IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Modern Techniques For Machine Learning-Based Security In Manets

Dr. S. Menaka[1] , Mr. P. Sivakumar[2] , Mrs. C. Meera Bai[3] and Mrs. N. Anandha Priya[4]

Department of Computer Applications,
Nehru Institute of Information Technology and Management, Coimbatore, Tamil Nadu, India

Abstract

Machine learning (ML) approaches, based on several logical and statistical processes, provide a system the ability to learn and promote adaptability to the environment. Recognizing complicated patterns and making judgments based on the findings is the main objective of machine learning. Different machine learning methods are used to protect mobile ad hoc networks. The lack of infrastructure in MANETs makes it extremely difficult to build security measures. The security strategies used in MANETs primarily concentrate on routing path security, outlier/bad-behaviour/selfish node removal, intrusion detection, and the mitigation of malicious assaults. In order to provide effective security solutions, the researchers have been utilizing cutting-edge technologies while taking into account the dynamic environment of MANETs. These technologies include machine learning, artificial intelligence (AI), approaches based on genetic algorithms, algorithms inspired by biological processes, and others. This examination of several contemporary methods for enhancing security in MANETs is thorough and methodical, and it is presented in this paper.

Keyword: MANET, Denial-of-Service, AODV, Neural Networks, Gray hole Attack.

1. Introduction

Mobile nodes that are connected via wireless technology form the basis of the dynamic, infrastructure-free MANET [1]. The special qualities of MANETs expand its use in fields like the military, virtual conferences, and rescue missions where installing infrastructure is impractical. Security in this network is a problem in important situations, such as combat communication. The network's flaws make it a desirable target for assaults that aim to compromise security. Therefore, it is crucial to pick a reliable and adaptable security system that is strong enough to block any hostile activity from the network.

The topology of the network is not stable since mobile nodes in MANETs are dynamic, which makes it extremely difficult to apply any security measures. The network is self-configured and self-deployed; there is no available central authority for communication [2]. The network is more vulnerable to mistakes and security concerns since nodes communicate with one another wirelessly. Each node is also linked to other nodes nearby, allowing for multi-hop communication, in which data packets are sent by several nodes along the way. As a result, numerous new areas of research in MANET security are made possible by the limitations of the dynamic architecture in MANETs [3]. In an ad hoc context, ML-based algorithms may be used to build a predictive model for identifying unknown security concerns. As a result, the remaining sections of this article clearly outline how ML-based algorithms contribute to MANET security.

2. Methods for MANET Security

Decentralization and other distinctive characteristics of MANETs, such as self-management, etc., make the network a target for several assaults. Several security measures have been put forward in the past ten years to both prevent and detect intrusions. Following is a general breakdown of various strategies:

The use of cryptography was a key component of the initial security protocols in MANETs. A threshold cryptography-based key management system was put into place in 1999 to provide authentication in ad hoc networks. A few nodes assumed the position of administrator, while some nodes carried out the work of servers in the suggested system. Additionally, a SAODV, or secure AODV, version was suggested [4]. The suggested approach utilized hash chains and digital signatures for cryptographic security in ad hoc networks. Many different cryptographic techniques relied on a central authority to distribute certificates for authentication. [5][6][7][8].

However, various other techniques, like to the PGP web of trust model, changed the idea of central oversight [9][10]. The authentication procedure in these approaches comprises a chain of certificates maintained at their endpoints since each node is equipped to keep its certificates. In the literature, it has been noted that cryptographic algorithms cause communication to lag significantly and require the maintenance of a previous link between nodes, which is impractical in ad hoc networks. Therefore, the researchers gathered a sizable number of hybrid techniques for MANET security augmentation.

The nodes in MANETs are vulnerable to both active and passive assaults of various types. Denial-of-service attacks, man-in-the-middle attacks, flooding, spoofing, impersonation, black hole and grey hole attacks, etc., are a few examples of frequent assaults. Different intrusion detection methods are used in literature to identify distinct types of assaults.

In a nutshell, a variety of cryptographic mechanisms were used in the past to add security features to MANETs. However, in the last ten years, there has been a change in network paradigm as a result of new technologies like machine learning, deep learning, AI, and genetic algorithms becoming a significant choice for researchers in order to find efficient and optimized solutions for security in MANETs. As a result, this paper discusses cutting-edge technologies that have shown to be highly successful in delivering security solutions. It featured a variety of machine learning-based secure routing algorithms and the detection, prevention, prediction, and mitigation of compromised nodes.

3. Security Solutions Based on Machine Learning

Any network function, including packets and routing protocols, must have security. Consideration must be given to the network's important security aspects while developing sensitive applications. Machine learning approaches aid in the creation of prediction models, which are evaluated using the remaining test data after being trained on the training data for certain attack patterns. The learning model's accuracy is evaluated depending on how well it can spot new assault patterns.

Nodes in MANETs are more vulnerable to several forms of assaults because of the open network environment, including black holes, worm holes, grey holes, floods, denial-of-service attacks, etc.

The nodes in MANETs also support multi-hop communication, which means that before reaching the destination node, the source node sends packets to a number of intermediate nodes. The cooperation of the nodes is a must for any communication. In order to prevent packets from being transmitted to any malicious or unreliable nodes in the network, it is crucial to determine the trustworthiness of the nodes. Numerous trust evaluation techniques have been put out in the literature to achieve this goal and increase network security. As indicated in Figure 1, security techniques in MANETs may be divided into the following groups.

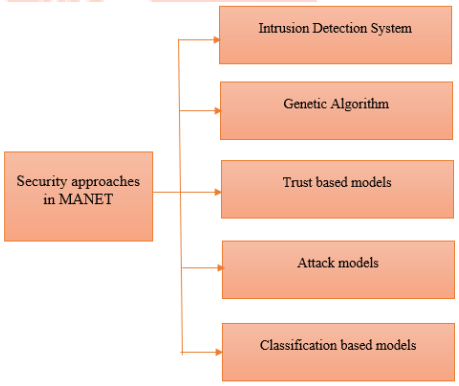

Figure 1. Classification of Security Approaches in MANETs

Additionally, ML is essential for boosting the security of mobile ad hoc networks. In MANETs, a variety of ML algorithms may be effectively used to recognize intrusions as well as certain attack patterns. However, a number of trustworthy systems are also suggested in the literature to enhance network security aspects. As a result, the following three ML-based security strategies for MANETs are described.

3.1 Machine Learning Based Intrusion Detection System

A defence system used in MANETs to monitor and look into ominous situations is called an IDS (Intrusion Detection System). It has a number of techniques for locating various kinds of network problems. Due to the

open nature of MANETs, nodes can join and depart at any moment, making the network more susceptible to many types of assaults. IDS's main goal is to spot malicious activity before it may do harm to the network. As a result, every node in MANETs has an IDS to block illegal access. Implementing IDS in real-world applications is quite difficult due to the resource limitations faced by nodes in MANETs. Machine learning methods assist in recognizing a wide range of fresh threats and weaknesses. IDS may be set up using a variety of machine learning methods, including fuzzy logic, genetic algorithms, Bayesian theory, and neural networks.

Anomaly detection systems, abuse detection systems, and signature-based detection systems are the three basic categories into which IDS may be divided [11]. By comparing a node's behaviours with the typical normal patterns, anomaly detection systems may exclude outlier or untrusted nodes. When a node exhibits unusual behaviour, it is classified as an incursion. On the other hand, because abuse detection systems and signature-based systems rely on the previously stored behaviour patterns or signatures, they cannot identify new threats. As a result, anomaly detection systems outperform other methods of vulnerability discovery since they are based on the assumption that an intrusive party would never adopt a typical attack strategy. However, they suffer from a high rate of false alarms.

In order to implement certain strategies that aid in minimizing the true negatives and false negatives in the systems and boosting security in MANETs, ML based IDSs have emerged as an intriguing option for the research community. The categorization of normal and intruder nodes in ML may be done using a variety of methods. In 2003, two innovative IDSs with distributed and hierarchical architectures were released [12]. The suggested frameworks used the SVM classification approach and were primarily created for network layer security.

Later, a different classification-based IDS was put out, and the authors created a hybrid model for adding security to MANETs based on Bayesian classifier, Markov chain rules, and Association rule mining [13]. The suggested approach offered security at many layers, including the MAC, routing, and application layers. The properties of the nodes at various tiers were then assessed in order to spot the fake nodes.

In addition, a multi-level hierarchical model was created for data collection and processing by applying ensembles classification methods with relation to developing ensemble classifiers for IDS [14]. Clustering approaches were examined in this to process the anomaly indexes. Using two distinct routing protocols and a multi-attack model, the ensemble model was tested.

The benefits of averaging with detection accuracy, which can get better as you move up the node-cluster hierarchy, were deduced by the authors in amazing ways. By using ANN-based IDS in MANETs, the security was increased even more [15]. The model was especially suggested for DoS-style assaults. Although the authors stated that the simulated model had a very high level of detection accuracy, it may perform even better if fewer characteristics were chosen for implementation.

In 2014 [16], a KNN-based unique IDS was suggested. To categorize the nodes based on information for anomaly detection, the model uses the Conformal Prediction K-Nearest Neighbour (CP KNN) algorithmic rule. Non-conformity score value was utilized for multilevel repetition to shorten the categorization time. High detection accuracy was observed in the model, with a high true positive rate and a low false positive rate. Even with noisy data, the authors claimed a high level of confidence.

Additionally, a brand-new IDS model that is independent of routing protocols and is based on SVM classification methodology was unveiled [17]. The suggested approach is designed to recognize DoS-style assaults. With a high detection rate of 94%, the nodes were divided into normal and pathological nodes. The scientists noted that, in contrast to node mobility in the network, system performance did not suffer and actually increased the network's resilience significantly.

In 2019 [18], a further impressive IDS-based ANN method was described. The malicious nodes in the network were found, classified, and blacklisted using the model's implementation of classification based on ANN. The suggested model's detection rate of 88% demonstrated its excellent accuracy.

3.2 Machine Learning-Based Detection of Compromised or Outlier Nodes in MANETs

The difficulty in identifying and mitigating different types of assaults is the main problem with how MANETs operate [19]. Due to the open wireless nature of the network, the nodes in MANETs are extremely unsafe. This has sparked the attention of various researchers in

maintaining their security by utilizing cutting-edge technology, some of which have been covered in the preceding section.

It was suggested to use the SVM classification technique to create a model for flooding attack detection [20]. The authors evaluated the model in a simulated environment after training the SVM with a variety of assault patterns, including flooding attacks.

The findings demonstrate that the model can accurately identify flooding attacks but is unable to produce results that are adequate for multi-attack models. In order to distinguish normal and misbehaving nodes based on their behaviour patterns, such as message forwarding rate, fluctuating number of destinations in sending messages, etc., an enhanced attack classification model using KNN (K Nearest Neighbours) for wireless networks was highlighted [21]. Although the implementation yields precise results, there is no method for producing datasets. Additionally, a novel approach for categorizing normal and misbehaving nodes in MANETs was established [22]. The categorization is carried out based on the nodes' behaviour in terms of packet dropping, and the authors used SVM model with Ad-hoc on-demand routing protocol. A calculation of the packet delivery ratio, packet modification, and misroute ratio was used to assess the performance of the technique.

In order to identify assaults, a hybrid strategy combining SOFM (Self Organized Features Maps) and genetic algorithms was put out in 2018 [23]. In this, Neutrosophic conditional variables in MANETs were defined using the SOFM's unsupervised learning capability. As input to the GA, these variables and training data are used to examine the fittest rules and find new attack patterns. The authors said that their method of identifying assaults was 99% accurate.

Additionally, a novel method for detecting Denial of Service Attacks based on SVM classification was demonstrated. The model's accuracy in accuracy detection and computing time were both examined by the authors. Researchers recently implemented a similar strategy that focused on processing time to identify rogue nodes [24][18]. They created a model for categorizing nodes into normal and banned nodes using an ANN classification technique. The accuracy of the prediction model created by the authors to detect numerous assaults in MANETs is only 88.23%.

2019 saw the description of a misbehaviour detection categorization into anomaly detection, intrusion detection, and misuse detection. The ability to recognize anonymous assaults for which a system is not taught is what the authors say the anomaly detection methods have over the other two approaches. An IDS (Intrusion Detection System) can, however, recognize an event that deviates from the expected pattern [11].

In order to determine the most effective model for predicting different types of assaults in MANETs, two categorization models were compared using input from simulated network packet data [17]. The accuracy and detection capability of both classification models—SVM and LR—with a low number of false alarms for network communication were evaluated. The findings demonstrated that LR outperformed SVM in terms of accuracy, detecting malicious assaults in the network with a 100% detection accuracy. In terms of specificity, sensitivity, accuracy, and misclassification rates, LR also maintained homogeneity. A location-based solution to misbehaviour detection for MANET security in 2020 was put forth [25]. The authors concentrated on the introduction of privacy through the use of effective cryptography algorithms and the optimal path computation utilizing Learning Automata.

3.3 A Trusted Machine Learning-Based System for Increasing Security in MANETs

The nodes in MANETs cooperate with one another to forward data packets while operating in an unstable environment. Therefore, each node is given or earned a trustworthiness value in order to safeguard the network. To ensure the network's dependability, several researchers are focusing on these security-related elements.

A trust system that evaluated the value of trust based on the opinions of K trustworthy entities over a predetermined period of time was introduced in 2004 [8]. The number of valid neighbours and the network's current state both affect the value of K. Conflicts within the network might, however, occasionally result from this. Fuzzy logic has been used to construct numerous trust approaches because trust measurements have dynamic, complicated, and fuzzy properties [26].

Based on condensed trust values, a worldwide strategy for assessing trust was offered [27]. In the described method, the trust model depended on a defined function to determine the level of confidence, and similarly, the researchers developed a trust strategy based on Bayesian theory [28]. In the dynamic context of MANETs, a reinforcement machine learning algorithm was constructed using a different strategy [29].

The authors assert that the method can forecast the network behaviour of new nodes without relying on past data. Additionally, an algorithm that can be

dispersed throughout the nodes must be picked while deciding on the optimum algorithm due to the physical dispersion of MANET information. It is advised to use a hybrid trust method that combines the trust values rather than taking into account direct and indirect trust individually. Additionally, a suggested enhanced trust model for MANETs based on deep learning and reinforcement learning [30]. By implementing the model using the AODV protocol and feeding simulated data into an RNN (Recurrent Neural Network), the authors were able to categorize nodes into trustworthy and untrustworthy nodes.

2019 saw the proposal of a fuzzy theory-based methodology for evaluating trust [31]. Three metrics, including Packet Drop Rate (PDR), Battery Discharge Rate (BDR), and Number of Link Requests (NLR), were employed in the suggested study. Comparing the suggested system to the current trust model on raising the fraction of malicious nodes, the new method offered more accuracy and reduced computational cost.[32]

4. Conclusion

Security implementation in MANETs is extremely difficult due to their dynamic nature. Numerous security strategies are put forward in the literature to lessen security hazards. Machine learning approaches have gained popularity among researchers because of their capacity to identify hidden or unidentified hazards. In this research, multiple ML algorithm-based security strategies for MANETs have been thoroughly characterized. The three categories of security techniques include machine learning-based IDS, attack detection models, and trust-based models.

References

[1] Goyal N and Gaba A 2013 A new approach of location aided routing protocol using minimum bandwidth in mobile ad- hoc network International Journal of Computer Technology and Applications 4 pp 653.

[2] Popli R, Garg K and Batra S 2016 SECHAM: Secure and efficient cluster head selection algorithm for MANET 3rd International Conference on Computing for Sustainable Global Development (INDIACom) pp 1776-1779 IEEE.

[3] Kamboj P and Goyal N 2015 Survey of various keys management techniques in MANET International Journal of Emerging Research in Management & Technology 4.

[4] Zapata M G and Asokan N 2002 Securing ad hoc routing protocols WiSE '02: Proceedings of the ACM workshop on Wireless security ACM Press.

[5] Zhou L, Hass Z J 1999 Securing ad hoc networks IEEE Network 13 pp 24-30.

[6] Buiati F, Puttini R, de Sousa R, Abbas C J B, Villalba L J G 2004 Authentication and Autoconfiguration for MANET Nodes 2004 Embedded and Ubiquitous Computing EUC 2004 Lecture Notes in Computer Science 3207 Springer.

[7] Asokan N, Ginzboorg P 2000 Key agreement in ad hoc networks Computer Communications 23 1627–1637.

[8] Seung Yi and Kravets R 2002 MOCA : Mobile Certificate Authority for Wireless Ad Hoc Networks OAI 2004.

[9] Hubaux J P, Buttyan L, and Capkun S 2001 The quest for security in mobile ad hoc networks Mobile Ad Hoc Networks Proceeding of the ACM Symposium on Mobile Ad Hoc Networking and Computing MobiHOC 2001.

[10] Capkun S, Buttya L and Hubaux J P 2003 Self-Organized Public-Key Management for Mobile Ad Hoc Networks IEEE Transactions on Mobile Computing 2.

[11] Hamza F and Vigila S M C 2019 Review of Machine Learning-Based Intrusion Detection Techniques for MANETs Proc. Computing and Network Sustainability pp 367-374 Springer.

[12] Deng H, Zeng Q and Agrawal D P 2003 SVM-based intrusion detection system for wireless ad hoc networks Proc 58th IEEE Vehicular Technology Conference (VTC03) 3 pp 2147–2151.

[13] Bose S, Bharathimurugan S and Kannan A 2007 Multi-layer intergraded anomaly intrusion detection for mobile ad hoc networks Proc IEEE International Conference on Signal Processing Communications and Networking (ICSCN 2007) p 360–365.

[14] Cabrera J.B.D., Gutirrez C., and Mehra R.K. 2008 Ensemble methods for anomaly detection and distributed intrusion detection in mobile ad hoc networks Information Fusion 9 pp 96–119.

[15] Moradi Z, Teshnehlab M and Rahmani A 2011 Implementation of neural networks for intrusion detection in MANET International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT).

[16] Lalli M and Palanisamy V 2014 A novel intrusion detection model for mobile ad-hoc networks using CP-KNN International Journal of Computer Networks & Communications (IJCNC) 6.

[17] Sebopelo R, Isong B and Gasela N 2019 Identification of Compromised Nodes in MANETs using

Machine Learning Technique International Journal of Computer Network and Information Security 11.

[18] Sowah R A, Ofori-Amanfo K B, Mills G A and Koumadi K M 2019 Detection and prevention of man-in-the-middle spoofing attacks in MANETs using predictive techniques in Artificial Neural Networks (ANN) Journal of Computer Networks and Communications.

[19] Goyal N, Sandhu J K, Verma L 2021 CDMA-Based Security Against Wormhole Attack in Underwater Wireless Sensor Networks Advances in Communication and Computational Technology Lecture Notes in Electrical Engineering 668 Springer pp 829-835.

[20] Patel M, Sharma S and Sharan D 2013 Detection and prevention of flooding attack using SVM Proc of the 3rd International Conference on Communication Systems and Network Technologies CSNT pp. 533–537.

[21] Wenchao Li, Ping Yi, Yue Wu, Li Pan and Jianhua Li 2014 A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network Journal of Electrical and Computer Engineering 2014 Article ID 240217.

[22] Patel N J and Jhaveri R H 2015 Detecting packet dropping misbehaving nodes using support vector machine (SVM) in MANET International Journal of Computer Applications 122.

[23] Elwahsh H, Gamal M, Salama A A and Henawy I M 2018 A novel approach for classifying MANETs attacks with a neutrosophic intelligent system based on genetic algorithm Security and Communication Networks 2018 Article ID 5828517 pp 1-10.

[24] Shams E A and Rizaner A 2018 A novel support vector machine based intrusion detection system for mobile ad hoc networks Wireless Networks 24 pp 1821-1829.

[25] Suma R, Premasudha B G and Ravi R V 2020 International Journal of Networking and Virtual Organisations 22 pp.17 – 41.

[26] Nefti S, Meziane F and Kasiran K 2005 A fuzzy trust model for e-commerce IEEE International Conference on ECommerce Technology pp 401–404.

[27] Damiani E, Vimercati S.D.C.D., Samarati P 2006 A wowa-based aggregation technique on trust values connected to metadata. Electron Notes Theor. Comput. Sci. 157 pp 131–142.

[28] Josang A and Quattrociocchi W 2009 Advanced features in Bayesian reputation systems TrustBus LNCS 5695 pp 105– 114 Springer.

[29] Jinarajadasa G, Rupasinghe L and Murray I 2018 A reinforcement learning approach to enhance the trust level of MANETs National information technology conference (NITC) pp 1-7 IEEE.

[30] Jinarajadasa G M and Liyanage S R 2019 A trust based advanced machine learning approach for mobile ad-hoc network security 4th International Conference on Advances in Computing and Technology (ICACT–2019).

[31] Popli R, Juneja V, Garg K and Gupta D V 2019 Fuzzy Based Trust Evaluation Model for Enhancing Security in MANETs International Journal of Engineering and Advanced Technology (IJEAT) 8 pp 506-510.

[32] Machine Learning Based Security Solutions in MANETs: State of the art approaches Renu Popli1 , Monika Sethi2 , Isha Kansal3 , Atul Garg4 and Nitin Goyal (ICMAI 2021)