermeasure or password policy is applied weather for 1 or 2 way of communication. If any of them is detected, a counter will start increasing; which aims to give us the total number of satisfied conditions in our microgrid system. Then depending on this value, the vulnerability indices is calculated in order to either isolate the system, require a reauthentication again, or to successfully access the financial data.

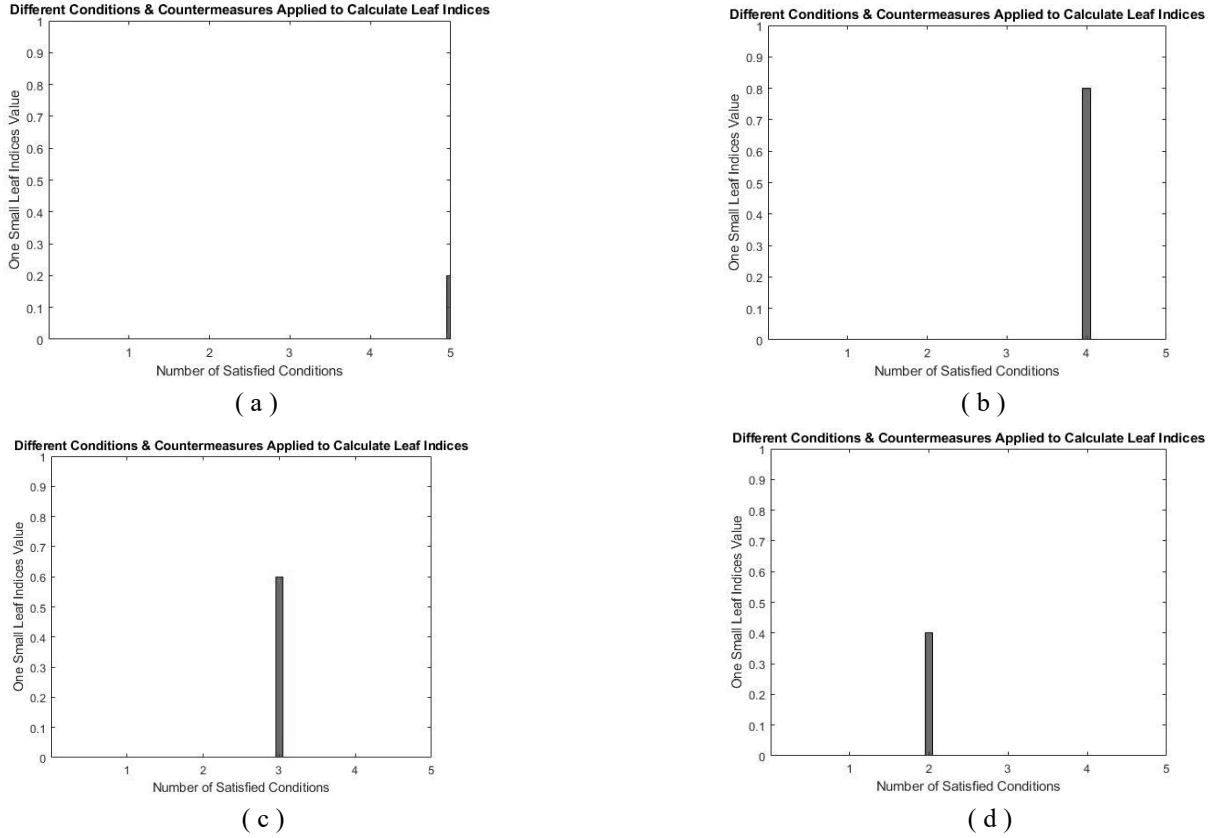


Figure 3: (a), (b), (c), (d) results for 5,4,3,2 conditions satisfied respectively

If number of conditions satisfied are either 2, 3, or 4; then a reauthorization for accessing the system will be required as shown below. This message could be transferred to the consumer screen to make attention and control over process.

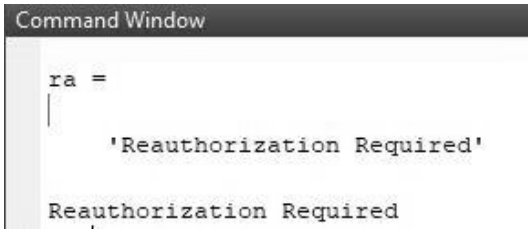


Figure 4: Appearing Message if 2,3 or 4 Conditions Satisfied

For 1 condition satisfied and detected by the program the result will be as in figure 5.

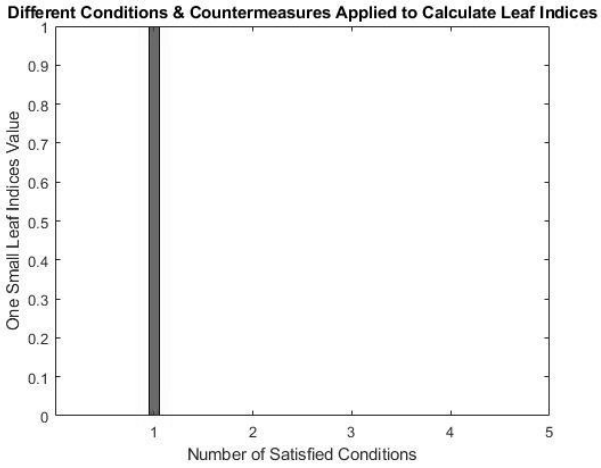


Figure 5: 1 Condition Satisfied

If number of conditions satisfied is 1; then an isolation of the area is required because the system is highly vulnerable and figure 6 shows the related message.

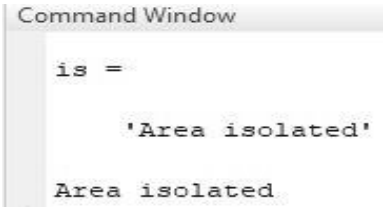


Figure 6: Appearing Message if 1 Condition Satisfied

Another code is applied for testing the microgrid if smart meter and AMI settings are changed or not. If not, the code will work correctly, if yes a message will appear in order to reload the steady state conditions for both and it is automatically loaded internally as shown in figure 7.

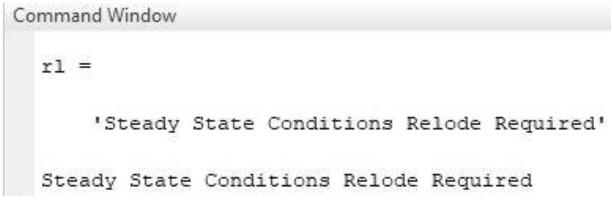


Figure 7: Appearing Message if bugs are inserted or settings between SS and actual readings are not in match

Results show that proposed algorithm and code are highly flexible and could easily be injected into the framework of the micro systems with zero cost and can detect the vulnerability degree over the system; then to either isolate, reauthorize or to successfully access for the system.

Conclusion

As the results show that, implementing defenses methods starting from the consumer side will ensure a higher level of security. On the other hand, two way of communication in smart meters provide the advantage of high response to isolate the risky area, if there is no chance to maintain it remotely. This isolation could be continued until maintenance team arrive to the concerned area. Then they can start by initializing setting of hardware such as AMI unites and smart meters and then load the latest safe information into it. That information is backed up instantly and could be separated than specific attack starting time.

Table 2: Comparison between previous work [7] and proposed algorithm.

Comparison Topic	Previous work	Proposed Work
Type of Grid	Smart Grid	Smart Grid
Assumed level of attacker to access information	Skilled attacker	Innocent attacker, or skilled one
Concerned attack types	DDoS	Not specific for only one, it is general
Cost effect	May need upgrading server in which data are stored. (for framework upgrade)	No need for any changes, only inserting the algorithm or the code in a programmable way for any framework generation will take direct effect.

Future Work

This paper could be used in developing other security ways, such as the use of firewalls, control the access for the network, and limitation of accessible data, to prevent cyber-attack over smart grid systems. Also it could be used to develop the proposed algorithm in paper here in order to enhance the security of the smart systems or to propose another algorithm which could be used on the both sides of communication channel between AMI's unites or between several microgrid data centers.

References

[1] B. A. Hamilton And J. Miller , "Smart Grid Implementation Strategy," In Understanding The Benefits Of The Smart Grid , National Energy Technology Laboratory, 2010, Pp. 1-33.

[2] P. C. Jain, "Trends In Smart Power Grid Communication And Networking," In International Conference On Signal Processing And Communication (ICSC), Noida, India, 2015, Pp 374-379.

[3] P. Umang And M. Mitul, "A Review On Smart Meter System," International Journal Of Innovative Research In Electrical, Electronics, Instrumentation And Control Engineering, Vol. 3, No. 12, Pp. 70-73, December 2015.

[4] Q. Sun, H. Li, Z. Ma, C. Wang, J. Campillo, Q. Zhang, F. Wallin And J. Guo, "A Comprehensive Review Of Smart Energy Meters In Intelligent Energy Networks," IEEE Internet Of Things Journal, Vol. 3, No. 4, Pp. 464-479, August 2016.

[5] C. W. Ten, G. Manimaran And C. C. Liu, "Cybersecurity For Critical Infrastructures: Attack And Defense Modeling," IEEE Transactions On Systems, Man, And Cybernetics—Part A: Systems And Humans, Vol. 40, No. No. 4, Pp. 853-865, July 2010.

[6] A. Stefanov And C. C. Liu, "Cyber-Power System Security In Smart Grid Environment," Science Foundation Ireland (SFI), Dublin, 2011.

[7] R. Diovu And J. Agee, "A Cloud-Based Openflow Firewall For Mitigation Against Ddos Attacks In Smart Gridami Networks.," In 2017 IEEE Pes Powerafrica, Accra, Ghana, 27-30 June 2017.

[8] X. Liu, P. Zhu, Y. Zhang And K. Chen, "A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack In Advanced Metering Infrastructure," IEEE Transactions On Smart Grid, Vol. 6, No. 5, Pp. 2435-2443, September 2015.