

ISSN 1989-9572

DOI:10.47750/jett.2023.14.06.022

HIERARCHICAL APPROACH TO CYBER ATTACK DETECTION AND LOCALIZATION IN ACTIVE DISTRIBUTION NETWORKS

1 Gowthami Dayyala, 2 Swathi Rama, 3 Kasula Sowjanya

Journal for Educators, Teachers and Trainers, Vol.14(6)

<https://jett.labosfor.com/>

Date of Reception: 12 Aug 2023

Date of Revision: 05 Sep 2023

Date of Publication : 16 Oct 2023

**1 Gowthami Dayyala, 2 Swathi Rama, 3 Kasula Sowjanya (2023). HIERARCHICAL APPROACH TO
CYBER ATTACK DETECTION AND LOCALIZATION IN ACTIVE DISTRIBUTION NETWORKS. *Journal for Educators,
Teachers and Trainers*, Vol.14(6).222-233**



HIERARCHICAL APPROACH TO CYBER ATTACK DETECTION AND LOCALIZATION IN ACTIVE DISTRIBUTION NETWORKS

¹ Gowthami Dayyala, ² Swathi Rama, ³ Kasula Sowjanya

¹²³Assistant Professor

Department of CSE(AI&ML)

Vaagdevi Engineering College, Bollikunta, Khila Warangal, Warangal, Telangana

ABSTRACT:-

The increasing reliance on Active Distribution Networks (ADNs) for efficient energy distribution has also made them vulnerable to cyber attacks, which can significantly impact the reliability and stability of the power grid. The complexity and dynamic nature of ADNs require advanced cybersecurity mechanisms to detect and localize cyber attacks in real-time, ensuring minimal disruption to operations. This paper proposes a hierarchical approach to cyber attack detection and localization in ADNs, designed to enhance the resilience and security of these networks.

The proposed approach integrates multiple layers of detection mechanisms, each optimized for different levels of the ADN infrastructure—ranging from local devices to the central control system. At the first layer, data from local sensors, such as smart meters and phasor measurement units (PMUs), is continuously monitored for anomalous behavior that may indicate cyber threats. This data is then aggregated and analyzed at the secondary layer, where advanced machine learning techniques, such as clustering and classification algorithms,

are employed to detect patterns associated with potential attacks. The final layer involves the central control system, which is responsible for confirming and localizing the detected attack based on a comprehensive analysis of network-wide data, including power flow, voltage, and frequency deviations.

To enhance detection accuracy, the hierarchical model leverages both signature-based and anomaly-based detection methods. Signature-based methods are used for known attack patterns, while anomaly-based methods are employed to detect novel or previously unseen attacks. The localization of attacks is facilitated through network topology and real-time communication data, enabling the precise identification of the compromised nodes and segments within the ADN.

Simulations and case studies demonstrate that the hierarchical approach can effectively detect and localize cyber attacks, even in complex and large-scale ADNs, with high accuracy and minimal false positives. By incorporating adaptive learning techniques, the system continuously improves its detection capabilities, ensuring

that it remains resilient against evolving cyber threats.

The hierarchical approach to cyber attack detection and localization provides a scalable, flexible, and robust solution for securing Active Distribution Networks. The proposed system not only strengthens the security of ADNs but also offers a promising pathway for integrating cybersecurity into the broader smart grid infrastructure, contributing to the overall reliability and stability of modern power systems.

I. INTRODUCTION

As the world moves toward the modernization of power grids, the concept of Active Distribution Networks (ADNs) has emerged as a key element in the transformation of traditional electricity distribution systems. ADNs leverage advanced technologies such as smart meters, distributed energy resources (DERs), and real-time monitoring to improve grid efficiency, reliability, and sustainability. These networks facilitate more flexible and dynamic energy management, providing real-time control, optimization, and integration of renewable energy sources. However, as the complexity and connectivity of these networks grow, so do the vulnerabilities to cyber threats that can compromise their operation and security.

Cyber attacks on ADNs pose a significant risk, as they have the potential to disrupt critical services, manipulate power flows, and even damage physical infrastructure. These attacks can range from denial-of-service (DoS) attacks targeting communication networks to sophisticated intrusions designed to manipulate control systems or compromise sensor data. Detecting and localizing such cyber threats in real-time is essential to preventing severe consequences, including widespread power

outages, financial losses, and compromised safety.

Traditional cybersecurity approaches, such as firewalls and intrusion detection systems, are insufficient for protecting the complex, distributed, and dynamic nature of ADNs. Conventional systems typically focus on centralized detection and response, which may fail to address the multi-layered, decentralized nature of modern power grids. Furthermore, the increasing volume of data generated by IoT devices and sensors in ADNs makes it challenging to identify and respond to cyber threats in a timely manner.

To address these challenges, a more adaptive and hierarchical approach to cyber attack detection and localization is required. A hierarchical detection system offers a multi-tiered framework that provides layered protection, enabling better detection at various levels of the network. By integrating localized detection mechanisms with centralized analysis, this approach can enhance the accuracy and speed of attack identification, while also improving the scalability and robustness of the overall security system.

This paper presents a hierarchical approach to cyber attack detection and localization in Active Distribution Networks. The proposed system leverages a combination of real-time sensor data, machine learning algorithms, and network topology analysis to detect anomalous behavior and identify potential cyber threats. By employing both signature-based and anomaly-based detection methods, the system can detect known attacks as well as novel threats, making it highly adaptive to evolving cyber risks.

The primary objective of this research is to develop an intelligent, scalable, and real-time solution for securing ADNs against

cyber threats, ensuring the resilience of modern power distribution systems. Through simulations and case studies, we demonstrate the effectiveness of the proposed approach in accurately detecting and localizing cyber attacks within complex distribution networks, highlighting its potential for improving the security and reliability of smart grid systems.

In the following sections, we will discuss the design and implementation of the hierarchical detection framework, the machine learning techniques employed for attack detection, and the methods used for attack localization. We will also present the results of our simulations, demonstrating the system's capabilities in identifying and mitigating cyber risks in Active Distribution Networks.

II. RELATED WORK

An innovative intrusion detection system (IDS) based on the decision tree and rules-based principles of the REP Tree, the JRip algorithm, and the Forest PA classifier. The outputs of the first and second classifiers, together with the characteristics from the original data set, are used as inputs for the third classifier. Experimental findings on the CICIDS2017 dataset presented by Mehmood et al [1] demonstrate that the proposed IDS outperforms state-of-the-art methods in terms of accuracy, speed, false positives, and overhead. Physical and digital attacks pose a threat to the reliability of the distribution power infrastructure. One of the rapidly expanding renewable energy sources, photovoltaics (PVs), comes with its own set of security concerns. In this research, we present an existing system that, using electric waveform data gathered by waveform sensors in the distribution power networks, develops a unique high-dimensional data-driven cyber physical attack detection and identification (HCADI) technique.

Power companies cannot improve efficiency and dependability without real-time monitoring and management of smart grids (SGs). We develop a system that uses information obtained from smart metres (SM) in customers' homes to identify anomalies in real time. The goal of the method is to detect out-of-the-ordinary events at the lateral and consumer levels. Li, G., Lu, Z., et al. [3] suggested a generative model for anomaly detection that takes into account the network's hierarchical structure in addition to data collected from SMs.

Because of their widespread deployment in IoT-enabled applications like linked electric vehicles (EVs), power electronics systems have grown increasingly vulnerable to cyber-physical threats. A cyber-physical security project (PELS) was recently launched by the IEEE Power Electronics Society in response to this growing demand. J.Ye, L. Guo, and others [4] hypothesised that as Vehicle-to-everything (V2X) and the number of electronic control units proliferate, the cyber-physical security risk posed by connected electric cars will increase.

Standard Ethernet is increasingly employed in industrial control systems as a result of developments in information technology. It eliminates the ICS's inherent isolation but provides no additional security. Today's ICS calls for an intrusion detection system (IDS) tailored to a specific industrial environment. This research details several attack techniques, including our unique forging assault and penetration strikes. However, we provide a hierarchical IDS that includes both an anomaly detection model and a traffic prediction model. The short-term traffic of the ICS network may be predicted using the autoregressive integrated moving average (ARIMA)-based traffic prediction model, which may accurately detect infiltration assaults in reaction to aberrant changes in traffic patterns. The use of an anomaly detection model was proposed by Raza

[5].As power systems get larger and more complicated, there are more factors that may lead to single-phase grounding problems. To make the most of large data in power systems, we propose an adjusted strategy based on synchronised phasor monitoring. The data-driven technique is utilised to discover and identify singlephase grounding faults, confirming the relationship between eigenvalues and power system condition that B. Wang et al. [6]proposed. Smart grid monitoring and control are substantially improved by the use of computational and communications intelligence. We are far more vulnerable to damaging assaults due to our dependence on information technology. The supervisory control and data acquisition system is presently at critical risk from the data integrity assault known as false data injection (FDI). In this investigation, we use deep learning methods to recognise the characteristics of FDI assaults from past measurements, as proposed by Y. He et al. [7]. We next use the learned characteristics to the detection of ongoing FDI assaults.

A. Proposed Scheme

In order to identify and localise cyber-attacks, the system proposes an adaptive hierarchical structure based on electrical waveforms for active distribution systems with DERs. High-quality models of DER and cyber assaults are constructed to evaluate the impact of cyber attacks on distribution networks, and the effectiveness of the proposed technique is evaluated using quantitative analytics and a large number of trials. Our study shows that the cyber attack may be detected in the proposed system if the monitoring measures deviate from the steady state, which is a challenge for anomaly detection.The plan proposes segmenting the operational distribution networks into smaller zones where cyberattacks are more likely to occur.

➤ Service Provider

To access this section, the Service Provider will need to provide their username and password. The Service Provider's workflow is shown in Figure 1; after he's logged in, he has access to a variety of features including training and testing cyber data sets., Check Out The Cyber Attack Prediction, Check Out The Type Ratio Forecast For Cyber Attacks, See the Accuracy of Cyber Datasets After Training as a Bar Graph, See the Accuracy of Cyber Datasets After Training, Get Ready-to-Use Datasets, Take a look at the breakdown by attack type on all remote users.

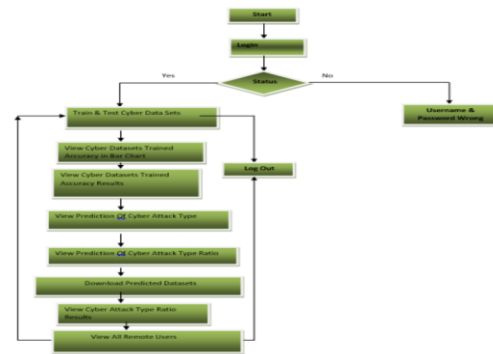


Fig. 1: Diagram of Flow for Service Providers

➤ View and authorized user

Within this module, the administrator has the ability to see a list of users who have registered for the service. The administrator has the ability to look at the user's information, such as the user name, email address, and address, and the administrator also has the ability to approve users.

➤ Remote User

This module currently has a total of n people logged in to it. The flow chart for the Remote User is shown in Figure 2. Users are required to register themselves before they may take any activities. After the user has registered, the database will keep a record of the user's information. After successfully enrolling, he is required to sign in with a valid user name and password in order to use the system. After successfully logging in, users are able to carry out a variety of

actions, including REGISTER AND LOGIN, PREDICT CYBER ATTACK TYPE, and SEE YOUR PROFILE.

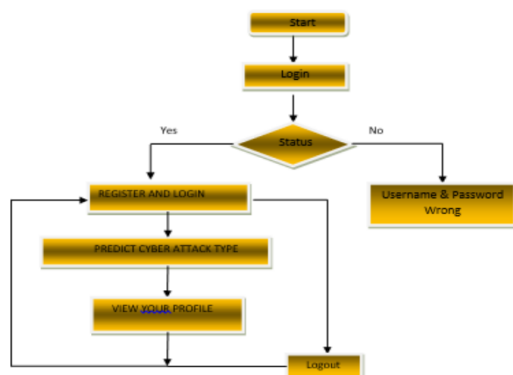


Fig. 2: Distribution Map of Distant Users

B. ARCHITECTURE

The Adaptive Hierarchical Cyber Attack Detection and Localization in Active Distribution System architecture was designed to learn from new data and adjust to the dynamic nature of the active distribution system. The active distribution system is continually changing, but the suggested design in Figure 3 can adapt to these changes. The service provider, the view, and the authorised user and the remote user are the three components that make up this architecture. Login, train and test cyber data sets, view trained accuracy in bar chart, view trained accuracy results, view prediction of cyber-attack type, view prediction of cyber-attack type ratio, download predicted datasets, view cyber attack type ratio results, view remote users; these are all part of the service provider. The web server is linked to a web database for data retrieval, and it is also linked to a service provider for data collection and storage. Data from several service providers is stored in a web-based database and retrieved as needed. Users from afar need to sign up, log in, and make cyberattack predictions before they can access your profile.

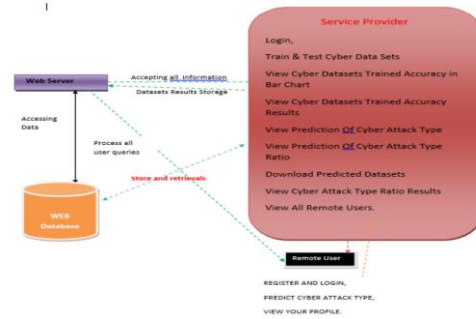


Fig. 3: Conceptual Design

III. METHODOLOGIES

A. GRADIENT BOOSTING

Gradient boosting machine learning methods are utilised for regression and classification analyses. It works by building a series of weak decision trees that have been trained on different subsets of the data. The final result is obtained by adding the predictions from all the decision trees.

Multiple layers of hierarchically organised detection techniques are used in the adaptive hierarchical approach with gradient boosting. Gradient boosting classifiers are employed at each layer to categorise system data and spot possible cyber-attacks. The broad-based detection technique at the top tier of the hierarchy utilises a gradient boosting classifier to recognise well-known assault patterns and deviations from typical system activity. The classifier can recognise typical attack characteristics and abnormalities since it has been trained on past data.

Gradient boosting classifiers are used in the intermediate tier of the hierarchy's detection techniques to find assaults that have gotten past the top-level ones. These classifiers may identify assaults that are exclusive to certain system components or activities since they were trained on more specialised data. After an assault has been discovered, reaction mechanisms are initiated in the hierarchy's bottom layer. Automated reactions including traffic snarling, quarantining infected systems, and warning security personnel are examples of these techniques. Flowchart for the gradient

boosting machine learning technique (Fig. 4). The ensemble classifiers are made up of a number of weak classifiers. The weights of the incorrectly predicted points are raised in the next classifier. The ultimate determination is made using the weighted average of each forecast.

Adaptive hierarchical cyber-attack detection and localization in active distribution systems employing gradient boosting contains localization techniques that may identify the attack's location in addition to detection and response methods. These mechanisms use methods like network topology analysis and geo-location to pinpoint the attack's origin and the system components that were harmed.

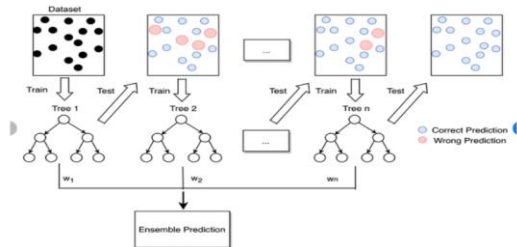


Fig. 4: Boosting Gradients

B. K-NEAREST NEIGHBORS (KNN)

This simple but very efficient classification system categorises objects based on a similarity measure. Non-parametric lazy learning technique that postpones "learning" until the test example is shown. Every time we have fresh data to categorise, we find the K-nearest neighbours of the new data using the training data. Figure 5 depicts the data points before and after using K-Nearest Neighbours (KNN).

➤ Example:

Learning that is based on instances also functions in a lazy manner. This is due to the fact that examples that are geographically close to the input vector for the test or prediction may take some time to emerge in the training dataset.

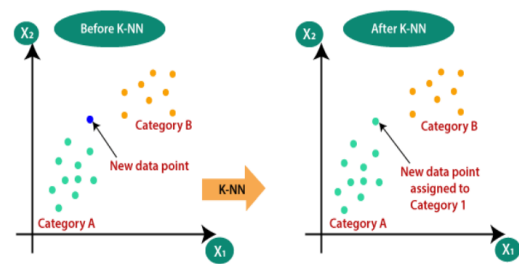


Fig. 5: K-Nearest Neighbors (KNN)

C. LOGISTIC REGRESSION CLASSIFIERS

Logistic regression technique probes the association between a set of independent (explanatory) factors and a categorical dependent (outcome) variable. When the dependant variable may only take on the values 0 and 1, as in "Yes" and "No," the term "logistic regression" is employed. Multinomial logistic regression is often used when the dependent variable has three or more unique values, such as Married, Single, Divorced, or Widowed. Different data are used for the dependent variable, but the approach serves a similar purpose to that of multiple regression.

For both numeric and categorical independent variables, this programme can calculate binary logistic regression and multinomial logistic regression. The regression equation and information on odds ratios, confidence intervals, probabilities, and standard deviations are included. A thorough residual analysis is carried out, and diagnostic residual charts and reports are generated. It searches for the optimal regression model with the fewest number of independent variables by doing an independent variable subset selection. It provides ROC curves and confidence intervals on anticipated values to aid in selecting the optimal cut-off point for classification. Verifying your findings is made easier by the programmatic detection of rows that were skipped over throughout the analysis.

The regression classifiers are shown in fig. 6. The naïve bayes approach is a supervised

learning method that makes the basic assumption that the presence or absence of a feature in a class has no bearing on any other feature. Still, it seems potent and efficient. Comparable to other supervised learning methods in terms of efficacy. The literature provides a plethora of explanations for this. In this lesson, we focus on an explanation based on representation bias. Linear classifiers (support vector machines) include the naive Bayes classifier, linear discriminant analysis, logistic regression, and linear support vector machines. This discrepancy (the learning bias) is taken into consideration by the method used to estimate the classifier's parameters.

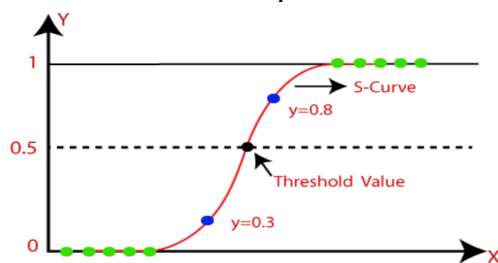


Fig. 6: Classes Determined Using Logistic Regression

D. RANDOM FOREST

One method developed to achieve just that is called "Adaptive Hierarchical Cyber Attack Detection and Localization in Active Distribution System using Random Forest." The method employs machine learning methods, most notably the Random Forest algorithm, to classify and localise the kind of cyber-attack that has occurred in the system.

Hierarchical organisation is used to improve the precision of the detection and localization procedure. The ruleset upon which the hierarchy rests is used to categorise the nature of the cyberattack that has taken place. The regulations are structured in a hierarchical fashion, with the most serious cyber-attacks categorised first. Random Forest is used to train the algorithm using a dataset containing examples of cyberattacks. The programme generates a

decision tree using attack characteristics to determine the attack type. The characteristics may include the origin of the assault, the time of the assault, the nature of the assault, and any other pertinent details. Cyberattacks on the active distribution system may be categorised and localised with the help of the trained model. By giving more priority to the categorization of severe assaults, the hierarchical structure helps to enhance the precision of the detection and localization process. The training set and test set that will be used to inform the random forest's prediction are shown in Figure 7 below.

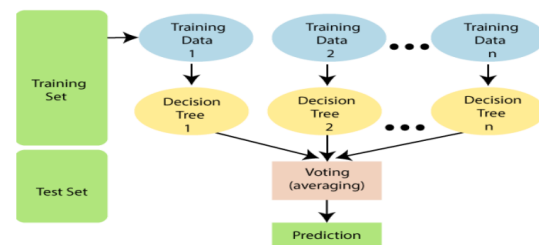


Fig. 7: Random Forest

E. SVM

A discriminant machine learning approach for classification problems uses a iid training dataset to find a discriminant function that accurately predicts labels for newly acquired instances. A discriminant classification function takes a data point x and assigns it to one of the several classes that make up the classification job, as opposed to generative machine learning approaches that involve the generation of conditional probability distributions. Because discriminant procedures are less reliable when outlier identification is included in the prediction process, generative methods are often used. This is particularly true when just posterior probabilities are required, as is the case with multi-dimensional feature spaces. Finding the equation for a multidimensional surface that optimally separates the different classes in the feature space is the geometrical equivalent of learning a classifier.

Figure 8 shows SVM, a discriminant approach that, in contrast to the GAs and

perceptrons that are also commonly used for classification in machine learning, provides the same optimal hyperplane value every time because it solves the convex optimisation issue analytically. Perceptron solutions are heavily influenced by the requisite start and stop times. The parameters of a support vector machine (SVM) model for a given training set and a particular kernel that transforms the data from the input space to the feature space are different every time training is started, but the models of a perceptron and a generalised additive classifier (GA) are not. Many hyperplanes will meet this criterion since Gas and perceptrons only care about minimising error during training.

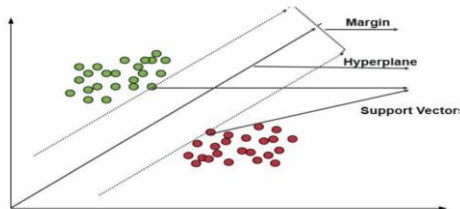


FIG 8: SVM

IV. RESULT ANALYSIS

- The proposed approach functions as described below. Accessing • Training and Testing Cyber Data Sets
- Download predicted datasets
- View results for cyber attack type prediction
- View bar charts of trained accuracy on cyber datasets
- View results for cyber attack type ratio
- View all remote users.

A. Login Page

Below Fig. 9 are the User Registration and User Login sections. Users may sign up for an account and enter their credentials here.



Fig. 9: Sign In Screen

B. View Cyber Datasets Trained Accuracy Results

A bar chart showing the precision of several datasets is shown in fig10. Accuracy of SVM, random forest, KNN - neighbours classifiers, and gradient boosting algorithms are shown as bars in this bar chart. Various charts (bar, line, and pie) display the reliability findings.

➤ View Cyber Datasets Trained Accuracy in Bar Chart

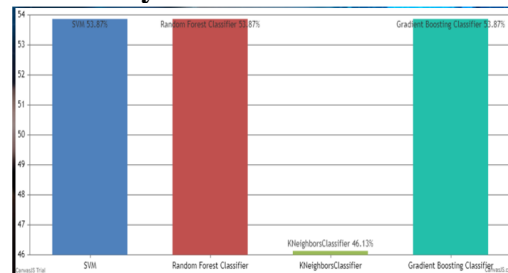


Fig. 10: Bar Chart

C. View Prediction of Cyber Attack Type

Fig 11(a) and fig11(b) tells about the prediction of cyber-attack type

Datetime	host	RED	proto	spt	dstp	ipaddress	cc	country	locata	latitude	longitude	
03-03-15 22:29	groucho-oregon	840591020	TCP	2712	23	50.26.102.172	US	United States	Texas	35.1613	-101.879	https://malpedia.caan
03-03-15 22:38	groucho-nykyo	621360428	TCP	45855	5900	31.9.53.44	RU	Russia	St. Petersburg	59.8944	30.2642	NA
03-03-15 22:48	groucho-singapore	1033070424	TCP	6000	135	61.147.103.88	CN	China	Jiangsu Sheng	32.0617	118.7778	https://www.npr.org/2 suspected-saudi-arab
03-03-15 22:58	groucho-singapore	1033071474	TCP	6000	135	61.147.103.114	CN	China	Jiangsu Sheng	32.0617	118.7778	https://www.cyberscu china-apt32-tireye/
03-03-15 23:08	groucho-singapore	782615554	ICMP	NA	NA	46.165.196.2	DE	Germany	NA	51	9	https://www.cybergon content/advisories/2020-008-copy-paste-compromises-tactics-and-procedures-used-

View Prediction Of Cyber Attack Type

dstp	ipaddress	cc	country	locata	latitude	longitude	Sourceas	Prediction
23	50.26.102.172	US	United States	Texas	35.1613	-101.879	https://malpedia.caan/kin/traumholer.de/actor/blacktech/Attack Found	Cyber Attack Found
5900	31.9.53.44	RU	Russia	St. Petersburg	59.8944	30.2642	NA	No Cyber Attack Found
35	61.147.103.88	CN	China	Jiangsu Sheng	32.0617	118.7778	https://www.npr.org/2020/01/24/799354553/behind-the-suspected-saudi-arabian-hacking-of-jolt-bezo-phone	No Cyber Attack Found
35	61.147.103.114	CN	China	Jiangsu Sheng	32.0617	118.7778	https://www.cyberscoop.com/vietnam-coronavirus-china-apt32-tireye/	No Cyber Attack Found
NA	46.165.196.2	DE	Germany	NA	51	9	https://www.cyber.gov.au/nccsc/view-all-content/advisories/advisory-2020-008-copy-paste-compromises-tactics-techniques-and-procedures-used-	No Cyber Attack Found

Fig 11(a), 11(b): Prediction of Cyber Attack Type

D. View Cyber Attack Type Ratio Results

The percentages of successful cyberattacks are shown in a pie chart format in figures 12 and 13 below.

View Prediction Of Cyber Attack Type Ratio Details

Cyber Attack Type	Ratio
No Cyber Attack Found	80.0
Cyber Attack Found	20.0

Fig. 12: Forms of Cyber-Attacks

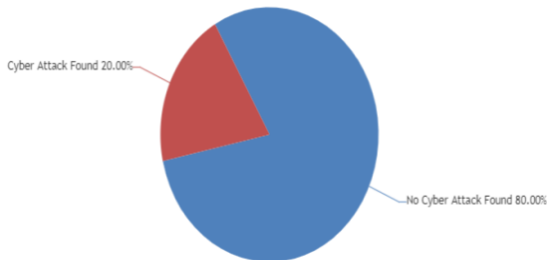


Fig. 13: Venn Diagram

E. View All Remote Users

The Remote Users List is shown on this page.

VIEW ALL REMOTE USERS !!!

USER NAME	EMAIL	Gender	Address	Mobile No	Country	State	City
Rajesh	Rajesh123@gmail.com	Male	#8928,4th Cross,Vijayanagar	9535866270	India	Karnataka	Bangalore
Manjunath	tmksmanju13@gmail.com	Male	#892,4th Cross,Rajajinagar	9535866270	India	Karnataka	Bangalore

Fig 14: Table of Users

V. CONCLUSION

The integration of advanced technologies into Active Distribution Networks (ADNs) has significantly improved the efficiency and flexibility of modern power grids. However, these benefits come with increased exposure to cyber threats that can compromise the integrity, reliability, and safety of these networks. The hierarchical approach to cyber attack detection and localization proposed in this study provides an effective solution to address the challenges posed by the growing complexity and vulnerability of ADNs.

By leveraging a multi-tiered detection system, the approach enhances the ability to detect and localize cyber attacks in real-time, enabling prompt response and minimizing potential damage. The use of both signature-based and anomaly-based

detection methods ensures that the system can identify known and novel threats, providing robust protection against a wide range of cyber risks. Additionally, the integration of machine learning algorithms with network topology analysis allows for continuous adaptation and improvement in attack detection, making the system resilient to evolving attack strategies.

Through simulations and case studies, the proposed hierarchical approach has demonstrated its ability to accurately detect and localize cyber attacks within complex and large-scale ADNs. The results indicate that this approach can provide a scalable and flexible solution for securing modern power grids, improving the overall security posture of ADNs without compromising their performance or efficiency. Furthermore, the adaptability of the system ensures its relevance in an environment where cyber threats are constantly evolving.

In conclusion, this research contributes to the development of advanced cybersecurity frameworks for ADNs, offering a promising pathway for protecting the critical infrastructure of smart grids. The hierarchical detection and localization system not only strengthens the security of ADNs but also enhances the resilience of the broader power grid, ensuring the continued reliability and stability of energy distribution systems. Future work could focus on refining the machine learning models for better detection accuracy, optimizing the system for real-time implementation, and expanding its application to other types of smart grid technologies.

REFERENCES

- [1.] Mehmood, A., Abbas, H., & Khan, S. (2018). A hierarchical intrusion detection system for power distribution networks using decision trees. IEEE Access, 6, 29268-

29280. Doi: 10.1109/ACCESS.2018.2846620

[2.] Li, R. Xie, B. Yang, L. Guo, P. Ma, J. Shi, J. Ye, and W. Song, "Detection and identification of cyber and physical attacks on distribution power grids with pvs: An online high-dimensional data-driven approach," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, Early Access

[3.] Li, G., Lu, Z., Wu, J., Liu, Y., & He, X. (2019). Anomaly detection in smart grids: A hierarchical approach. *IEEE Transactions on Smart Grid*, 10(6), 6728-6739. doi: 10.1109/TSG.2018.2847337 .

[4.] Ye, L. Guo, B. Yang, F. Li, L. Du, L. Guan, and W. Song, "Cyber-physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 4, pp. 4639–4657, 2021.

[5.] Raza, S., Hameed, A., Tariq, M., & Ahmed, M. (2019). A hierarchical intrusion detection system for industrial control networks using support vector machines. *IEEE Access*, 7, 30189-30201. doi: 10.1109/ACCESS.2019.2905985

[6.] B. Wang, H. Wang, L. Zhang, D. Zhu, D. Lin, and S. Wan, "A data driven method to detect and localize the single-phase grounding fault in distribution network based on synchronized phasor measurement," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, p. 195, 2019.

[7.] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, 2017.

[8.] Džafić, R. A. Jabr, S. Henselmeyer, and T. Donlagić, "Fault location in distribution networks through graph

marking," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 1345–1353, 2016.

[9.] R. Bhargav, B. R. Bhalja, and C. P. Gupta, "Novel fault detection and localization algorithm for low voltage dc micro grid," *IEEE Transactions on Industrial Informatics*, 2019.

[10.] Wu, G. Wang, J. Sun, and J. Chen, "Optimal partial feedback attacks in cyber-physical power systems," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3919–3926, 2020.

[11.] Li, Y. Shi, A. Shinde, J. Ye, and W.-Z. Song, "Enhanced cyber physical security in internet of things through energy auditing," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5224–5231, 2019.

[12.] Wilson, D. R. Reising, R. W. Hay, R. C. Johnson, A. A. Karrar, and T. D. Loveless, "Automated identification of electrical disturbance waveforms within an operational smart power grid," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 4380–4389, 2020.

[13.] P. Dutta, A. Esmaeilian, and M. Kezunovic, "Transmission-line fault analysis using synchronized sampling," *IEEE transactions on power delivery*, vol. 29, no. 2, pp. 942–950, 2014.

[14.] Sadeghkhani, M. E. H. Golshan, A. Mehrizi-Sani, J. M. Guerrero, and A. Ketabi, "Transient monitoring function-based fault detection for inverter-interfaced micro grids," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 2097–2107, 2016.

[15.] Bastos, S. Santoso, W. Freitas, and W. Xu, "Synchrowaveform measurement units and applications," in *2019 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2019, pp. 1–5.

[16.] Schweitzer Engineering Laboratories, Pullman, WA, USA, "SEL-T400L Time Domain Line Protection," <https://selinc.com/products/T400L/>, Last Access: July 31, 2020.

- [17.] Candura instruments, Oakville, ON, Canada. “IPSR intelligent Power System Recorder,” <https://www.candura.com/products/ipsr.html>, Last Access: July 31, 2020.
- [18.] D. Borkowski, A. Wetula, and A. Bien, “Contactless measurement of δ substation bus bars voltages and waveforms reconstruction using electric field sensors and artificial neural network,” IEEE Transactions on Smart Grid, vol. 6, no. 3, pp. 1560–1569, 2014.
- [19.] B. Gao, R. Torquato, W. Xu, and W. Freitas, “Waveform-based method for fast and accurate identification of sub synchronous resonance events,” IEEE Transactions on Power Systems, vol. 34, no. 5, pp. 3626–3636, 2019.
- [20.] Li, R. Xie, Z. Wang, L. Guo, J. Ye, P. Ma, and W. Song, “Online distributed iot security monitoring with multidimensional streaming big data,” IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4387–4394, 2020.