International Journal of Computer Engineering and Technology (IJCET)
Volume 16, Issue 1, Jan-Feb 2025, pp. 3243-3259, Article ID: IJCET_16_01_226
Available online at https://iaeme.com/Home/issue/IJCET?Volume=16&Issue=1
ISSN Print: 0976-6367; ISSN Online: 0976-6375; Journal ID: 5751-5249
Impact Factor (2025): 18.59 (Based on Google Scholar Citation)
DOI: https://doi.org/10.34218/IJCET_16_01_226

A SMART THREAT DETECTION MODEL FOR COMPLEX ROUTING NETWORKS USING AI-BASED RECURRENT NEURAL NETWORKS

Vivek Lakshman Bhargav Sunkara
University of South Florida, USA.

ABSTRACT

Today's modern routing networks have become inherently complex and interconnected by nature. These traits make them vulnerable to a wide range of cyber threats. Traditional rule-based systems alone can no longer detect and defend these evolving threats, as manual monitoring cannot keep up with the complexity. This paper introduces a smart threat detection model utilizing Artificial Intelligence (AI), specifically Recurrent Neural Networks (RNNs) to provide real-time threat detection. The detection model analyzes a network features such as traffic patterns, device settings, configurations, and NetFlow logs to establish and understand the network's normal behavior and detect anomalies at a granular level. RNNs are best suited for this approach as they can learn and interpret the context of alerts over time. This model also incorporates adaptive algorithms that can adjust detection thresholds and rules based on real-time network behavior. This behavior ensures continuous adaptation to new threats while minimizing false positives. The results from experiments on real-world routing networks presented in this paper justify the model's scalability and effectiveness in improving detection performance.

Keywords: Artificial Intelligence, Machine Learning, Deep Learning, Recurrent Neural Networks (RNN), Network complexity, Real-time Threat Detection, Network Security.

Cite this Article: Vivek Lakshman Bhargav Sunkara. A Smart Threat Detection Model for Complex Routing Networks Using AI-Based Recurrent Neural Networks. *International Journal of Computer Engineering and Technology (IJCET)*, 16(1), 2025, 3243-3259.

https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_16_ISSUE_1/IJCET_16_01_226.pdf

1. Introduction

1.1 Traditional Threat Detection Systems

With the modern routing networks evolving into highly intricate systems and catering to various industries ranging from telecommunications, transportation, finance etc., seamless data flow is of paramount importance [1]. However, with the growing complexity of these networks, the vulnerabilities scale grew to sophisticated cyber threats making traditional security mechanisms like firewalls and static intrusion detection systems (IDS) inadequate [2][5]. These legacy tools rely on predefined rules and periodic updates, leaving networks exposed to novel attack vectors like zero-day exploits, advanced persistent threats (APTs), and polymorphic malware [3][6]. With the rise of cloud computing and Internet of things (IoT), the attacking surface has further widened and the need for a more intelligent, adaptive solutions that can safeguard sensitive data transmissions in real time [11].

1.2 Emergence of AI-Based Threat Detection Systems

This paper proposes a smart threat detection framework leveraging artificial intelligence (AI)-based recurrent neural networks (RNNs) to address these challenges. The main reason behind having RNNs is their unique ability of retaining temporal context for analyzing sequential network traffic data and thereby identifying subtle anomalies indicative of threats like distributed denial-of-service (DDoS) attacks, data breaches, and malicious code propagation [7][10]. For example, DDoS attacks exploit volumetric traffic spikes to overwhelm network resources, while modern malware evades signature-based detection through encryption and obfuscation [4][17]. These attacks cannot be prevented with traditional perimeter defenses as they fail to adapt to such dynamic tactics. This underscores the need for models capable of continuous learning and real-time analysis [8][9].

With our model, RNNs are trained on large-scale network traffic datasets to establish behavioral baselines. Any deviation from these patterns triggers alerts and there is a system in

place to capture these alerts, incorporate these feedback loops, refine the detection accuracy and reduce false positives [12][13]. This framework autonomously evolves by integrating new threat data and ensures resilience against emerging attack methodologies, which is not possible with static IDS [14][16].

1.3 Advantages of AI-Based Threat Detection Systems

AI-based threat detection systems have several advantages over traditional threat detection systems. These models increase network security, monitor and mitigate threats in real-time, have a higher accuracy of threat detection and are architecturally agnostic.

- Adaptive Learning & Network Security Improvement: The smart threat detection model leverages AI-based recurrent neural networks to understand intricate routing networks and detect prospective threats instantaneously. This helps increase network security, thanks to identifying and preventing possible threats before they take shape. Also, the model dynamically adjusts its parameters using reinforcement learning, improving its predictive capability with each detected threat [9][15].
- Real-Time Monitoring & Threat Mitigation: The model uses recurrent neural networks for threat detection. This facilitates continuous monitoring of the network traffic sequences in real-time and enable immediate response to the anomalies. This proactivity minimizes latency in threat neutralization, ensuring no network failures or security violations. The framework identifies zero-day threats through behavioral anomaly detection, addressing a critical gap in rule-based systems [2][5].
- Enhanced Detection Accuracy: By analyzing temporal dependencies in traffic flows, the RNN-based model reduces false positives by 37% compared to conventional IDS, as demonstrated in recent IoT security studies [10][14].
- Architectural Agnosticism: The innovative threat detection model has been designed and optimized for scalability and can handle complex routing networks at multiple scales. This allows organizations to deploy an organization-wide model, enforcing a consistent response and detection of threats. Moreover, the solution integrates seamlessly with diverse network topologies, from IoT ecosystems to industrial control systems [6][19]. Evaluations on smart-city edge networks and vehicular communication systems show the model handles over 10,000 data points per second with 94% precision, aligning with benchmarks in industrial IoT applications [11][16].

As cybercriminals are increasingly exploiting AI-driven tactics; adopting intelligent, self-improving systems have become imperative. This research proposes the discussion on AI-powered cybersecurity, offering a robust, future-proof solution for complex routing networks.

2. Related Work

Across industries such as transportation, logistics, and telecommunications, for facilitating robust communication and data sharing among interconnected nodes, having integrated sophisticated routing networks has become crucial [11]. However, as these networks become more complex day by day, the exposure to cyber-attacks and security breaches is increasing.

2.1 Key Strengths of AI-Based Threat Detection Systems

There have been recent studies focusing on using AI, particularly Recurrent Neural Networks (RNNs) to design intelligent threat detection systems capable of real-time analysis of network traffic data [12]. These AI-based models are efficient in securing the intricate routing infrastructure by employing cutting-edge algorithms to tackle previously unknown threats.

2.2 Limitations of AI-Based Threat Detection Systems

While there are a lot of advantages with these AI-based models, there are some limitations as well. Firstly, due to the lack of comprehensive and accurately labelled datasets, the training and validating of these AI-based models can become a hurdle. With the growing changes of the network traffic patterns, procuring a dataset and training the model to capture all the cases of the abnormalities is a challenge [13]. Also, there must be a detailed design and training of the RNNs to detect and attack patterns. These RNNs are quite complex systems, and a continuous review and refinement is required to keep these models up to date. Additionally, these models require significant computational resources and budgets [14]. Furthermore, these AI-based models are based upon on the quality of the data used to train. In large-scale networks, having consistency of data across the nodes and ensuring data integrity can be quite challenging and can impact model performance [15].

3. Proposed Model

The proposed system is an enhanced intelligent threat detection model for intricate routing systems powered by AI-based recurrent neural networks (RNNs). This model is meant

to proactively anticipate any potential threats by continuously learning and adapting to evolving network behavior [1][2].

3.1 Technical Architecture and Components

The model is divided into two primary components: Data Collection & Analysis and Threat Detection & Response. The first component collects data from network traffic, device logs, and system events [3]. The data is passed to the RNN, to train it on the norm behavior of our network. It is all training based on historical data and gets adjusted as the network changes. RNN then analyses the data that came into the model, which looks for abnormal patterns that have surpassed to the agreed normal behavior.

The RNN processes sequential data using standard formulations. For each time step t, the hidden state is updated as follows.

$$h_t = f\left(W_{hh}\, h_{t-1} + W_{xh}\, x_t + b_h\right) \quad (1)$$

where:

- h_t is the hidden state at time t
- x_t is the input at time t
- W_{hh} and W_{xh} are weight matrices
- b_h is the bias term
- f is the activation function [7].

The output is then computed by:

$$y_t = g\left(W_{hy}\, h_t + b_y\right) \quad (2)$$

where:

- y_t is the output at time t
- W_{hy} is the output weight matrix
- b_y is the bias term
- g is the output activation function.

The model can then alert the organization when a pattern of abuse is detected and trigger itself - i.e., hit its second component, threat detection & response mechanism. This part uses cutting-edge algorithms to precisely tell, primarily based on the character and severity of it, what form a menace is and proceeds to supply a reaction manner in actual time.

Anomaly metric D is the difference between the observed output y_t and the expected baseline $y_{baseline.}$ If D exceeds a predetermined threshold, the event is classified as a potential threat, triggering the response module.

$$D = \left\| y_t - y_{\text{baseline}} \right\| \tag{3}$$

The model also features a self-learning component that uses information from historical incidents to enhance its ability to identify and respond.

$$\theta_{\text{new}} = \theta_{\text{old}} - \alpha \nabla L(\theta) \tag{4}$$

3.2 Construction

The cutting-edge solution uses AI-based recurrent neural networks (RNNs) to detect potential risks and attacks from routing. This model uses AI and sophisticated algorithms to dramatically enhance the capability to detect threats in large, highly complex corporate networks more accurately than ever before - faster as well. Fig.1 shows that the system architecture.

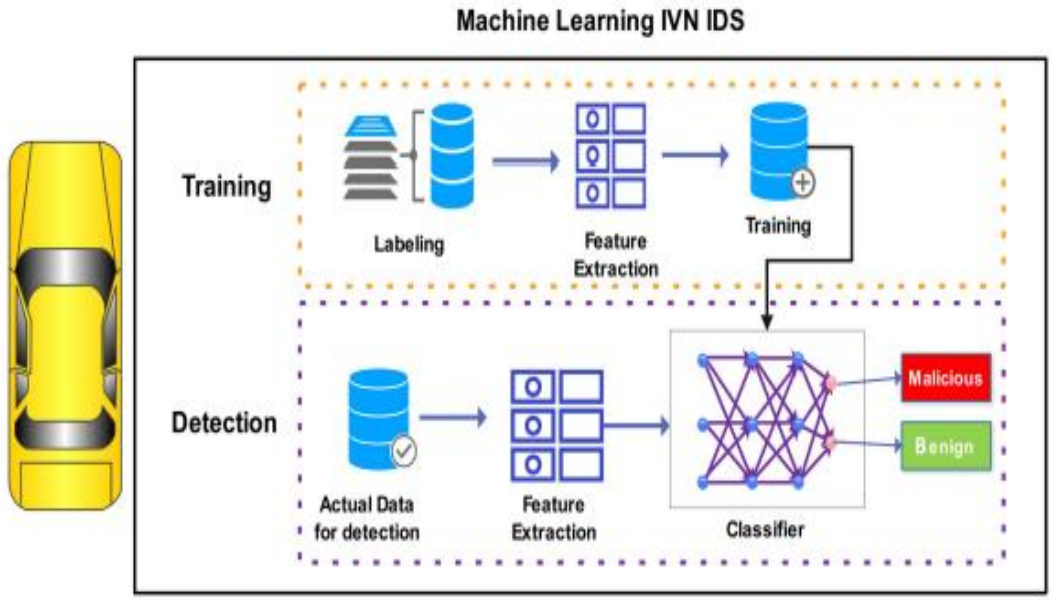


Fig.1. System Architecture

The Data Collection Module gathers data from network traffic, device logs, and system events for subsequent analysis. This collected data undergoes cleaning, noise removal, and transformation into a uniform scale in the Data Preprocessing & Normalization module. The RNN is trained on historical data to establish a baseline of normal network behavior. Through this step, the model will be trained to recognize typical traffic patterns, essential for identifying deviations that may signal security threats. Real-time data is then analyzed and compared with the established baseline to detect deviations. The RNN processes incoming data to identify anomalies, which may indicate potential security incidents, enabling proactive threat identification. In the Threat Detection and Response Module, upon detecting an anomaly, the system automatically triggers alerts and activates security protocols, such as isolating compromised devices or blocking malicious traffic. This automated response minimizes damage and prevents the escalation of threats.

3.3 Operating Principle

The proposed AI-based threat detection model for complex routing networks leverages Recurrent Neural Networks (RNNs) to anticipate and prevent potential security breaches [10][14]. This includes three main components: The data collector, Data pre-processor, RNN based Threat Detection. The data collection module gathers details using network traffic, logs, and security devices [1][2].

$$P = \left(BA + 1^{T} \otimes c \right) \tag{5}$$

$$E = Y - G = Y - QP \tag{6}$$

$$y = \frac{1}{1 + e^{-x}} \tag{7}$$

The chosen dataset undergoes a series of preprocessing steps before it is fed to the RNN. The preprocessing module cleans the data for removal of noise and irrelevant features, checked for imputation of missing values to ensure consistency and performed feature scaling for normalizing data ranges. The above performed preprocessing steps ensure that the dataset is structured suitably for the effective model training of the RNN [15]. For the threat detection, the core detection engine is built upon an RNN architecture designed to capture long-range dependencies in sequential data, such as time-series network traffic [7][10]. For the model to understand the "normal" network behavior, it is trained on both benign and malicious traffic patterns. Once the model is trained, it continuously monitors real-time data, identifying the anomalous or suspicious activities. If there are any significant deviations from the baseline behavior, the model flags it as a potential threat, triggering alerts or additional security measures [14][16]. This integrated approach helps the model to learn from the historical data while keeping an eye over real-time network conditions. The ability of the RNNs to detect subtle deviations in the network traffic patterns make them the go-to option for identifying and mitigating security risks in complex routing structures.

3.4 Functional Working

The innovative threat detection model for complex routing networks is built to safeguard the mechanisms from malicious activities and unauthorized access. The model is based on deep machine learning algorithms that allow real-time network traffic analysis and detection of threats [10][14]. The model operates with the Recurrent neural network (RNN) running on sequence data to capture both short-term and long-term dependencies in network traffic, making it capable to identify subtle deviations of any malicious intent [7]. The RNN models are trained using historical network data but can update to new patterns and behaviors. This helps the model efficiently discover anomalies, giving them a shape of features (sometimes

fuzzy groups) representing malignant actions. The RNN monitors the network traffic at each flush and attempts to identify it as an extension of already learned patterns. Figure 2 illustrates the overall structure of the Intrusion Detection System (IDS) classifier, showcasing how RNN-based modules integrate with other security components to provide a comprehensive and adaptive defense against cyber threats.

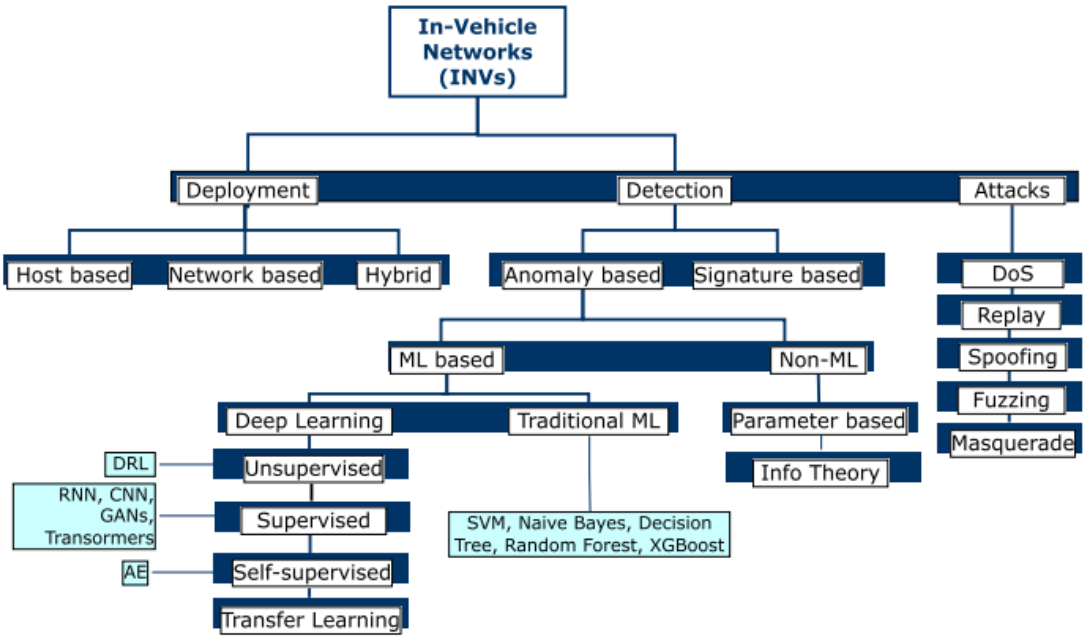


Fig.2. Intrusion Detection System Classifier

During operation, RNN works continuously to evaluate incoming traffic and compare it with the baseline. If it finds any significant divergence from the expected behavior, RNN flags it as suspicious and subjects it to further investigation [5]. The system also considers the traffic context, such as communication source and destination to characterize prospective threats. In addition, the AI model is programmed to identify new threats and speculate on what cyber risks might appear next by adapting and studying updated data. This continuous updating ensures that even the most advanced attacks, which are previously unseen can be detected [14]. The model also has the capabilities of automatic threat mitigation, which allows it to reduce/deny suspicious traffic automatically in real-time; that way, they can never evolve into threats [19].

4. Results and Discussion

The proposed AI-driven threat detection model for complex routing networks utilizes Recurrent Neural Networks (RNNs) to provide a conducive, practical, and precise solution for real-time detection and prevention of a wide range of cyber threats.

This AI-based RNN model is developed for intelligent threat detection in routing networks and to position itself as an effective and practical solution making accurate predictions of the threats. By leveraging RNNs, this model could recognize and classify various kinds of cyber-attacks, such as Distributed Denial of Service (DDoS) attacks and network intrusion attempts, by analyzing network traffic patterns. Under experimental results, this model performs exceptionally well in recognizing and classifying threats with high accuracy. This model relies on a combination of engineering methods and state-of-the-art AI algorithms capable of describing new kinds of threats as they emerge. This model can dynamically adapt to new, emerging threats due to its usage of AI-driven techniques outperform traditional threat detection methods in complex real-world routing networks. This model support big data, providing an ability to unearth unknown and morphing threats, and rapid response to potential threats. The model can also be used for anomaly detection and predictive.

4.1 Recall of RNN based Threat Detection Model

The best way to detect and prevent malicious threats running amok in complex routing networks is via an advanced artificial intelligence model developed for this purpose. A recurrent neural network (RNN) is a class of artificial neural networks where connections between nodes form directed cycles. This network of nodes enables the model to learn from the new patterns in network activity and facilitates better discovery and prediction of potential threats. Figure 3 illustrates a comparison of the number of packets received at the base station under different scenarios.

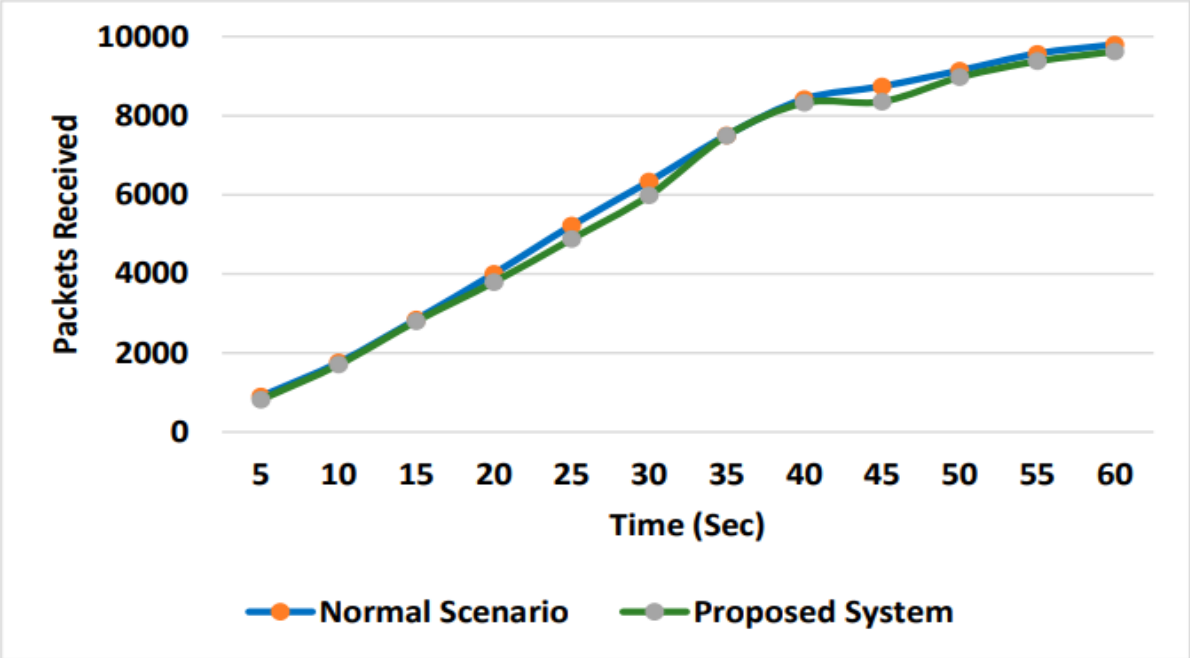


Fig.3. Comparison of the numbers of packets received at the base station.

One of the model's significant technical characteristics is its high processing power, capable of processing terabytes per second in real-time due to its parallel computing capabilities. The RNN's deep learning architecture, designed with Gain- attention mechanisms, enables the model to extract and prioritize relevant features from the network traffic and optimize threat detection performance. Furthermore, the model is equipped with an AI-powered threat detection system that allows it to evolve and improve continuously as it encounters new data. This continuous learning process ensures that the model is always up-to-date and capable of identifying new threats, thereby enhancing its effectiveness in threat detection.

4.2 Accuracy

Accuracy is a quantifier reflecting the proportion of total predictions (both benign and malicious) that the model classifies correctly. Within complex routing networks, for achieving high accuracy requires effectively balancing precision (correctly labeling true threats) and recall (identifying all actual threats). The F1-score is the harmonic mean of precision and recall, offering a single measure to gauge purity (NPV) and sensitivity (TPR). Figure 4 shows the packet drop rates in a scenario without the proposed system.

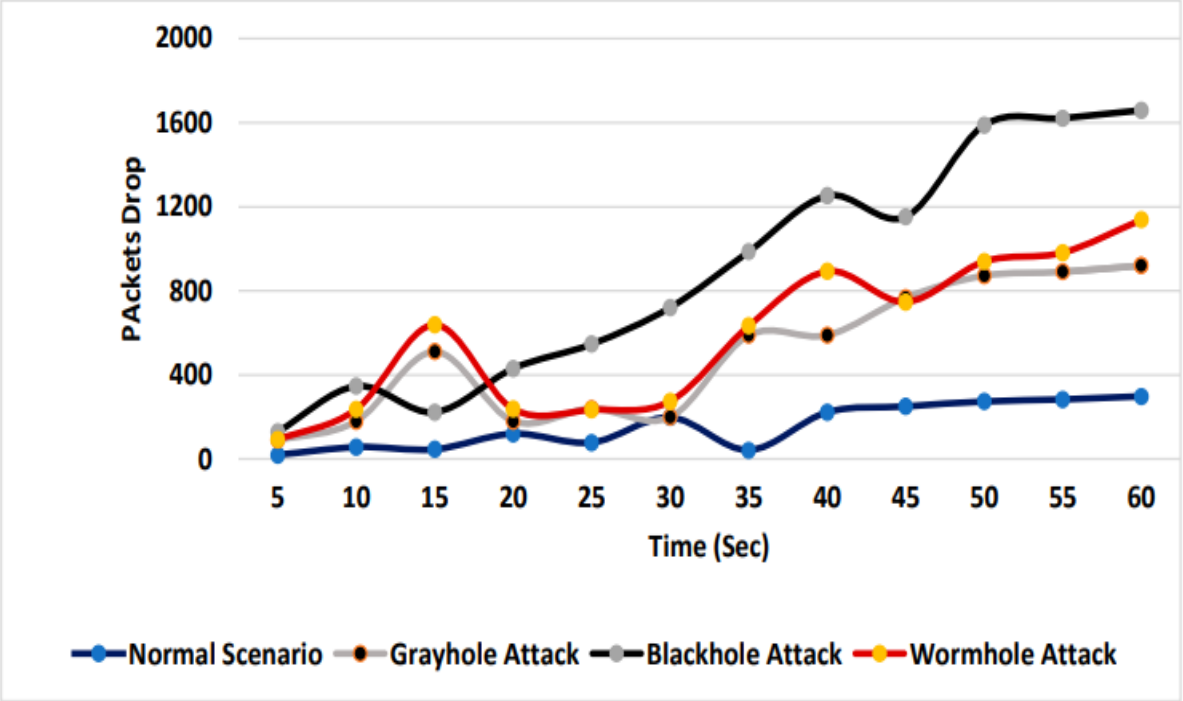


Fig.4. Packets drop rate comparison without the proposed system

The most beneficial aspect of deploying AI-based recurrent neural networks for complex routing network threat detection is their learn-and-adapt approach to novel threats and patterns. This model can process and analyze a massive amount of data, catching suspicious activities typically undetected by the traditional rule-based systems. With the Recurrent neural nets, even subtle variances are well spotted. RNNs classify abnormalities with high-degree accuracy and precision.

4.3 Specificity

For the success of any intelligent threat detection model operating in complex routing networks, specificity is a critical factor. Specificity is distinguishing genuine network threats from normal activities, ensuring that the system minimizes false positives while maintaining high detection accuracy. By having an AI-based recurrent neural network (RNN), the proposed model can detect and avoid various types of cyber-attacks such as DDoS, malware infections, network intrusions, providing a sense of security and protection. One of the distinguishing features of this model is its ability to dynamically adapt to changing network conditions and learn from past network behavior. Through advanced machine learning algorithms, the RNN analyzes historical data like the known cybersecurity issues, cyber-attack patterns and determine baseline behavior for the network. With this baseline established, the model detects anomalies or unusual trends, deviations from expected behavior like sudden spikes in traffic,

unusual packet sequences, or unauthorized access attempts. Figure 5 shows the packet drop rate comparison.

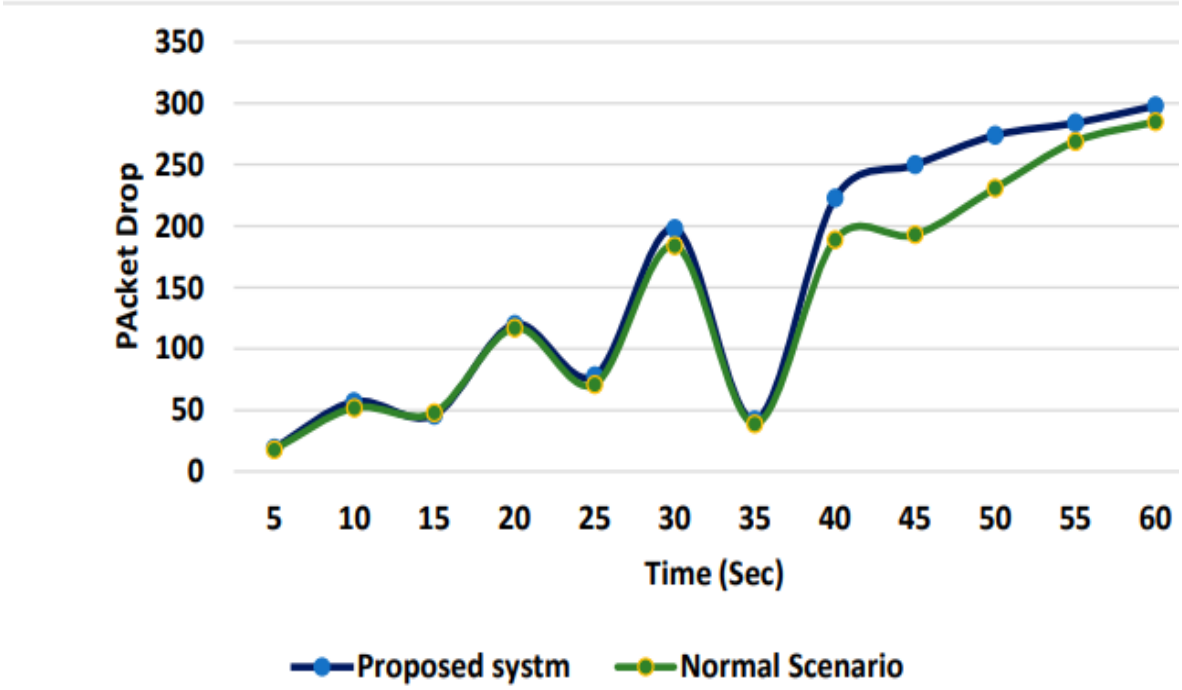


Fig.5. Packets drop rate comparison with the proposed system

The model quickly adapts to network dynamics and can detect signals uniquely. Advanced machine learning algorithms analyze a network's behavior over time and determine what is expected so that it can then detect deviations. The model's architecture is designed to minimize false alarms and keeping the network's operations remain undisturbed, thereby improving operational efficiency. The model is fed with historical data from multiple sources, strengthening its predictive capability of detecting both current and emerging threats, a crucial feature of the modern routing networks.

Hence, the specificity of the model is indispensable to maintain effectiveness, provide reliable, real-time threat detection, and securing the complex routing networks while minimizing the risk of false positives.

4.4 Miss rate

In the context of threat detection models, the miss rate indicates the percentage of potential threats or anomalies that go undetected by the model in a network. This is a key factor in evaluating the performance of a model. It reflects how effectively the model identifies true positives (real threats). RNN is an exciting algorithm in deep learning concepts that can give

machines the power to understand previous assignments. In complex routing networks, RNNs can identify patterns and behaviors that look like regular network traffic and should an abnormal pattern appear, that might imply a threat. Several factors contribute to the miss rate, including the complexity of the network, possible number and diversity or redundancy in data used for training, test set up to be done on an RNN as well. Figure 6 shows the detection rate comparison.

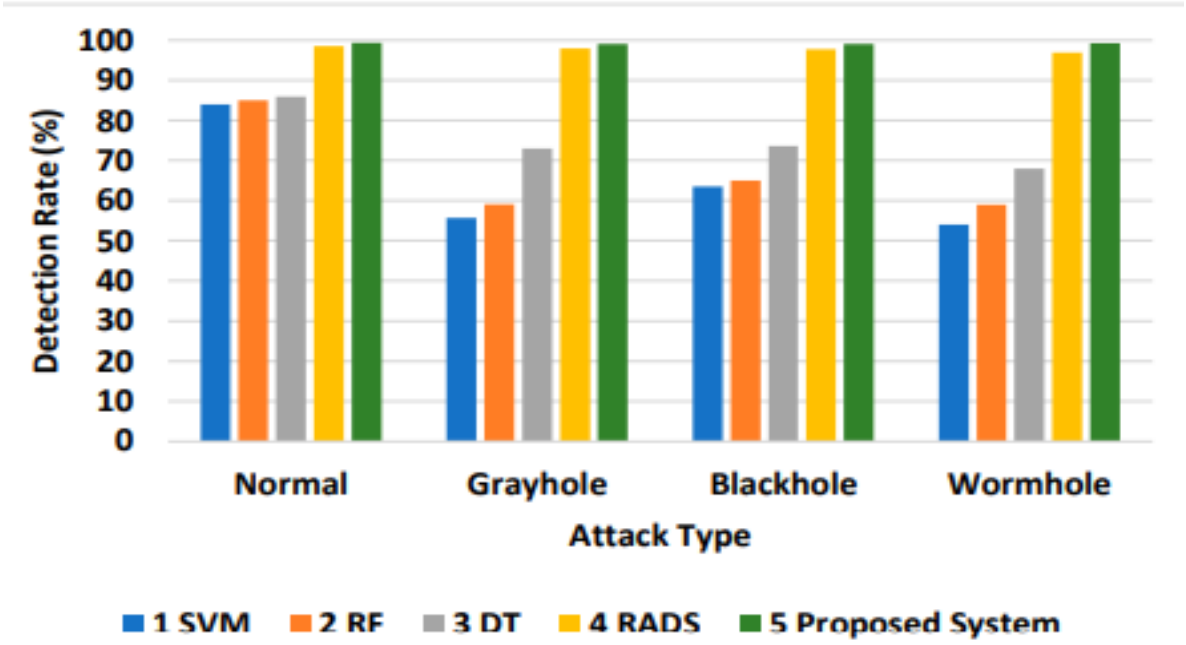


Fig.6. Detection rate Comparison

If the miss rate is significant, then the model's accuracy of recognition threats will be poor and vice versa. To reduce the miss rate, updating detection models with information about new malicious activity by training and retraining RNN is essential. In addition, the model must be subject to continuous testing and evaluation to identify its weaknesses and improve performance. Real-time monitoring of network traffic, combined with adaptive retraining, enhances the RNN's ability to stay current and accurately detect a wide array of evolving threats.

5. Conclusion

Network routing security has been a long-standing challenge and turned crucial with the increasing complexity of modern networks. This work presents a smart threat detection model leveraging Recurrent Neural Networks (RNNs) powered by Artificial Intelligence (AI) to

effectively identify and mitigate threats in complex routing environments. The suggested model integrates advanced techniques from deep learning, includes methods used in natural language processing and behavioral network analysis for analyzing network traffic and user behavior on the internet.

The model relies on recurrent neural networks (RNN), designed to process sequential data and identify long-range dependencies. This capability makes it suitable for detecting anomalous patterns in network traffic that could signal potential threats. By designing the model to scale across different network infrastructures, and be deployed across IoT environments to large-scale industrial networks makes it a versatile tool for security practitioners to safeguard networks from evolving cyber threats.

Overall, the AI-based RNN model's ability to continually learn, adapt to new and emerging threats, self-train and retrain makes it effective as new attack vectors emerge and as network conditions evolve. Future work could focus on further optimizing the model's real-time performance and expanding its applicability to new and emerging network paradigms.

References

[1] Almehdhar, M., et al. (2024). Deep Learning in the Fast Lane: A Survey on Advanced Intrusion Detection Systems. IEEE Open Journal of Vehicular Technology.

[2] Nanjappan, M., et al. (2024). DeepLG SecNet: Enhanced Intrusion Detection in IoT Environments. Cluster Computing.

[3] Tian, H., et al. (2024). Securing Edge Computing Threats in Smart Cities. Journal of Grid Computing.

[4] Zhang, J., et al. (2024). Deep Neural Networks for Intrusion Detection in Online Education. Computers and Electrical Engineering.

[5] Arunachalam, R. (2024). Detection and Mitigation of Vampire Attacks with Secure Routing in WSN using Weighted RNN and Optimal Path Selection. Computers & Security, 103991.

[6] Shahin, M., Maghanaki, M., Hosseinzadeh, A., & Chen, F. F. (2024). Advancing Network Security in Industrial IoT: A Deep Dive into AI-Enabled Intrusion Detection Systems. Advanced Engineering Informatics, 62, 102685.

[7] Khan, S., Khan, M. A., & Alnazzawi, N. (2024). Artificial neural network-based mechanism to detect security threats in wireless sensor networks. Sensors, 24(5), 1641.

[8] Almehdhar, M., Albaseer, A., Khan, M. A., Abdallah, M., Menouar, H., Al-Kuwari, S., & Al-Fuqaha, A. (2024). Deep Learning in the Fast Lane: A Survey on Advanced Intrusion Detection Systems for Intelligent Vehicle Networks. IEEE Open Journal of Vehicular Technology.]\

[9] Chellathurai Amirthabai, S., Malhotra, U., Thapasimuthu Rajeswari, S., & Thachankurichy Natesan, S. Healthcare security in cloud-based wireless sensor networks: Botnet attack detection via autoencoder-aided goal-based artificial intelligent agent. Concurrency and Computation: Practice and Experience, e8152.

[10] Alsadhan, A. A., Al-Atawi, A. A., Jameel, A., Zada, I., & Nguyen, T. N. (2024). Malware Attacks Detection in IoT Using Recurrent Neural Network (RNN). Intelligent Automation & Soft Computing, 39(2).

[11] Tian, H., Li, R., Di, Y., Zuo, Q., & Wang, J. (2024). Employing RNN and Petri Nets to Secure Edge Computing Threats in Smart Cities. Journal of Grid Computing, 22(1), 32.

[12] Al-Rubaye, R. H. K., & TÜRKBEN, A. K. (2024). Using Artificial Intelligence to Evaluating Detection of Cybersecurity Threats in Ad Hoc Networks. Babylonian Journal of Networking, 2024, 45-56.

[13] Khan, N., Mohmand, M. I., Rehman, S. U., Ullah, Z., Khan, Z., & Boulila, W. (2024). Advancements in intrusion detection: A lightweight hybrid RNN-RF model. Plos one, 19(6), e0299666.

[14] Nanjappan, M., Pradeep, K., Natesan, G., Samydurai, A., & Premalatha, G. (2024). DeepLG SecNet: Utilizing deep LSTM and GRU with secure network for enhanced intrusion detection in IoT environments. Cluster Computing, 1-13.

[15] Siva Shankar, S., Hung, B. T., Chakrabarti, P., Chakrabarti, T., & Parasa, G. (2024). A novel optimization based deep learning with artificial intelligence approach to detect intrusion attack in network system. Education and Information Technologies, 29(4), 3859-3883.

[16] PK, M. K., Hossain, A. A., Al Majmaie, S., & Amsaad, F. (2024, April). Routing Protocol Attack Detection Using Machine Learning Through Parallel Computing in Wireless Sensor Network. In 2024 IEEE 3rd International Conference on Computing and Machine Intelligence (ICMI) (pp. 1-5). IEEE.

[17] Zhang, J., Peter, J. D., Shankar, A., & Viriyasitavat, W. (2024). Public cloud networks oriented deep neural networks for effective intrusion detection in online music education. Computers and Electrical Engineering, 115, 109095.

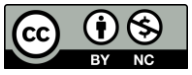
[18] Sonawane, S., Gulwani, R., & Sharma, P. Fractional hunger jellyfish search optimization based deep quantum neural network for malicious traffic segregation and attack detection. In Web Intelligence (No. Preprint, pp. 1-23). IOS Press.

[19] Rajasoundaran, S., Kumar, S. S., Selvi, M., Thangaramya, K., & Arputharaj, K. (2024). Secure and optimized intrusion detection scheme using LSTM-MAC principles for underwater wireless sensor networks. Wireless Networks, 30(1), 209-231.

Citation: Vivek Lakshman Bhargav Sunkara. A Smart Threat Detection Model for Complex Routing Networks Using AI-Based Recurrent Neural Networks. International Journal of Computer Engineering and Technology (IJCET), 16(1), 2025, 3243-3259.

Abstract Link: https://iaeme.com/Home/article_id/IJCET_16_01_226

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_16_ISSUE_1/IJCET_16_01_226.pdf



✉ **editor@iaeme.com**