Detection of False Data Injection Attacks Using K-Means Clustering Algorithm

Mrs. Vaishali Sanap[1] , Adsule Vaishnavi[2], Chakre Preeti[3], Gaikwad Vishwajeet[4], Kalekar Rohan[5]

[1]Lecturer, Dept of Computer Engineering, A.I.S.S.M.S. Polytechnic Pune, Maharashtra, India
[2]Student, Dept of Computer Engineering, A.I.S.S.M.S. Polytechnic Pune, Maharashtra, India

---

Abstract :- *In this system, we've got to implement within attack in sub-network mistreatment camera. Whenever the external person redirects into server that point server can find so apprize to admin regarding within attack .False information injection attacks from associate degree individual's purpose of read associate degreed displayed what it takes for an adversary to launch a made attack. False information injection attacks on state estimation ar those within which associate degree assaulter manipulates the sensing element measures to induce associate degree discretionary modification within the calculable price of state variables while not being known by the dangerous measurement detection formula of the state calculator.*

KeyWords*:-Camera,CyberAttack, Security, False Data Injection Attack ,WirelessSensor Networks*

1. INTRODUCTION

In this system, false information injection attacks from AN someone's purpose of read ANd displayed what it takes for an adversary to launch a prosperous attack.

False information injection attacks on state estimation area unit those during which AN aggressor manipulates the detector measurings to induce AN absolute variation within the certain worth of state variables while not being known by the unhealthy measurement detection formula of the state calculator.

The malicious information injection at the applying layer may mean reduced application productivity with higher development prices. In random false information injection, the someone goals to search out any attack path that injects absolute errors into the estimates of state variables . In targeted false information

injection,the someone goals to search out AN attack path that injects definite errors within the estimates of definite state variables chosen by him.

The aim to develop a wireless application that offers several novel challenges, such as, reliable information transmission, node quality support and quick event detection, Whenever the skin person pause camera certain quantity time.

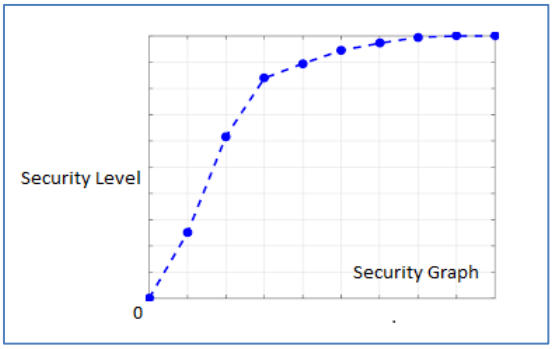

Fig - 1 : Security Graph

2. LITERATURE SURVEY

1.There have been many reports of cyber intrusions, hacking, unauthorized operations and malicious attacks on the electric power system. Many of these reports are uncorroborated and support the uncertainty of the very people in position to prevent these invasions. One vulnerability that has drawn significant discussion is the Aurora vulnerability, which focuses on electric power generators. Since the dramatic video and interview on the television news in 2007 showing how to cause severe damage to a generator, many generation providers are concerned they could become a victim.

2.Cyber-attacks have become increasingly common in recent years. Capable of shutting down nuclear filters, air

defense systems, and electrical grids, cyber-attacks pose a serious danger to national security[2]. As a result, some have recommended that cyber-attacks should be treated as acts of war.

3.A power grid is a composite system connecting electric power generators to clients through power transmission and sharing networks across a large geographical area. System checking is necessary to ensure the reliable operation of power grids, and state estimation is used in system monitoring to best estimate the power grid state through analysis of meter measurements and power system copies. Various techniques have been recognized to detect and recognize bad measurements, including the interacting bad measurements introduced by arbitrary, non random causes. At first glimpse, it seems that these means can also defeat malicious measurements injected by attackers, since such malicious measurements can be considered as cooperating corrupt measurements.

4. Analytical methods for executing vulnerability analysis of state estimation when it is subject to a concealed false data injection cyber-attack on a power grid's SCADA system. Specifically, we consider ac state estimation and define how the physical possessions of the scheme can be used as an gain in guarding the power system from such an attack. We present an algorithm based on graph theory which allows determining how many and which measurement signals an attacker will attack in order to reduce his efforts in keeping the attack hidden from bad data detection. This provides control on which measurements are vulnerable and need improved protection. Hence, this paper provides perceptions into the weaknesses, but also the characteristic strengths provided by ac state estimation and network topology features such as automobiles deprived of power injections.

5. This paper completely matures the concept of load redistribution (LR) attacks, a superior type of false data injection attacks, and examines their damage to power system operation in dissimilar time steps with dissimilar attacking source limitations. Based on destructive effect analysis, we differentiate two attacking goals from the adversary's view point, i.e., direct attacking goal and delayed attacking goal. For the direct attacking goal, this paper recognizes the most destructive LR attack through a max- min attacker-defender model. Then, the principle of determining effective protection approaches is explained. The effectiveness of the proposed model is tested on a 14- automobile system. To the author's finest knowledge, this is the major work of its kind, which quantitatively examines the harm of the false data injection attacks to power system procedure and security. Our analysis, hence provides an in- depth perception on effective attack prevention with limited protection source budget.

3. EXISTINGSYSTEM

In Existing system, no such system available that detect inside attack in network.

Disadvantages of Existing System

1. Lesssecure.
2. Cannot protect insideattacker.
3. More energyconsumption
4. Less networklifetime
5. High computationalcost.

4. PROPOSED SYSTEM

In this system, we have to implement inside attack in sub- network using camera. Whenever the outside person pause camera specific amount time. That time server will detect. And inform to admin about inside attack.

Advantages of Proposed System

- Highly secured
- Easy tohandle

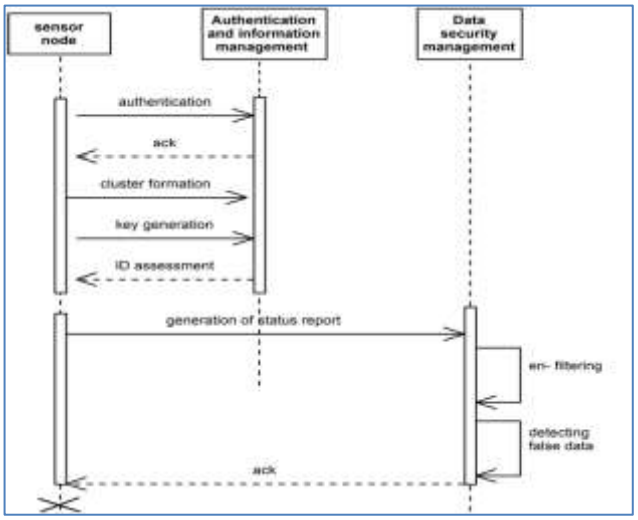

Fig:3.a:System Architecture

5. ARCHITECTURAL DESIGN

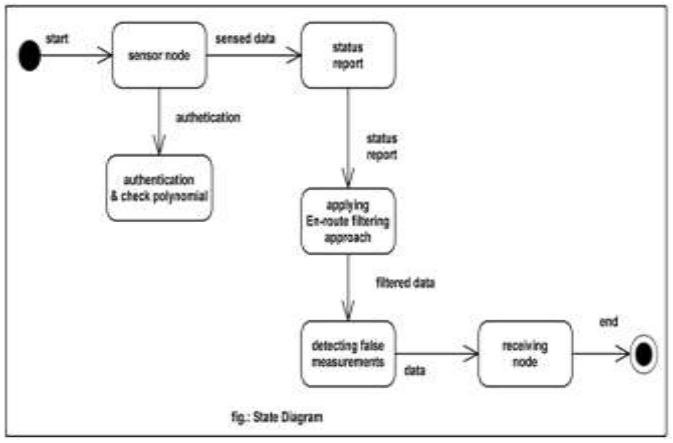

Fig – 3.b:System Architecture

6. ALGORITHM

K-MEANS CLUSTERING:

k-means is one in all the best unattended learning algorithms that solve the well-known cluster drawback. The procedure follows a straightforward and straightforward thanks to classify a given information set through a definite range of clusters (assume k clusters) fastened apriority. the most plan is to then k

centers, one for every cluster. These centers ought to be placed during a crafty means attributable to totally {different|completely different} location causes different result. So, the higher alternative is to put them the maximum amount as doable far-off from one another. consecutive step is to require every purpose happiness to a given information set and associate it to the closest center. once no purpose is unfinished, the primary step is completed associate degreed an early cluster age is completed. At this time we'd like to re-calculate k- new centroids as centre of mass of the clusters ensuing from the previous step. when we've these k new centroids, a brand new binding should be done between constant information set points and therefore the nearest new center. A loop has been generated. As a results of this loop we have a tendency to could notice that the k centers modification their location step by step till no a lot of changes square measure done or in different words centers don't move from now on. Finally, this formula aims at minimizing associate degree objective operate recognize as square error operate given by:

$$J(V) = \sum_{i=1}^{c} \sum_{j=1}^{c_i} \left(\left\| x_i - v_j \right\| \right)^2$$

where,

$\|x_i - v_j\|$ is the Euclidean distance between x_i and v_j

c_i is the number of data points in i^{th} cluster.

'c' is the number of cluster centers.

Algorithmic steps for k-means clustering

Let X = {x1,x2,x3,.....,xn} be the set of data points and V = {v1,v2,.....,vc}be the set of centers.

1) Randomly select cluster centers.

2) Calculate the distance between each data point and cluster centers.

3) Assign the data point to the cluster center whose distance from the cluster centeris minimum of all the cluster centers

4) Recalculate the new cluster center using:

$$v_i = (1/c_i) \sum_{j=1}^{c_i} x_i$$

Where, xn represents the number of data points in fifth cluster.

5) Recalculate the distance between each data point and new obtained cluster centers.

6) If no data point was reassigned then stop, otherwise repeat from step 3).

7. CONCLUSION

In this system, we've projected within attack in sub-network employing a camera. Whenever the surface person pauses camera certain amount time. that point server can observe. And inform to admin regarding within attack. False knowledge injection attacks on state estimation ar those within which AN assaulter manipulates the detector measures to induce AN impulsive modification within the calculable price of state variables while not being detected by the corrupt measurement detection formula of the state calculator.

8. REFERENCES

1. Y. Liu, M. K. Reiter, and P. Ning, “False data injection attacks against state estimation in electric power grids,” in CCS ’09: Proceedings of the 16th ACM conference on Computer and communications security. NewYork,NY,USA: ACM, 2009, pp. 21–32.

2. H. Merrill and F. Schweppe, “Bad data suppression in power system static state estimation, ”Power Apparatus and Systems, IEEE Transactions on, vol.PAS-90, no.6, pp.2718– 2725, Nov.1971.

3. E. Handschin, F. Schweppe, J. Kohlas, and A. Fiechter, “Baddata analysis for power system state estimation,” Power Apparatus and Systems, IEEE Transactions on, vol.94, no. 2, pp.329–337, Mar1975.

4. D. Falcao, P. Cooke, and A. Brameller, “Power system tracking state estimation and bad data processing, ”Power Apparatus and Systems, IEEE Transactions on, vol.PAS-101, no. 2, pp. 325–333, Feb.1982.