Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 12, December -2018

False Data Injection Attack on Control System

[1] Komal Gholap, [2] Komal Hole, [3] Gunjal Maya

[1]*BE, Student, skn lonawala, Pune, Maharashtra, India*
[2]*BE, Student, skn lonawala, Pune, Maharashtra, India*
[3]*BE, Student, skn lonawala, Pune, Maharashtra, India*

Abstract — *In this system, we have to implement within attack in sub-network exploitation camera. Whenever the surface person pause camera certain quantity time. that point server can notice. And inform to admin regarding within attack. False data injection attacks from an adversary's purpose of read and showed what it takes for an adversary to launch a no-hit attack. False knowledge injection attacks on state estimation ar those within which an offender manipulates the sensor measures to induce associate degree arbitrary modification within the calculable price of state variables while not being detected by the bad measurement detection rule of the state calculator.*

Keywords: *Cyber-physical system, Cyber-security, falsedata injection attacks, state estimation, multiple linear regression, bi-level optimization*

I. INTRODUCTION

In this system, false data injection attacks from an opposer's purpose of read and showed what it takes for an adversary to launch a palmy attack. False knowledge injection attacks on state estimation are those during which an attacker manipulates the device activitys to induce an whimsical modification within the calculable price of state variables while not being detected by the unhealthy measurement detection rule of the state calculator. The malicious data injection at the application layer would possibly mean reduced application potency with higher development prices. In random false data injection, the adversary aims to search out any attack vector that injects whimsical errors into the estimates of state variables. In targeted false data injection, the adversary aims to search out an attack vector that injects specific errors into the estimates of specific state variables chosen by him.

II. LITERATURE SURVEY

According to literature survey after studying different IEEE paper, collected some related papers and documents some of the point discussed here:

1.Myth or Reality – will the Aurora Vulnerability pose a Risk to My Generator
Authors: Mark Zeller.
Description:There are several reports of cyberintrusions, hacking, unauthorized operations, and malicious attacks on the electrical power grid. several of those reports ar 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 tv news in 2007 showing a way to cause severe harm to a generator, several generation suppliers ar involved they may become a victim. This paper discusses the Aurora vulnerability, however it's enforced, what the chance factors ar, World Health Organization is vulnerable, and what steps can mitigate this risk.

2.The Law of Cyber-Attack
Authers: Oona A. Hathaway, Rebekah Crootof, Duke of Edinburgh Levitz, 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.

3.False knowledge Injection Attacks against State Estimation in electrical power Grids
Authors: Yao Liu, PengNing, Michael K. Reiter
Description: A power grid could be a 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.

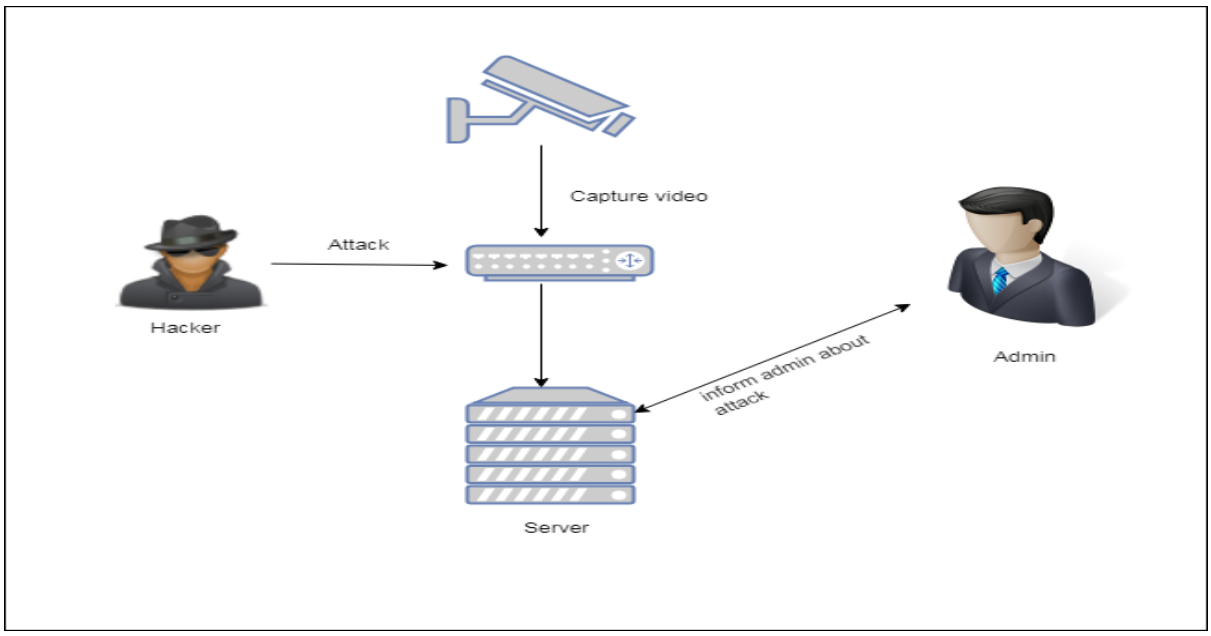
4. Vulnerability Assessment of AC State Estimation With relevance False knowledge Injection Cyber-Attacks.
Authors: Gabriela Hug, Joseph Apostle Giampapa
Description: This paper introduces new analytical techniques for playacting vulnerability analysis of state estimation once it's subject to a hidden 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 that measurements ar 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.

5. 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 max-min 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.

III. PROPOSED SYSTEM

In this system, we have to implement inside attack in sub-network mistreatment camera. Whenever the outside person pause camera certain amount time. that point server can detect. And inform to admin regarding inside attack.

IV. SYSTEM DESIGN



V. ADVANTAGES

Advantages of Proposed System

- Highly secured
- Easy to handle

VI. CONCLUSION

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

REFRENCES

[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 Cutsem, 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 estimationidentification 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.

