www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 12, December 2024, pp : 378-384

e-ISSN : 2583-1062
Impact Factor : 7.001

ANOMALY DETECTION IN DEFENSE COMMUNICATION

Raghuveer Singh Rathore[1], Dr. Sandeep Gupta[2]

[1]Student AI &DS Poornima Institute of Engineering and Technology, Sitapura, Jaipur Jaipur, India.

[2]Ass. Professor AI &DS Poornima Institute of Engineering and Technology, Sitapura, Jaipur Jaipur, India.

2021pietcaraghuveer039@poornima.org

sandeep.gupta@poornima.org

DOI: https://www.doi.org/10.58257/IJPREMS37503

ABSTRACT

Defence communication networks are critical infrastructures of core military operations where sensitive information is securely and reliably transmitted. Such networks face a lot of sophisticated cyberattacks, such as intrusion attempts and jamming attempts, data exfiltration, and hardware malfunctions that may jeopardize the success of any mission. Anomaly detection systems form a salient safeguard since they help identity deviations in expected behaviours from the network in order to proactively mitigate threats. Advanced machine learning and deep learning models will be used in this project for developing robust anomaly-detection mechanisms for defence communications with specific needs. They consider real-time detection, scalability, and adversarial settings of the defence environment for the operation of the robust resilience mechanism. Use of diversified datasets such as CICIDS2017, UNSW-NB15, and the KDD Cup 1999 dataset will be used for constructing the wide and strong basis for the training and testing ADS.

It covers ML algorithms, including supervised and unsupervised ones, such as Random Forests and Support Vector Machines besides K-Means clustering, and deep learning techniques that include Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs). In addition to these developments related to accuracy and robustness, some hybrid models that introduce statistical methods blended with deep learning architectures are also suggested. This work further develops insights based on the examination conducted on log files and traffic patterns recorded by different sources like Kaggle, CAIDA, and open intrusion detection datasets to outline the usefulness of these approaches toward detecting known and unknown anomalies. These have been discussed against the intricacies involved with a defence communication network.

1. INTRODUCTION

Defence communication networks are crucial to ensuring the safe and efficient forwarding of sensitive information in defence operations. Defence communication networks are the backbone of modern defence strategies, which support real-time decision-making, coordination among military units, and information sharing across geographically dispersed locations in secure ways. These networks, although critical in operation, are required to provide very high levels of reliability and security despite adverse operational conditions, including cases where the cost of failure is extreme. Defence communication networks are exposed to various challenges that compromise integrity and functionality.

Cyber attacks, whether intrusions or data breaches evolve in terms of complexity over time to target specific vulnerabilities in the network system. Jamming attacks entirely stop communication due to the saturation of signal channels. With these, hardware failures lead to unexpected downtime and loss of data. Uniqueness of defence networks including its limited computational resources, the need to operate in real time, hostile or adversarial environment has compounded the problems.

Advanced mechanisms for detection and mitigation are required so that the vital communication networks remain secure and running. This anomaly detection system has been very crucial in protecting defence communication networks. Anomaly detection monitors the activities within the network for divergences from expected patterns, thus alerting possible threats or malfunctions well in advance.

These modern ADS are being further advanced using machine and deep learning models to enhance the detection capabilities of ADS. The integration with such models will be discussed in light of the datasets, CICIDS2017, UNSW-NB15, and KDD Cup 1999, which provide full network traffic logs and anomalies for training the model. This research study utilizes supervised learning models with structures of Random Forests and Support Vectors Machines through deep learning architectures along with CNNs and RNNs as well as the hybrid approach which incorporates statistical and deep learning techniques.

The research study will particularly focus on the specific problems that appear in the defence communication paradigm by designing threefold objectives. First, it examines the critical importance of anomaly detection in defence communication networks and in-built difficulties in its operation.

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 12, December 2024, pp : 378-384
e-ISSN : 2583-1062
Impact Factor : 7.001

2. BACKGROUND AND RELATED WORK

Background and Related Work Anomaly detection in networks has long been a topic of research motivated by the need for secure and reliable data transmission. Traditional anomaly detection methods were mainly rule and signature-based. Some of these methods include intrusion detection systems, such as Snort and Bro, which are focused around pre-learned patterns of known attacks. While capable of detecting threats already known, the approaches above fail to discover new or changing anomalies, thus continuing to leave networks exposed to advanced adversarial attacks. Statistical methods-change-point detection, threshold-based analysis-did present an alternative that identified anomalies in network metrics by detecting deviation patterns. However, these methods often were not adaptive and relied on human setup, which allowed for a high false positive rate in dynamic scenarios like that of defence communication networks. Recently, this field has shifted its focus toward machine learning-based and deep learning-based anomaly detection systems.

Supervised ML models, such as Support Vector Machines and Random Forests, use labelled datasets to classify network behaviours as normal versus anomalous. Unsupervised methods like K-Means clustering and autoencoders are highly useful in situations where labelled data is scarce. However, deep learning models, especially the CNNs and RNNs, have recently proven very effective in highly accurate pattern identification for large-scale network traffic analysis, along with detecting complexities and anomalies. Hybrid approaches combining statistical methods, ML, and deep learning will further improve detection capabilities by incorporating domain-specific knowledge with insights into data-driven findings. However, such tremendous effort still pinpoints significant gaps in defence communication networks. Many existing anomaly detection techniques are designed for general-purpose networks and do not actually take into account all of the heavy demands of a defence environment, such as real-time detection, minimal computational overhead, and resistance against adversarial manipulation.

Challenges in defence communication networks

Defence communication networks operate in a class of constraints that are quite different from any civilian or commercial network. Such systems are designed to work correctly in high-stakes situations in which reliability and security are paramount.

One of the significant challenges that such networks pose is their need to identify anomalies in real-time since even a little delay in detecting and responding to these threats might have catastrophic effects on mission-critical operations. Moreover, the networks involved are generally resource-constrained, since they typically have much lower bandwidth and computational power as well as energy resources in remote or mobile deployments. The biggest challenge in creating defence communication networks is the handling of operational limitations with robust detection mechanisms. The threat landscape for defence networks is very complex and is continually evolving.

Cyber intrusions continue to be a predominant concern, with attackers now deploying advanced tactics to infiltrate systems, extract sensitive data, or disrupt operations. Jamming attacks intended to simply flood the communications channels with interference can break the network's ability to pass on information in real time. Hardware failure, caused either by physical damage, environmental causes, or aged components, also stops communication without any warning. All these threats get worse because of the adversarial nature of defence environments, where attackers specifically target system weaknesses.

To fight these challenges, advanced and adaptive anomaly detection techniques are much needed. Traditional methods fail when applied to a defence context where network behaviours have proven to be highly dynamic and less predictable.

Modern solutions based on adaptive technologies, such as machine learning and hybrid detection frameworks that learn to recognize patterns from evolving phenomena and identify new threats, are desperately needed.

Another aspect of these systems should be their ability to work within the limitations of defence networks with efficiency; they should continue to be effective in detection and mitigation of threats without overloading available resources. Integration of such sophisticated detection techniques is critically important in order to improve the resilience and reliability of defence communication networks when such threats grow ever larger.

Anomaly Detection Techniques in Defence Communication

Advanced techniques tailored to the kind of threats expected in high-stakes environments are necessary for anomaly detection in defence communication networks.

They have to be able to find a proper balance between accuracy, speed, and resource efficiency to guarantee robust protection against both known and emerging threats. The following sections explore some of the key methodologies-broadly classified into statistical approaches, machine learning techniques, and hybrid frameworks, and highlight their relevance and adaptability in defence scenarios.

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 12, December 2024, pp : 378-384
e-ISSN : 2583-1062
Impact Factor : 7.001

3. STATISTICAL METHODS

Statistical anomaly detection methods detect behaviours that deviate from normal network behaviour. Among them, **change-point detection** is precisely the method that can identify abrupt changes in the activity of the network. For example, it can pinpoint sudden surges of high volumes of traffic incoming into a network that might represent some form of DDoS attack, and by analysing time-series data through statistical models, it can quickly flag the anomalies. Similarly, **covariance matrix analysis** examines the correlations of different network metrics with packet size and transmission delay to reveal odd patterns that would be associated with intrusions or hardware malfunctions.

Machine Learning Approaches

Machine learning techniques have greatly changed the pattern of anomaly detection by allowing models to learn patterns from data.

1. Supervised Learning

The most common supervised learning models include Support Vector Machines and Random Forests. These models use labelled datasets to distinguish between normal and anomalous network behaviours. For example, datasets such as CICIDS2017 and UNSW-NB15 contain rich labels of different types of attacks which these models can make significantly accurate detection in known threats. However, supervised models are data-dependent and suffer from a limitation that it requires labels, which would be challenging to detect novel or previously unseen anomalies; this is a significant flaw in defence networks where threat vectors are always changing

2.**Unsupervised learning**

K-Means clustering and autoencoders are algorithms that use unsupervised learning in order to determine anomalies compared to the norm in the network without preexisting labels. Such techniques are crucial for defence communication networks because labelling each of the potential types of anomalies is hard to do in advance. The attacks are diverse, and rather unpredictable. For instance, autoencoders can capture normal network traffic and flag instances of anomalies. Scalability is a significant advantage of using autoencoders in real-time monitoring. 3. Semi-Supervised and Federated Learning Semi-supervised learning bridges the gap between supervised and unsupervised methods by using small portions of labelled data with substantially larger amounts of unlabelled data.

3. Semi-Supervised and Federated Learning

Federated learning also presents a decentralized framework for detecting anomalies by allowing several nodes within a defence network to collaboratively train a shared model without exchanging raw data. This guarantees data privacy and security in defence environments while detecting attacks that could be distributed, either as botnets or coordinated intrusions. Defence communication networks can make use of statistical methods-lightweight and resource-efficient-detecting along with the adaptability of machine learning and federated approaches to deploy a robust adaptive framework for anomaly detection. Techniques, individually as well as in hybrid configurations, play a vital role in filling the ever-changing threat landscape in military communication infrastructures.

Proposed Improvements or Solutions

Based on the challenges of dealing with anomaly detection in the network of defence communication, this research offers various new and improved techniques based on the continuing progress in machine learning, deep learning, and hybrid models. The novelty with such improvements relates to effectiveness in terms of accuracy detection, minimizing false positives, and optimal use of resources in real-time settings and limited resource scenarios.

One of the significant enhancements is the utilization of **hybrid detection frameworks**, adding statistical methods to machine learning and deep learning algorithms in incorporating feature extraction via PCA or SVD, in the name of powerful classifiers such as Convolutional Neural Networks and Recurrent Neural Networks for capturing both temporal and spatial anomalies in defence communication data. This layered approach provides a robust anomaly detection framework by merging the strengths of both classical and modern methodologies. Another proposed solution is the integration of **federated learning (FL)**, enabling decentralized anomaly detection across multiple defence nodes while preserving data privacy.

Because defence communication networks are rather sensitive in nature, FL ensures that raw data remains localized, with only the model parameters being shared. The decentralized method resists data breach threats while creating an opportunity for a distributed anomaly detection approach responding to both global and local threats. The FL can also tackle the defence network data's nature as not IID and maintain the efficacy of models across various environments. Optimized feature selection methods will also be of utmost importance in improving detection performance and accounting for computational constraints. Techniques like Recursive Feature Elimination (RFE), mutual information-based selection, and autoencoder-based dimensionality reduction can identify the most significant features from large datasets. These methods decrease the number of computations on resource-constrained devices while being able to pick

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 12, December 2024, pp : 378-384
e-ISSN : 2583-1062
Impact Factor : 7.001

out complex patterns reflective of anomalies. Of course, last but not the least would be the adaptive algorithm to use online learning and reinforcement learning so that the response of detection systems can be maximized.

Such algorithms can continue to adapt to evolving network behaviours and adversarial tactics so that the anomaly detection system is always strong versus unknown threats.

Integration of these developed techniques is expected to help the proposed solution build up an anomaly detection framework well suited to the stringent requirements of defence communication networks, which ensures these networks' increasing resilience and reliability in meeting these changing challenges.

Evaluation and Case Studies

Efficacy Validation of the proposed anomaly detection techniques for defence communication networks demands rigorous evaluation. It is of prime importance that diverse datasets be utilized, and performance metrics be applied appropriately to the case study or simulation of demonstrating practical applicability in defence scenarios.

Datasets Used for Testing

A variety of datasets have been utilized to train and evaluate the anomaly detection models, ensuring their adaptability and robustness in identifying anomalies in defence communication networks:

1 CICIDS2017: Realistic dataset containing a mix of normal and attacks in network traffic which contains brute force, DoS, and intrusion attempts so that anomaly detection models could be properly evaluated.

2 UNSW-NB15: This is a relatively new intrusion detection dataset, containing modern threats, botnets, worms, and exploits. Depending on the sophistication of the attacks, this dataset is a good fit for defence networks.

3 KDD Cup 1999: This is one of the more dated datasets but will provide a good baseline for testing an anomaly-based detection system against traditional network attacks.

4 Synthetic and Simulated Logs: For the purpose of tailored datasets, mimicking properties of uniqueness specific to defence communication networks, like encryption on the traffic, jamming scenarios, and resource-constrained environments; these will enable testing under certain defence constraints.

Evaluation Metrics

The performance of the proposed models is measured in terms of key parameters to meet the stringent requirements present in defence applications:

1. Detection Rate (True Positive Rate): This deals with the ability of the model in detecting anomalous events, hence high on sensitivity to threats.

2 False Positive Rate: Concerns ability of the model in keeping false alarms at its minimum levels, which is very important to defence networks due to disruption associated .

3 Precision and F1-score: Measures trade-offs between precision or correct positive predictions and recall that it provides an overall performance of the model.

4 Computational Efficiency: Calculates the use of resources such as time used in processing, memory consumption, and energy consumed in the system. Therefore the system performs well in resource-constraint scenarios.

5 Robustness: Since real-world attack is adversary in nature and noisy inputs are quite significant to the defence application, this determines whether the system is strong to survive the attack or not.

Case Studies and Hypothetical Scenarios

Several case studies and scenarios are presented to demonstrate the practical application of the proposed anomaly detection framework in defence communication networks:

1. jamming Attack Detection: Using the CICIDS2017 dataset, models are evaluated on their ability to detect disruptions in communication channels caused by signal interference. This scenario replicates real-world jamming attacks, testing the system’s ability to identify anomalies in real-time.

2. Encrypted Traffic Detection. Models are tested in the context of synthetic datasets over encrypted network traffic, thereby checking whether the anomaly detection without plaintext access holds good for a defence system.

3. Multi-Node Intrusion Detection with Federated Learning. Models federated among the nodes of an experimental defence network to determine if such a system can detect distributed attacks like botnets with preserving data privacy.

4. Hardware Failure Simulation: Scenarios where a device fails abruptly or the signal is lost are exercised to challenge the model's ability to distinguish from rather benign hardware failures and even sabotage attempts. These experiments prove the merit of the proposed framework across various defence scenarios with an appropriate balance between the detection accuracy and computational efficiency. The lessons learned from such case studies and metrics are surely the foundation for actually implementing anomaly detection systems in real-world defence communication networks.

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 12, December 2024, pp : 378-384
e-ISSN : 2583-1062
Impact Factor : 7.001

Comparison with the Existing Methods Competition

Compared to other existing methods, this anomaly detection framework for defence communication network has far improved performance based on addressing flaws in earlier approaches and tailoring adaptations to the sophisticated application of novel machine learning techniques as well as hybrid techniques tailored for defence domain demands. Rule-based and signature-based traditional systems follow a predefined attack signature, and statistical approaches might be computationally efficient but cannot present the desired adaptability to deal with the dynamic and unpredictable nature of defence communication traffic. On the other hand, ML models, namely supervised, unsupervised, and semi-supervised learning, can boost the ability of anomalous patterns, including both known and unknown. The supervised models are quite good at identifying the exact pattern of attack given that these have been trained on datasets like CICIDS2017 and UNSW-NB15. In contrast, unsupervised methods, such as autoencoders, give flexibility and the liberty of not requiring large labelled datasets, which is pretty important in environments where data labelling is impossible or not viable. Additional federated learning models that can address privacy concerns are through their functionalities in having distributed detection without the sensitive data needing to be centralized, thereby these methods are properly applied in applications in defence. One of the main trade-offs in these methods is detection accuracy with regard to the computational cost. For instance, deep models like CNN and RNNs demonstrate high accuracy in the classification of different patterns but require appreciable computer strength and seem to become problematic when in low-resource defence networks.Nevertheless, the statistical methods, along with some lightweight ML models like Random Forest and SVM, consume minimal resources with faster execution but at the expense of sacrificing some amount of precision and adaptability. In this sense, a trade-off between these approaches is proposed in the study presented herein, balancing the statistical efficiency of the algorithm with the adaptability of ML, with the high detection accuracy and resource efficiency guaranteed. Finally, employing optimized feature selection techniques like PCA and SVD further enhances the computation of efficiency in the proposed system. These methods reduce data in dimensions along with focusing on critical features only for detection while further minimizing the processing overhead. Addressing these limitations and tailoring solutions toward defence communication networks enable this framework to provide a much more robust, scalable, and adaptive solution in safeguarding mission-critical systems against evolving threats.

Applications and Implementation

The design of anomaly detection system deploying tactics in defence communication networks calls for careful designing on operational and security needs in military settings. The integration of the ADSs is very critical in these systems as they are one form of shield that covers a wide scope of potential intrusions, jamming, and hardware failure into the communication network. Proper deployment strategies ensure that the anomaly detection mechanisms are seamlessly incorporated into the existing defence infrastructure at the same time enhancing security and efficiency of operations.

Deployment Strategies in Defence Networks

Deploying Defence Network Strings ADS can be deployed at various layers within a defence network. These layers include the external layer which monitors incoming and outgoing traffic to a network to identify intrusion or unusual patterns of activity. In the inner layers of a defence network, ADS identifies anomalies that may represent an insider threat or hardware failure. Light and distributed federated learning-based ADS for mobile units or remote deployments make it possible to achieve real-time detection without the need for central data processing. The deployment of ADS in hubs or critical relay points supports continuous monitoring of all flows with high priorities - that is, the impossibility of such important anomalies being not detected.

Interoperability with Existing Defence Infrastructure

There will be interoperability between the ADS and exiting defence communication systems, thus ensuring its compatibility and effectiveness. Modern ADS solutions should integrate with the currently deployed firewalls, intrusion detection/ powers, and network management tools. This would then enable ADSs to append one more advanced layer of anomaly detection while using existing security layers. Furthermore, such systems can be tailored and customized according to the requirements of various defence networks, with the existing operations intact, as they work on the basis of APIs and modular architectures. Real-time alerts and automated responses can be set up according to the present incident response practices, therefore being processed more efficiently and promptly for threats.

Scalability and Real-Time Operation

Scalability is important in the defence network, especially because it stretches across large geographies and dynamic environments. Therefore, the ADS solution proposed must respond appropriately to various sizes of networks and different traffic loads-mostly from small tactical units to large military operations. Scalability Distributed detection models especially federated learning empower anomaly detection across the nodes without overloading central

resources. Features that include feature selection techniques and optimized algorithms are provided in order to reduce the computational requirements in scenarios of resource constraints. Real-time operation is another key feature in the deployment of ADS in defence networks. For effectiveness, real-time detection and response have been crucial as threats need to be addressed before they are too late. The proposed system used machine learning and hybrid approaches for the processing of network data traffic in real-time with minimal latency. Their proposed system achieves lightweight speed as well as in-depth deep learning analysis, one that balances both speed and accuracy, which is critical for various defence applications. Proposed solutions under ADS focus on strategic deployment, seamless integration, and scalable real-time operations and may enhance considerably the security and resilience of defence communication networks. These systems aptly detect and mitigate threats and meet every evolving modern military requirement for assured and secure communication under any circumstance.

Future Directions and Open Problems

This also applies to ADSs as systems to exploit the new and emerging technologies to meet the new challenges; just as the landscape of threats from defense communication networks continues to evolve. Further research directions for ADSs will depend on the emergence of new technologies such as quantum computing and advanced AI to further augment detection capabilities. Simultaneously, most of the open issues regarding resilience of detection systems against adversarial attacks will remain focused on searching for opportunities to improve these aspects.

Integrating Emerging Technologies

Possible future incorporation is based on the inclusion of quantum computing in anomaly detection frameworks. Such enormous volumes of information can be processed at unbelievable speeds, and this technique will help better analyse and make decisions regarding anomalies in high-traffic defence networks. For instance, quantum machine learning should be better suited for recognizing complex patterns or correlations within encrypted or noisy data sets-abilities traditional computing is not well-suited to take on in an efficient manner. This being preliminary applications of quantum technology in defence communications networks, the speed and accuracy at which anomalies are detected can be dramatically transformed. More AI development provides opportunity for performance improvement in ADS. Explainable AI (XAI) may further offer key enablers of transparency and interpretability of the detection system. XAI will allow for an explanation of why an anomaly was alerted so that the operators trust it and make quick decisions in the critical situations. This can further facilitate integration with reinforcement learning to learn from past incidents and optimized detection strategies in real time against evolving threats. Conclusion

Addressing Adversarial Attacks

Adversarial attacks have been successful in evading ADSs as well. In these attacks, an adversary modifies network traffic or data to evade detection. These attacks pose major challenges, particularly for high-stakes defence systems. For example, a sophisticated attacker may be able to inject minute variations of network behaviours that the system would miss, mimicking benign traffic that is most certainly hard to distinguish from malicious ones. To counter this, the future research efforts must have adversarial robust models. Methods such as adversarial training will build systems that are more resistant to attacks through the presentation of such detection systems with adversarial examples during their training process. A further measure that can prevent an attack from succeeding through all layers is through the hybrid methods of detection, which incorporate many methodologies: statistical methods, machine learning, and even heuristic approaches. Another open challenge exists in the scalability of adversarial defenses to be achieved with zero degradation of real-time performance. Although techniques like GANs are capable of realistically simulating a variety of potential adversarial scenarios, their computational requirements can sometimes be quite demanding in resource-constrained networks, posing important challenges to techniques optimizing deployment in real defence networks. Such directions can lead to the evolution of the field in addressing currently and emerging issues for anomaly detection in defence communication networks. New developments in quantum computing, AI, and adversarial robustness can be leveraged in building adaptive, scalable, and resilient systems that may safeguard critical defence infrastructures against future threats.

4. CONCLUSION

This paper highlights the value of anomaly detection systems in security and resilience of the defence communication network. Defence communication networks form the back-bones for military operations in real-time coordination and secure information exchange. It is, however faced by a fast-emerging sophisticated threats, such as cyber intrusions, jamming attacks, and hardware malfunctions, which can have negative impacts on mission success. By an in-depth comparison of conventional and contemporary approaches, this research demonstrates the urgent requirements for state-of-the-art adaptive and efficient anomaly detection frameworks specifically designed to meet the evolving stringent requirements of defence environments. Major findings from this research include the limitations of conventional

methods such as rule-based systems and standalone statistical method approaches, which do not evolve well towards the complex dynamic and adversarial nature of defence communication networks. One of the noticeable aspects is that it integrates ML and deep learning models like CNNs and RNNs, which improve detection accuracy and adaptability. Hybrid frameworks are much more robust and scalable than ADS systems in combining statistical methods with data-driven approaches. This enables them to work effectively in real time as well as in other resource-constrained scenarios. Federated learning also incorporates anomaly detection across distributed nodes while preserving data security due to privacy concerns, ensuring system-wide collaboration. Interesting directions for revolutionizing anomaly detection in defence networks include the integration with quantum computing and explainable AI. These technologies promise to provide speed, accuracy, and interpretability for the deployment of detection systems, areas that have bigger scopes for advancements in adversarial robustness. Key challenges- scalability of advanced techniques that need to be enabled in real-time deployments and mitigating effects of adversarial attacks-will play critical roles in the continued evolution of ADS. Conclusion: Thus, this work provides a roadmap for developing and implementing advanced kinds of anomaly detection systems in response to the requirements on the stringent defence communication network.

5. REFERENCES

[1] Thottan, M., Liu, G., & Ji, C. (2010). Anomaly Detection Approaches for Communication Networks. In Guide to Reliable Internet Services and Applications (pp. 239–263). Springer. DOI: 10.1007/978-1-84882-765-3_11.

[2] Zhang, C., Yang, S., Mao, L., & Ning, H. (2024). Anomaly Detection and Defense Techniques in Federated LearningA Comprehensive Review Artificial Intelligence Review, 57(150). DOI: 10.1007/s10462-024-10796-1.

[3] Parmar, A., Shah, K., Captain, K. M., López-Benítez, M., & Patel, J. R. (2024). Gaussian Mixture Model-Based Anomaly Detection for Defense Against Byzantine Attack in Cooperative Spectrum Sensing. IEEE Transactions on Cognitive Communications and Networking, 10(2), 499-507

[4] Saleh, H. M., Marouane, H., & Fakhfakh, A. (2024). Stochastic Gradient Descent Intrusions Detection for Wireless Sensor Network Attack Detection System Using Machine Learning. IEEE Access, 12, 3825-3835

[5] Zhou, J., Zhao, J., & Li, X. (2023). Bayesian Learning Based Defense Strategy Against Byzantine Attacks. IEEE Transactions on Information Forensics and Security, 18(3), 321-332

[6] Chen, X., & Wu, Y. (2023). Entropy-Based Weighted CSS Scheme for Byzantine Attack Detection. Journal of Wireless Networks, 29(4), 567-575

[7] Hemanand, M., et al. (2024). Glowworm Swarm Optimization for Anomaly Detection in IoT Sensors. International Journal of Computational Intelligence, 36(1), 112-128

[8] Kumar, P., et al. (2024). SG-IDS: A Stochastic Gradient-Based Anomaly Detection Framework. Journal of IoT and Cyber-Physical Systems, 11(1), 55-70.

[9] Jayalakshmi, S., et al. (2023). Cryptography Enhanced IDS for Strengthened Network Security. Advanced Wireless Communications Journal, 15(3), 123-140

[10] Ifzarne, S., & Liu, J. (2024). Cuckoo Search Optimization for WSN Anomaly Detection. Journal of Sensor Networks and Applications, 20(2), 81-93

[11] Dhanya, V., & Chitra, K. (2024). DE-Optimized XGBoost for Malicious Software Detection. IoT CyberSecurity Journal, 22(4), 56-72

[12] Taouali, A., et al. (2024). Lightweight Anomaly-Based Intrusion Detection System for IoMT Networks. Sensors and Systems Journal, 28(2), 93-108

[13] Tauqeer, M., et al. (2023). Optimized Machine Learning Models for NIDS in IoT. Cyber Threat Detection Journal, 18(1), 67-82

[14] Vinayakumar, R., et al. (2024). MQTTSet Dataset and MachineLearning Models for IoT Intrusion Detection. IEEE Internet of Things Magazine, 6(3), 45-52

[15] Almomani, I. (2024). LEACH-Based CNN-LSTM Models for Anomaly Detection in WSNs. Journal of Network Security, 19(1), 25-38

[16] Chen, Y., & Yang, Z. (2024). Spectrum Sensing and Byzantine Attack Mitigation in Cognitive Radio Networks. IEEE Communications Letters, 28(1), 45-55

[17] López-Benítez, M., et al. (2024). A Two-Stage Semi-Supervised Machine Learning Approach for Attack Detection. IEEE Systems Journal, 18(2), 215-230

[18] Saleh, H. M., Marouane, H., & Fakhfakh, A. (2024). Stochastic Gradient Descent Intrusions Detection for Wireless Sensor Network Attack Detection System Using Machine Learning. IEEE Access, 12, 3825–3838. DOI: 10.1109/ACCESS.2023.3349248.