Scientific Journal of Impact Factor (SJIF): 4.72

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

International Journal of Advance Engineering and Research Development

Volume 4, Issue 5, May -2017

Jamming Attack Detection and Prevention in Cyber System

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

Abstract — *This paper proposes cyber-attack detection and interference of Cyber Physical System. The Chi sq. detector and symbolic logic based attack classifier (FLAC) were accustomed verify distributed denial of service and false info injection attacks. The fuzzy attributes for selecting the mentioned attacks ar activity identification, average packet rate, modification purpose detection algorithmic rule, consume algorithmic rule, unexpired session of users, injected incomplete information, apply of session key. Associate example state of affairs has been created victimization Op NET machine. Simulation results depict that the use of Chi-square sight or and FLAC are ready to sight the mentioned cyber physical attacks with high accuracy. Compared to existing symbolic logic based attack detector, the planned model outperforms the conventional distributed denial of service and false info detector.*

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

I. INTRODUCTION

In this equipment era of data and communication technologies, physical objects unit presently connected with each different through cyber networks unit conjointly referred to as cyber physical system. Wise grid is Associate in nursing example of such a system wherever grid is automatic, controlled and has accessed via web. The wise grid infrastructure monitors the customer's real time demand to see a dynamic and interactive reference to the purchasers. Wise grid provides bifacial communication between centre and shopper [5]. Wise grid contains self-healing characteristics, it'll merely accommodate renewable energy sources like electrical device, wind, hydro-electric, recurrent event and biomass. It's main objectives unit to supply power faithfully, reduce energy consumption and blackouts [1]. Regardless of the domain, a cycle has 3 principal characteristics square measure (1) atmosphere Coupling: CPSs square measure terribly tightly as well as their atmosphere (physical process) – any modification within the behaviour of the atmosphere leads to a modification within the CPS' behaviour and vice-versa. Distinguished examples embrace medical devices like ICDs. (2)Diverse Capabilities: CPSs square measure typically created of various heterogeneous entities with order of magnitude distinction in capabilities. Sensors deeply embedded in physical processes for watching functions have restricted capabilities, whereas those entities that manage them square measure far more capable. as an example, a health watching cycle is typically created of restricted size medical sensors for usability reasons, however the bottom station managing the sensors is typically a portable computer.

A direct consequence of this no uniformity is potential bottleneck in terms of computation, communication and memory within the work flow. (3) Networked: CPSs, in contrast to ancient complete embedded systems, typically need a channel between its parts, either embedded inside the physical processes or external thereto, so as to supply its (usually coordinated) services [4]. As an example, in Associate in nursing automobile cycle, a sensing element watching the automotive transmission communicates with the automotive radio so as to alter it to extend the degree mechanically because the speed will increase, so compensating for the additional noise.

This paper addresses good grid cyber security considerations by analysing the coupling between the ability management applications and cyber systems. the subsequent terms square measure introduced to supply a typical language to handle these ideas throughout the paper:

• power application: the gathering of operational management functions necessary to keep up stability inside the physical power system;

• supporting infrastructure: the cyber infrastructure as well as computer code, hardware, and communication networks. This division of the grid's command and management functions are going to be used to point out however cyber security considerations are often evaluated and eased through future analysis. attempts makes Associate in Nursing attempt tries to reinforce the present cyber security posture ought to explore the event of secure power applications with additional strong management algorithms that may operate dependably within the presence of malicious inputs whereas deploying a secure supporting infrastructure that limits an adversary's ability to
Manipulate important cyber resources.

II. LITERATURE SURVEY

1]Title : Cyber Security for Smart Grid, Cryptography, and Privacy
Authors: Pierangela Samarati.
We can say the demand for electricity is larger than its give. The demand is not entirely high but together unsteady. we tend to might consider renewable resources like alternative energy and wind energy to satisfy the present wish, but sadly,

they find yourself to be unsteady too. the great grid enhances the usefulness of the flexibility delivery system. usually this can be often potential as a results of sensible grid uses sensors communications, computation, and management therefore on produce the system sensible and by applying intelligence to it among the type of management through feedback or in several words by pattern a pair of manner communication. Therefore on utilize the accessible resources; customers have to be compelled to modification, which they have to be compelled to act lots of "smart". They have to vary from being passive customers to being active customers [1]. Sensible grids aim to reduce the energy consumption, guarantee dependableness of power give, reduce carbon foot print, and minimize the costs associated with power consumption.

2]Title: Detecting False Data Injection Attacks on DC State Estimation

Authors: Rakesh B. Bobba, Katherine M. Rogers.

State estimation could be a vital facility application that is accustomed estimate the state of the power transmission networks victimization (usually) a redundant set of detector measurements and configuration knowledge. many facility applications like contingency analysis trust the output of the state reckoned. until recently it had been assumed that the techniques accustomed notice and establish unhealthy detector activities in state estimation can also thwart malicious detector activity modification. However, recent work by Liu et al. [1] incontestable that Associate in Nursing soul, armed with the knowledge of network configuration, can inject false data into state estimation that uses DC power flow models whereas not being detected. throughout this work, we tend to tend to explore the detection of false data injection attacks of [1] by protecting a strategically elite set of detector lineaments and by having the best thanks to severally verify or live the values of a strategically elite set of state variables. Specifically, we tend to tend to indicate that it's a necessity and comfy to protect a gaggle of basic measurements to note such attacks.

3]Title: Crawling for domain specific hidden web resources.

Authors: Nurjahan, Farhana Nizam, Shudarshon Chaki.

This paper proposes cyber attack detection and hindrance of Cyber Physical System. The Chi sq. detector and system of logic based totally attack classifier (FLAC) were accustomed establish distributed denial of service and False data injection attacks. The fuzzy attributes for selecting the mentioned attacks unit activity identification, average packet rate, modification purpose detection rule, consume rule, unexpired session of users, injected incomplete data, apply of session key. Associate in nursing example state of affairs

Has been created exploitation Op NET machine. Simulation results depict that the utilization of Chi-square discoverer and FLAC unit able to sight the mentioned cyber physical attacks with high accuracy. Compared to existing system of logic based totally attack detector, the planned model outperforms the quality distributed denial of service and False data detector.

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

Authors: By Siddharth Sridhar

The development of a trustworthy wise grid desires a deeper understanding of potential impacts succeeding from triple-crown cyber attacks. Estimating attainable attack impact desires Associate in Nursing analysis of the grid's dependency on its cyber infrastructure and its ability to tolerate potential failures. an additional exploration of the cyber–physical relationships at intervals the wise grid and a selected review of potential attack vectors is important to figure out the adequacy of cyber security efforts. This paper highlights the importance of cyber infrastructure security in conjunction with power application security to prevent, mitigate, and tolerate cyber attacks. A superimposed approach is introduced to evaluating risk supported the protection of every the physical power applications and conjointly the supporting cyber infrastructure. A classification is given to specialize in dependencies between the cyber–physical controls required to support the wise grid and conjointly the communication and computations that possesses to be protected from cyber attack. The paper then presents current analysis efforts intermeshed toward enhancing the wise grid's application and infrastructure security. Finally, current challenges ar acknowledged to facilitate future analysis efforts.

5] Cyber Attack Impact on Critical Smart Grid

Authors: Kallisthenis I. Sgouras, Athina D. Birda, Dimitris P. Labridis.

Electrical Distribution Networks face new challenges by the great Grid activity. the required metering infrastructures add new vulnerabilities that need to be taken into account therefore on notice sensible Grid functionalities whereas not sizeable dependability trade-off. Throughout this paper, a qualitative assessment of the cyber attack impact on the Advanced Metering Infrastructure (AMI) is initially tried. Attack simulations square measure conducted on a sensible Grid topology. The simulated network consisted of fine Meters, routers and utility servers. Finally, the impact of Denial-of- Service and Distributed Denial-of-Service.

III. PROBLEM STATEMENT

A novel system placed at the network egress purpose that aims to efficiently and effectively notice APT malware infections supported malicious DNS and traffic analysis. The system uses malicious DNS analysis techniques to note suspicious APT malware C & C domains, then analyses the traffic of the corresponding suspicious scientific discipline victimization the signature-based and anomaly based detection technology

IV. PROPOSED SYSTEM

His paper proposes cyber-attack detection and interference of Cyber Physical System. The Chi sq. detector and logical system based attack classifier (FLAC) were accustomed confirm distributed denial of service and false data injection attacks. The fuzzy attributes for selecting the mentioned attacks square measure activity identification, average packet rate, modification purpose detection algorithmic rule, consume algorithmic rule, unexpired session of users, injected incomplete information, apply of session key.

V. 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

VI.SYSTEM ARCHITECTURE

We have designed associate rule that detects intrusion among the network through deep packet scrutiny. Packets will come into the network through wide house network (W AN). Initially Firewall will veto the unknown or restricted packets. Initially every packet square measure captured and later they are going to be analysed. Then they are going to be filtered out at a lower place a signature file comparison. Signature will notice if packets have cryptographically signature or not. they are going to put together check for payload packet, sin packet. later on protocol instrument will check for acceptable protocols. as AN example, spamming is feasible through internet message access protocol (IMAP).
Where IMAP has no usefulness, protocol instrument will discard it. Finally, packets square measure checked by anomaly detector. Anomaly indicates the packets containing massive ping size, mounted behaviour characteristic of hardware half like network interface card and repetitive redundant packets from same offer. If any quite anomaly is detected, then the packet will get discarded and log server will keep the log of the event. Later on administrator square measure afraid and connections square measure prohibited from that internet protocol offer.

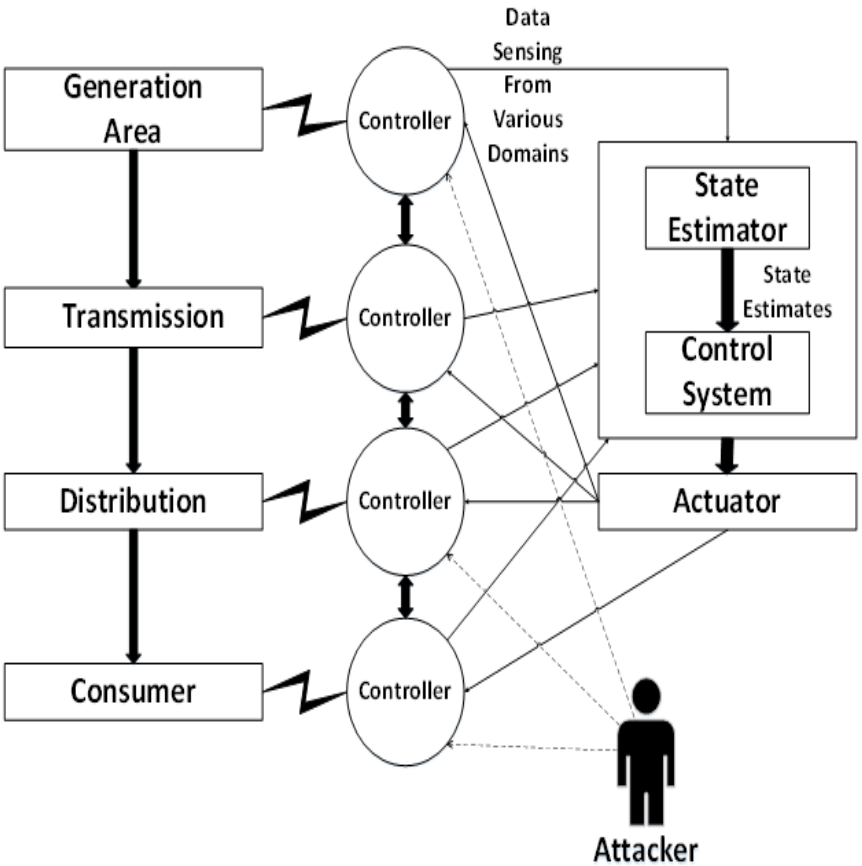


Fig.1. Block diagram of Utility System

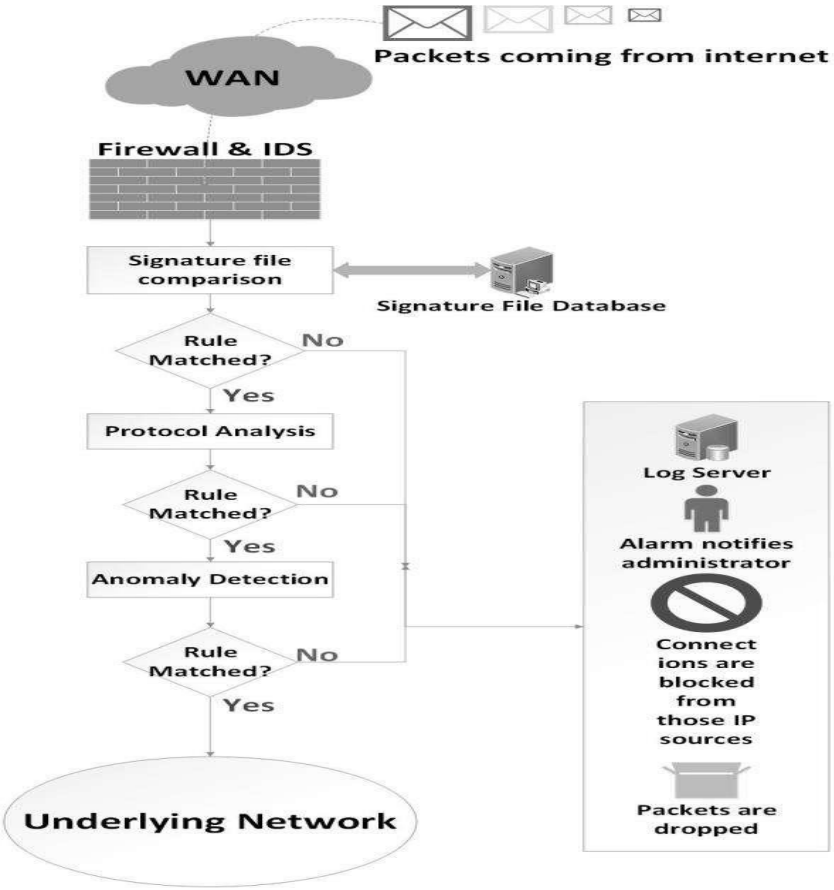


Fig. Types of Attacks occurred in the underlying network

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 applied bloom filter mechanism to decrease the error rate ie 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.

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}

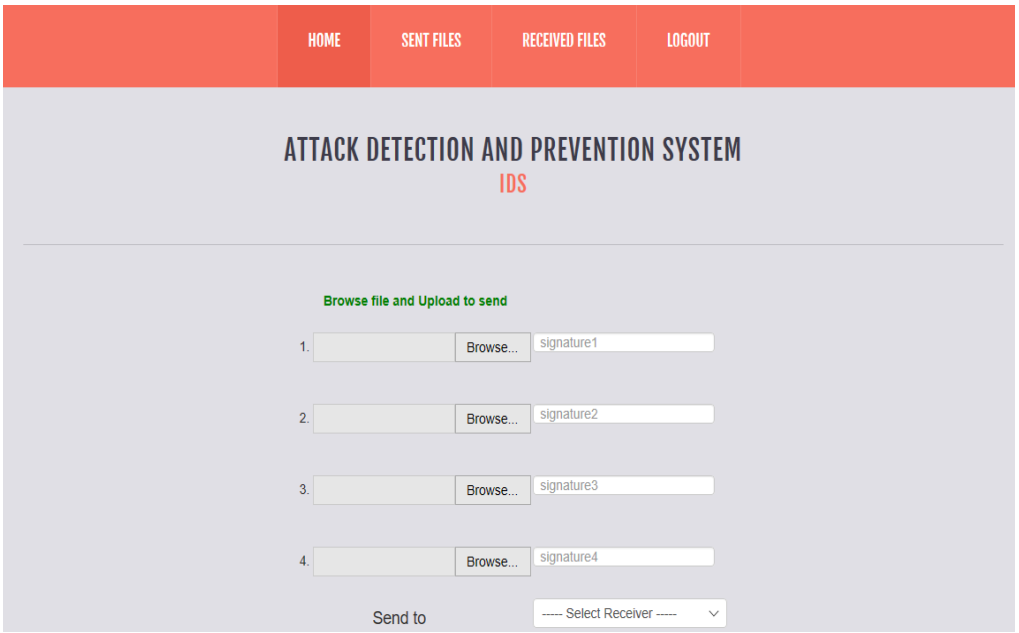
Where,

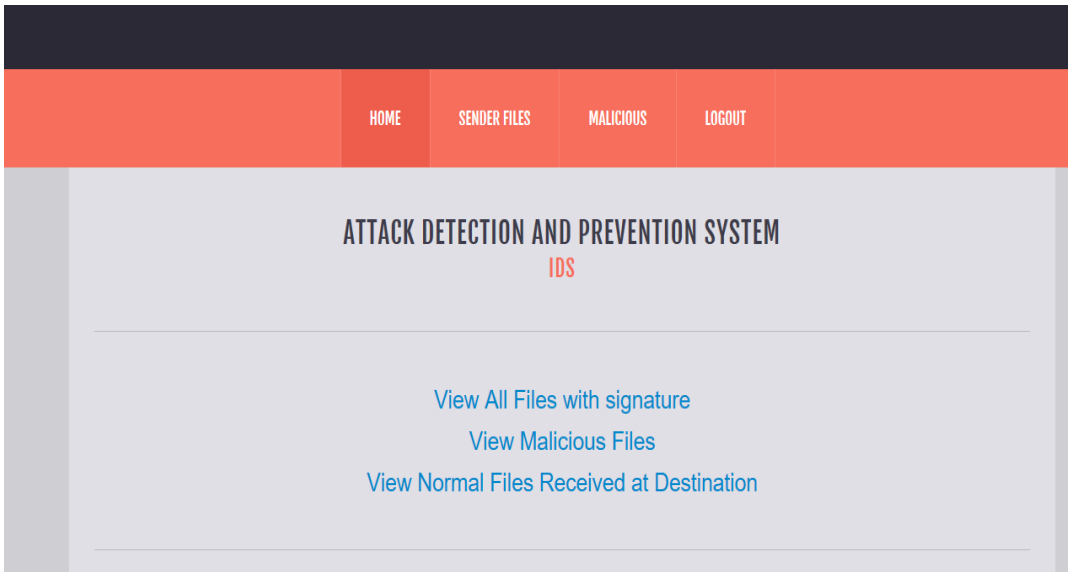
D is the set of data collector.

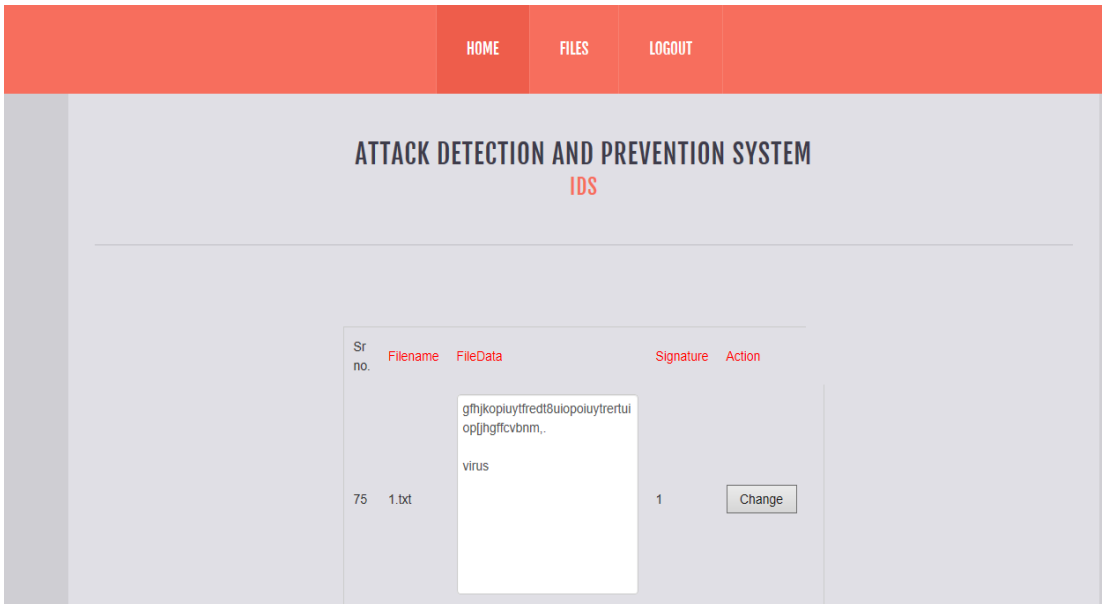
MDNS is the set of malicious DNS detector which detects the malicious IP at DNS server traffic.

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. RESULT ANALYSIS







IX.CONCLUSION

To determine DDoS and False information injection attack, our planned detector uses chi-square distribution and symbolic logic controller. 1st discovered and expected information ar collected by Least Mean sq. (LMS) filter. Then our chi-square detection technique determines whether or not there's AN attack or not. If there's AN attack detected, symbolic logic controller determines the precise attack name supported 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," Proc

