False Data Injection Attacks in Insider Attack

Afiya Shaikh[1], Ayush Sharma[2], Saniya Satarkar[3], Pranita Shitole[4]

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

---***---

Abstract - *In this system, we have to implement inside attack in sub-network using camera. Whenever the external person redirects into server that time server will detect and then notify to admin about inside attack. False data injection attacks from an adversary's point of view and displayed what it takes for an adversary to launch a successful attack. False data injection attacks on state estimation are those in which an attacker manipulates the sensor measurements to induce an arbitrary change in the estimated value of state variables without being identified by the bad measurement detection algorithm of the state estimator.*

Key Words: *Camera, Cyber Attack, Vulnerability, Time server , Security etc*

1. INTRODUCTION

In this system, false data injection attacks from an adversary's point of view and displayed what it takes for an adversary to launch a successful attack.

False data injection attacks on state estimation are those in which an attacker manipulates the sensor measurements to induce an arbitrary variation in the predictable value of state variables without being identified by the bad measurement detection algorithm of the state estimator.

The malicious data injection at the application layer might mean reduced application productivity with higher development costs. In random false data injection, the adversary goals to find any attack path that injects arbitrary errors into the estimates of state variables. In targeted false data injection, the adversary goals to find an attack path that injects definite errors into the estimates of definite state variables chosen by him

2. SCOPE OF PROJECT

The aim to develop a wireless application which offers many novel challenges, such as, reliable data transmission, node mobility support and fast event detection, Whenever the outside person pause camera specific amount time. That time server will detect. And inform to admin about inside attack.

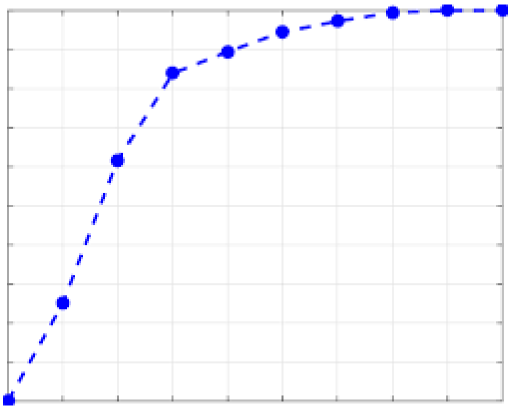

Fig - 1 : Security Graph

3. LITERATURE SURVEY

A) Myth or Reality – Does the Aurora Vulnerability Pose a Risk to My Generator?

Authors: Mark Zeller.

Description:

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. This paper discusses the Aurora vulnerability, how it is applied, what the risk factors are, who is vulnerable, and what steps will mitigate this risk.

B) The Law of Cyber-Attack

Authors: Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix

Description:

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. As a result, some have recommended that cyber-attacks should be treated as acts of war. Yet the attacks look slightly like the armed attacks that the law of war has traditionally regulated. This Article surveys how current law may be applied—and altered and amended—to meet the distinctive challenge posed by cyber-attacks.

C) False Data Injection Attacks against State Estimation in Electric Power Grids

Authors: Yao Liu, Peng Ning, Michael K. Reiter

Description:

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, nonrandom 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.

D) Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks.

Authors: Gabriela Hug, Joseph Andrew Giampapa

Description:

This paper presents new 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.

E) Modeling Load Redistribution Attacks in Power Systems

Authors: Yanling Yuan, Zuyi Li, Kui Ren

Description:

State estimation is an important element in today's power systems for consistent system procedure and control. State estimation assembles information from a large number of meter measurements and explores it in a centralized manner at the control center. Current state estimation approaches were usually assumed to be able to accept and detect arbitrary corrupt measurements. They were, however, recently shown to be vulnerable to planned false data injection attacks. 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 viewpoint, 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.

4. EXISTING SYSTEM

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

Disadvantages of Existing System

1. Less secure.
2. Cannot protect inside attacker.
3. More energy consumption
4. Less network lifetime
5. High computational cost.

5. 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 to handle

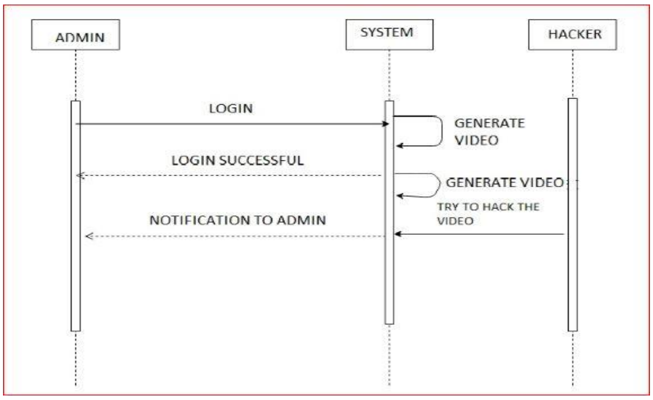

Fig – 2 : Suspicious Activity Detection

6. HARDWARE & SOFTWARE COMPONENT

A) Hardware:-

There should be required devices to interact with software.

• System	: Pentium IV 2.4 GHz.
• Hard Disk	: 40 GB.
• Ram	: 256 Mb.

B) Software:-

Operating system	:	Windows XP/7.
Web server	:	Apache Tomcat 7.
Front End	:	JSP, CSS etc.
Back End	:	MySQL

7. ARCHITECTURAL DESIGN

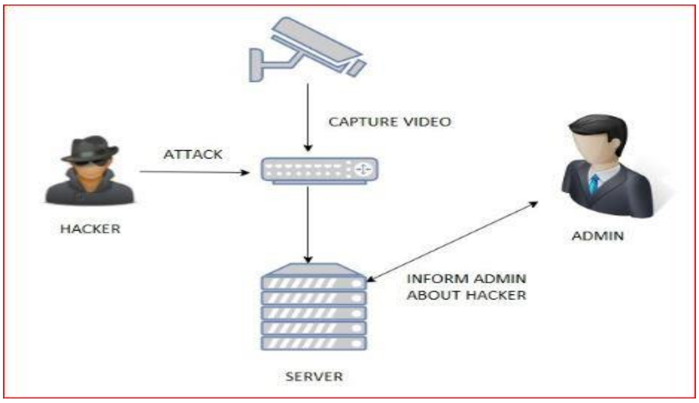

Fig – 3: System Architecture

8. ALGORITHM

A) BLOOM FILTERS

An void Bloom filter is a bit array of m bits, all fixed to 0. There must also be k dissimilar hash functions defined, each of which maps or hashes some set component to one of the m array positions with a uniform random distribution. Typically, k is a constant, much smaller than m, which is proportional to the number of components to be added; the precise choice of k and the constant of proportionality of m are determined by the proposed false positive rate of the filter.

B) AES ALGORITHM

AES algorithm is the very popular algorithm. It is the most used symmetric encryption algorithm. It is six times faster than 3DES (Triple DES algorithm). Since the key size in DES was too small there was a need for a better replacement algorithm. It has increased computing power and it is vulnerable against attacks. 3DES was developed initially to overcome this shortcoming but it was slow.

And so AES was developed. Some of the features of AES are:

1. Stronger and Quicker than 3 DES
2. Less prone to attacks
3. Symmetric key and block cipher
4. 128 bit data
5. 128,192,256 bit keys

AES is an iterative cipher based on substitution permutation network. It consists of linked operations involving substitutions and permutations. All its operations are done on bytes instead of bits, which imply that 128 bits of plain text is considered as 16 bytes. These bytes are treated as a matrix with bytes ordered in four rows and columns. The number of circles depends on the size of the key. Generally, it uses 10, 12 and 14 rounds for 128, 192 and 256-bit keys. Each round uses another 128 bit key that is calculated from original key. In our work, we have randomly generated keys for each book. Those keys are encrypted using AES and stored in DB when a user requests a resource. When the resource is approved by the admin it is decrypted and the user is allowed to store in his local system.

9. CONCLUSION

In this system, we have proposed 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. False data injection attacks on state estimation are those in which an attacker manipulates the sensor measurements to induce an arbitrary change in the estimated value of state variables without being sensed by the corrupt measurement detection algorithm of the state estimator.

10. FUTURE SCOPE

- To detect the inserted false into the system.
- To reveal such potential risks.
- To convey a starting formulation to analyze, prevent such class of cyber attack

11. 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.