JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CYBER-PHYSICAL ATTACK CONDUCTION AND DETECTION IN DECENTRALIZED POWER SYSTEMS

Dr J Sarada,[1] N Teja Vignesh[2]
[1] Professor Department of Computer Applications , Chadalawada Ramanamma Engineering College Tirupati , Andhra Pradhesh, India.
[2] Student, Department of Computer Applications, Chadalawada Ramanamma Engineering College Renigunta Rd, Tirupati, Andhra Pradesh, India

Abstract-The expansion of power systems over large geographical areas renders centralized processing inefficient. Therefore, the distributed operation is increasingly adopted. This work introduces a new type of attack against distributed state estimation of power systems, which operates on inter-area boundary buses and show that the developed attack can circumvent existing robust state estimators and the convergence-based detection approaches. Afterward, carefully design a deep learning-based cyber-anomaly detection mechanism to detect such attacks and system reveal that the developed framework can obtain a very high detection accuracy. Centralised processing is inefficient due to the spread of power systems over vast geographic areas. As a result, distributed operations are being used more and more. This paper offers a novel inter-area boundary bus-based attack against distributed state estimation of power systems. We demonstrate how the created attack may defeat the convergence-based detection techniques as well as the current robust state estimators. Then, in order to identify such assaults, we carefully construct a deep learning-based cyber-anomaly detection system. A very high detection accuracy may be obtained using the provided framework, according to simulations performed on the IEEE 14-bus system. Additionally, experimental findings show that the proposed detector outperforms existing machine learning-based detection methods.

Keywords— Conduction, Detection, Cybet Physical systems, Power systems.

I. INTRODUCTION

- Expansion of power systems over large geographical areas has made it challenging to implement centralized processing methods.
- Extending the power system to a wide area requires a complex and extensive network for centralized operation and near real-time processing of the collected measurements.
- This has accelerated the move towards distributed operation. specifically focus on distributed state estimation (DSE) in this work.
- In DSE, the grid is divided into many smaller areas, and each area independently collects measurements from its nodes and estimates the per-area system state.
- The power grid's overall state is computed by exchanging the per-area system state through an iterative process.
- Given the growing interest in DSE, understanding its potential vulnerabilities is essential. Cyberattacks against DSE can cause serious consequences, e.g., cascading failures

This work introduces a new type of attack against distributed state estimation of power systems, which operates on inter-area boundary buses

II. RELATEDWORKS

- In Existing system, proposes a denial of service (DoS) attack detection technique based on the development of mean squared disagreement across areas and a mitigation mechanism based on individual areas' opinions about the attack point
- Focuses on the distributed state estimation security against DoS attacks and the distributed resilient filtering challenge for a distributed power system subject to DoS attacks is addressed.
- In another approach, addressed the challenge of joint attack detection and state estimation by using hybrid Bernoulli random set densities to aggregate prior information about signal attacks and system status.
- A secure DSE algorithm via consensus-based distributed non-convex optimization protocols is developed

Disadvantages of Existing system

- Affect the security.
- Lose the redundancy
- Cannot able to use effectively

1. Title : Structure-preserved power system transient stability using stochastic energy functions
Author : M L Crow
Description : With the increasing penetration of renewable energy systems such as plug-in hybrid electric vehicles, wind and solar power into the power grid, the stochastic disturbances resulting from changes in operational scenarios, uncertainties in schedules, new demands and other mitigating factors become crucial in power system stability studies. This paper presents a new method for analyzing stochastic transient stability using the structure-preserving transient energy function. A method to integrate the transient energy function and recloser probability distribution functions is presented to provide a quantitative measure of probability of stability. The impact of geographical distribution and signal-to-noise ratio on stability is also presented.

2.Title : A stealth integrity targeted cyber-attack in distributed electric power networks with local model information
Author : F Ahmadloo
Description : Electric power networks are critical infrastructures, and their correct operation is of vital importance. Nowadays, these systems are prone to cyber-attacks because of new vulnerabilities in the system and access to shared networks. In this paper, a novel Stealth Integrity Targeted Attack (SITA) is proposed in the context of distributed power systems. A distributed power system comprises several sub-networks, or zones with dedicated control and monitoring centers. The overall system is represented by linear time invariant state space models with coupled dynamical and algebraic equations. In the proposed strategy, the attacker has access to only one of the sub networks; therefore, the attacker only requires local information about one of the power system zones. Primarily, the proposed attack policy is defined based on zero-dynamics of the sub network. The intruder injects predesigned signals to both the local generation unit controller as well as local unsecured and controllable loads in the attacked zone.

3.Title : Cybersecurity in distributed power systems
Author : F Li
Description : This paper presents the application of cybersecurity to the operation and control of distributed electric power systems. In particular, the paper emphasizes the role of cybersecurity in the operation of microgrids and analyzes the dependencies of microgrid control and operation on information and communication technologies for cybersecurity. The paper discusses common cyber vulnerabilities in distributed electric power systems and presents the implications of cyber incidents on physical processes in microgrids. The paper examines the impacts of potential risks attributed to cyberattacks on microgrids and presents the affordable technologies for mitigating such risks. In addition, the paper presents a minimax-regret approach for minimizing the impending risks in managing microgrids. The paper also presents the opportunities provided by software-defined networking technologies to enhance the security of microgrid operations.

III. PROPOSED SYSTEM ARCHITECTURE

- In this work, take advantage of the reduced redundancy to propose a coordinated FDIA to disrupt the DSE and utilize deep learning techniques to develop a real-time intelligent attack detection that captures the temporal correlation in power systems between consecutive time slots to differentiate malicious measurements from the normal ones.

The main contributions of this project can be summarized as follows:
1) Design a distributed FDIA that can bypass the current robust distributed estimator as well as the convergence-based detection method.
2) Then formulate a deep learning-based algorithm to capture the temporal correlation in power system measurements and detect the introduced attack.
3) Provide a comparison between the conventional classification algorithms and the carefully designed framework

Advantages of proposed system

- ❑ Secure
- ❑ Reduce Redundancy
- ❑ Effective

Modules

1. Admin

In this module, the Admin has to login by using valid user name and password. After login successful he can do some operations such as Login, Browse and Train & Test Data Sets, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View Prediction Of Cyber Attack Type, View Cyber Attack Type Ratio, Download Trained Data Sets, View Cyber Attack Type Ratio Results,, View All Remote Users.

2. End User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like Register And Login, Predict Cyber Attack Type, View Your Profile.

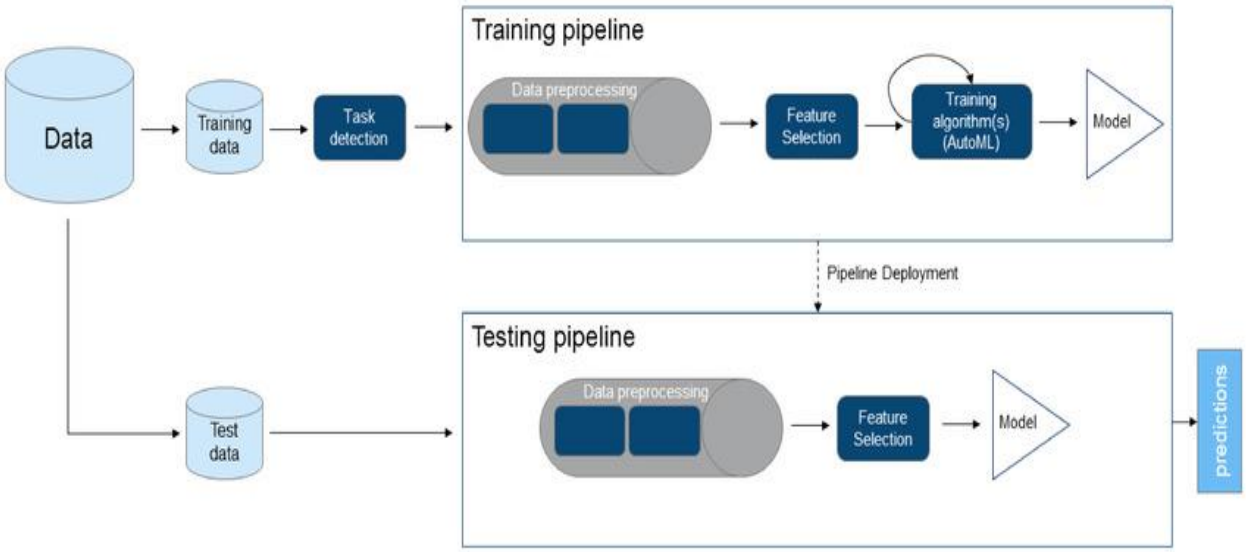

Fig.1 Architecture of proposed system

IV. RESULTS AND DISCUSSION

The output screens obtained after running and executing the system are shown from Fig.2 to Fig.6

Fig.2 Home page

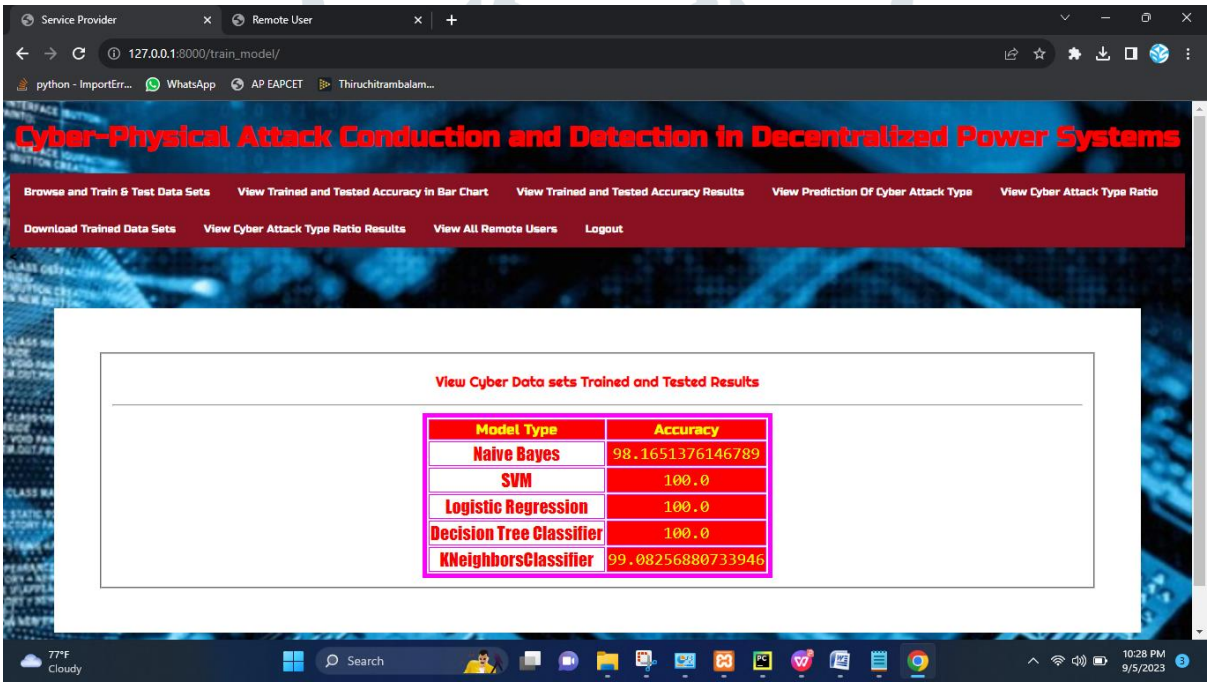

Fig.3 view cyber data sets trained and tested results

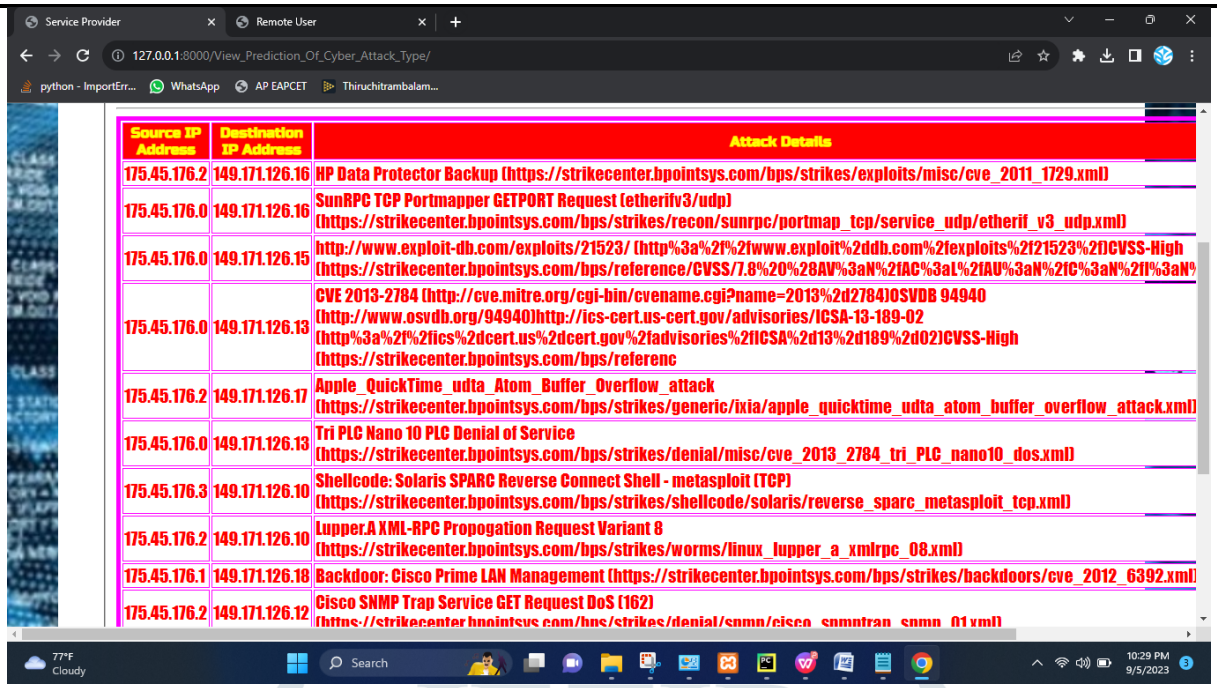

Fig.4 attack details

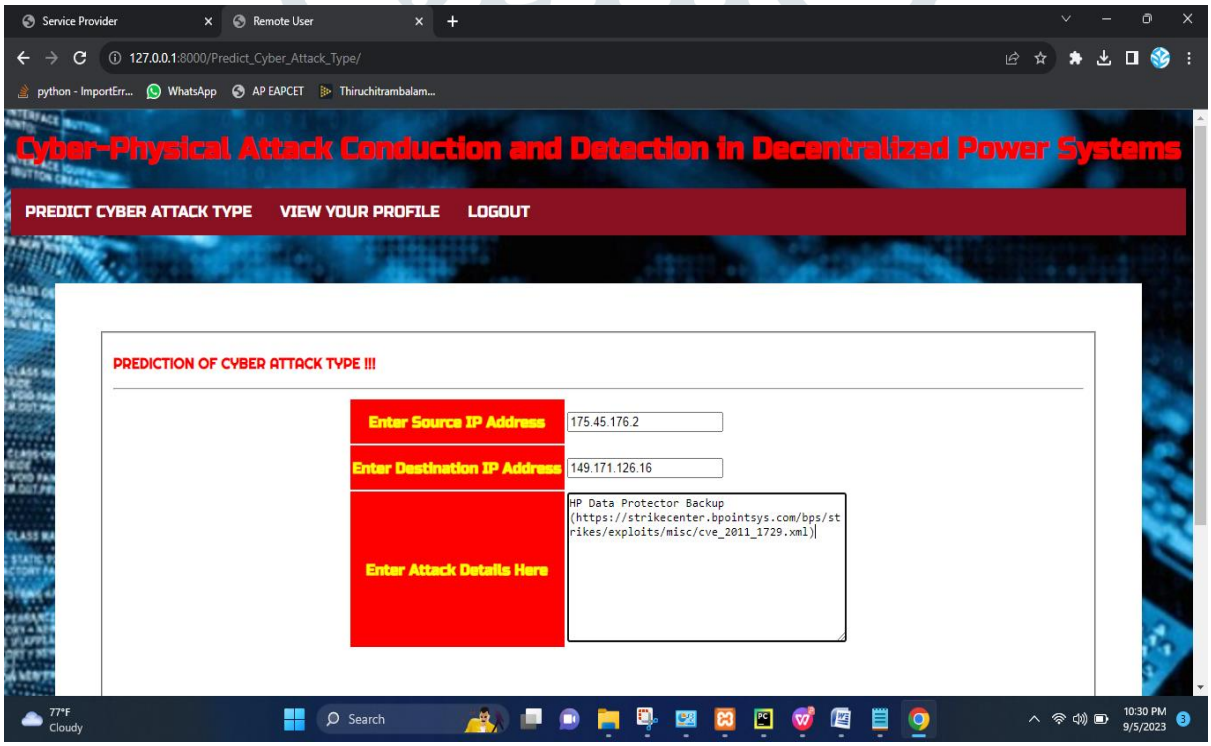

Fig.5 predict type of attack

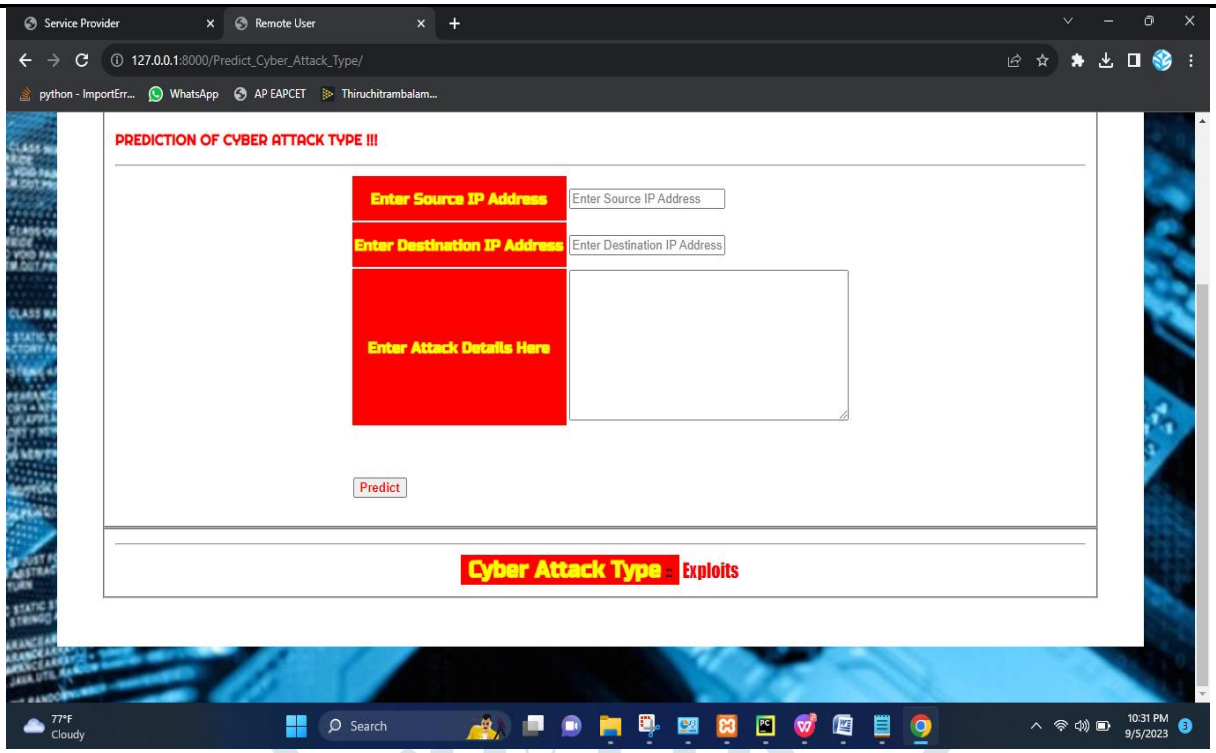

Fig.6 predict results

V. FUTURE SCOPE AND CONCLUSION

This work introduces a detection of attack against distributed state estimation of power systems, which operates on inter-area boundary buses and show that the developed attack can circumvent existing robust state estimators and the convergence-based detection approaches.

REFERENCES

[1] F. Zhang, H. A. D. E. Kodituwakku, J. W. Hines, and J. Coble, “Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data,” IEEE Transactions on Industrial Informatics, vol. 15, no. 7, pp. 4362–4369, 2019.

[2] R. Ma, P. Cheng, Z. Zhang, W. Liu, Q. Wang, and Q. Wei, “Stealthy Attack Against Redundant Controller Architecture of Industrial Cyber- Physical System,” IEEE Internet of Things Journal, vol. 6, no. 6, pp. 9783–9793, 2019.

[3] E. Nakashima, “Foreign hackers targeted U.S. water plant in apparent malicious cyber attack, expert says.” [Online]. Available: https://www.washingtonpost.com/blogs/checkpointwashington/ post/foreign-hackers-broke-into-illinois-water-plant-controlsystem- industry-expert-says/2011/11/18/gIQAgmTZYN blog.html.

[4] R. D. Zimmerman, C. E. Murillo-Sánchez and R. J. Thomas, "MATPOWER: Steady-state operations planning and analysis tools for power systems research and education", *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12-19, Feb. 2011.

[5] M. Mohammadpourfard, I. Genc, S. Lakshminarayana and C. Konstantinou, "Attack detection and localization in smart grid with image-based deep learning", *Proc. IEEE Int. Conf. Commun. Control Comput. Technol. Smart Grids (SmartGridComm)*, pp. 121-126, Oct. 2021.

[6] D. Kingma and J. Ba, "Adam: A method for stochastic optimization", *Proc. 3rd Int. Conf. Learn. Representations*, pp. 1-14, Jul. 2015.

[7] G. E. Hinton, N. Srivastava, A. Krizhevsky, I. Sutskever and R. R. Salakhutdinov, "Improving neural networks by preventing co-adaptation of feature detectors" in arXiv:1207.0580, 2012.

[8] Z. C. Lipton, J. Berkowitz and C. Elkan, "A critical review of recurrent neural networks for sequence learning" in arXiv:1506.00019, 2015.

[9] S. Hochreiter and J. Schmidhuber, "Long short-term memory", *Neural Comput.*, vol. 9, no. 8, pp. 1735-1780, 1997.

[10] S. Hochreiter, Y. Bengio, P. Frasconi, J. Schmidhuber, S. C. Kremer and J. F. Kolen, "Gradient flow in recurrent nets: The difficulty of learning long-term dependencies", *A Field Guide to Dynamical Recurrent Networks*, 2001.

[11] P. J. Werbos, "Backpropagation through time: What it does and how to do it", *Proc. IEEE*, vol. 78, no. 10, pp. 1550-1560, Oct. 1990.

[12] Y. LeCun, Y. Bengio and G. Hinton, "Deep learning", *Nature*, vol. 521, pp. 436-444, May 2015.

[13] H. Moayyed, M. Mohammadpourfard, C. Konstantinou, A. Moradzadeh, B. Mohammadi-Ivatloo and A. P. Aguiar, "Image processing based approach for false data injection attacks detection in power systems", *IEEE Access*, vol. 10, pp. 12412-12420, 2022.