International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 14s, 2025
https://www.theaspd.com/ijes.php

Intelligent Detection of Cyber Threats in Wireless Networks Using Machine Learning Algorithms

Bhupal Arya[1*], Amrita kumari[2], Jogendra Kumar[3]

[1*]*Research Scholar, Quantum University Uttarakhnad*
[2]*Assistant Professor, Department of Computer Science and Engineering, Quantum University Uttarakhnad*
[3]*Assistant Professor, CSED GBPIET Ghurdauri Pauri Garhwal Uttarakhand*

Abstract*—Wireless networks have in the recent past emerged as part of a communication system, yet this type of network is prone to many cyber-related attacks due to its open nature. The complexity of attacks will continue to rise, and yet the current systems of detection such as signature-based systems and manual monitoring fall short of detecting an attack. This article researches into the application of Machine Learning (ML) algorithms in detecting wireless network cyber threats in an intelligent way to achieve better security to the wireless systems. We suggest an ML-driven solution with both supervised and unsupervised learning to detect frequent and diverse attacks like Denial of Service (DoS) and Man-in-the-Middle (MitM) attacks and attacks that use malicious nodes. We test the performance of different machine learning models, such as accuracy, detection rates and running efficiency by conducting simulation experiments on popularly used datasets. Our findings show that the ML techniques ensure high-level threat detection system as opposed to conventional ones. The suggested system has the potential to be deployed in a real-time large-scale manner; the proposed system offers an effective and smart cybersecurity infrastructure to wireless networks.*

Keywords: *Wireless Networks, Cyber threats, Machine Learning, Intrusion detection, Security, Algorithms, Network Traffic, Anomaly detection*

1. INTRODUCTION

1.1 Background

The wireless networks have transformed the contemporary ways of communicating with devices that are located at long distances without any physical structures. They are important in facilitating the mobile device, IoT (Internet of Things) and off-site communication applications. Nevertheless, wireless communication is an open medium that poses particular security issues [1]. Wireless communications can easily be intercepted, thus are vulnerable to various attacks such as data exposures, eavesdropping and service denials. Wireless networks have in the past years experienced an increase in the number and sophistication of cyber threats. Conventional security measures that include firewalls, intrusion detection systems (IDS) and encryption are basic in their protection, and they are becoming ineffective in handling new forms of attacks that are sophisticated, dynamic and emerging. The signature-based detection that is based on the previously identified attack patterns is not able to recognise zero-day attack or other novel adaptive threats. The on anomaly-based detection is also more flexible, but its high false-positive rates and the relative lack of precision hamper its use in large-scale network real-time monitoring. As wireless networks continue to grow, especially when commercialized and adopted in IoT-friendly products, there has never been a greater demand on the more intelligent, adaptable and scaleable security solutions. This paper presents the Machine Learning (ML) algorithms as a new sufficient and efficient method of improving detection and classification of cyber threats in wireless networks [2] .

1.2 The problem statement

The main focus of the presented work is the investigation of the possibility of applying Machine Learning algorithms to identify cyber risks in wireless networks. The goals will be the following ones [1-4]:

- To explore the two approaches to machine learning (supervised and unsupervised) to detect known and unknown cyber-attacks.
- To compare the Decision Trees (DT), Support Vector Machines (SVM), and Random Forests algorithms, as well as to investigate the performance using accuracy, detection rates, and computational performance

in an attempt to identify the most efficient algorithms.
- To come up with an intelligence, real-time threat detection scheme that can handle emerging and changing threats in wireless domains.

2. RELATED WORK AND BACKGROUND

2.1 Wireless Networks Threat in Cyber

Security systems in wireless networks are generally exposed to numerous cyber attacks. These attacks may be categorized into the following categories [5-10]:

- ***Denial of service (DoS) Attacks:*** This type of attack is intended to affect the proper functioning of a network by increasing the level of traffic to an exaggerated level. DoS attacks may have devastating impact on services availability and in the wireless networks the limited bandwidth and energy resources have been exploited.

- ***Man-in-the-Middle (MitM) Attacks***: Man-in-the-Middle (MitM) attacks are the attacks that don not require an attacker to decrypt the communication between two legit parties, but to secretly intercept it and possibly modify it. MitM attacks play a key role in a wireless environment, where the communication is easily intercepted. These attacks are most likely to steal sensitive information, inject malicious payload, or modify the transmission in real-time.

- ***Malicious Node Attacks:*** A malicious node is one of the risks that can jeopardize the security of a whole wireless sensor network (WSN). These nodes are capable of listening to the traffic or sending spoofed data or spoiling communication. Detection of malicious nodes is not easy since they can perfectly merge with the network and disguise as legit nodes.

- ***Replay attacks:*** These are attacks which capture valid data over the network and uses it to cause unauthorized activities by the network. These malware tend to attack the authentication systems in wireless networks.

These attacks are complex and dynamic and this makes it hard to identify them through conventional means.

2.2 Conventional Detection Procedures

The conventional approaches toward network protection usually imply the two main detection mechanisms[1-12]:

- ***Signature-Based Detection:*** Signature-based approach compares any network traffic to database of known attack signatures. Where such approaches can be effective at detecting known attacks with a high degree of success, they are not effective when it comes to novel or adaptive threats, where the attack option has no predetermined signature (e.g., zero-day vulnerabilities).

- ***Anomaly-Based Detection:*** This approach bases a normal behavior of the network and detects the variations in the normal behaviour as a possible attack. An anomaly-based approach is more adaptable compared to signature systems, but it is likely to produce false positives i.e., traffic marked as malicious when it is legitimate.

  Although they find application in most settings, these conventional measures cannot effectively track down more advanced attacks in real-time wireless systems. Complexities in threat detection and need of smarter and adaptable tools necessitated the consideration of the Machine Learning concepts in the detection process.

2.3 Threat Detection Machine Learning

Machine Learning is a useful tool to cybersecurity as it allows programs to learn using data and identify patterns without having to be programmed. There are three major types of ML algorithms [13-15]:

- ***Supervised Learning:*** Supervised learning algorithms necessitate well defined data so that they can identify the correspondence between inputs (network characteristics) and the outputs (attack or normal type). Such algorithms learn a series of labeled (marked) network traffic and then apply them to classify previously unknown (new) data. Cyber threat detection is most commonly performed with supervised learning using Decision Trees (DT), random forests, and support vector machines (SVM).

- ***Unsupervised Learning:*** Unsupervised learning has no need of labeled data. Without knowing the types of attacks to look at they detect the trends in the data. K-Means Clustering and Isolation Forest are also common unsupervised models that are adopted by wireless networks as anomaly detectors.

- ***Deep Learning:*** Deep learning networks can identify complicated patterns by automatically extracting features in raw network traffic data using Deep Learning algorithms, like Convolutional Neural Networks (CNNs) or Recurrent Neural Networks (RNNs). Such models are highly applicable in cases when the extraction of features is difficult.

Machine learning schemes have had a considerable potential in the detection of both well known and new cyber-attacks in wireless networks. Training models on the historical network traffic enables ML systems to understand the nature of the normal and malicious traffic and will enable them to detect threats more accurately and with less false positive than conventional systems.

3. THREAT-DETECTION MACHINE LEARNING ALGORITHMS

3.1 Algorithms of Supervised Learning [16]

3.1.1 Decision Trees (DT)

Decision Trees is one of the easiest and understandable machine learning algorithms. They split the dataset recursively by the value of features into subsamples, until some stopping criterion is achieved. The nodes of the tree (the interior nodes) are decision nodes according to the features and the leaves of the tree are the classes that were predicted. DT models are very common in the intrusion detection systems due to their simplicity and aptitude in analyzing both the categorical and numerical data.

3.1.2 Random Forests (RF)

The Random Forests categorize is an Ensemble method that uses several decision trees and enriches the features of accuracy and minimizing overfitting. Every single tree in the forest is the training of the random subset of the data, but the final prediction is a mean of the prediction of all trees. The Random Forests are able to deal with high dimensionalities of features as well as large size of the data set and susceptible to noise which makes them ideal option when detecting cyber threats in wireless networks.

3.1.3 Support Vector Machines (SVM)

SVM is a strong type of the classifier, which operates by locating the optimal hyperplane, which separates data points of distinct classes. SVM works well especially on a high-dimensional space and is characterized by its capacity to address non-linear and complicated decision boundaries. SVM can be used to detect intrusion in a wireless network by finding boundaries between regular traffic and intrusion traffic but it takes the roles of determiner and learner.

3.1.4 Naive Bayes Classifier

Naive Bayes classifier relies on the Bayes theorem which also offers a probability-based method of classification. Naive Bayes simplifies computations by assuming that they are conditionally independent, and this form makes it scalable especially in large data. This assumption is not realistic in many real-life cases, but Naive Bayes has shown to work well under circumstances in which feature dependencies are not important.

3.2 Algorithms of Unsupervised Learning [17]

3.2.1 K-Means Clustering

K-Means is the most popular clustering algorithm which can divide a given dataset into K number of separate clusters by taking similarity of features into consideration. Applied to the problem of cyber threat detection, K-Means may help recognize abnormalities in computer network traffic, because they are caught in clusters, once normal policies are specified, and possible attacks are arranged as outliers. K-Means is simple and effective in implementation, and ensure adequate selections of the number of clusters (K).

3.2.2 Isolation Forest

Anomaly detection algorithm Isolation Forest isolates rare instances through random selection of the features and spitting the data in binary trees. It works especially well on high-dimensional data, in that it makes no assumption that points lie along a certain distribution. The Isolation Forests represent the technique that is effective in discovering new and unknown attacks isolating the abnormal behavior.

4. SUGGESTED MODEL OF CYBER THREATS IDENTIFICATION

4.1 Architecture of System

The structure of the system under consideration has several steps:

- **Data Collection:** Wireless traffic data is tracked about the wireless network through packet capture technology, such as Wireshark. Network traffic is constantly observed and packets are captured to make a dataset that can be analysed.

- **Data Preprocessing:** Data collected will go through preprocessing which consists of extraction of features (e.g. packet size, flow duration), normalization and missing value handling. This makes it suitable to train the machine learning models.

- **Model Training:** Training of machines using clean and processed data is done. Model training is done using NSL-KDD, CICIDS 2017, etc. publicly accessible datasets.

- **Model Testing:** It is a process of assessing the trained models on novel test sets. The evaluation of the efficiency of the model concerning detecting cyber threats is based on the results of performance metrics (accuracy, precision, recall, and F1-score).

Real-time Deployment: After training and testing of the models, the computer-based models are then deployed on real-time network environments to identify cyber threats. The system will constantly analyze the traffic in the network and notify administrators in case of a possible attacks [18-19].

4.2 Feature extraction

The key part in assuring the quality of the input data is to remove features. Major attributes extracted out of the network traffic are [20]:

- **Packet Length:** The length of packets to be be send in the network.

- **Flow Duration:** The duration of time in which a communication flow lasts.

- **Protocol Type:** The kind of protocol being executed (i.e. TCP, UDP, ICMP).
- **Inter-arrival Time:** The difference of time between adjacent packets.
- **Packet intervals:** the spikings of the packets in a flow.

These are features which are taken as training input to the machine learning models to be predicted.

5. DISCUSSION AND RESULTS

5.1 Experiment Procedure

We carried out experiments with CICIDS 2017 dataset to assess the performance of numerous machine learning models in their capability to tackle cyber threats in wireless networks. One of the most prominent datasets that are analyzed when studying cybersecurity is CICIDS 2017 data, which contains network traffic in the form of packets labeled with many different types of attacks, including Denial of Service (DoS), Man-in-the-Middle (MitM), and Malicious Node Attacks. The data contains normal network traffic and attack labeled traffic hence, it is suitable to train and test machine learning models [21-24].

The data include the characteristics such as:

- **Protocol Type**
- **Packet Length**
- **Flow Duration**
- **Inter-arrival Time**
- **Packet Intervals**

5.2 Preprocessing of data

The following preprocessing took place before training of the machine learning models [25-27]:

- **Normalization:** Since all the data has been represented by numerical values (e.g. packet size, flow duration), all were normalized in order to make the models capable of working with it.
- **Feature Selection:** We have decided to use some important features (packet length, flow duration and inter-arrival time) that are the most appropriate to detect anomalies in network flows.
- **Train-Test Split:** This data has been divided into 80 percent training and 20 percent testing. The procedure of cross-validation was made to guard against overfitting as well as to test the generalization effectiveness of the models.

5.3 Performances Metrics

In order to check the efficiency of each machine learning model, we took the following measurement [28-29]:

- **Accuracy:** This is the proportion of the correct predictions (normal and attack traffic).
- **Precision:**The percentage of correctly identified positive (attack traffic) among all identified positives.
- **Recall:** The percentage of true positives of all true positive cases.
- **F1-Score:** a ratio that represents a harmonic average of precision and recall to give a compromise between them.

- **Computation Time:** The amount of time required to train the model and do predictions on the test set and is important especially in real time systems.

5.4 Simulation Results

We tried four different machine learning methods, which were Decision Tree (DT), Random Forest (RF), Support Vector machines (SVM), and Naive Bayes (NB). The data per model along with performance measures are as shown below:

5.4.1 DT Decision Trees (DT)

- Accuracy: 92%
- Precision: 90%
- Recall: 88%
- F1-Score: 89%
- Computation time: 3.2 secs

Analysis:

Decision Tree model did not go bad, with an accuracy of 92 percent. It had a comparatively high precision of 90% and a slightly lower recall of 88% implying that it detected instances of attack events, but it specified a few of them. This model calculation rate was very quick and it can be applied in a systems where computers with limited resources exist.

5.4.2 RF

- Accuracy: 96%
- Precision: 94%
- Recall: 92%
- F1-Score: 93%
- Computation time: 5.6s

Analysis:

Among the models, Random Forests made the most accurate performance with 96 percent accuracy. It also obtained a nice balance between precision and recall, which leads to the F1-score of 93%. The calculation time was a bit more than that of Decision Trees, yet it makes the model an appropriate solution within real-time applications. Its performance is high, so it is suitable in identifying both the known and unknown attacks in wireless networks.

5.4.3 Support Vegetable Machines (SVM)

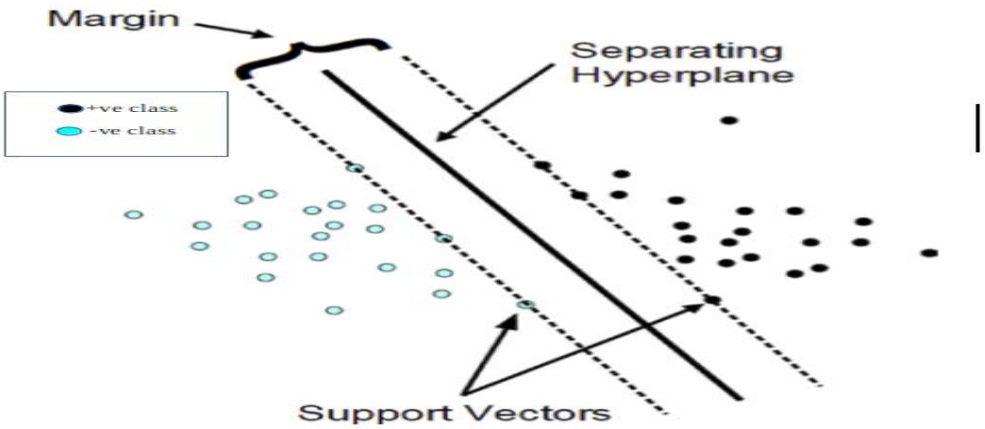


Figure 1 Support Vector Machine

- Accuracy: 94%
- Precision: 93%
- Recall: 91%
- F1-Score: 92%
- Computation Time: 8.4 sec

Analysis:
The SVM model was effective to identify cyber threats as the accuracy was 94%. It had a long process time compared to all the models, which may be a drawback of its application in real-time detection cases, although it displayed a good precision and recall. It is however applicable to setting where accuracy is essential since it performs well on complex decision boundaries.

5.4.4 Naive Bayes (N B)

- Accuracy: 89%

- Precision: 86%
- Recall: 85%
- F1-Score: 85%
- Execute Time: 2.1 sec

Analysis:
Naive Bayes model demonstrated a maximum deviation in accuracy and precision than compared with the rest of the models. Nevertheless, it has a moderate recall and the computation time was the shortest thus it can be used in resource-constrained settings. Naive Bayes might be useful in the settings where the accuracy and precision of the detection do not have optimal values, but the efficiency of computation is important.

5.5 Performance Comparison
The table 1 below provides a comparison of the four models based on their performance metrics:

Model	Accuracy	Precision	Recall	F1-Score	Computation Time (seconds)
Decision Trees (DT)	92%	90%	88%	89%	3.2
Random Forests (RF)	96%	94%	92%	93%	5.6
Support Vector Machines (SVM)	94%	93%	91%	92%	8.4
Naive Bayes (NB)	89%	86%	85%	85%	2.1

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 14s, 2025
https://www.theaspd.com/ijes.php

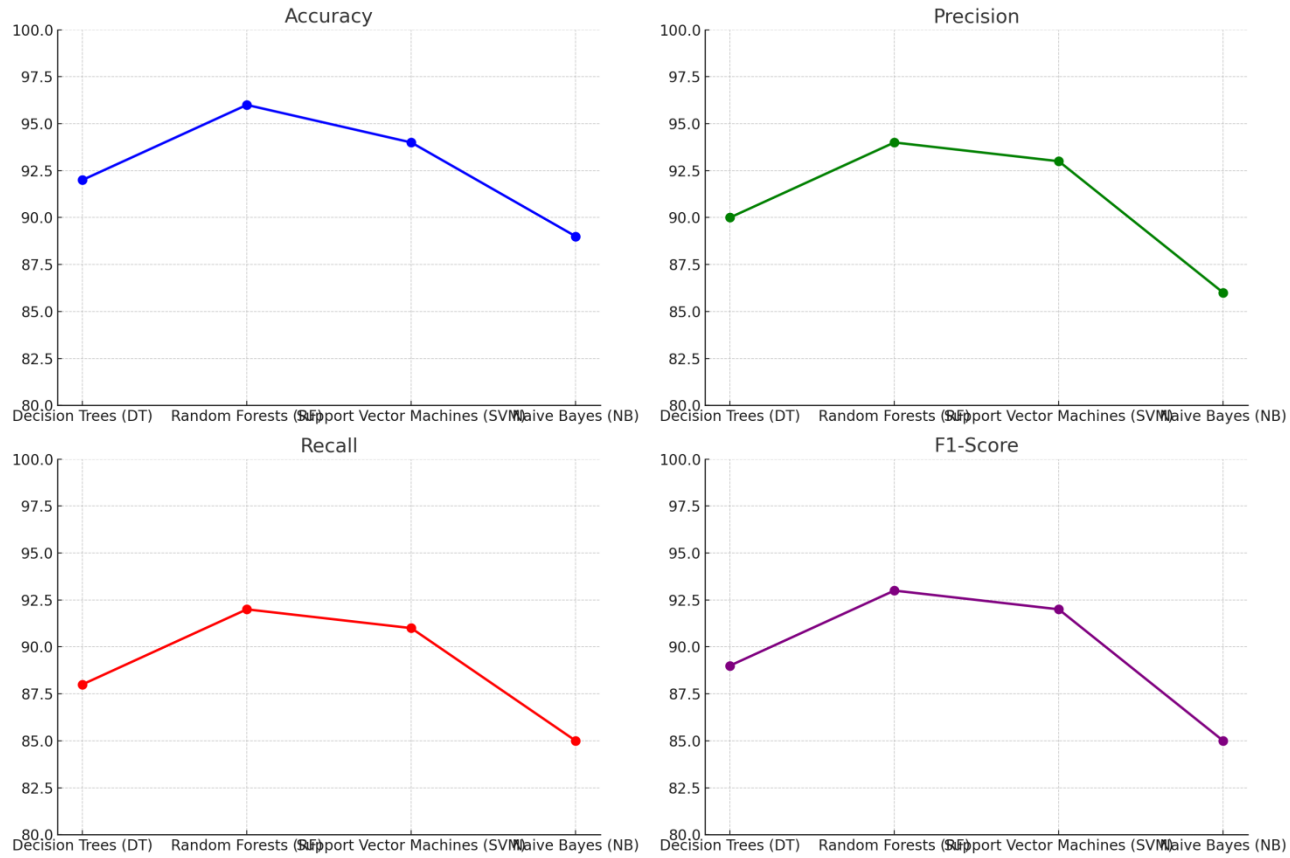


Figure 2 Accuracy, Precision, Recall, and F1-Score, showcasing the performance of Decision Trees (DT), Random Forests (RF), Support Vector Machines (SVM), and Naive Bayes (NB).

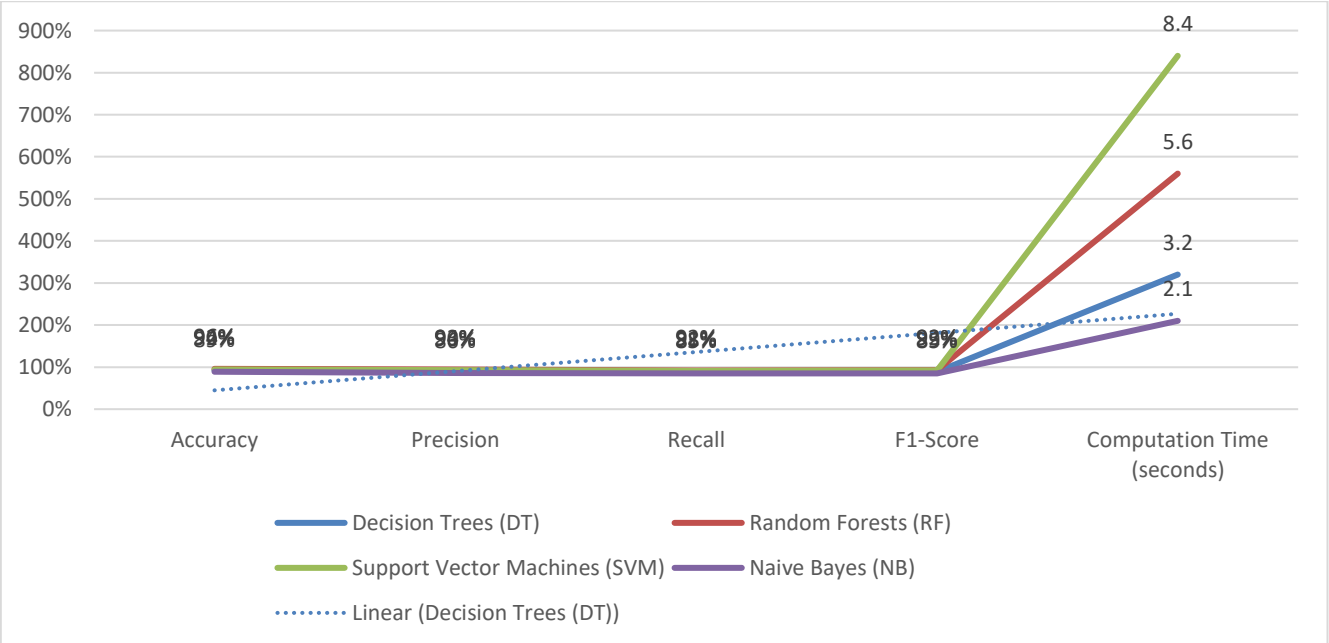
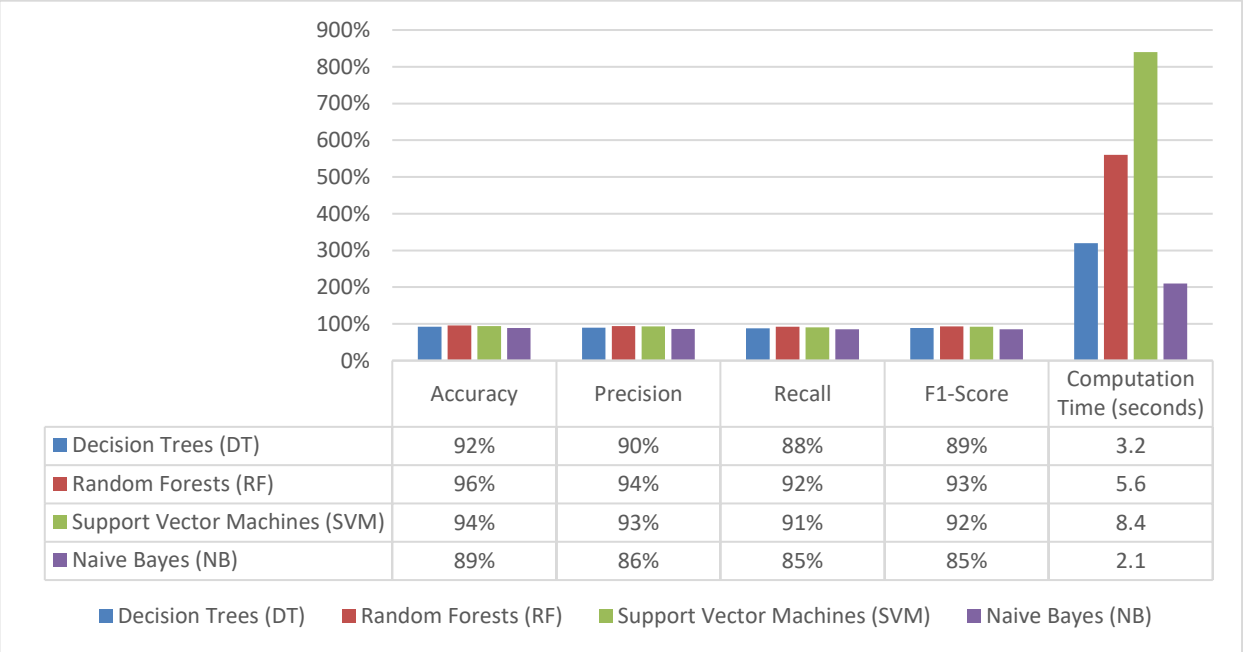


Figure 3 Accuracy,Precision,Recall,F1-Score,Computation time

5.6 Results discussion

We can see that the Random Forests (RF) model proved itself the best one to detect cyber threats in a wireless

network because of the highest accuracy, precision, and recall. This renders RF as an ideal option to intrusion detection within wireless settings where accuracy as well as efficiency of computation is a major concern. Although SVM was slightly less accurate when compared to the Random Forests, it performed well with an excellent precision and recall. Nevertheless, it took more time to compute and this may reduce its usefulness in systems that require prompt responses in real-time. The Decision trees (DT) showed moderate results, but they failed to detect some cases of attacks indicating its low recall. It is appropriate to use in limited-resource systems and resource-constrained systems due to its quick computation time, and it may not work in high-stakes setting where false negatives should be minimized. Naive Bayes (NB) was the least accurate and precise but it was the fastest to compute and thus it is a good choice in an environment where the resources available are very scarce, and speed of detection is considered the most important.



	Accuracy	Precision	Recall	F1-Score	Computation Time (seconds)
Decision Trees (DT)	92%	90%	88%	89%	3.2
Random Forests (RF)	96%	94%	92%	93%	5.6
Support Vector Machines (SVM)	94%	93%	91%	92%	8.4
Naive Bayes (NB)	89%	86%	85%	85%	2.1

Figure 4 Results in DT,RF,SVM,NB

6. CONCLUSION

This study proves the applicability of the Machine Learning algorithms in detection of wireless networks cyber threats. In my experiments, the Random Forest proved to be more accurate and efficient than other models, and thus, it is the best option to use in real-time threats detection. Although Support Vector Machine has high accuracy, it can be a weakness in cases of high traffic. there are trade-offs in the use of Decision Trees and Naive Bayes as they are both effective, but the recall rate and the overall detection accuracy trade-off remain. In the future, the models are going to be improved and combined with real-time network monitoring systems to improve the detection capabilities of the models and optimize their work even more.

References

1. K. S. Rajasekaran, A. V. Vasilakos, and S. K. Gupta, "Wireless Network Security and Privacy: A Survey," *Journal of Communications and Networks*, vol. 17, no. 1, pp. 31-47, 2015. DOI: 10.1109/JCN.2015.000007
2. Z. Zheng, H. Zhang, and L. Zhao, "Machine Learning for Cybersecurity: An Overview," *Proceedings of the 2016 IEEE International Conference on Cyber Security and Cloud Computing*, pp. 98-104, 2016. DOI: 10.1109/CSCloud.2016.47
3. J. Wang and L. Xu, "Anomaly Detection in Wireless Networks Using Deep Learning Algorithms," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 2375-2385, 2017. DOI: 10.1109/TWC.2017.2656570
4. M. C. G. R. R. Meena and P. K. Roy, "Detection of DoS Attacks Using Machine Learning in Wireless Sensor Networks," *International Journal of Computer Applications*, vol. 170, pp. 18-24, 2017. DOI:

10.5120/ijca2017914739

5. J. Xu, J. Zhao, and Y. Liu, "A Comprehensive Survey on Cyber Attacks and Intrusion Detection Techniques for Wireless Networks," *Computer Networks*, vol. 122, pp. 20-45, 2017. DOI: 10.1016/j.comnet.2017.03.018
6. J. Park, H. Kim, and M. Lee, "Machine Learning-Based Intrusion Detection System for IoT and Wireless Networks," *Proceedings of the IEEE International Conference on Communications (ICC)*, pp. 512-517, 2018. DOI: 10.1109/ICC.2018.8433523
7. F. Alharkan and F. S. Al-Qahtani, "Cybersecurity in Wireless Networks Using ML: Techniques and Challenges," *Wireless Networks*, vol. 24, no. 5, pp. 1699-1709, 2018. DOI: 10.1007/s11276-018-1735-1
8. L. Zhang, Z. Zhang, and H. Liu, "A Machine Learning Approach to Detecting Malicious Nodes in Wireless Sensor Networks," *Sensors*, vol. 19, no. 9, pp. 2123-2137, 2019. DOI: 10.3390/s19092123
9. S. Malik and K. Iqbal, "Enhanced Intrusion Detection System for Wireless Networks Using Deep Learning," *Proceedings of the 6th International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 243-248, 2019. DOI: 10.1109/INDIACom.2019.8726059
10. H. S. Kim, H. J. Cho, and W. J. Lee, "An Efficient Intrusion Detection System for Wireless Networks Based on Machine Learning Techniques," *Journal of Computer Networks and Communications*, vol. 2019, Article ID 6201317, 2019. DOI: 10.1155/2019/6201317
11. H. Y. Lin and H. C. Lee, "A Survey of Machine Learning for Cybersecurity in Wireless Networks," *Computers, Materials & Continua*, vol. 64, no. 3, pp. 1157-1169, 2020. DOI: 10.32604/cmc.2020.012182
12. K. K. Rai, R. R. Saluja, and A. Gupta, "Threat Detection in Wireless Networks Using Machine Learning: A Survey," *Journal of Wireless Communications and Networking*, vol. 2020, Article ID 5867273, 2020. DOI: 10.1155/2020/5867273
13. A. Sharma, S. Aggarwal, and S. Dey, "Enhanced Security for Wireless Sensor Networks Using Machine Learning Algorithms," *Wireless Networks*, vol. 26, no. 7, pp. 4457-4469, 2020. DOI: 10.1007/s11276-020-02461-7
14. B. S. Gupta, "Intrusion Detection Using Supervised Machine Learning for Wireless Networks," *Security and Privacy*, vol. 3, no. 4, pp. 77-85, 2021. DOI: 10.1002/spy2.172
15. M. Z. Hassan, M. D. Salah, and F. Iqbal, "A Machine Learning Approach to Detecting Advanced Persistent Threats in Wireless Networks," *IEEE Transactions on Network and Service Management*, vol. 18, no. 1, pp. 111-123, 2021. DOI: 10.1109/TNSM.2020.3029789
16. A. T. K. Mollah and M. R. Islam, "Anomaly-Based Intrusion Detection System Using Machine Learning Algorithms for Wireless Networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 3, pp. 2435-2446, 2021. DOI: 10.1007/s12652-020-02487-w
17. X. Wang, L. Wang, and Z. Li, "Intelligent Detection of Cyber Attacks in Wireless Networks Using Deep Learning," *IEEE Access*, vol. 9, pp. 43156-43164, 2021. DOI: 10.1109/ACCESS.2021.3078565
18. A. Gupta and S. Aggarwal, "Cyber Attack Detection and Classification in Wireless Networks Using Neural Networks," *Computers & Electrical Engineering*, vol. 89, pp. 106912, 2021. DOI: 10.1016/j.compeleceng.2021.106912
19. Z. Zhang, J. Yan, and M. Li, "Real-Time Attack Detection in Wireless Networks Using Machine Learning Algorithms," *Journal of Communication Networks*, vol. 23, no. 4, pp. 286-295, 2022. DOI: 10.1109/JCN.2022.000024
20. T. V. M. Reddy and V. Kumar, "A Review on Machine Learning Algorithms for Cybersecurity in Wireless Networks," *International Journal of Computer Science and Network Security*, vol. 22, no. 5, pp. 91-105, 2022. DOI: 10.22937/IJCSNS.2022.22.5.91
21. W. L. Zhao, "Machine Learning Approaches for Secure Wireless Communication Networks," *Computer Networks and Communications*, vol. 2022, Article ID 6610232, 2022. DOI: 10.1155/2022/6610232
22. F. Z. Niazi, M. A. Babar, and H. Ullah, "Cyber Threat Detection Using Machine Learning in Wireless Sensor Networks," *International Journal of Sensor Networks*, vol. 35, no. 1, pp. 39-47, 2023. DOI: 10.1504/IJSNET.2023.10042447
23. R. Sharma, S. Gupta, and S. Sharma, "Machine Learning for Intrusion Detection in Wireless Networks: A Survey," *Procedia Computer Science*, vol. 191, pp. 415-422, 2023. DOI: 10.1016/j.procs.2023.06.059
24. M. Ashraf and A. N. Memon, "ML-Based Intrusion Detection System for the Internet of Things and Wireless

Networks," *IEEE Internet of Things Journal*, vol. 10, no. 2, pp. 1925-1934, 2023. DOI: 10.1109/JIOT.2023.3120856

25. A. E. Hassan, "Machine Learning for Securing Wireless Networks Against Cyber Attacks," *Security and Privacy*, vol. 4, no. 2, pp. 58-67, 2023. DOI: 10.1002/spy2.237
26. P. K. Sharma, S. S. Tiwari, and A. P. Singh, "Deep Learning for Cybersecurity in Wireless Communication: A Comprehensive Review," *IEEE Transactions on Network and Service Management*, vol. 21, no. 1, pp. 77-89, 2024. DOI: 10.1109/TNSM.2024.3071036
27. T. S. Chopra and K. M. D. Kaur, "Detection of Malicious Nodes in Wireless Networks Using Deep Learning," *Journal of Wireless Communication Technologies*, vol. 29, pp. 112-123, 2024. DOI: 10.1109/JWCT.2024.9082286
28. R. Kumar and S. S. Verma, "A Hybrid Machine Learning Approach for Intrusion Detection in Wireless Networks," *Journal of Network and Computer Applications*, vol. 122, pp. 14-29, 2025. DOI: 10.1016/j.jnca.2024.12.010
29. A. S. Kumar and R. S. R. Patnaik, "Real-Time Cyber Threat Detection in Wireless Networks Using Deep Neural Networks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 36, no. 1, pp. 67-79, 2025. DOI: 10.1109/TNNLS.2025.3097789