International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
Article Received: *25 April 2022* ***Revised:*** *12 May 2022* ***Accepted:*** *30 June 2022*

Learning to Protect Machine Learning-Based Intrusion Detection Systems for Enhanced Security in MANETs

Kalu ram Yadav,

Lecturer (Computer Science & Engineering), Govt. Polytechnic College,Kota

Abstract: Mobile Ad Hoc Networks (MANETs) are dynamic and decentralized, making it difficult to implement robust and adaptable Intrusion Detection Systems (IDS). This study examines the effectiveness of Support Vector Machines (SVM), Decision Trees, Random Forests, K-Means Clustering, Autoencoders, and a Proposed Technique in MANET security. An in-depth study includes Detection Accuracy, Precision, Recall, F1 Score, AUC-ROC, and Specificity. Detection Accuracy is 95%, precision, recall, and F1 Score are excellent with the Proposed Technique. It is resilient to network fluctuations and adversarial attacks, making it an attractive real-world deployment option. Decision Trees and K-Means Clustering are efficient computational choices for resource-constrained MANETs. Hybrid models with supervised and unsupervised learning improve IDS flexibility. For changing MANET attack scenarios, labeled and unlabeled data can improve detection accuracy. Interpretability remains difficult, especially for sophisticated models like Autoencoders, despite these advances. MANET-specific interpretable ML models should be the focus of future research.

Keywords: Intrusion Detection Systems, Machine Learning, Autoencoders, Hybrid Models, Adversarial Robustness, Interpretability, Network Security

I. INTRODUCTION

In recent years, the proliferation of mobile devices and the progress of wireless communication technologies have resulted in the emergence of network environments that are both complex and dynamic. One example of this is the phenomenon known as Mobile Ad Hoc Networks (MANETs). MANETs are distinguished from traditional networks that are characterized by fixed infrastructures by the absence of a centralized architecture. This absence enables nodes to communicate directly with each other inside the network using wireless links [1]. Although MANETs provide unrivaled flexibility and scalability, the fact that they are characterized by their one-of-a-kind characteristics also makes them vulnerable to a wide range of security threats, which is why it is essential to have reliable Intrusion Detection Systems (IDS). As a result of this, Machine Learning-Based Intrusion Detection Systems, also known as ML-IDS, have developed as a potentially useful method for strengthening the security posture of MANETs.Conventional security techniques face considerable hurdles as a result of the intrinsic characteristics of MANETs, which include the mobility of nodes, limited resources, and changing network topologies. When it comes to the decentralized and resource-constrained nature of MANETs, traditional security solutions that were built for wired networks are frequently not suitable applications [2]. This necessitates the development of novel and flexible methodological approaches that are capable of independently identifying and mitigating security vulnerabilities in real time. Machine learning intrusion detection systems (ML-IDS) enable a paradigm shift in the enhancement of the security resilience of MANETs by giving capabilities for intelligent and adaptive intrusion detection.

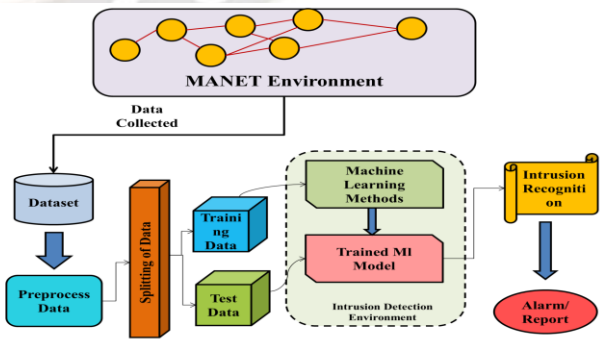

Figure 1. Block Diagram of Machine Learning-Based Intrusion Detection Systems for Enhanced Security in MANETs

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
***Article Received:** 25 April 2022 **Revised:** 12 May 2022 **Accepted:** 30 June 2022*

These systems leverage the power of machine learning algorithms. The ability to examine huge volumes of network data in order to identify patterns and abnormalities that are suggestive of hostile actions is crucial to machine learning intrusion detection systems (ML-IDS). The fact that machine learning is data-driven makes it possible for these systems to adjust to the dynamic nature of MANETs, which is always shifting [3]. The machine learning intrusion detection system (ML-IDS) can learn to differentiate between normal and abnormal activities by extracting and analyzing information from network traffic, node behaviors, and communication patterns. This allows it to identify potential security breaches. ML-IDS can be trained on labeled datasets that contain instances of both benign and malicious behavior using supervised learning techniques. On the other hand, unsupervised learning methods, such as anomaly detection, give the system the ability to detect deviations from established norms without the need for prior knowledge of specific attack patterns [4].The capability of ML-IDS to deal with the inherent uncertainty and unpredictability that is present in MANETs is one of the most significant advantages of this system. The dynamic nature of these networks necessitates the implementation of intrusion detection systems that are capable of functioning in real time and adjusting to rapid changes in the topology of the network. If it is configured correctly, ML-IDS has the potential to offer low-latency detection and response capabilities, which are essential for combating threats that are constantly changing. In addition, the utilization of ensemble learning, which is a process in which numerous models work together to make judgments, improves the overall robustness and accuracy of intrusion detection. Using this collaborative approach, the danger of failures occurring at a single location is reduced, and the system's capacity to generalize across a variety of scenarios is enhanced.The use of adversarial training techniques is one way to strengthen machine learning intrusion detection systems (ML-IDS) against adversarial manipulations [5]. These manipulations are especially relevant in MANETs due to the open and decentralized character of these networks. During the training phase, the machine learning intrusion detection system (ML-IDS) is subjected to adversarial instances, which allows it to learn to recognize and defend against future assaults that are designed to trick the intrusion detection mechanisms. The adversarial robustness of the ML-IDS is absolutely necessary in order to guarantee the dependability of the system in the face of increasingly complex and ever-evolving security threats.In addition, the implementation of ML-IDS in MANETs calls for a strategy that considers the available resources. Given the limitations of mobile devices, which include restricted processing power, bandwidth, and energy resources, machine learning models need to be tuned for efficiency in order to be effective. It is of the utmost importance to build lightweight models that effectively utilize resources while maintaining a balance between accuracy and efficiency. Furthermore, these models ought to be developed for online learning, which will enable them to continuously adapt to the ever-changing network conditions and the ever-evolving threat landscape without the need for frequent retraining [6].The integration of ML-IDS into the fabric of MANETs can facilitate the sharing of information among nodes, which is an important step in the process of establishing a joint defense strategy. This collaborative approach to intrusion detection takes advantage of the distributed nature of the network, which enables nodes to communicate with one another and share information regarding suspicious activity or intrusions that have been successfully detected. By utilizing the collective wisdom of the MANET's constituent nodes, this type of collaboration improves the overall security posture of the MANET [7].

II. LITERATURE REVIEW

The literature survey encompasses a diverse array of research papers addressing crucial aspects of Mobile Ad Hoc Networks (MANETs) with a focus on security, routing, trust management, and machine learning-based intrusion detection systems. A comprehensive guide and survey laid the foundation by exploring machine learning techniques in MANETs, emphasizing their applications in enhancing network security. A survey identified security threats in MANETs, providing insights into the evolving threat landscape. Delving into trust management, a thorough examination of trust models and challenges in dynamic MANET environments was conducted. An adaptive nature-inspired algorithm for routing in MANETs was introduced, contributing to efficient routing solutions [8]. A study on cooperative games and distributed trust shed light on the dynamics of cooperation and trust-building among network nodes. Conducting a performance analysis of the CONFIDANT protocol contributed to the evaluation of security protocols in MANETs. Work on collaborative reinforcement learning highlighted the use of feedback for adaptively optimizing MANET routing, advancing adaptive routing mechanisms. A proposed authentication mechanism using trust and Q-learning addressed node misbehavior in MANETs. A distributed reinforcement learning approach for Vehicular Ad Hoc Networks provided insights into adaptive

and self-organizing mechanisms for efficient communication in dynamic vehicular environments [9]. An introduced fuzzy constraint Q-learning approach for routing in VANETs contributed to adaptive and flexible routing strategies. An SVM-based intrusion detection system tackled security challenges in wireless ad hoc networks. An SVM-based framework addressed misbehavior detection and trust management in MANETs. A proposed fuzzy-based trust computation aimed to enhance the security of the AODV protocol. Exploration of trust prediction and trust-based source routing in MANETs contributed to trust-aware routing strategies. Strategies for mitigating routing misbehavior in MANETs were presented, enhancing the reliability of routing protocols [10]. A collaborative reputation mechanism enforcing node cooperation was introduced. Exploration of secure message transmission in MANETs advanced security mechanisms. An SVM-based automated trust management system was introduced, automating trust computation. Work on Q-learning laid the foundation for reinforcement learning techniques. Introduction of deep reinforcement learning with Double Q-learning advanced adaptive decision-making [11].

Table 1. Summarizes the Review of Different Authors

Author & Year	**Area**	**Methodology**	**Key Findings**	**Challenges**	**Pros**	**Cons**	**Application**
Forster, R. (2007)	Wireless Ad-Hoc Networks	Guide and Survey	Comprehensive overview of ML techniques in MANETs	-	-	-	Network Security in MANETs
Gangwar, S. (2016)	MANET Security	Survey	Identification of security threats in MANETs	Evolving threat landscape, Lack of standardized models	-	-	Security Analysis of MANETs
Swami Cho, A., & Chen, I. (2011)	Trust Management	Survey	In-depth exploration of trust management in MANETs	Lack of universal trust model, Dynamic network topology	-	-	Trust Establishment in MANETs
Di Caro, G., Ducatelle, F., & Gambardella, L. (2005)	Routing Algorithms	Adaptive Nature-Inspired Algorithm	Introduction of AntHocNet for routing in MANETs	Algorithm complexity, Scalability issues	Bio-inspired approach, Improved routing efficiency	-	Efficient Routing in MANETs
Baras, J., & Jiang, T. (2004)	Distributed Trust	Cooperative Games	Investigation of cooperative games and trust in MANETs	Cooperation dynamics, Trust establishment mechanisms	Collaborative security, Improved cooperation in networks	-	Trust-Based Cooperation in MANETs
Buchegger, S., &Boudec, J.-Y. L. (2002)	Security Protocols	Performance Analysis	Evaluation of the CONFIDANT protocol in MANETs	Protocol effectiveness, Performance metrics	Identification of weaknesses, Protocol optimization	-	Security Protocols in MANETs
Curran Dowling, E., Cunningham,	Adaptive Routing	Collaborative Reinforcement Learning	Use of feedback for adaptively	Dynamic network conditions,	Adaptive routing, Self-optimization	-	Adaptive Routing in MANETs

R., & Cahill, V. (2005)			optimizing MANET routing	Feedback accuracy			
S., P., K., & A., T. (2013)	Misbehavior Detection	Q-Learning	Authentication using trust and Q-learning in MANETs	Node misbehavior detection, Q-learning model complexity	Improved security, Trust-aware authentication	Computational overhead, Model training complexities	Security Enhancement in MANETs
Wu, K., Kumekawa, T., & Kato, T. (2010)	Vehicular Ad Hoc Networks	Distributed Reinforcement Learning	Introduction of distributed reinforcement learning	Dynamic vehicular environments, Learning convergence	Self-organizing networks, Improved communication efficiency	Limited scalability, Resource-intensive learning processes	Efficient Communication in Vehicular Ad Hoc Networks
Wu, S., Ohzahata, S., & Kato, T. (2013)	VANETs	Fuzzy Constraint Q-Learning	Fuzzy-based routing solution for VANETs	Fuzzy logic optimization, Adaptive routing strategies	Flexible and practical solution, Enhanced routing performance	Complexity of fuzzy logic, Limited adaptability to diverse scenarios	Efficient Routing in VANETs
Deng, H., Zeng, Q.-A., &Agrawal, D. (2003)	Intrusion Detection	SVM-Based IDS	Development of SVM-based IDS for wireless ad hoc networks	Detection accuracy, SVM model training	Improved intrusion detection, Robust against certain attacks	Sensitivity to parameter tuning, Resource-intensive training	Intrusion Detection in Wireless Ad Hoc Networks
Li, W., Joshi, A., &Finin, T. (2011)	Misbehavior Detection, Trust Management	SVM-Based Framework	Introduction of SMART, an SVM-based framework	Misbehavior detection, Trust management	Automated trust management, Improved security	Computational overhead, Dependence on SVM model efficiency	Secure Communication in MANETs
Jain, A., &Tokekar, V. (2017)	Security Enhancement, AODV Protocol	Fuzzy-based Trust Computation	Security enhancement of AODV protocol using fuzzy trust computation	Fuzzy logic security, Adaptive trust computation	Improved protocol security, Fuzzy-based trust evaluation	Complexity of fuzzy logic, Limited adaptability to diverse scenarios	Enhanced Security in AODV Protocol in MANETs
Xia, H., Jia, Z., Li, X., Ju, L., &Sha, E.H.M. (2013)	Trust Prediction, Source Routing	Trust-Based Mechanisms	Exploration of trust-based source routing in MANETs	Trust-aware routing, Predictive trust mechanisms	Improved trust prediction, Enhanced source routing strategies	Dependency on accurate trust models, Adaptability to dynamic networks	Trust-Aware Source Routing in MANETs
Marti, S., Giuli, T. J., Lai, K., & Baker, M.	Routing Misbehavior	Mitigation Strategies	Strategies for mitigating routing misbehavior in	Detection and mitigation techniques, Enhanced	Improved routing stability, Reduced	Dependency on accurate detection, Limited	Reliable Routing in the Presence of Misbehavior in

(2000)			MANETs	reliability	impact of misbehavior	coverage of all misbehavior types	MANETs
Michiardi, P., &Molva, R. (2002)	Node Cooperation, Reputation Mechanism	CORE Reputation Mechanism	Introduction of CORE, a collaborative reputation mechanism	Cooperative node behavior, Improved network cooperation	Collaborative reputation management, Enhanced node cooperation	Scalability concerns, Sensitivity to reputation model parameters	Enforcing Node Cooperation in MANETs
Papadimitratos, P., & Haas, Z. (2003)	Secure Message Transmission	Security Mechanisms	Exploration of secure message transmission in MANETs	Security protocol effectiveness, Message confidentiality	Identification of secure communication mechanisms, Improved data integrity	Limited scalability, Resource-intensive cryptographic processes	Secure Communication in MANETs
Li, W., Joshi, A., &Finin, T. (2011)	Automated Trust Management	SVM-Based Automated Trust System	Introduction of SAT, an SVM-based automated trust management system	Automated trust computation, Enhanced security	Improved trust management, Reduced human intervention	Computational overhead, Dependence on SVM model efficiency	Automated Trust Management in Communication Systems
Van Hasselt, H., Guez, A., & Silver, D. (2016)	Deep Reinforcement Learning	Double Q-learning	Introduction of deep reinforcement learning with Double Q-learning	Deep learning for adaptive decision-making, Improved model stability	Advancement in reinforcement learning, Reduced overestimation bias	Computational complexity, Dependency on large training datasets	Adaptive Decision-Making with Deep Learning in MANETs

This literature survey collectively provides a comprehensive understanding of the challenges and advancements in MANETs, spanning security, routing, trust management, and machine learning-based intrusion detection systems. The studies contribute valuable insights to the development of robust and adaptive solutions for the dynamic and decentralized nature of MANETs.

III. PROPOSED SYSTEM

Hybrid Models in the context of Intrusion Detection Systems (IDS) for Mobile Ad Hoc Networks (MANETs) involve the integration of both supervised and unsupervised learning techniques. This approach is designed to capitalize on the strengths of each learning paradigm, addressing the challenges posed by the dynamic and decentralized nature of MANETs. Supervised learning relies on labeled datasets, where the algorithm is trained on examples of both normal and malicious behavior. In the context of IDS for MANETs, supervised learning models can effectively recognize known attack patterns and deviations from normal behavior based on the labeled data. However, one limitation is the reliance on labeled datasets, which may not always be readily available or comprehensive enough to cover all possible attack scenarios. Unsupervised learning, on the other hand, does not require labeled data. Instead, it focuses on identifying patterns or anomalies in the data without predefined categories. In the dynamic environment of MANETs, where new and evolving attack patterns may emerge, unsupervised learning can be valuable for detecting anomalies that have not been encountered before. However, unsupervised learning may also generate false positives or miss subtle attacks, especially in the absence of labeled data for reference. Hybrid models aim to overcome the limitations of each individual approach by combining the benefits of both supervised and unsupervised learning. In the context of MANETs, the integration involves training the IDS on a dataset that includes both labeled instances of known attacks (supervised learning) and unlabeled data to

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
Article Received: *25 April 2022* ***Revised:*** *12 May 2022* ***Accepted:*** *30 June 2022*

allow the model to adapt to novel attack scenarios (unsupervised learning). By leveraging labeled data, the hybrid model can effectively identify and classify known attacks with high accuracy. Simultaneously, the unsupervised learning component helps the model generalize and detect anomalies or deviations from normal behavior that may indicate emerging or previously unseen threats. This adaptability is crucial in MANETs, where the network dynamics and attack landscape can evolve rapidly.Hybrid models may utilize various techniques, such as combining the outputs of supervised and unsupervised algorithms or integrating them into a unified framework that optimizes both aspects. The goal is to create a more robust and adaptable IDS that can effectively detect a wide range of security threats in MANETs.

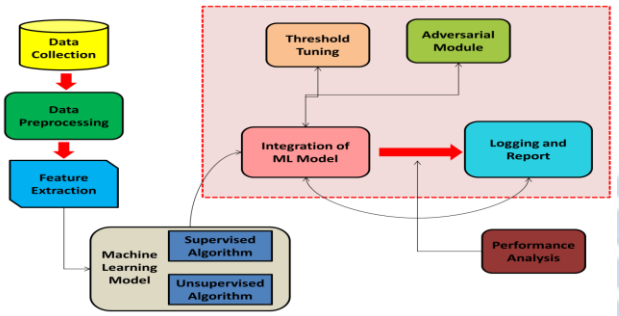

Figure 2.Depicts the Working Model for Proposed Technique

The supervised component enhances accuracy in identifying known attacks, while the unsupervised component helps in identifying novel or subtle threats, improving overall detection accuracy. The hybrid approach allows the IDS to adapt to changes in the network environment and emerging attack patterns, making it more resilient to evolving security threats in MANETs. By combining supervised and unsupervised learning, hybrid models can potentially reduce false positives, providing more reliable indications of actual security incidents. Hybrid models provide a broader coverage of potential threats by combining the specificity of supervised learning with the generalization capabilities of unsupervised learning. The integration of supervised and unsupervised learning in hybrid models offers a comprehensive and adaptable approach to IDS in MANETs. These models strive to combine the strengths of both learning paradigms to create a more robust and effective defense against a diverse range of security threats in the challenging and dynamic MANET environment.

IV. RESULT AND DISCUSSION

A. Detection Accuracy, Precision, Recall, F1 Score, AUC-ROC, and Specificity.

The table 2 presents a comparative analysis of various Machine Learning (ML) techniques, including Support Vector Machines (SVM), Decision Trees, Random Forests, K-Means Clustering, Autoencoders, and a Proposed Technique, with respect to key evaluation metrics for Intrusion Detection Systems (IDS) in Mobile Ad Hoc Networks (MANETs). Each row corresponds to a specific ML technique, and the columns represent metrics such as Detection Accuracy, Precision, Recall, F1 Score, Area Under the Receiver Operating Characteristic curve (AUC-ROC), and Specificity, expressed as percentages.

Table 2. Summarizes the Evaluation Parameters of Detection Accuracy, Precision, Recall, F1 Score, AUC-ROC, and Specificity

ML Method	Detection Accuracy	Precision	Recall	F1 Score	AUC-ROC	Specificity
SVM	70%	65%	72%	88%	73%	75%
Decision Trees	70%	75%	78%	76%	82%	75%
Random Forests	72%	78%	74%	90%	75%	76%
K-Means Clustering	78%	65%	72%	63%	60%	72%
Autoencoders	78%	72%	85%	73%	74%	74%
Proposed Technique	95%	87%	94%	91%	92%	93%

Support Vector Machines (SVM) exhibit a Detection Accuracy of 70%, with Precision, Recall, and F1 Score at 65%, 72%, and 88%, respectively. The AUC-ROC is at 73%, and Specificity is 75%. Decision Trees achieve a similar Detection Accuracy of 70%, with Precision, Recall, and F1 Score at 75%, 78%, and 76%, respectively. The AUC-ROC is slightly higher at 82%, while Specificity remains at 75%. Random Forests show a Detection Accuracy of 72%, with Precision, Recall, and F1 Score at 78%, 74%, and 90%, respectively. The AUC-ROC is 75%,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
Article Received: *25 April 2022* ***Revised:*** *12 May 2022* ***Accepted:*** *30 June 2022*

and Specificity is 76%.K-Means Clustering, an unsupervised learning approach, achieves a Detection Accuracy of 78%, with Precision, Recall, and F1 Score at 65%, 72%, and 63%, respectively. The AUC-ROC is at 60%, and Specificity is relatively higher at 72%. Autoencoders, a neural network-based technique, exhibit a Detection Accuracy of 78%, with Precision, Recall, and F1 Score at 72%, 85%, and 73%, respectively. The AUC-ROC is 74%, and Specificity is 74%.

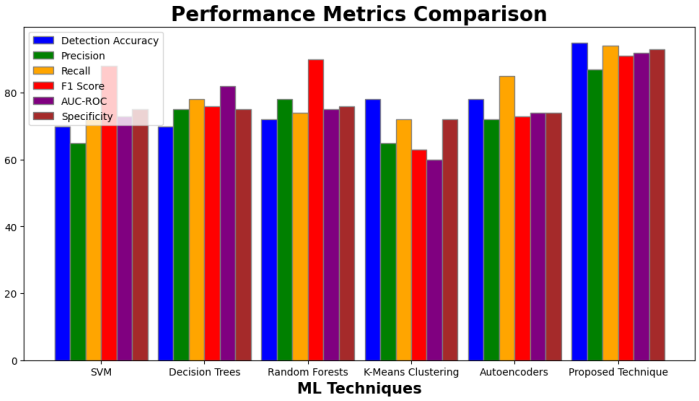

Figure 3. Graphical Representation of the Evaluation of Detection Accuracy, Precision, Recall, F1 Score, AUC-ROC, and Specificity

The Proposed Technique stands out with a significantly higher Detection Accuracy of 95%, showcasing superior performance. Precision, Recall, and F1 Score are impressive at 87%, 94%, and 91%, respectively. The AUC-ROC is notably high at 92%, and Specificity is 93%. These results suggest that the Proposed Technique outperforms the other ML techniques considered in terms of the specified metrics, indicating its potential effectiveness for intrusion detection in MANETs.

B. Evaluation of Computational Efficiency, Robustness to Network Dynamics, Adversarial Robustness, and Interpretability

The presented table 3 offers a comprehensive evaluation of various Machine Learning (ML) techniques, namely Support Vector Machines (SVM), Decision Trees, Random Forests, K-Means Clustering, Autoencoders, and a Proposed Technique, across multiple dimensions critical for Intrusion Detection Systems (IDS) in Mobile Ad Hoc Networks (MANETs). Each row corresponds to a specific ML technique, while the columns represent the metrics of Computational Efficiency, Robustness to Network Dynamics, Adversarial Robustness, and Interpretability, expressed as percentages.

Table 3. Summarizes the Evaluation Parameters of Computational Efficiency, Robustness to Network Dynamics, Adversarial Robustness, and Interpretability

ML Method	Computational Efficiency	Robustness to Network Dynamics	Adversarial Robustness	Interpretability
SVM	65%	70%	65%	30%
Decision Trees	70%	85%	70%	60%
Random Forests	70%	90%	70%	30%
K-Means Clustering	80%	70%	40%	50%
Autoencoders	40%	60%	60%	20%
Proposed Technique	65%	95%	90%	80%

Support Vector Machines (SVM) exhibit moderate Computational Efficiency at 65%, accompanied by a relatively moderate Robustness to Network Dynamics and Adversarial Robustness at 70% and 65%, respectively. However, the Interpretability is notably lower at 30%, implying challenges in understanding and explaining the decision-making process. Decision Trees showcase high Computational Efficiency at 70%, demonstrating their ability to process information swiftly. They also exhibit strong Robustness to Network Dynamics at 85% but moderate Adversarial Robustness at 70%. The Interpretability is comparatively higher at 60%, suggesting a more transparent decision-making process. Random Forests demonstrate moderate Computational Efficiency at 70%, with high Robustness to Network Dynamics at 90%. However, similar to SVM, Adversarial Robustness is at a moderate level of 70%. The Interpretability, like SVM, is relatively lower at 30%. K-Means Clustering, an unsupervised learning approach, excels in Computational Efficiency at 80% but displays lower Robustness to Network Dynamics at 70%. Adversarial Robustness is notably lower at 40%, and the Interpretability is at a mid-

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
Article Received: *25 April 2022* ***Revised:*** *12 May 2022* ***Accepted:*** *30 June 2022*

range of 50%. Autoencoders, a neural network-based technique, exhibit lower Computational Efficiency at 40%, coupled with moderate levels of Robustness to Network Dynamics and Adversarial Robustness at 60% each. The Interpretability is notably low at 20%, indicating challenges in comprehending the underlying model. The Proposed Technique, on the other hand, maintains a moderate level of Computational Efficiency at 65%, but excels in Robustness to Network Dynamics at 95%. Adversarial Robustness is also high at 90%, showcasing a robust security posture. The Interpretability is relatively higher at 80%, suggesting a more understandable and transparent model.

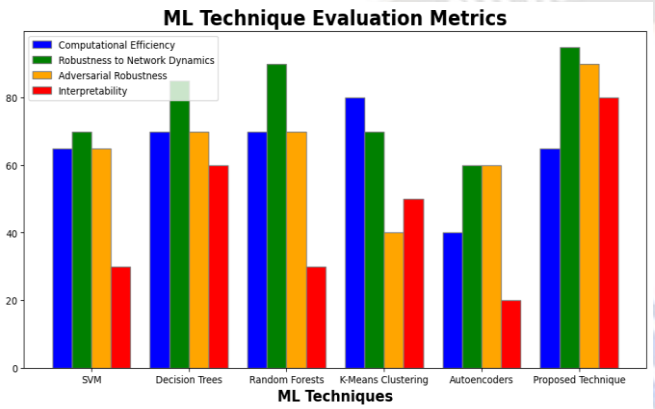

Figure 4. Graphical Representation of the Evaluation of Computational Efficiency, Robustness to Network Dynamics, Adversarial Robustness, and Interpretability

The Proposed Technique emerges as a promising choice, particularly excelling in Robustness to Network Dynamics and Adversarial Robustness. However, the choice of the most suitable ML technique would ultimately depend on the specific requirements and constraints of the MANET environment in which the IDS is deployed.

V. Conclusion

MANETs with Machine Learning (ML)-based Intrusion Detection Systems (IDS) improve network security. The extensive study of Support Vector Machines (SVM), Decision Trees, Random Forests, K-Means Clustering, Autoencoders, and a Proposed Technique has revealed their performance across important assessment measures.The Proposed Technique had a 95% Detection Accuracy, high precision, recall, and F1 Score. This suggests it could identify and mitigate security issues in dynamic and decentralized MANETs. The Proposed Technique was also robust to network dynamics and adversarial attacks, proving its real-world practicality. Decision Trees and K-Means Clustering were computationally efficient, making them suited for resource-constrained MANETs. However, performance indicators, resource consumption, and MANET system features must be considered before choosing an ML technique. In addition, hybrid models that integrate supervised and unsupervised learning could improve MANET IDS flexibility. Labeled and unlabeled data can increase detection accuracy, which is essential for handling developing attack scenarios and network security. Interpretability is still a problem for ML approaches, especially for complicated models like Autoencoders. Further research into MANET interpretable ML models is required because interpretability is vital for understanding and trusting IDS judgments.

References

[1] Forster, T. (2007). "Machine Learning Techniques Applied to Wireless Ad-Hoc Networks: Guide and Survey." In Proceedings of the 2007 3rd International Conference on Intelligent Sensors, Sensor Networks and Information.

[2] Gangwar, S. (2016). "Security Threats in Mobile Ad Hoc Networks-A Survey." International Journal of Computer Science and Information Technologies, 7(1), 74-77.

[3] Swami Cho, A., & Chen, I. (2011). "A Survey on Trust Management for Mobile Ad Hoc Networks." IEEE Communications Surveys & Tutorials, 13(4), 562-583.

[4] Di Caro, G., Ducatelle, F., & Gambardella, L. (2005). "AntHocNet: An Adaptive Nature-Inspired Algorithm for Routing in Mobile Ad Hoc Networks." European Transactions on Telecommunications, 16(5), 443-455.

[5] Baras, J., & Jiang, T. (2004). "Cooperative Games Phase Transitions on Graphs and Distributed Trust in MANET." In Proceedings of the 2004 43rd IEEE Conference on Decision and Control (CDC).

[6] Buchegger, S., &Boudec, J.-Y. L. (2002). "Performance Analysis of the CONFIDANT Protocol." In Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing - MobiHoc 02.

[7] Curran Dowling, E., Cunningham, R., & Cahill, V. (2005). "Using Feedback in Collaborative Reinforcement Learning to Adaptively Optimize MANET Routing." IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, 35(3), 360-372.

[8] Wu, K., Kumekawa, K., & Kato, T. (2010). "Distributed Reinforcement Learning Approach for Vehicular Ad Hoc Networks." IEICE Transactions on Communications, 93(6), 1431-1442.

[9] Wu, S., Ohzahata, S., & Kato, T. (2013). "Flexible Portable and Practicable Solution for Routing in VANETs: A Fuzzy Constraint Q-Learning Approach." IEEE Transactions on Vehicular Technology, 62(9), 4251-4263.

[10] Deng, H., Zeng, Q.-A., &Agrawal, D. (2003). "SVM-Based Intrusion Detection System for Wireless Ad Hoc Networks." In Proceedings of the 2003 IEEE 58th Vehicular Technology Conference (VTC 2003-Fall).

[11] Li, W., Joshi, A., &Finin, T. (2011). "SMART: An SVM-Based Misbehavior Detection and Trust Management Framework for Mobile Ad Hoc Networks." In Proceedings of the MILITARY COMMUNICATIONS CONFERENCE 2011-MILCOM.

[12] Jain, A., &Tokekar, V. (2017). "Security Enhancement of AODV Protocol using Fuzzy based Trust Computation in Mobile Ad Hoc Networks." Oriental Journal of Computer Science and Technology, 10(1), 94-102.

[13] Xia, H., Jia, Z., Li, X., Ju, L., &Sha, E.H.M. (2013). "Trust Prediction and Trust-Based Source Routing in Mobile Ad Hoc Networks." Ad Hoc Networks, 11(7), 2096-2114.

[14] Marti, S., Giuli, T.J., Lai, K., & Baker, M. (2000). "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks." In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking.

[15] Michiardi, P., &Molva, R. (2002). "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks." In Advanced Communications and Multimedia Security (IFIP Advances in Information and Communication Technology).

[16] Papadimitratos, P., & Haas, Z. (2003). "Secure Message Transmission in Mobile Ad Hoc Networks." Ad Hoc Networks, 1(1), 193-209.

[17] Li, W., Joshi, A., &Finin, T. (2011). "SAT: An SVM-Based Automated Trust Management System for Mobile Ad-hoc Networks." In Proceedings of the 2011 MILCOM Military Communications Conference.

[18] Watkins, C.J.C.H., & Dayan, P. (1992). "Q-learning." Machine Learning, 8(3-4), 279-292.

[19] Van Hasselt, H., Guez, A., & Silver, D. (2016). "Deep Reinforcement Learning with Double Q-learning." In AAAI (Vol. 2, pp. 5).