ISSN 2395-1621

Jamming Attack Detection and Prevention in the Cyber System

[#1]Meenal Kulkarni, [#2]Diksha Patil, [#3]Jeba Shaikh, [#4]Rekha Gaganmale, [#5]Nitin V. More

[1]kulkarni.minal100@gmail.com
[2]dikshagpatil8087@gmail.com
[3]zebashaikh226@gmail.com
[4]rekhagaganmale@gmail.com

ABSTRACT

This paper proposes cyber-attack detection and interference of Cyber Physical System. The Chi sq. detector and mathematical logic primarily based attack classifier (FLAC) were accustomed determine distributed denial of service and false information injection attacks. The fuzzy attributes for choosing the mentioned attacks are activity identification, average packet rate, modification purpose detection algorithmic program, consume algorithmic program, unexpired session of users, injected incomplete data, apply of session key. Associate example state of affairs has been created victimization OpNET machine. Simulation results depict that the employment of Chi-square sight or and FLAC are able to detect the mentioned cyber physical attacks with high accuracy. Compared to existing mathematical logic primarily based attack detector, the planned model outperforms the normal distributed denial of service and false information detector.

ARTICLE INFO

Article History

Received: 24th February 2017

Received in revised form :

24th February 2017

Accepted: 27th February 2017

Published online :

3rd March 2017

Keywords: FLAC, cyber-attack detection and prevention, Networking, C.2 Computer-Communication Networks.

I. INTRODUCTION

In In this electronic equipment era of information and communication technologies, physical objects area unit currently connected with every other through cyber networks area unit jointly known as cyber physical system. Sensible grid is AN example of such a system where grid is automatic, controlled and has accessed via internet. The sensible grid infrastructure monitors the customer's real time demand to determine a dynamic and interactive connection with the customers. Sensible grid provides bidirectional communication between centre and consumer [5]. Sensible grid contains self-healing characteristics, it will simply accommodate renewable energy sources like solar panel, wind, hydro-electric, periodic event and biomass. Its main objectives area unit to provide power dependably cut back energy consumption and blackouts [1]. Irrespective of the domain, a CPS has three principal characteristics are (1) Environment Coupling: CPSs are very tightly coupled with their environment (physical process) – any change in the behaviour of the environment results in a change in the CPS' behaviour and vice-versa. Prominent examples include medical devices such as ICDs. (2)Diverse Capabilities:

CPSs are usually made up of diverse heterogeneous entities with order of magnitude difference in capabilities. Sensors deeply embedded in physical processes for monitoring purposes have limited capabilities, while those bottleneck in terms of computation, communication and memory in the workflow. (3) Networked: CPSs, unlike traditional stand-alone embedded systems, usually require a communication channel between its components, either embedded within the physical processes or external to it, in order to provide its (usually coordinated) services [4]. For example, in an automobile CPS, a sensor monitoring the car transmission communicates with the car radio in order to enable it to increase the volume automatically as the speed increases, thus compensating for the extra noise. This paper addresses smart grid cyber security concerns by analyzing the coupling between the power control applications and cyber systems. The following terms are introduced to provide a common language to address these concepts throughout the paper:

- Power application: the collection of operational control functions necessary to maintain stability within the physical power system;
- Supporting infrastructure: the cyber infrastructure including software, hardware, and communication networks.

This division of the grid's command and control functions Will be utilized to show how cyber security concerns can be Evaluated and mitigated through future research. Attempts to enhance the current cyber security posture should explore the development of secure power applications with more robust control algorithms that can operate reliably in the presence of malicious inputs while deploying a secure supporting infrastructure that limits an adversary's ability to manipulate critical cyber resources.

II. GOALS AND OBJECTIVES

1. Understanding the threats, and possible consequences of attacks.
2. Identifying the unique properties of cyber-physical systems and their differences from traditional IT security, and
3. Discussing security mechanisms applicable to cyber-physical systems

III. LITERATURE SURVEY

1] Title: Cyber Security for Smart Grid, Cryptography, and Privacy, Pierangela Samarati.

We can say the demand for electricity is larger than it's provided. The demand isn't solely high however conjointly unsteady. We may have confidence renewable resources like solar power and wind energy to fulfil the current want, however sadly, they end up to be unsteady too. The good grid enhances the practicality of the ability delivery system. This is often potential as a result of good grid uses sensors communications, computation, and management so as to create the system good and by applying intelligence thereto within the kind of management through feedback or in different words by mistreatment 2 manner communications. So as to utilize the accessible resources, customers got to amendment, and that they got to act a lot of "smart". They need to vary from being passive customers to being active customers [1]. good grids aim to scale back the energy consumption, guarantee reliableness of power provide, scale back carbon foot print, and minimize the prices related to power consumption.

2] Title: Detecting False Data Injection Attacks on DC State Estimation, Rakesh B. Bobba, Katherine M. Rogers.

State estimation is a very important facility application that's wont to estimate the state of the facility transmission networks victimization (usually) a redundant set of detector measurements and configuration data. Several facility applications like contingency analysis have confidence the output of the state reckoner. Till recently it had been assumed that the techniques won't to notice and establish unhealthy detector activities in state estimation also can thwart malicious detector measurement modification. However, recent work by Liu et al. [1] incontestable that Associate in nursing soul, armed with the information of network configuration, will inject false knowledge into state estimation that uses DC power flow models while not being detected. during this work, we tend to explore the detection of false knowledge injection attacks of [1] by protective a strategically elite set of detector livements and by having the simplest way to severally verify or measure the values of a strategically elite set of state variables. Specifically, we tend to show that it's necessary and comfortable to guard a group of basic measurements to notice such attacks.

3] Title: Crawling for domain specific hidden web resources, Nurjahan, Farhana Nizam, Shudarshon Chaki.

This paper proposes cyber attack detection and hindrance of Cyber Physical System. The Chi sq. detector and mathematical logic primarily based attack classifier (FLAC) were accustomed establish distributed denial of service and False knowledge injection attacks. The fuzzy attributes for choosing the mentioned attacks area unit activity identification, average packet rate, modification purpose detection algorithmic program, consume algorithmic program, unexpired session of users, injected incomplete info, apply of session key. Associate in nursing example situation Has been created victimisation OpNET machine. Simulation results depict that the employment of Chi-square discoverer and FLAC area unit ready to detect the mentioned cyber physical attacks with high accuracy. Compared to existing mathematical logic primarily based attack detector, the planned model outperforms the standard distributed denial of service and False knowledge detector..

4] Cyber–Physical System Security for the Electric Power Grid, Siddharth Sridhar

The development of a trustworthy sensible grid needs a deeper understanding of potential impacts ensuing from triple-crown cyber attacks. Estimating possible attack impact needs Associate in nursing analysis of the grid's dependency on its cyber infrastructure and its ability to tolerate potential failures. an extra exploration of the cyber–physical relationships at intervals the sensible grid and a particular review of potential attack vectors is critical to work out the adequacy of cyber security efforts. This paper highlights the importance of cyber infrastructure security in conjunction with power application security to stop, mitigate, and tolerate cyber attacks. A superimposed approach is introduced to evaluating risk supported the protection of each the physical power applications and also the supporting cyber infrastructure. A classification is conferred to focus on dependencies between the cyber–physical controls needed to support the sensible grid and also the communication and computations that has got to be shielded from cyber attack. The paper then presents current analysis efforts geared toward enhancing the sensible grid's application

and infrastructure security. Finally, current challenges ar known to facilitate future analysis efforts.

5] Cyber Attack Impact on Critical Smart Grid, Kallisthenis I. Sgouras, Athina D. Birda, Dimitris P. Labridis.

Electrical Distribution Networks face new challenges by the good Grid readying. the desired metering infrastructures add new vulnerabilities that require to be taken under consideration so as to realize good Grid functionalities while not sizeable dependableness trade-off. during this paper, a qualitative assessment of the cyber attack impact on the Advanced Metering Infrastructure (AMI) is at first tried. Attack simulations are conducted on a practical Grid topology. The simulated network consisted of good Meters, routers and utility servers. Finally, the impact of Denial-of-Service and Distributed Denial-of-Service.

IV. PROBLEM STATEMENT

A novel system placed at the network egress purpose that aims to expeditiously and effectively notice APT malware infections supported malicious DNS and traffic analysis. The system uses malicious DNS analysis techniques to notice suspicious APT malware C & amp; C domains, and so analyses the traffic of the corresponding suspicious information processing victimization the signature-based and anomaly based mostly detection technology.

V. PROPOSED SYSTEM

This paper proposes cyber-attack detection and interference of Cyber Physical System. The Chi sq. detector and mathematical logic primarily based attack classifier (FLAC) were accustomed determine distributed denial of service and false information injection attacks. The fuzzy attributes for choosing the mentioned attacks are activity identification, average packet rate, modification purpose detection algorithmic program, cusum algorithmic program, unexpired session of users, injected incomplete data, apply of session key.

VI. SYSTEM ARCHITECTURE

We have designed associate rule that detects intrusion within the network through deep packet scrutiny. Packets can return into the network through wide space network (WAN). At first Firewall can veto the unknown or restricted packets. At first each packet are captured and later they're going to be analysed. Then they're going to be filtered out beneath a signature file comparison. Signature can notice if packets have cryptographically signature or not. They’re going to conjointly check for payload packet, syn packet. Afterward protocol analyser can check for acceptable protocols. As an example, spamming is possible through net message access protocol (IMAP).

Where IMAP has no practicality, protocol analyser can discard it. Finally, packets are checked by anomaly detector. Anomaly indicates the packets containing large ping size, fastened behavior characteristic of hardware part such as network interface card and repetitive redundant packets from same supply. If any kind of anomaly is detected, then the packet can get discarded and log server can keep the log of the event. Afterward administrators are afraid and connections are prohibited from that net protocol supply.

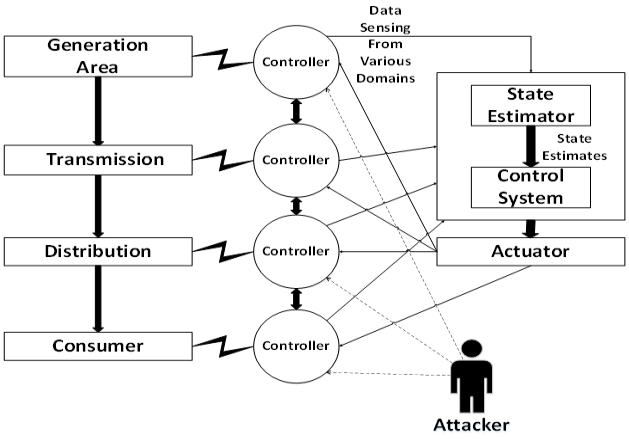

Fig.1. Block diagram of Utility System

VII. IMPLIMENTATION

PC required: 3
1st PC:

- It sender pc, it will send multiple (4 files) to destination (3rd PC).
- While sending assign different signature to each file.
- The sender will send the malicious or virus content file along with other files knowingly which specifies false data injection attack by sender node in the network.

2nd PC:

- It is main pc (i.e. server or IDS), which will detect the malicious files and the files which has been infected due to malicious file in the network flow,

- While detecting the IDS will note down the signature attribute of the file.
- Suppose, in future particular file are detected in network with same signature attribute i.e. the signature attribute by which the malicious file has infected another file, then IDS will also detect that file and dump it

Bloom Filter:

- The IDS system will apply bloom filter mechanism to decrease the error rate i.e. to recover the infected files in the network because of malicious files.

3rd PC:

- Destination pc will receive the normal files as well as recovered files.

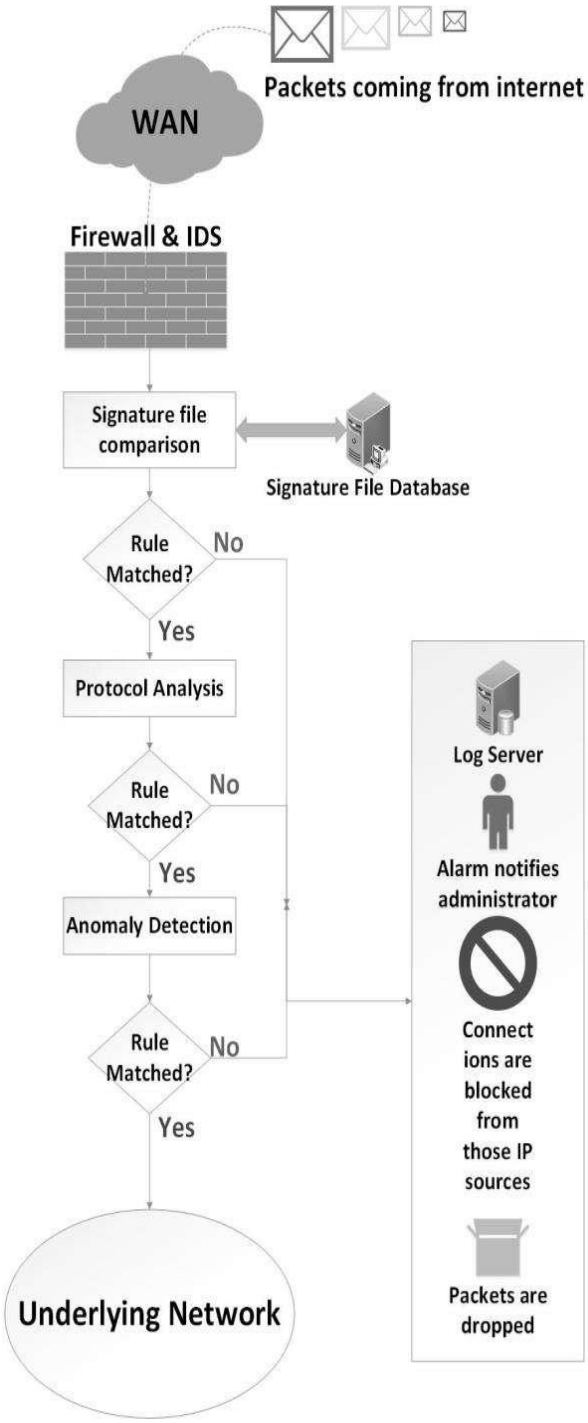

Fig 2. Types of Attacks occurred in the underlying network

RELEVANT MATHEMATICS ASSOCIATED WITH THE PROJECT

System Description:

Let W is the set of whole of system which consists:

W= {input, process, output}.

Input= {D, MDNS, RE, NTA}

Where,

D is the set of data collector.

MDNS is the set of malicious DNS detector which detects the malicious IP at DNS server traffic.

NTA is the network traffic analyzer which detects the network traffic.

RE is the reputation engine which calculates the reputation score of an IP address.

VIII. CONCLUSION

To determine DDoS and False data injection attack, our Proposed detector uses chi-square distribution and fuzzy logic controller. First observed and expected data are collected by Least Mean Square (LMS) filter. Then our chi-square detection technique determines whether there is an attack or not. If there is an attack detected, fuzzy logic controller determines the specific attack name based on some parameters.

ACKNOWLEDGMENT

We express our sincere thanks to all the authors, whose papers in the area of cyber physical system are published in various conferences proceedings and journals.

REFRENCES

[1] Z. Tan, A. Jamdagni, X. He, P. Nanda, L. R. Ping Ren, J. Hu, Detection of denial-of-service attacks based on computer vision techniques, IEEE Transactions on Computers 64 (9) (2015) 2519–2533.

[2] K I. Sgouras, A D. Birda and D. P. Labridis, "Cyber Attack Impact on Critical Smart Grid Infrastructures", in Innovative Smart Grid Technologies Conference (ISGT), 2014 IEEE PES, Washington, DC, 2014, pp. I -5.

[3] K Manandhar, X. Cao, and Y. Liu, "Detection of Faults and Attacks Inc1uding False Data Injection Attack in Smart Grid Using KaIman Filter", IEEE transactions on control of network systems, vol. 1, no. 4, pp. 370-379, 2014.

[4] A. Lara and B. Ramamurthy, “OpenSec: a framework for implementing security policies using OpenFlow,” in IEEE Globecom Conference, Austin, Texas, USA, December 2014.

[5] D. He, S. Chan, S. Tang, and M. Guizani, “Secure data discovery and dissemination based on hash tree for wireless sensor networks,” IEEE Trans. Wireless Commun., vol. 12, no. 9, pp. 4638–4646, Sep. 2013.

[6] Least mean squares filter, "https:llen.wikipedia.org /wiki/Least_mean_squares_filter", [Accessed: 28- Nov-2015]..

[7] S. Iyer, "Cyber Security for Smart Grid, Cryptography, and Privacy", International Journal of Digital Multimedia Broadcasting, vol. 2011, p.p. 1-8 pages, 2011.

[8]K. Manandhar, X. Cao, and Y. Liu, "Detection of Faults and Attacks Including False Data Injection Attack in Smart Grid Using Kalman Filter", IEEE transactions on control of network systems, vol. 1, no. 4, pp. 370-379, 2014..

[9] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system Security for the electric power grid", Proceedings of the IEEE, vol. 100, No. 1, pp. 210-224, 2012

[10] R. B. Bobba, K.M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt and T. J. Overbye, "Detecting False Data Injection Attacks on DC State Estimation", First Workshop on Secure Control Systems (SCS 2010), CPSWEEK2010, Stockholm Switzerland, 2010..

[11] Qingyu Yang, Jie Yang, Wei Yu, Dou An, Nan Zhang, and Wei Zhao, "On False DataAttacks against Power System State Estimation: Modeling and Counter-measures", IEEE Transactions On Parallel And Distributed Systems, 2013.

[12] http://www.cse.iitm.ac.in/

[13] http://www.cyphylab.ee.ucla.edu/

[14] US-CERT. Control Systems Security Program. US Department of Homeland Security, http://www.us-cert.gov/control systems/index.html, 2008.

[15] D. G. Eliades and M. M. Polycarpou, "A fault diagnosis and security framework for water systems," IEEE Transactions on Control Systems Technology, vol. 18, no. 6, pp. 1254–1265, 2010

[17] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 667 –674, 2011.

[18] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in Allerton Conf. on Communications, Control and Computing, Monticello, IL, USA, Sep. 2010, pp. 911–918.

[19] A. A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. A. Perrig, and S. S. ´ Sastry, "Challenges for securing cyber physical systems," in Workshop on Future Directions in Cyber-physical Systems Security, Newark, NJ, USA, Jul. 2009.

[20] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," Proceedings of the IEEE, vol. 99, no. 1, pp. 1–15, 2012.

