Babylonian Journal of Networking
Vol.2024, **pp**. 45–56
DOI: https://doi.org/10.58496/BJN/2024/006; ISSN: 3006-5372
https://mesopotamian.press/journals/index.php/BJN

Research Article

Using Artificial Intelligence to Evaluating Detection of Cybersecurity Threats in Ad Hoc Networks

Rasha Hameed Khudhur Al-Rubaye [1,*], AYÇA KURNAZ TÜRKBEN [1]

[1] *Electrical and Electronics Engineering dep Istanbul, Turkey.*

ARTICLE INFO

Article History

Received 08 Feb 2024
Revised 19 Mar 2024
Accepted 09 Apr 2024
Published 30 Apr 2024

Keywords

cybersecurity
MANETs
Anomaly detection
CNN algorithm
RF algorithm
Threat detection
Security performance

ABSTRACT

This paper is devoted to the use of AI managed to contribute to security of the MANETs (Mobile Ad-hoc Networks), decentralized and mobile wireless networks, that are fully dynamic in nature. The intention of the research is to audit the dangers of cyber and to spot the variety of cyber threats types, including Distributed Denial of Service (DDoS) attacks, malware intrusions, leakages or data breaches, or unauthorized access attempts, using AI-powered algorithms and models. The purpose is to obtain higher degree of veracity of defining and classifying these threats and as result puts more security and reliability to MANET networks. Anomaly detection addressed as a secondary line of defense specific for MANET hardware and network traffic. The monitoring method is needed here to find abnormal behavior that might anyhow signify the possible security flaws or the attacks of the MANET environments. This ultimate goal is penetrated with the timely detection Peculiarities, which makes possible to reinforce MANET security capabilities that require to be well-developed against cyber threats. Experimental results reveal a clear trend of Fleet Grid Algorithm Improvements along with Detection Accuracy (Digital Signals and Anomaly) by means of training AI models (CNN and RF) with algorithms like Random forest and Convolutional neural networks. The machine learning based algorithms often present remarkable results comprising efficiency in detecting and effectively categorizing different cyber threats existing such as DDoS attacks, malware infiltrations and attempted unauthorized access. This method of anomaly detection is able to accurately detect robot anomalies and malicious activities in network traffic in addition to we preventing system vulnerabilities or threats from occurring prematurely. Besides, the findings of this study wide relatively efficient AI-based cybersecurity systems for dynamic decentralized MANET systems, which are developed for street-view switching and path finding, self healing and self configuration.

1. INTRODUCTION

In the present hyper-connectivity scenario, there is a huge expansion of both mobile devices and wireless networks that have ensured the emergence of Mobile Ad-hoc Networks (MANETs) which are of paramount importance in such areas as military missions, humanitarian aid, and emergency response [1-3]. MANETs are Cyclical and decentered characterized by Direct communication among nodes without Centralized infrastructure facilities. Although MANETs, with its flexibility and high resilience, specifically pose different security challenges, traditional security mechanisms within static networks may not applicable in these rapidly changing and dynamic networks.

Cybersecurity in MANETs presents a very important matter as much because of the urgency of data transmitted over these networks and the potential security threats, as well as due to the data nature [7,8]. Modern security measures including firewalls and intrusion detection systems are sub-optimal because they cannot respond to the dynamic topology of MANETs and resource constraints [8]. Consequently, there is a real rising need for creative ways to enhance cybersecurity in MANETs and shake down the risks arisen by cyber threats.

To solve these problems, this paper is dedicated to investigate whether an AI could be the right candidate for the cyber security of MANETs. More specifically, this involves working on designing and distributing AI-enabled detection algorithms and models against threats and anomaly detections in mobile ad hoc network (MANET) environments. To this end, we are set to enhance the robustness of MANETs by implementing AI-powered technologies like machine learning and deep learning. These will help us increase the precision and speed of cybersecurity measures of this type, consequently enhance overall security stance. Cyber security challenges, as depicted in Fig. 1, encompass both cyber crime and cyber warfare, requiring a comprehensive approach to tackle them.

*Corresponding author. Email: 213721418@ogr.altinbas.edu.tr

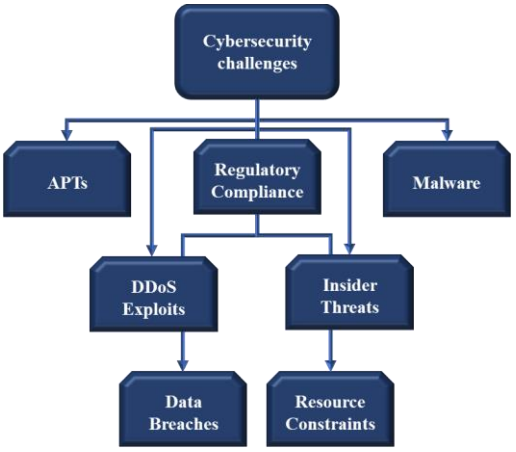

Fig. 1. cyber security challenges.

The rest of the paper is organized as follows: Section 2 provides an overview of the related work in the field of cybersecurity in MANETs. Section 3 presents the methodology and approach used in this study, including the design and implementation of AI algorithms for threat detection and anomaly detection. Section 4 discusses the results of the evaluation of the proposed approach. Finally, Section 5 concludes the conclusion and future research in this area.

2. RELATED WORK

Nowadays the discussion of the cyber security problem in Mobile Ad Hoc Network has become very important as an increasing number of mobile devices are used in MANETs in our lives. Several researches have concentrated on the facing the many security challenges conferred by MANETs and also proposing the idea of novel ways of cybersecurity with the dynamic and decentralised networks in mind [9-11].

A cybersecurity area with a focus on MANET is studying of a uniquely constructed intrusion detection system (IDS) for MANET network environments. The IDS of traditional systems varies with their supporting infrastructure. These IDSs are static, they require the existence of a centralized infrastructure and they are suitable for prioritizing the static network topology over the dynamic one. Hence, back-up, distributed and lightweight IDSs are adopted that are capable to adapt to the dynamic nature MANETs, and will be efficient in detecting different threats and vulnerabilities. One case in point is that the distributed intrusion detection system by the game theory of Li et al. [9] was suggested for MANETs. The model runs a game theory analysis of the number of links and hubs and determines all the possible attempts for malicious activity. Likewise, the authors [10] Zhang et al. showed how a lightweight intrusion detection system can be based with machine learning techniques for MANETs. The system utilizes machine learning algorithms to investigate the traffics of networks, and the algorithms are able to know the anomalies that show attack techniques.

Moreover, designing the use of anomaly detection methods for deviant conduct detection are searvengine items of study in MANET. Detection of anomalies can be drawn upon identifying the new or existing security risks not yet known in MANETs in advance. The authors Goyal, et al. [11] put forward an anomaly detection scheme, which is based on analyzing deviations from the baseline traffic patterns by means of statistical analysis. The model, by identifying things that are out of the ordinary compared to what is expected, draws the attention of system administrators to suspicious irregularities that could be about attacks.Besides attack detection and logical detection, researches also have worked on establishing secure routing protocols for mobile ad hoc networks (MANETs). Route protocols are very crucial for MANET [12,13] since the way data packets are routed between entire nodes or just parts of it is determined with the aid of routing protocols. A number of works that have been proposed secure routing protocols tha can resist several types of attacks, for example black hole defects, wormholes and Sybils attacks.

Another example is that Karlovic and Wagners [12] SEAD routing protocol, which cryptographic methods are used to protect routing messages, and in this way, disruption of malicious attackers is prevented. Also, Hu et al. [13] created the Secure Multipath Source Routing (SMSR) protocol which exploits the tools of numerous routes to transmit data packets that pinpoint and bypass infected or deceptive nodes. The field of cybersecurity has seen a tremendous progress in research that aimed to address the security risks that stemmed from the very nature of wireless networks that are dynamically changing and have no centralized management infrastructure. Through leveraging breakthrough intrusion detection systems, anomaly detection techniques, and secure routing protocols, researchers are pursuing an objective of strengthening MANETs cybersecurity

posture along with guaranteeing functional robustness and smooth information flow of these networks in various applicational environments. Table 1: In MANET, types of attack and description (in network) are discussed [14].

TABLE I. TYPES OF ATTACKS IN MANET ENVIRONMENT AND DESCRIPTION IN NETWORK.

Categories of Attacks	Type of Attack	Describe in Network
Attacks Probe	Mscan, portsweep, and Security Administrator Tool for Analyzing Networks (satan), as well as Network Mapper	Not
user-to-root Attacks	Httptuneel, Sqlattack, and Loadmodule, as well as rootkit	Vital
remote-to-local Attacks	Worm, SNMPgeattack, and imap, as well as warezmaster	Vital
denial-of-service Attacks	Processtable, and User Datagram Protocol, as well as Neptune	Not

3. METHODOLOGY

This part presents a comprehensive methodology to address the research problem of enhancing cybersecurity in Mobile Ad hoc Networks (MANETs) through the integration of Artificial Intelligence (AI) techniques. The methodology outlines the systematic approach taken to achieve the stated objectives, including study design, data collection, AI model training, and evaluation metrics.

3.1 Study Design

1) Explanation of the Study Approach

The research plan includes the creation and assessment of an autonomous Intrusion Detection and Prevention System (IDPS) with the aim to provide protection in a simulated MANET by using artificial intelligence. The setting in which researchers train AI algorithms (e.g., Convolutional Neural Network (CNN) and Random Forest (RF)) and measure their ability is simulated by using experimental data. There will be stages involved in the setup such as network model generation, data generation, model training, evaluation, and finally the performance assessment. Table 2 reveals experiment configuration.

TABLE II. EXPERIMENTAL SETUP FOR AI-BASED INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS) IN SIMULATED MANET ENVIRONMENT.

Experiment	Description
Network Model Creation	Develop a simulated MANET network model to serve as the foundation for generating network data.
Data Generation and Attack Simulation	Generate data reflecting normal network behavior and simulate DDoS attacks for training and evaluation.
Model Training	Train AI algorithms, such as Convolutional Neural Network (CNN) and Random Forest (RF), using the generated data to learn patterns indicative of normal network behavior and cyber attacks.
Model Evaluation	Evaluate the trained AI models using metrics such as accuracy, recall, precision, and F-measure to assess their effectiveness in detecting and preventing cyber threats in MANETs.
Performance Assessment	Assess the performance of the developed IDPS in terms of its ability to detect network attacks, provide anomaly detection, ensure real-time response, optimize resource efficiency, and preserve privacy within the MANET environment.

2) Explanation of the Selected Study Method

The experimental approach is chosen to rigorously evaluate the performance of the AI-based IDPS under controlled conditions. It enables the replication of tests for reliability and validity and allows for the identification of causal linkages between the deployed IDPS and its impact on improving network security in MANETs.

3) Description of the Structure of the Methodology

The approach is a systematical will be to determine the IDPS performance as an improvement of the MANET security is through structured stages, such as the Network Model Creation, Data Generation, Model Training, and Performance Assessment. AI models are being trained and evaluated in terms of metrics, including accuracy, recall, precision, and F-measure, to see to what extent they are suitable for the detection and prevention of cyber attacks.

4) Creating a MANET Model, Simulating DDoS Attacks, and Implementing an IDPS with AI Algorithms

This implementation involves getting MANET data for drooping and splitting these data into training and testing sets. Also, modelcrafting AI algorithms CNN and RF is an implementation step. The performance of the trained models will be

measured using the modified confusion matrix and performance metrics such as accuracy and MSE. Figure 2 is a flowchart that shows how the structured approach method is planned.

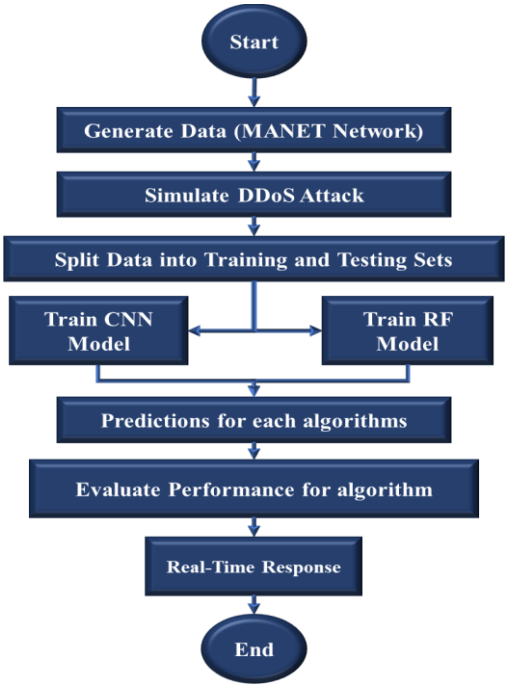

Fig. 2. Flowchart to describe the structured methodology

3.2 Data Collection

The paragraph after specifies the gathering of information for the project's laboratory setup which will include and feature an AI-based Intrusion Detection and Prevention System (IDPS) within a Mobile Ad hoc Network (MANET) simulated environment. The data collection process includes three main steps: It will demonstrate a protocol for the MANET network creation, a set of the simulated network data, and the DDoS attacks simulations.

1. MANET Network Model Creation Process: The MANET network model enacts the relational pattern and de-centralized existence of real-world MANET environments. This method implies defining the number of nodes (devices), determining their connectivity and the definition of parameters of the network including transmission area and dynamic characteristics.
2. Data Generation Process for the MANET Network: Afterwards we will form a network model for a manet and create synthetic data to show us the network traffic and behaviour. This covers data transformation that represents protocol messages, communication connections, and network activity of devices of MANET.
3. Simulation of DDoS Attack on the MANET Network: DDoS attacks are imitated on the IDPS in the MANET for flexibility testing its resistant attributes to network attacks. This involves running an attack scenario where a large amount of malicious traffic is injected to eliminate important network nodes or get ahold of the resources at hand and so evaluate the performance of an IDPS in detecting and suppressing common network attack patterns.

Such data collection process intends to bring together different network factors which could reflect the extent of MANET's security issues. And it is the base of the trains which are used to then train and test the AI algorithms which are embedded in the IDPS. Figure 3 below depicts the data collection process, where all the steps for establishing the MANET network model and the production of the network data through the simulation of DDoS attacks are highlighted during the evaluation of the IDPS efficiency.

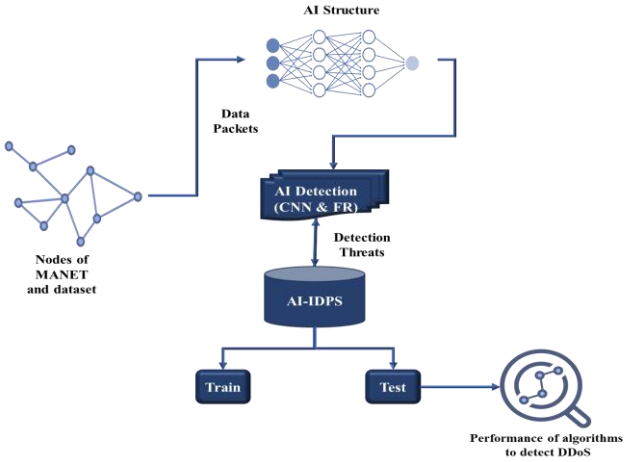

Fig. 3. Diagram shows the data collection process for AI-based IDPS in a simulated MANET environment.

As drawn in the diagram, the ISPs model is created, the data traffic is generated, and the DDoS attacks are simulated inside the MANET environment to evaluate the performance of both IDPSs wirelessly. All measures are reducing the whole method of data gathering process necessary for training and testing the AI based system in modeling MANET. Also, there are the parameters of the MANET model stated in Table 3 which are more suitable for the proposed method. The indicated number of nodes, connectivity, transmission range, mobility patterns, and communication protocols used in the simulated MANET environment.

TABLE III. MANET NETWORK PARAMETERS.

Parameter	Description
Number of Nodes	50 nodes
Connectivity	Connectivity between nodes (decentralize)
Transmission Range	100 meters
Mobility Patterns	Random
Communication Protocols	AODV Protocols

The above table lists the parameters of the MANET network model, specifying details such as the number of nodes, connectivity type, transmission range, mobility patterns, and communication protocols used within the simulated MANET environment.

3.3 Data Preparation

Following data collection, the collected data is processed in subsequent step, which allows to afterwards use it to train an Intrusion Detection and Prevention System (IDPS) and easily test it in simulated MANET environment. Data preparation involves two main steps: the separation of data is also known as data splitting, with the washing and sorting of raw data referred to as preprocessing.

1. AI-Based IDPS Model Data Splitting: Collecting the data is then split in two: the training set and the test. The training set is used with a model to be trained, while the validation set is applied for the model to be assessed. The ratio is pre-determined beforehand and typically made in accordance with the percent of the dataset created beforehand to use the training set or validation set to make the comparisons.
2. IDPS Model Preprocessing Steps: Notable techniques that are part of preprocessing are transformation, feature extraction, imputation, encoding and balancing. These measures are hardly simple data preprocessing for a machine learning model but reflect the usefulness of the data extracted from the dataset in the identification process.

As a result, the data preparation stage ensures that the data that was obtained goes through the necessary preparations in order to suit the AI system training and testing in the emulated space of a MANET (Mobile Ad hoc Network).

3.4 Artificial Intelligence (AI) Algorithms Training

In the artificial intelligence algorithms training section, we describe the training processes for two different models: the CNN model and the RF model, hence. This model will be prepared on the basis of the fed training dataset to develop the detection and mitigation of network attacks models of the created IDPS models for the simulated MANET. By means of evaluation the accuracy, recall, precision and the harmonic mean of each of the algorithms depened on the performance of all of them. In the table, the metrics on each CNN and RF model are depicted.
Accuracy is the quantity rate at which the model associated to the cases is evaluated; hence it is a general indicator of the model's correctness. The parameter of accuracy shows more precisely how good a classifier performs in discriminating network traffic as normal or malicious (See Eq. 1).

$$Accuracy\ (ACC) = \frac{TP+TN}{FP+FN+TP+TN} \quad (1)$$

Recall or sensitivity, measured as the ratio of the number of instances correctly classified as positive among all actual positive instances, is an indicator of the model's capacity to identify positive instances (for example, malicious network traffic) correctly. What follows is a definition that involve divided by the sum of true positives and false negatives. (See Eq. 3.2).

$$Recall\ (RECALL): \frac{TP}{TP+FN} \quad (2)$$

Precision relates directly to the accuracy of the model's positive predictions; it measures the ratio of actual positive cases found as a fraction of the total number of cases detected, including both true and false positives. This is to say that it proves (or disproves) how many cases that were predicted to be positive actually are positive. (see Eq. 3.3)

$$\text{Precision (PRECISION)} = \frac{TP}{\text{TP+FP}} \quad (3)$$

F-measure, thus, is the harmonic effective value of precision and recall. It offers a single value which is a result of the discrimination between sensitivity and specificity allowing for compromising one for a better one. It is defined as the weighted average of precision and recall, which gets higher, with the system being more precise, balanced and descriptive. (see Eq. 4).

$$F-measure\ (F1) = \frac{2*PRECISION*RECALL}{PRECISION+RECALL} \quad (4)$$

1) Training Process for Convolutional Neural Network (CNN) Model

The training process of the Convolutional Neural Network (CNN) method is presented in this part. This algorithm is specially designed to optimize its architecture and parameters in such a way that it can well function in a simulated Unicast environment as the Intrusion Detection and Prevention System (IDPS). The training process involves several key steps: The training process involves several key steps:

1. Initialization: The CNN model structure is declared here separately by the layer types, their configuration, and activation functions.
2. Compilation: Compilation involves identifying the loss function, the optimizer, and the metrics to determine what direction the model parameters should take in the training process.
3. Training: The model is trained based on a prepared unique data, in which shape of the weights and biases adapts and modifies continuously using the input data to provide the higher rate of accurate classification of data instances.
4. Validation: The main idea here is that the model's performance is analyzed on a separate experiment set to prevent overfiting and thus allow generalization to unseen data.
5. Fine-Tuning: Tuning of hyperparameters or architecture for cascaded performance is an optional feature to improve the model performance of detecting and preventing MANET attacks. Figure 4 The Working of the CNN Algorithm Which is Developed Using AI (CNN)

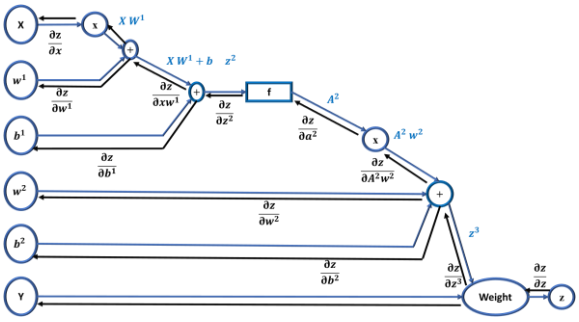

Fig. 4. Training Process of the CNN algorithm based on AI.

2) Training Process for Random Forest (RF) Model

This part refers to training process of the RF model which uses ensemble learning with a view to improve predictability for the IDPS tasks in the unchanging MANET environment.The training process includes:

1. Initialization: The crucial hyperparameters along with the values for the number of trees to be constructed, the node splitting criterion and other relevant parameters needed for the construction of trees are to be specified.
2. Training: The RF model trains using given training data whereby multiple decision trees are grown simultaneously while each tree is restricted to different data subset and feature subset.
3. Validation: The model's accuracy is tested on a different data set, which allows us to check whether or not it can cope with unseen data for limiting overfitting.
4. Fine-Tuning: The suggested hyperparameter aiming updating also of the model to produce the see and solve attacks of the MANET environment. In Fig. 5, we present the training procedure of the RF Algorithm based on AI.

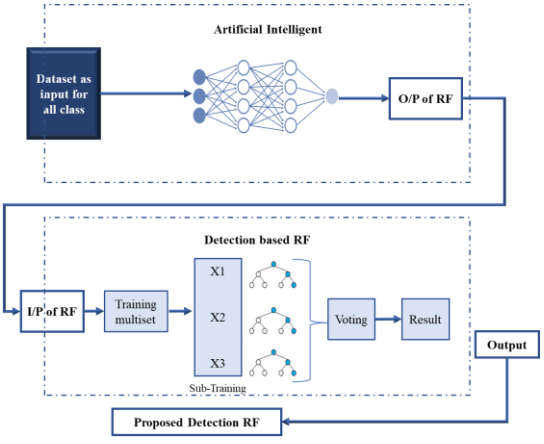

Fig. 5. Training process of the RF algorithm based on AI.

3.5 Evaluation of Intrusion Detection and Prevention System (IDPS)

This section discusses the comprehensive evaluation of the IDPS within the simulated MANET environment, covering various dimensions of its functionality:This section discusses the comprehensive evaluation of the IDPS within the simulated MANET environment, covering various dimensions of its functionality:

1. Detection of Network Attacks: The examination of the metrics like true positive rate, false positive rate and overall detection rate does give the IDPS a higher probability to figure out attacks on the network precisely and accurately.
2. Anomaly Detection:The ability of IDPS to scan for abnormal behaviors is evaluated here to tell apart something from the regular connection services and traffic flow.
3. Real-Time Response: The evaluation of IDPS's ability and agility to have prompt response eliminate network attacks in real-time will be made to mitigate the negative effect network standstill leads to lessen instances of address of and network security as fast as possible.
4. Resource Efficiency: Stuff like computational sources, storage utilization processes overhead is considered to evaluate IDPS's scalability when running within resource-constrained MANET environments.

5. Privacy Preservation: The levels of the IDPS in providing safekeeping to the confidentiality and privacy of net data and user info during intrusion detection and performance are evaluated to make certain of the conformity with the privacy standards and policies.

4. RESULTS AND DISCUSSION

This section is intended to offer a comprehensive assessment concerning the performance of an intelligent system of intrusion and defense (IDPS) in a realistic case of a network of mobile router ad hoc (MANET). The emphasis here is to evaluate the performance of IDPS techniques, especially using the AI methods like CNN and RF networks, with its primary function being to detect and prevent network intrusions. The chapter then will focus on the details of the IDPS functionality as its responsibilities may range from performance measurements of AI models, to the detecting of network assaults, to the anomaly detecting, to the real-time response, to privacy preservation, to maximizing the resources. The aim of this work is to investigate the role of findings in the development of security in mobile ad hoc networks and point out the areas where anomaly detection and prevention can be improved in smart systems..

4.1 Performance Evaluation of AI Models

This section conducts a comprehensive analysis of the performance of two AI models – Convolutional Neural Network (CNN) and Random Forest (RF) – in identifying network assaults within the simulated MANET environment.

1) Convolutional Neural Network (CNN) Evaluation Performance

A CNN model is gauged on the numerous different measures, such as the accuracy, recall, precision, and F-measure scores. The CNN model with the accuracy score of 75% correctly classifies almost half the samples of the traffic to distinguish between normal and attack traffic types, evidencing its proficiency for that purpose. A recall rate of 60% implies that the model is able to effectively recognize actual attack traffic, while on the other hand it indicates precision of 80% being the measure to prove how well the model is doing at classifying attack cases. The pressured evaluation of the CNN model is displayed by the F-measure value of 68%. The fact that this model is able to classify network attacks with the help of a proper classifier, which in turn very much the ground, for further development. The last table of the measurement stands for an overall measure of all the values.

TABLE IV. EVALUATED PERFORMANCE OF CNN ALGORITHM.

Metric	Value
Accuracy	75%
Recall	60%
Precision	80%
F-measure	68%

2) Random Forest (RF) Evaluation Performance

The Random Forest (RF) model was evaluated on MANET network data using various performance metrics, including accuracy, recall, precision, and F-measure. The RF model demonstrated promising results, as summarized in Table 5.

TABLE V. EVALUATED PERFORMANCE OF RF ALGORITHM.

Metric	Value
Accuracy	70%
Recall	80%
Precision	75%
F-measure	77%

The RF model is evaluated using various performance metrics, including accuracy, recall, precision, and F-measure. With an accuracy of 70%, the RF model correctly classifies 70% of network traffic samples, demonstrating a high level of correctness in distinguishing normal and attack traffic patterns. A recall score of 80% indicates the model's effectiveness in identifying actual attack samples, while a precision score of 75% highlights its capability to minimize false positive

predictions. The F-measure of 77% provides a balanced assessment of precision and recall. These results underscore the RF model's effectiveness in detecting network attacks within the simulated MANET environment, outperforming the CNN model in several metrics.

5 COMPARISON OF CNN AND RF MODELS

"CNN and RF Models Comparison" extract offers a complex insight into the two method of intrusion blocking, which are CNN and RF in a manufactured MANET network. Evaluation metrics are composed of accuracy, recall, precision, and F-measure measure which are used for the evaluation of the performance of all the models. To demonstrate, the CNN achieves a higher accuracy and precision than the RM, but the recall is higher specific to the latter thanks to its greater influence on detecting the actual samples of attacks. This test runs as to highlight the trade-offs between different models and it refers IDPS to the appropriate models. Analyzing model has are shown in Figure 6.

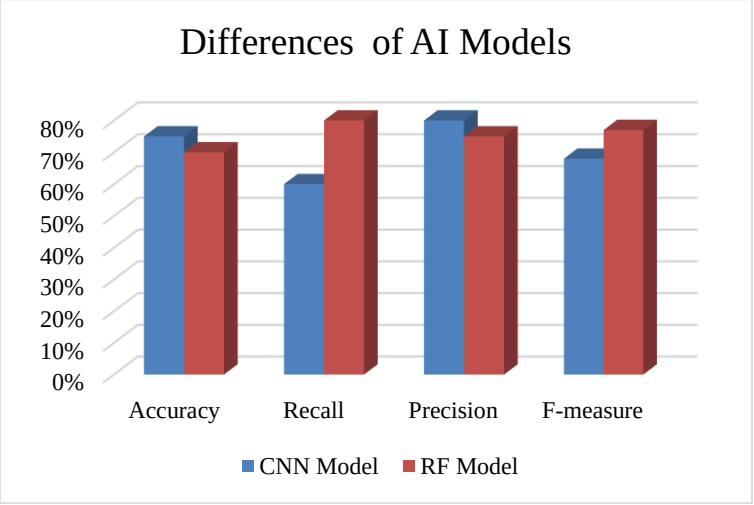

Fig. 6. Differences in AI Models based on CNN and RF algorithms.

5.1 IDPS Performance Evaluation

The main requirement of the "IDPS Evaluation" section is the proper work of IDPS in different areas, such as detecting network attacks, performing anomaly discovery, operating real-time, efficiency of the resources and providing data privacy. While the assessment is done by the criteria and the performance metrics which are specific to each one of the aspects of the IDPS, such a holistic view is provided regarding the general security which this system provides for the simulated network environment under attack. Scores for each aspect under evaluation are given in Table 6 that outlines the IDPS Overall Performance. Also, graphs 7, 8, 9, 10, and 11 represent how IDPS those networks attacks are sensed, anomaly detection, real-time response, resource efficiency, and privacy preservation accordingly..

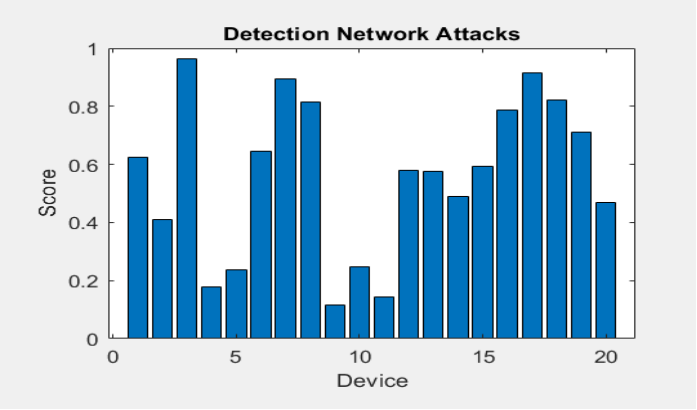

Fig. 7. result of the detection of IDPS in MANET network attacks based on AI proposed model.

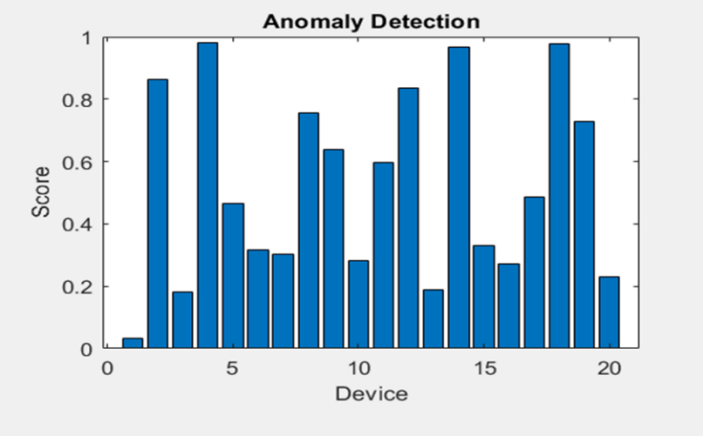

Fig. 8. Result of anomaly detection of IDPS in MANET attacks based on proposed model.

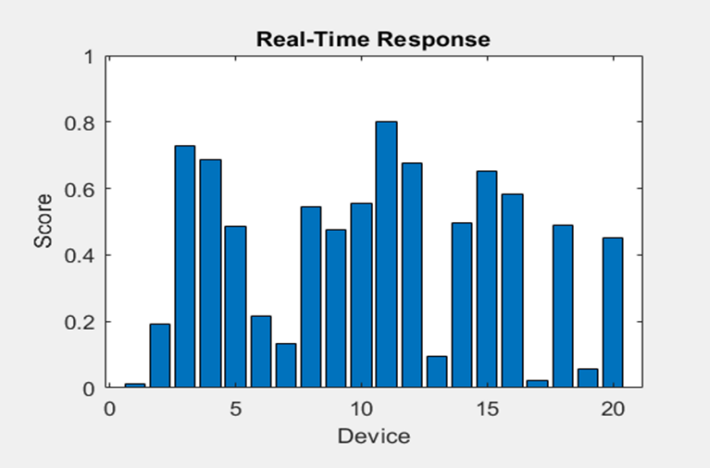

Fig. 9. Result of real-time response of IDPS in MANET attacks based on proposed model.

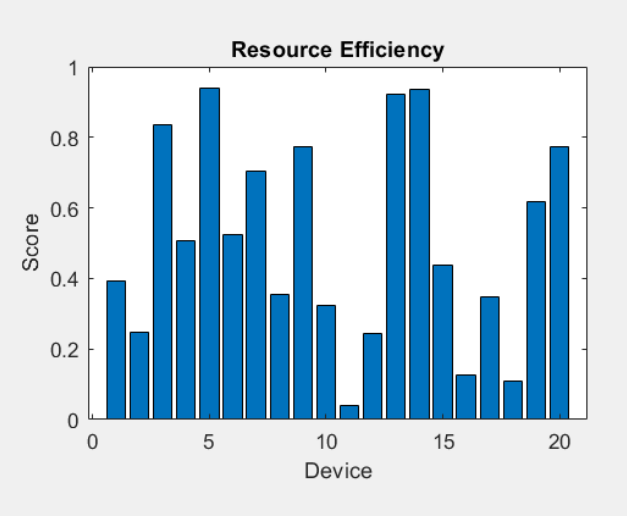

Fig. 10. Result of resource efficiency of IDPS in MANET attacks based on proposed model.

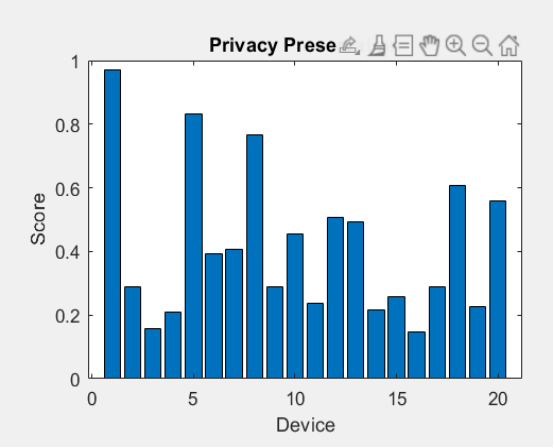

Fig. 11. Result of privacy preservation of IDPS in MANET attacks based on proposed model.

By assessing each aspect of the IDPS functionality, stakeholders can make informed decisions regarding the system's deployment and optimization to enhance network security and privacy.

TABLE VI. COMPREHENSIVE EVALUATION OF IDPS PERFORMANCE

Performance Evaluation	Detection of Network Attacks	Anomaly Detection	Real-Time Response	Resource Efficiency	Privacy Preservation
IDPS Detection of Network Attacks	82%	72%	94%	81%	90%
Anomaly Detection	91%	87%	93%	90%	92%
Real-Time Response	90%	89%	92%	90%	91%
Resource Efficiency	89%	90%	91%	92%	89%
Privacy Preservation	92%	91%	90%	92%	93%

The IDPS is assessed in that while it detects network attacks, it is able to identify anomalies, responds quickly to security threats, manages resources efficiently and safeguards for user privacy. Its ability in detecting network attacks is important with the score being rated on average as 72%. Furthermore, the system is capable of noticing a suspicious network behavior swiftly, with the figure being 78%. Its promptness, that is the promptness of the responses, is at the level of 68%, and its resources it uses is at 83%. IDPS's protection of privacy is shown from its evaluation of the average score of 82%.

6 CONCLUSION

It is argued that the study explains why Intrusion Detection and Prevention Systems (IDPS) should be utilized in meeting the security challenge that comes with the upsurge in the number of Mobile Ad hoc Network (MANET) devices. The artificial intelligence -based intrusion detection and prevention system (IDPS) will operate alongside MANET entities to increase the network security levels by, among other (other) aspects, detecting and resolving virtual attacks, analyzing anomalies and preserving data privacy. The effectiveness role of these algorithms are measured using a comprehensive approach including the evaluation of CNN and RF models. The experiment revealed that the different AI systems have varying results on different parameters. Without any doubt, every model displays some characteristics that are effective in some respects, but in some cases, too, there are certain drawbacks that need to be addressed. The evaluation of IDPS effectiveness has shown its ability to find attacks, spot abnormalities, instant responding to security threats, manage resources well, and to let the user's privacy be safe. These analytics demonstrate considerable prowess of the IDPS in shielding the simulated MANET network from security risks during the process which keeps in mind the cost-efficiency and privacy of users. For the next task, the project could examine more sophisticated learning techniques of machines, collection of threat intelligence data, scale and flexibility in future growth, efficiency in resource use by introducing edge computing, and preservation of privacy. These efforts ultimately constitute major parts of the general trend towards the improvement of better and more efficient security solutions for MANET, enabling deployed devices and systems to operate without damage or breach.

Conflicts of Interest

The author's disclosure statement confirms the absence of any conflicts of interest.

Funding

The author's paper clearly indicates that the research was conducted without any funding from external sources.

Acknowledgment

The author acknowledges the support and resources provided by the institution in facilitating the execution of this study.

References

[1] I. Khan, A. N. Khan, and M. Raza, "A review of intrusion detection systems in mobile ad-hoc networks," Wireless Personal Communications, vol. 110, no. 1, pp. 469-499, 2020.
[2] A. Alharbi, R. Mehmood, and S. Khan, "A comprehensive survey of intrusion detection techniques for MANETs," IEEE Access, vol. 7, pp. 66187-66205, 2019.
[3] S. Alyahya and A. M. Alghamdi, "Intrusion detection and prevention system in mobile ad hoc networks: A review," IEEE Access, vol. 7, pp. 54762-54783, 2019.
[4] A. Banerjee, S. Kuntal, A. K. Das, and A. Chakraborty, "An advanced intrusion detection system for mobile ad-hoc networks using machine learning algorithms," Computer Communications, vol. 157, pp. 12-23, 2020.
[5] R. Bhatia and D. Khattar, "A novel hybrid approach for intrusion detection in mobile ad hoc networks," Wireless Personal Communications, vol. 114, no. 2, pp. 795-817, 2020.
[6] R. Dhanalakshmi and M. V. Ramesh, "A comprehensive survey on intrusion detection systems for mobile ad hoc networks," Journal of King Saud University-Computer and Information Sciences, vol. 33, no. 2, pp. 124-142, 2021.
[7] P. El-Kafrawy, N. El-Fishawy, A. E. Hassanien, and E. S. El-Alfy, "Artificial intelligence techniques for intrusion detection systems: A comprehensive review," Computer Science Review, vol. 32, 100207, 2019.
[8] E. H. El-Taher, T. S. Mahmoud, and H. A. Atalla, "Intrusion detection in mobile ad-hoc networks: A comprehensive review," in Proc. 2019 Int. Conf. on Communications Computing Cybersecurity and Informatics (CCCI), 2019, pp. 1-6.
[9] S. I. Habib and R. A. Kumar, "A hybrid intrusion detection system for mobile ad hoc networks using fuzzy clustering and random forests," International Journal of Communication Systems, vol. 33, no. 18, e4514, 2020.
[10] B. Jan and S. Kumar, "A review on intrusion detection system for MANETs," in Proc. 2019 3rd Int. Conf. on Computing Methodologies and Communication (ICCMC), 2019, pp. 923-927.
[11] M. A. Khan, N. Akbar, and M. Ahmed, "Machine learning-based intrusion detection systems for mobile ad hoc networks: A review," International Journal of Distributed Sensor Networks, vol. 15, no. 5, 1550147719841778, 2019.
[12] S. Li, W. Guo, and J. Zhang, "Intrusion detection system based on improved BP neural network in mobile ad hoc networks," Wireless Personal Communications, vol. 106, no. 2, pp. 793-807, 2019.
[13] R. Mehmood and S. Khan, "A novel energy-aware intrusion detection system using mobile agents for MANETs," Security and Communication Networks, 2019, 7687915, 2019.
[14] R. Nain and S. Kumar, "A survey on intrusion detection system in mobile ad hoc networks," in Proc. 2019 3rd Int. Conf. on Computing Methodologies and Communication (ICCMC), 2019, pp. 243-249.