Providing a Security to Smart Grid Communication System against False Data Injection Attacks

Ashwini[1] Chaitra Desai[2]

[1,2]Reva Institute of Technology and Management

Abstract— The process of changing the conventional energy networks to smart grid and it can help in making major changes in the energy industry in terms of reliability, performance and manageability. As increasing the connectivity in smart grid and its bidirectional communication leads to a security problem. In this letter we found a new technique to secure smart grid, the chi-square detector and cosine similarity matching approaches are used for finding an attack in the smart grid. And kalman filter estimation is used major any variation from the actual measurements.

Key words: Attack detection, cyber-security, machine learning, power systems security

I. Introduction

Smart grid is an electricity network and it is based on the digital technology it transfer the electricity to consumers by using a two way digital communication.

If the connectivity of the smart grid is increases and also they have bidirectional energy transmitting and receiving. This feature of the smart grid is leads to so many insecurity of communication in the smart grid. This will become a main target for the cyber terrorism.

From the Earnest Orlando Lawrence Berkeley National Laboratory [1], is reported that the transmitting of the power cost over $80 billion every year in the U.S. And in the 2014 Washington D.C based Bipartisan policy center is given that more than 150 cyber attack found in the energy sector 2013 and 79 attacks in the 2014.

So for this transformation of conventional energy to smart grid needs an security. To achieving this we need provide security between the communication endpoints so that they can easily transmitting and receiving energy in both directions within a communication network in the smart grid.

II. Literature reviews

So many people's are investigated many techniques to secure an smart grid, this literature shows what are technique are used to proving a security to the smart grid.

For this more connectivity in the smart grid and their two way communication this feature of the smart grid become an main goal for the cyber attacks to damage the electric power grids also components like, transmission line, generators, transformers. So for controlling this attack in this we identify the new bilevel mathematical models and algorithm to identify the cyber attack, but it is sufficient to secure smart grid [2][9].

A light weight message authentication scheme [3], in which each message should be authenticate between the sender and receiver and the receiver is also checks that any forge is made to the message during transmission. For this they have designed to two protocols, first protocol is for the authentication between the sender and receiver is maintained. And second protocol is for the message should be authenticate between them. For current solution for this is traditional public key based, Diffie-Hellman key establishment protocol and hash based authentication is used for secure distributed meters, but method of security is not suitable for large communication network and it also not suited to smart meters.

Another one attack is the malicious attack against power system, these attacks can damage the power system and they can easily change the meter reading without being detected.

There are two types of attacks, first attack is where the attacker can attack sufficient number of meters and this attack is not detected by the control center. The attacker can systematically construct an attack vector, it will not change the state estimation but the result will get change, the control center could go undetected. This problem is examined by using graph theoretic approach.

Another type of attack is weak attack the attacker can attack a small number of meters; this problem is solved by using a decision theoretic perspective. These attacks are undetected by control center. The control center proposed that the generalized likelihood ratio detector is proposed that collect all historical data based on that it will tell about the attacker, but it is suited for only parametric references, it is not suitable for the non parametric references [4].

The power grid is a large communication network connecting a electric power generator to consumers via power transmission and distribution across a large geographical area [6].

It tells about new type of attack called false data injection attack against electric power grid of the state estimation. The attacker can destroy the structure of a power system by introducing the attack vector into state variable. Here we have two situation types of attacks; one in which attacker is forced to some meters, to do change their reading of meter at physically protected locations any small or substations, such attacker can add errors in to state variables will not be detected by the estimator.Another type of attacker is having only less number resources, so that attacker take some agreement from meters, in both situation the attacker can easily build attack vector and will not change result of the state estimation , but also change their values of results.

Here the kalman filter [7] estimation is used to achieve state estimation and also it finds the deviation between the systems. An attacker makes that the state estimator to believe an attacker, then attacker will take the sensor reading and manipulates the readings. So then attacker can inject false sensor measurements without being detected by the state estimator.

In this they have proposed, ellipsoidal algorithm to compute an inside and outside approximation.

To provide a security we are used some supervised learning algorithm but these are failed to detect the newer attack and false data injection attack.

Here we are used game theory concept, according to this is tell about electricity prices [8].

So attacker can increase or decrease the price of electricity. The attacking at every measurement is impossible for the attacker and securing all measurement at every time is also impossible, this is called zero sum game between an attacker and security agent. These results are examined by using PJM-5 bus system.

III. Proposed Work

In this letter to overcome all the drawback of the existing system, we proposed that chi-square detector and cosine similarity matching approach.

These two techniques are used to detect attack where exactly false data injected. Whereas kalman filter estimation is used to calculate difference between the expected value with the actual measurements.

And it compares with the predefined threshold ,if the value is less than the threshold then it shows no attack in the system, but if the value is more than the threshold it triggers an alarm, it indicate that there is an attack in the system and sends message to the manager.

To detect an attack we are using an chi-square detector and cosine similarity matching approach.

A. Chi-Square Detector

This detector will capable detecting an attack like DOS attack, random attack but it fails to detect false data injection attack. This approach is fast for detecting an attack and implementation is easy.

B. Cosine Similarity Matching Approach

To overcome from the chi-square detector this technique is developed, it has capability to detect all attacks including false data injection attack.

1) System Architecture

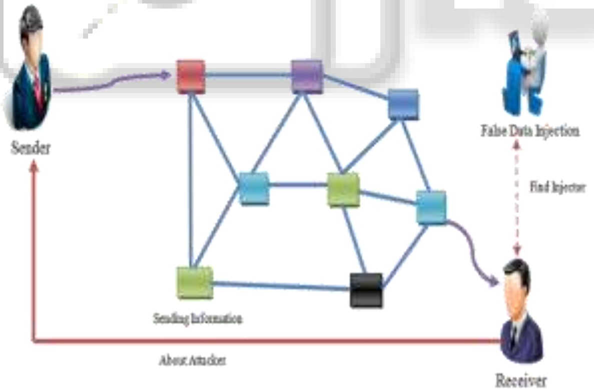

Fig. 1: System Architecture

In this technique it compares the value of the expected value with the actual measured value; these values should be equal to one. Then it says there is no attack in the communication system.

Some tests are taken here to detect attack against given threshold:

a) No Attack

Kalman filter estimated value and measured value should be equal and it is less than the given threshold.

The chi-square and cosine similarity matching approach are shows value below the given threshold then we say there is no attack in the system.

b) Random Attack

In this the attacker can simply manipulate their sensor reading, in between of the communication they can add attack vector. It compares value of kalman filter estimation and sensor measurement it does not shown similar value, it shows that there is attack. Here chi-square detector and cosine similarity values shows above the threshold.

c) False Data Injection Attack

Here the attacker is familiar to the system and it parameter, it easily construct attack vector and inject in to state variable without being change state estimation.

The expected value and actual measured value is equal to one, and it shows that above the threshold then it takes a preventative action avoid risk. But here the chi-square detector shows value below the given threshold so that it fails to detect an attack in the system.

IV. Conclusion

This paper is mainly for giving security for the smart grid, the kalman filter is used to get an expected value and sensor are used to get actual value, and it compares with an given threshold.

In this we are concluding that cosine similarity matching approach is strongest technique to detect a false data injection attack, where as chi-square detector is incapable of detecting false data injection attack.

References

[1] K.H. La Commare and J.H.Eto, Understanding the cost of power interruptions to U.S electricity consumers, Sep, 2004.

[2] J. Salmeron, K.Wood, and R.Baldik, “Analysis of electric grid security under terrorist threat,” IEEE Trans. Power Systems , vol.19,no 2,pp.905-912,2004.

[3] M.M.Fouda, Z.M. Fadlullah, N.Kato, R. Lu, and X. Shen,”lightweight message authentication scheme for smart grid communications,” IEEE trans.smart Grid, vol. 2, no.4 pp.675-685, 2011.

[4] O.Kosut, L. Jia, R. J. Thomas, and L.Tong, “Malicious data attacks on the smart grid”, IEEE Trans. Smart grid, vol2, no.4, pp. 645-658, 2011.

[5] M. Ozay, I. Esnaola, F. T. Yarman Vural, S.R. kulkarni, and H. V. Poor, “smarter security in the smart grid”, in 2012 IEEE third in.Conf.Smart Grid communications (SmartGridComm’ 12), 2012, pp.312-317.

[6] Y.Liu, P. Ning, and M.K.Reiter,”False data injection attacks against stateestimation in electric power grids,’ ACM Trans.Inf.Syst.Secur. vol. 14, no.1,p.13, 2011.

[7] Y.Mo, E.Garone, A.Casavola, and B.sinopoli,”false data injection attacks against state estimation in wireless sensor network.” In 2010 49th IEEE Conf.Decision and control, 2010,pp. 5967-5972.

[8] M.Esmalifalak,G.Shi, Z.Han, and L.Song,”Bad data injection attack and defense in electricity market using game theory study,” IEEE trans,Smart Grid, Vol. 4, no.1, pp. 160-169,2012.

[9] D.B.Rawat and C.Bajracharya, “cyber security for smart grid systems: status, challenges and perspectives,” in Proc .IEEE south-eascon2015, fort Lauderdale, FL, USA,Apr. 9-12,2015,”,”, vol. , pp.-,.