False Data Injection Attack Exploration on Control System

K. R. Gholap[1], M. S. Gunjal[2], K. U. Hole[3], S. D. Gunjal[4]

[1,2,3]B.E. Student, Department of Computer Engineering, Savitribai Phule University, Pune, India

[4]Professor, Department of Computer Engineering, Savitribai Phule University, Pune, India

***Abstract*: The control systems like alarm, remote, camera's which using as security purpose in the fields like industry, medical, education, banking etc. control system are being exposed to cyber-attacks due to highly increase in information Technology and communication network one of the issue is FDI attack. FDI attack stands for False data injection attacks on state estimation are those in which a Hacker handles the sensor measurements to generate a change in the estimated value of state value and variables without get detected by the bad measurement detection algorithm of the state estimator. Although many research works have been previously reported on addressing same problem such as effect of nonlinearity, optimal attacking region that requires reduced network information, unobservable state-and-topology cyber-physical attacks, bi-level optimization problem, AC state estimation with incomplete network Information etc. most of them made very strong assumption that some measurement absolutely protected but costing is high and some existing monitoring are weak so we have to implement inside attack in sub-network using camera. Whenever the outside person pause camera in specific amount of time. That time server will detect, and inform to admin or server about inside attack. False data injection attacks from an opponent's point of view and showed what it takes for an adversary to launch a successful attack, using AES algorithm.**

***Keywords*: - Cyber-physical system, Cyber-security, false data injection attacks, state estimation, AES algorithm, bi-level optimization, multiple linear regressions.**

1. Introduction

In this system, false data injection attacks from an opponent's purpose of read and showed what it takes for an enemy to launch a malicious attack. False knowledge injection attacks on state estimation are those during which a Hacker manipulates the device activity to produce an unusual modification within the measurable value of state variables while not get detected by the unhealthy measurement detection rule of the state calculator. The malicious data injection at the application layer would possibly mean decreased application potential with higher development prices. In random false data injection, the opponent aims to search out any attack vector that injects unusual errors into the estimates of state variables and values. In targeted false data injection, the adversary aims to detect an attack vector that inserts specific errors into the estimates of specific state variables chosen by hacker.

2. System architecture

A. False data injection attack detection system architecture

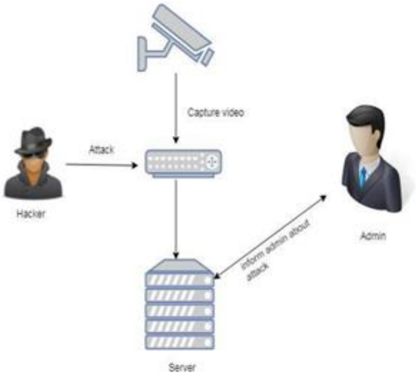

Fig. 1. False data Injection attack detection System architecture

There are 5 components in this system namely hacker, admin, camera, system and server. System camera capturing video form data. Whenever the surface person pause camera certain quantity time. That point server can notice. And inform to admin regarding within attack.as shown in figure the hacker attacking on system to insert false data and due to time lapse server will detect that attack and then inform to the admin.

3. Related work

Will the Aurora Vulnerability pose a Risk to My Generator Authors: Mark Zeller. Description: There are several reports of cyber intrusions, hacking, unauthorized operations, and malicious attacks on the electrical power grid. several of those reports a unsupported and strengthen the skepticism of the terribly individuals in position to stop these invasions. One vulnerability that has drawn substantial discussion is that the Aurora vulnerability, that focuses on electrical power generators. Since the dramatic video and interview on the news in 2007 showing a way to cause severe harm to a generator, several generation suppliers are involved they may become a victim. This paper discusses the Aurora vulnerability, however it's enforced, and what the chance factors. World Health Organization is vulnerable, and what steps can mitigate this risk [1].

The Law of Cyber-Attack Authors: Oona A. Hathaway, Rebekah Crootof, Duke of EdinburghLevitz, Haley Nix Description: Cyber-attacks became more and more common in recent years. Capable of motility down nuclear centrifuges, defence systems, and electrical grids, cyber-attacks cause a significant threat to national security. As a result, some have prompt that cyber- attacks ought to be treated as acts of war. however, the attacks look very little just like the armed attacks that the law of war has historically regulated. this text examines however existing law is also applied—and tailored and amended—to meet the distinctive challenge display by cyber-attacks [2].

False knowledge Injection Attacks against State Estimation in electrical power Grids Authors: Yao Liu, PengNing, Michael K. Reiter Description: A power grid could be an advanced system connecting electrical power generators to customers through power transmission and distribution networks across an oversized region. System watching is important to make sure the reliable operation of power grids, and state estimation is employed in system watching to best estimate the facility grid state through analysis of meter measurements and power grid models. varied techniques are developed to observe and determine unhealthy measurements, together with the interacting unhealthy measurements introduced by discretional, nonrandom causes. initially look, it looks that these techniques can even defeat malicious measurements injected by attackers, since such malicious measurements may be thought of as interacting unhealthy measurements.[3]

Vulnerability Assessment of AC State Estimation With relevance false knowledge Injection Cyber-Attacks. Authors: Gabriela Hug, Joseph Apostle Giampapa Description: This paper introduces new analytical techniques for playacting vulnerability analysis of state estimation once it's subject to a hidden false knowledge injection cyber-attack on an influence grid's SCADA system. Specifically, we have a tendency to contemplate ac state estimation Associate in Nursingd describe however the physical properties of the system may be used as a plus in protective the facility system from such an attack. we have a tendency to gift Associate in Nursing rule supported graph theory that permits decisive what percentage Associate in Nursingd that measuring signals an assaulter can attack so as to attenuate his efforts to keep the attack hidden from unhealthy knowledge detection. This provides steering on those measurements vulnerable and wish enlarged protection. Hence, this paper provides insights into the vulnerabilities however conjointly the inherent strengths provided by ac state estimation and constellation options like buses while not power injections [4].

Modeling Load distribution Attacks in Power Systems Authors: Yanling Yuan, Zuyi Li, KuiRen Description: State estimation could be a key component in today's power systems for reliable system operation and management. State estimation collects data from an oversized range of meter measurements and analyzes it during a centralized manner at the center. Existing state estimation approaches were historically assumed to be ready to tolerate and observe random unhealthy measurements. They were, however, recently shown to be liable to intentional false knowledge injection attacks. This paper totally develops the conception of load distribution (LR) attacks, a special kind of false knowledge injection attacks, and analyzes their harm to power grid operation completely different in several in numerous} time steps with different assaultive resource limitations. supported damaging result analysis, we have a tendency to differentiate 2 assaultive goals from the adversary's perspective, i.e., immediate assaultive goal and delayed assaultive goal. For the immediate assaultive goal, this paper identifies the foremost damaging LR attack through a maxmin attacker-defender model. Then, the criterion of decisive effective protection methods is explained. The effectiveness of the planned model is tested on a 14-bus system. To the author's best data, this is often the primary work of its kind that quantitatively analyzes the harm of the false knowledge injection attacks to power grid operation and security. Our Associate in Nursingalysis therefore provides an in-depth insight on effective attack interference with restricted protection resource budget.[5]

4. Implementation

System performs the video capturing while external person or we can say as Hacker or attacker attacking on the system whenever the camera get pause or does anything other it will detect time server and send information to admin. The data is in Encrypted form using AES algorithm. the attack is detected by bloom filter algorithm

System Description: Let W be the whole system which consists: W=[IP, PRO, OP] Where, 1. IP is the input of the system. I = [P, O, H, A] Where,

_ P is the false data injection attack
_ O is the original data in the system
_ H is the Hacker
_ A is the Admin

1. PRO is the procedure of our proposed system: False Data Injection Attack On Control System

   _ P = We have implemented inside attack in sub-network using camera.

   _ O=Original Data here we define as in matrix form [x y z]

   _ Attacked data can be defined as, P*[x y z]=[Px Py Pz] Px ,Py, Pz is data after an attack estimate wrong System.

   _ Probability of an Attack can be define as, [p1,p2,p3……pn] Where,
   _ p1 is Increpted data
   _ p2 is image form
   _ p3 is IP address
   _ p4 is deceptive file
   _ p5 is fake pages and so on

2. OP is the outputs of the system Where, the system provides some data available on the server database in detect the inside attacks. The Probability to Getting Output is defined as follows: [O] =Data set is null due to camera is off, [O1] =camera is on but time server extend,

   [O2]=camera is on and attack found in specific time Interval.

   AES algorithm: AES has 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

1. *Key Expansion*-round keys are derived from cipher key. AES requires a separate 128-bit round key block for each round plus one more.
2. *Initial round key addition:*

AddRoundKey-each byte of the state is combined with a block of the round key using bitwise xor.

3. 9, 11 or 13 rounds:

- *SubBytes*-a non- linear substitution step where each byte is replaced with another according to a lookup table.
- *ShiftRows*-a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
- Mix Columns-a linear mixing operation which operates on the columns of the state, combining the four bytes in each column.
- *AddRoundKey* Final round (making 10, 12 or 14 rounds in total):

1. SubBytes
2. ShiftRows
3. AddRoundKey

5. Application

- Banking System.
- Examination hall
- Industry.

6. Conclusion and Future Work

In this system, we have to planned among attack in sub-network using camera. Whenever the outside person pauses camera certain quantity time. that time server will notice. And inform to admin about among attack.

False injection attacks on state estimation measure unit those within which associate degree attacker manipulates the detector activity to induce associate absolute change among the derived price of state variables while not being detected by the bad measurement detection algorithmic rule of the state expert.

We have implemented false data injections to represent the camera from the external network and developed a multiple linear regression model for the attacker to learn the relationship between pseudo-boundary injections and the data injections inside the attack sub- network.

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. New York, 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, "Bad data analysis for power system state estimation," Power Apparatus and Systems, IEEE Transactions on, vol. 94, no. 2, pp. 329–337, Mar 1975.

[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.

[5] W. Kotiuga and M. Vidyasagar, "Bad data rejection properties of weughted least absolute value techniques applied to static state estimation," Power Apparatus and Systems, IEEE Transactions on, vol. PAS101, no. 4, pp. 844–853, April 1982.

[6] X. Nian-de, W. Shi-ying, and Y. Er-keng, "A new approach for detection and identification of multiple bad data in power system state estimation," Power Apparatus and Systems, IEEE Transactions on, vol. PAS-101, no. 2, pp. 454– 462, Feb. 1982.

[7] A. Monticelli and A. Garcia, "Reliable bad data processing for real-time state estimation," Power Apparatus and Systems, IEEE Transactions on, vol. PAS-102, no. 5, pp. 1126–1139, May 1983.

[8] T. Van Custom, M. Ribbens-Pavella, and L. Mili, "Hypothesis testing identification: A new method for bad data analysis in power system state estimation," Power Apparatus and Systems, IEEE Transactions on, vol. PAS-103, no. 11, pp. 3239–3252, Nov. 1984.

[9] X. N. de, W. Shi-ying, and Y. Ers-keng, "An application of estimation identification approach of multiple bad data in power system state estimation," Power Apparatus and Systems, IEEE Transactions on, vol. PAS-103, no. 2, pp. 225– 233, Feb. 1984.

[10] W. Peterson and A. Girgis, "Multiple bad data detection in power system state estimation using linear programming," in System Theory, 1988., Proceedings of the Twentieth Southeastern Symposium on, Mar 1988, pp. 405–409.