ML-Based Detection of Sybil Attack on MANETS

Humaira Ashraf , Mamona Nawaz , NZ Jhanjhi *

Posted Date: 5 January 2024

doi: 10.20944/preprints202401.0508.v1

Keywords: Sybil Attacks; MANETs; Detection Techniques

Article

ML-Based Detection of Sybil Attack on MANETS

Dr. Humaira Ashraf [1], Mamona Nawaz [1] and NZ Jhanjhi [2,*]

[1] Department of Computer Science, IIU; humaira.ashraf@iiu.edu.pk (H.A.); mamoonanwaz62@gmail.com (M.N.)
[2] Scholar of Computer Science, SCS, Taylors University, Subang Jaya, Malaysia
* Correspondence: noorzaman.jhanjhi@taylors.edu.my

Abstract: Mobile Ad hoc Networks (MANETs) play an important role in the technological era by enabling wireless communication in dynamic and infrastructure-free contexts. Because of Manet's unique qualities and decentralized nature, MANETs are subject to many attacks such as the Blackhole attack, grey hole attack, Byzantine attack, Wormhole attack, and Sybil attack. Sybil attacks pose a substantial risk to MANETs. A Sybil attack occurs when a malicious node impersonates many identities inside the network, resulting in the creation of multiple suspicious nodes that appear as independent entities. This study presents a thorough analysis of the literature on the detection of Sybil attacks on MANETs. To find gaps in the literature, current surveys are also looked at. Also taken into consideration are several contemporary systems built on distinct techniques. In terms of throughput, detection rate, low energy consumption, packet delivery ratio, and end-to-end latency, some recent methods-based approaches are also evaluated severely. To address the stated state-of-the-art issues in Sybil attack detection, this paper suggests ML-based strategies as the most suitable answer. Machine learning has huge potential for effective wireless network management. According to the researcher, this is the first comprehensive assessment of ML-based techniques for Sybil attack detection in wireless networks. Finally, we considered the unsolved issues in Sybil assault detection in wireless networks.

Keywords: Sybil Attacks; MANETs; Detection Techniques

1. Introduction

Wireless networks made up of mobile nodes that may connect without a fixed infrastructure are known as mobile ad-hoc networks (MANETs). Due to their dynamic nature, these networks are susceptible to several assaults, including Sybil, Byzantine, Black hole, Gray hole, and gray hole attacks. An exclusive kind of association layer attack in a mobile ad-hoc network is the Sybil attack. In this assault, a fake hub appears that offers a direct route to the target.. [1]

The Sybil nodes can be used to launch several types of attacks, for example, routing table poisoning or selective forwarding attacks, which can disrupt the network's operation or compromise its security. Detecting and preventing Sybil attacks on MANETs is necessary to ensure the network's security, reliability, resource utilization, and trustworthiness.

The detection of Sybil attacks in MANETs is important for ensuring the security and reliability of the network. By interfering with communication and clogging the network, sybil assaults can significantly affect the performance of MANETs and increase the risk of a denial of service (DoS) attack. Additionally, Sybil attacks can be used to launch additional assaults such as a black holes, wormholes, and sinkhole attacks, which can further compromise the network. Therefore, the detection of Sybil attacks is critical for the effective operation of MANETs.

This research aims to develop an ML-based approach for detecting Sybil attacks in MANETs. This method will use the power of machine learning algorithms to discover patterns and abnormalities in network data and identify Sybil nodes with high accuracy and low false-positive rates. The suggested technique for Sybil attack detection in MANETs will be compared to established approaches, and the results will be assessed in terms of detection accuracy, false-positive rate, and

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 January 2024 doi:10.20944/preprints202401.0508.v1

computing complexity. However, this research aims to prevent MANETs from Sybil attacks by providing Machine Learning detection techniques currently being employed to overcome security challenges within MANETs.

The research question for detecting Sybil attacks in MANETs is how can we develop an effective and efficient Sybil detection mechanism using machine learning techniques to accurately identify Sybil nodes and distinguish them from legitimate nodes in MANETs while minimizing the falsely positive and falsely negative rates and minimizing the computing cost of the detection process.

The detection of Sybil attacks in MANETs has a broad scope, which involves the creation of effective and efficient Sybil detection algorithms utilizing machine learning techniques. The scope of the research comprises identifying Sybil nodes, distinguishing these nodes from genuine nodes, and evaluating the detection mechanism's effectiveness in terms of accuracy, false-positive and false-negative rates, and computing overhead.

The detection of Sybil attacks in MANETs also has some limitations. The following are some of the limitations of detecting Sybil attacks in MANETs:

1. The detection of Sybil attacks using machine learning techniques requires computational resources, which can increase the overhead of the detection mechanism. Therefore, the research needs to focus on developing efficient detection mechanisms that minimize the computational overhead.
2. MANETs have a dynamic network topology, which can make it challenging to detect Sybil attacks. The research needs to explore how to adapt the detection mechanism to changes in the network topology and improve the performance of the mechanism under such conditions.

   MANETs lack a centralized authority, which makes it difficult to manage and secure the network. The research needs to explore how to develop Sybil detection mechanisms that can operate in a decentralized network environment.

Various machine learning algorithms, such as decision trees, random forests, support vector machines, and deep learning approaches, can also be investigated, to enhance the performance of the detection mechanism.

Aim:

To find better accuracy with the help of Support Vector Machine (SVM) Scheme for detection of sybil attack on MANETs by using some selected features of NSL-KDD Dataset like protocol types, source and destination IP addresses, duration and flags.

Objectives:

To propose an efficient technique based on machine learning for detecting Sybil attacks by focusing on detection accuracy and power consumption keeping in view.

Problem Statement:

Existing methods for detecting Sybil attacks on MANETs are not effective properly in real-time to minimize the impact on network performance. The detection mechanism should consider high-power consumption. The effectiveness of the detection mechanism is not evaluated through different experiments, considering factors such as detection accuracy, false positive and false negative rates.

The table summarizes known surveys of Sybil detection systems. The brief specifies the primary emphasis of the existing surveys. The distinction between existing surveys and this article is also discussed.

Table 1. Summary of surveys of Sybil detection attack techniques.

Year	Main Focus of the Survey	Major Contributions	Enhancement in Research Papers

 doi:10.20944/preprints202401.0508.v1

2022	A Complete Analysis of Security Attacks in MANET	Bharti et al. [2] reviewed to provide us with various types of security attacks like Sybil Attacks, Blackhole Attacks, Security Attacks, and Rushing Attacks. This paper is useful to prevent networks from security challenges.	The researcher gives a critical study, compares outcomes, and identifies holes in all known methodologies.
2022	A Comprehensive Review of Various Attacks in Mobile Ad Hoc Networks	Shekhar et al. [3] introduce mobile ad hoc networks (MANETs) and numerous sorts of attacks in MANETs, as well as preventative measures stated by many researchers to limit their impact on network performance.	The researcher provides a thorough comparison review of all available methodologies as well as a detailed critical critique.
2022	An Overview of Risk Identification, Intrusion Detection, and Machine Learning Techniques used concerning MANETs	Micheal et al. [4] provide an overview of existing studies on MANETs. It also Introduces a new technique to identify the primary Risk Profile of MANETS by using machine learning techniques. It discovers new areas of probability-based methods to further enhance the existing impact-based techniques for evaluating threats within MANETs.	The researcher provides a thorough literature study as well as a solution to detect holes in existing strategies for preventing Sybil attacks on MANETs.

 doi:10.20944/preprints202401.0508.v1

2021	Review on Security Attacks and Intrusion Detection Techniques in MANETs	Alazab et al. examined intrusion detection systems in the context of the mobile ad-hoc network. In MANET, however, a single classifier was employed to detect the amount of infiltration. Using a random forest model, a hybrid intelligent approach was developed to handle the challenges associated with a mixture of classifiers and minimize the best possible false alarm rates. Though the false positive rate was reduced by using several classifiers and increasing node density at different time intervals, the strategy was not an efficient model.	The researcher provides a full literature overview of existing methodologies as well as a thorough critical critique. It also incorporates strategies based on machine learning.
2022	An Analysis of Essential Challenges and Attacks on MANET Security Appraisal	Singla et al. [5] identify a variety of attacks on MANET and strategies for countering them. This research examines various security features, challenges, attacks, and solutions for repelling attacks in several stages.	The researcher conducts a thorough critical examination of all available approaches. However, research gaps and problems are noted as well.
2015	A Review on Sybil attack detection techniques	Kamani et al. [6] The surveyed document provides a brief overview of several	The researcher thoroughly describes all existing procedures and identifies a

 doi:10.20944/preprints202401.0508.v1

		Sybil attack detection mechanisms in VANET.	superior technique. Furthermore, future research difficulties are indicated.
2015	Review on deduction and mitigation of Sybil attack in the Network	Bhise et al. [7] A review of the deduction method of Sybil's attacks in the social network system has been provided and debated. Several strategies for mitigating the Sybil attack have been investigated. The detection rate, false positive rate, false negative rate, and non-trustworthy rate of the investigated mechanisms were all calculated.	The researcher gives a critical study, compares outcomes, and identifies holes in all known methodologies.

Looking into the above-mentioned Table. There are significant gaps in the available surveys, which have been identified. The surveys are not presented systematically or completely, and they do not give us full and all-inclusive critical and comparative evaluations. Furthermore, the surveys do not include new tools for detecting and countering Sybil attacks, such as artificial intelligence-based techniques and machine learning techniques. As a result, we submit this comprehensive literature evaluation to contribute to the area by filling gaps in previous surveys. This study presents cutting-edge approaches and schemes for avoiding and detecting Sybil attacks in MANETs.

MANETs are increasingly being used in a variety of industries. completed a comprehensive study that gives a detailed understanding of various MANETs applications in the actual world, as well as the nature of the security required for those MANETs.

The objectives of SLR are to identify research gaps in the detection and prevention of Sybil attacks in MANETs. To identify research gaps, research publications from the previous four years (2020, 2021, 2022, and 2023) were comprehensively examined in three databases, including IEEE, Springer, Research Gate, and Elsevier. Each string was searched for three synonyms, and seven papers were chosen for each string. Newspapers, theses, and white papers were excluded. Papers that appeared in several strings were eliminated. The papers were then sorted by title and abstraction. This SLR examines all methods for detecting and preventing Sybil attacks in MANETs. Based on the objectives, all approaches were thoroughly researched. This study gives a thorough critical examination of existing approaches. This SLR gives a full performance analysis of all Sybil mitigation systems after a careful study of all strategies, followed by a section describing the highlighted problems. Finally, this SLR states that several researchers offered various strategies depending on various aims. The detection accuracy, performance, additional hardware utilized, packet delivery ratio, and energy usage of various approaches are all analyzed. Figure 2 presents the organization of the paper.

The research has made the following significant contributions:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 January 2024 doi:10.20944/preprints202401.0508.v1

1. A full study is undertaken to analyze the difficulties in cutting-edge Sybil attack detection approaches.
2. In this research, ML approaches are offered as the best answer to current challenges in Sybil detection in MANETs.
3. The open research issues are recognized, and the relevant literature is cited.

The following is how this research paper is structured: Section 2 has a systematic literature review, Section 3 contains comprehensive material, and Section 4 contains a performance analysis. Critical analysis, comparison analysis, and highlighted difficulties are used to split the performance analysis into subsections. Section 5 addresses the best options, followed by Section 6, which offers us conclusions. Table 2 lists the acronyms and meanings used in this research report.

However, SLR in this paper involves a methodical and comprehensive approach to identifying, evaluating, and synthesizing existing research on this topic The paper includes a systematic review of the research literature on the issue, with stages such as formulating the research question, identifying relevant databases, doing the search, screening and choosing studies, extracting data, synthesizing results, and reporting conclusions included. This review can give important insights into the current state of the art, highlight gaps and limits, and influence future research paths in this subject. In our investigation of Sybil attack detection in Mobile Ad Hoc Networks (MANETs), our research builds upon foundational insights presented in [31–49]

2. Systematic Literature Review

In this work, a systematic literature review is conducted using a thorough methodology to identify, evaluate, and synthesize existing research on this topic. The paper includes a systematic review of the research literature on the issue, with stages such as formulating the research question, identifying relevant databases, doing the search, screening and choosing studies, extracting data, synthesizing results, and reporting conclusions included. This review can give important insights into the current state of the art, highlight gaps and limits, and influence future research paths in this subject.

2.1. Searching Protocol

This research followed a searching protocol to identify relevant research papers on machine learning-based detection of Sybil attacks in MANETs. The search was limited to publications from 2019 to 2023, and ten synonyms for each keyword were used in combination with four databases, namely IEEE, Springer, Elsevier, and Research Gate. The search criteria were restricted to selecting only six papers for each search string. Figure 1 shows the search strategies employed in this protocol.

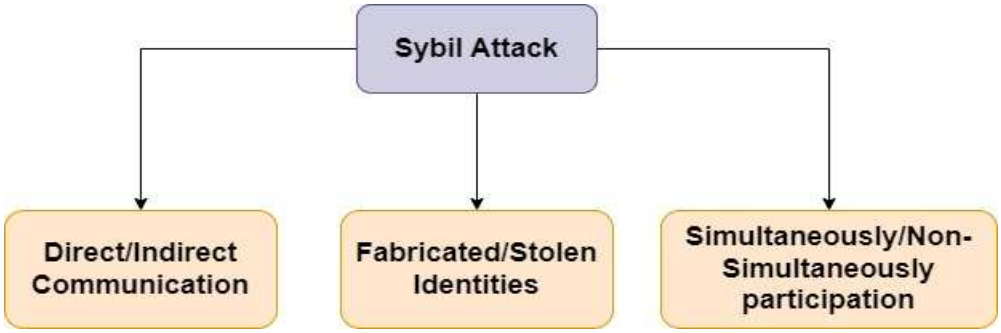

Figure 1. Classification of Sybil attack.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 January 2024 doi:10.20944/preprints202401.0508.v1

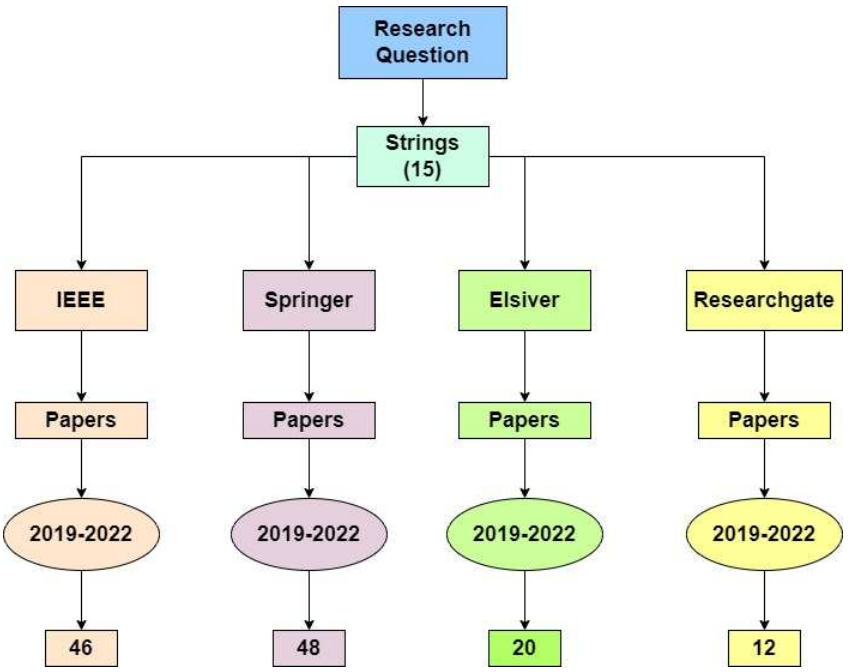

Figure 2. Search Strategies using various databases.

2.2. String Development

The strings were established by using synonyms of each keyword.

Table 2. String Development.

Word	Synonym 1	Synonym 2	Synonym 3
Detection	Identification	Recognition	Finding
Machine Learning based identification of Sybil attack Recognition of Sybil attack based on Machine learning Finding Sybil's attack on MANET			
Word	**Synonym 1**	**Synonym 2**	**Synonym 3**
Machine Learning	Deep Learning	Artificial Neural Networks	Computational Learning
Detection of Sybil attack based on deep learning Role of artificial neural networks in the Detection of Sybil Attack Sybil attack detection based on computational learning			

2.3. Inclusion Criteria

The research methodology employed an inclusion criterion to select research papers from diverse journals. Only those papers that had already been published were considered for inclusion, while any research articles that were yet to be published were excluded from this study.

2.4. Filtering

The initial stage of the filtering process used title-based filtering, as shown in Figure 3. This stage entailed removing any publications from the databases that were judged extraneous to the study issue under consideration.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 January 2024 doi:10.20944/preprints202401.0508.v1

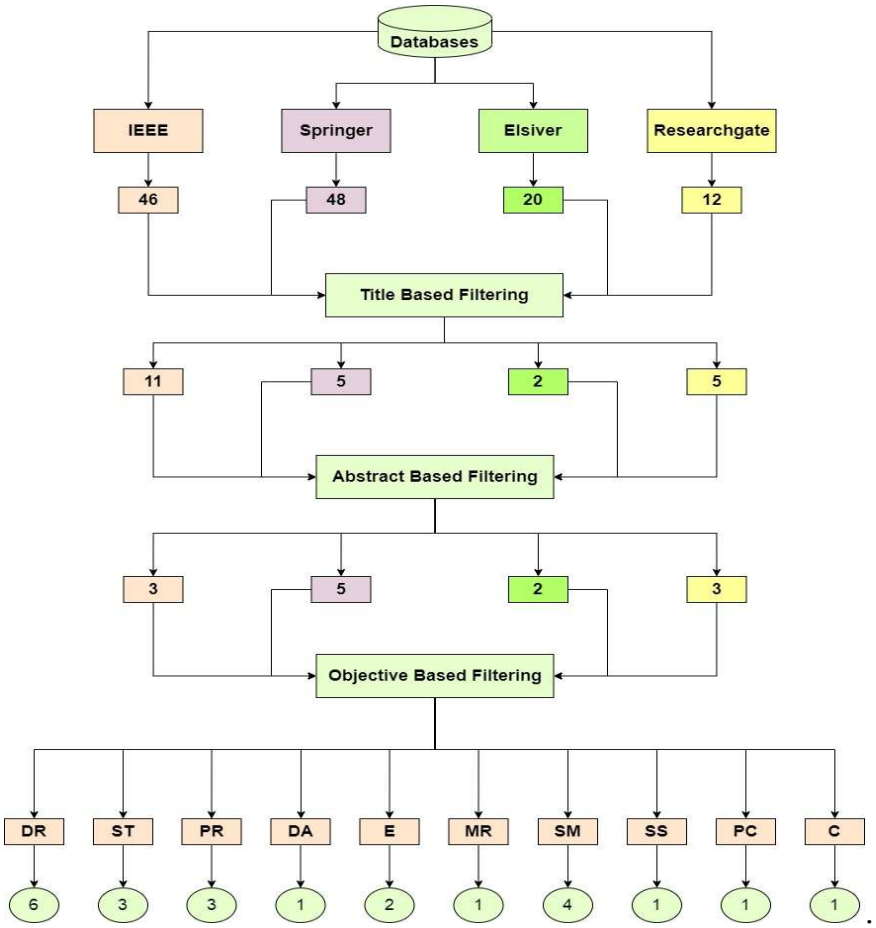

Figure 3. Screening for research articles selection to deduce the research objectives.

The second phase of the filtering process involved abstract-based screening, where all research papers with useless abstracts were removed from the databases. As shown in Figure 2, objective-based clustering was used in the third phase of filtering. The research articles were classified according to their stated aims, and a table was created to illustrate the classified papers. Following the completion of the title and abstract-based screening, the research articles' aims were recognized and classified into certain groups presents the results of the objective-based filtering, which classified the research objectives into the following categories: Detection Rate, Secure Transmission, Performance Rate, Detection Accuracy, Effectiveness, Measuring Risk, Security Measurement), Secure Storage, Power Consumption, and Credibility.

Table 3. Notations and their definitions.

Acronyms	Definition
DR	Deduction Rate
ST	Secure Transmission
PR	Performance Rate
DA	Detection Accuracy
E	Effectiveness
MR	Measuring Risk
SM	Security Measurement
SS	Secure Storage

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 January 2024 doi:10.20944/preprints202401.0508.v1

PC	Power Consumption
C	Credibility

Table 4. Objective-based screening.

Papers	DR	ST	PR	DA	E	MR	SM	SS	PC	C
[8]	✓									
[9]	✓	✓	✓	✓						
[10]	✓				✓					
[4]						✓				
[2]							✓			
[11]							✓	✓	✓	
[12]	✓				✓					
[13]			✓							
[14]	✓		✓							
[15]	✓									
[16]		✓					✓			
[17]										✓
[18]		✓					✓			

3. Detailed Literature

The primary goal of these studies was to detect and prevent Sybil attacks on MANETs.

3.1. Fuzzy Logic

The research of Ref. [9] proposes a fuzzy logic-based intrusion detection system (IDS) for Mobile Ad Hoc Networks (MANETs). The technique involves first defining a set of fuzzy rules based on network parameters such as packet loss, delay, and traffic congestion.

3.2. Machine Learning

The research of Ref. [19] proposes a classification-based approach for detecting Sybil nodes in mobile ad hoc networks that are based on a Random Forest (RF) classification algorithm, which is an ensemble learning technique that combines multiple decision trees to improve the accuracy and robustness of the classification model. The feature vector for each node is then used as input to the Random Forest algorithm to classify the node as either Sybil or legitimate. The proposed approach is evaluated using simulations on various network scenarios, such as varying node densities and attack intensities.

The research of Ref. [14] explores various machine-learning techniques for detecting fake profiles in online social networks. They use a feature-based approach that uses various machine learning algorithms, such as Decision Trees, SVM, and Random Forests, to detect fake profiles in online social networks. The approach uses features extracted from profile data, such as the number of friends and activity level, to distinguish between real and fake profiles.

The research of Ref. [16] uses an artificial intelligence (AI) system to detect and classify different types of security threats, such as DoS attacks and blackhole attacks. The system uses a

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 January 2024 doi:10.20944/preprints202401.0508.v1

combination of supervised and unsupervised learning techniques to learn patterns and anomalies in network traffic data.

3.3. ANN Artificial Neural Network

The research of Ref. [15] proposes using a combination of Artificial Neural Networks (ANNs) and Fuzzy Logic to classify nodes in a MANET as either normal or malicious. The approach involves extracting a set of features, such as node mobility, battery level, and traffic behavior, and using these features as input to the ANNs and Fuzzy Logic algorithms. They evaluate the proposed approach using simulation experiments on various scenarios, such as varying node densities and attack intensities.

Table 5. Summary of methodologies of Sybil Attack detection schemes.

Ref.	Scheme	Methodology
[9]	Fuzzy Logic Scheme	Fuzzy logic is a mathematical approach that allows for imprecise reasoning and decision-making by representing uncertainty and ambiguity using linguistic variables and fuzzy sets.
[14]	Support Vector Machines (SVM)	SVM is a supervised learning algorithm that can be used for binary classification of nodes as either genuine or Sybil based on input features such as the number of neighbors, message transmission frequency, and signal strength.
[9]	Decision Trees	Decision trees are another supervised learning algorithm that can be used to classify nodes as genuine or Sybil. Decision trees use a hierarchical tree structure to recursively partition the input space and make decisions based on the input features.
[11]	Random Forest	Random forest is an ensemble learning method that combines multiple decision trees to improve the accuracy of classification. It is a powerful technique that can handle high-dimensional feature spaces and noisy data.
[10]	Convolutional Neural Networks (CNNs)	CNNs are a type of neural network commonly used for image recognition. However, they can also be used for

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 January 2024 doi:10.20944/preprints202401.0508.v1

		detecting Sybil attacks in MANETs. CNNs use convolutional layers to extract features from the input data and learn spatial relationships between the features.

4. Performance Analysis

Performance analysis held from my research is as follows.

4.1. Critical Analysis

The research of Ref. [9] Limited evaluation: The evaluation of the IDS is limited to simulations, which may not accurately reflect the performance of the IDS in real-world MANETs. The paper does not compare the proposed IDS with other intrusion detection techniques or approaches, making it difficult to assess the relative performance of the IDS [20].

The research of Ref. [19] Scalability: The proposed approach may not scale well to larger MANETs or more complex attack scenarios, as it relies on a limited set of features and may require a larger training dataset to achieve high accuracy [21]. The proposed approach does not provide a complete solution to the Sybil attack problem and may be vulnerable to attacks that evade feature-based detection [22].

The research of Ref. [14] The paper only uses a relatively small dataset to train and test the proposed models, which may limit the generalizability of the findings[23].

The research of Ref. [16]While the paper evaluates the proposed system's performance using a real-world dataset, the evaluation is limited to a single scenario and may not reflect the diversity of security threats and concerns in MANETs [24].

The research of Ref. [15]While the paper proposes an AI-based approach, it does not offer significant novelty compared to existing research. Similar AI-based approaches for MANET security have been proposed in the literature, and the paper does not differentiate its approach or provide a compelling argument for its superiority [25].

Table 6. Summary of critical analysis of Sybil Attack detection schemes.

Detection Algorithm	Effort Year	Technique	Shortcoming
[9]	2022	Fuzzy Logic Scheme	The evaluation of the IDS is limited to simulations, which may not accurately reflect the performance of the IDS in real-world MANETs [20]
[19]	2020	Support Vector Machines (SVM)	The proposed approach may not scale well to larger MANETs or more complex attack scenarios [17]
[14]	2023	Decision Trees	The paper only uses a relatively small dataset to train and test the proposed models, which may limit the generalizability of the findings [18]

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 January 2024 doi:10.20944/preprints202401.0508.v1

[16]	2020	Random Forest	The paper evaluates the proposed system's performance using a real-world dataset, the evaluation is limited to a single scenario [19]
[15]	2021	Convolutional Neural Networks (CNNs)	The paper proposes an AI-based approach, it does not offer significant novelty compared to existing research [20]

4.2. Identified Challenges:

This section emphasized the concerns and limitations of all of the methods for identifying and avoiding Sybil attacks stated in Table 7. It briefly explains the limits of each method. These difficulties might be viewed as open study topics for scholars, where further research can be conducted to solve the concerns and challenges addressed by the schemes.

Table 7. Identified challenges of wormhole detection schemes.

Category	Challenges	Solutions
Resource limitations [2]	In simulations, it is often assumed that nodes have unlimited computational resources, memory, and energy. However, in real-world MANETs, nodes have constrained resources, and the IDS needs to operate within these limitations. The impact of resource constraints on the performance and effectiveness of the IDS cannot be accurately assessed through simulations alone.	The solution to this challenge is Dataset analysis. It means analyzing real-world datasets collected from MANETs to evaluate the IDS's performance. [26]
Lack of Scalability [25]	MANET security mechanisms should be scalable to accommodate the dynamic nature of the network, frequent topology changes, and node mobility. The proposed approach may lack the flexibility to adapt	Cross-layer design strategies allow information to be sent between layers of the network protocol stack, increasing the efficiency and scalability of security measures. [27]

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 January 2024 doi:10.20944/preprints202401.0508.v1

	to varying network conditions or changing security requirements. This can limit its ability to scale well and provide robust security in larger MANETs or under complex attack scenarios.	
Limited Dataset [9]	Using a relatively small dataset to train and test the proposed model is a big challenge that can limit the generalizability of the findings.	Augmenting your existing dataset can help increase its size and diversity. This technique involves generating synthetic samples by applying transformations to the original data. By doing so, you can effectively expand your dataset and improve the generalizability of your models. [28]
Lack of significant novelty [5]	Proposing an AI-based approach without significant novelty is a big challenge because it does not provide a specific novelty compared to existing research.	Explainable AI (XAI) addresses the lack of novelty by focusing on the interpretability and explainability of the AI system. [29]

5. Optimal Solutions

First of all, some features of NSL-KDD Dataset like protocol types, source and destination IP addresses, duration and flags will be extracted by using Principal Component Analysis (PCA) technique which helps to reduce the number of features while retaining the most informative ones. Then support vector machine scheme (SVM) will be applied on extracted features. SVM is a machine learning algorithm that can be used for the detection of Sybil attacks on Mobile Ad hoc Networks (MANETs). With proper feature selection and model training, the SVM scheme can provide accurate and reliable detection of Sybil attacks in MANETs, aiding in maintaining network integrity and security.

To detect Sybil attacks on MANETs using an SVM scheme, we need to prepare a labeled dataset of NSL-KDD dataset with selected features representing legitimate and Sybil nodes. Extract relevant features, preprocess the data, and split it into a training and validation set. Train the SVM model on

the training set, evaluating its performance on the validation set using metrics like accuracy and precision etc. On the base of this process, deduction accuracy of Sybil attack will be improved.

Dataset:

The NSL-KDD dataset (Network Security Laboratory - Knowledge Discovery in Databases) will be used. It is a well-known dataset used for intrusion detection research in network security. Researchers often use the NSL-KDD dataset to develop and evaluate machine learning algorithms. A brief about this dataset is shown in the below table:

Reference	Name of Dataset	Features
[30]	NSL-KDD dataset	It consists of approximately 1,074,992 single connection vectors each of which contains 41 features

6. Conclusions

This study discusses ML based detection of Sybil attack on Mobile Ad hoc Networks (MANETs). Sybil attacks pose a substantial risk to MANETs. This work also presents a thorough analysis of the literature on the detection of Sybil attacks on MANETs. To find gaps in the literature, current surveys are also looked at. A scheme based on Support Vector Machine (SVM) for detection of Sybil attack has been proposed for improving detection accuracy of Sybil attack on MANETs. The proposed scheme (SVM) will achieve an average detection accuracy of Sybil attack using some selected features of NSL-KDD benchmark dataset. However, the basic aim of this study is to find with the help of Support Vector Machine (SVM) Scheme for detection of sybil attack on MANETs by using some selected features of NSL-KDD Dataset like protocol types, source and destination IP addresses, duration and flags.

References

1. M. ADIL, “BLACK HOLE ATTACKS PREVENTION THROUGH MAC BASED AODV PROTOCOL IN CONSTRAINT ORIENTED NETWORKS”.
2. M. Bharti, S. Rani, and P. Singh, “Security Attacks in MANET: A Complete Analysis,” in 2022 6th International Conference on Devices, Circuits and Systems (ICDCS), IEEE, 2022, pp. 384–387.
3. S. Shekhar, M. Mahajan, and S. Kaur, “A Comprehensive Review of Various Attacks in Mobile Ad Hoc Networks,” in 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI), IEEE, 2022, pp. 638–643.
4. H. Michael and A. Jedidiah, “Mobile Adhoc Networks-An Overview of Risk Identification, Intrusion Detection and Machine Learning Techniques used,” in 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), IEEE, 2022, pp. 1–5.
5. R. Singla, N. Kaur, D. Koundal, and A. Bharadwaj, “Challenges and developments in secure routing protocols for healthcare in WBAN: a comparative analysis,” Wireless Personal Communications, pp. 1–40, 2022.
6. J. Kamani and D. Parikh, “A Review on Sybil Attack Detection Techniques,” vol. 01, no. 01.
7. A. M. Bhise and S. D. Kamble, “Review on Detection and Mitigation of Sybil Attack in the Network,” Procedia Computer Science, vol. 78, pp. 395–401, 2016, doi: 10.1016/j.procs.2016.02.080.

8. C. Chethana, P. K. Pareek, V. H. C. de Albuquerque, A. Khanna, and D. Gupta, "Deep Learning Technique Based Intrusion Detection in Cyber-Security Networks," in 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), IEEE, 2022, pp. 1–7.
9. E. Sing and S. M. C. Vigila, "Fuzzy based intrusion detection system in MANET," Measurement: Sensors, p. 100578, 2022.
10. B. Hammi, M. Y. Idir, and R. Khatoun, "A machine learning based approach for the detection of sybil attacks in C-ITS," in 2022 23rd Asia-Pacific Network Operations and Management Symposium (APNOMS), IEEE, 2022, pp. 1–4.
11. F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh, and F. AlTamimi, "Security challenges and attacks in dynamic mobile ad hoc networks MANETs," in 2019 IEEE jordan international joint conference on electrical engineering and information technology (JEEIT), IEEE, 2019, pp. 28–33.
12. Y. Jiang, Y. Li, Y. Zhou, and X. Zheng, "Sybil Attacks and Defense on Differential Privacy based Federated Learning," in 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE, 2021, pp. 355–362.
13. H. Ali, I. Malik, S. Mahmood, F. Akif, and J. Amin, "Sybil Detection in Online Social Networks," in 2022 17th International Conference on Emerging Technologies (ICET), IEEE, 2022, pp. 125–129.
14. N. S. G. Bharti and P. Gulia, "Exploring machine learning techniques for fake profile detection in online social networks," International Journal of Electrical and Computer Engineering (IJECE), vol. 13, no. 3, pp. 2962–2971, 2023.
15. A. Vani, "Deplete And Discernment Of Security Hazards In Mobile Ad-Hoc-Networks (Manet) Using Artifical Intelligence," International Journal of Future Generation Communication and Networking, vol. 14, no. 1, pp. 925–942, 2021.
16. M. Madanan and A. Venugopal, "Designing an Artificial Intelligent MANET to reduce and detect security threats and concerns," in Proceedings of the 2006 14th IEEE International Conference on Network Protocols, 2020, pp. 75–84.
17. A. Kumari, S. Dutta, and S. Chakraborty, "Detection and Prevention of Black Hole Attack in MANET using Node Credibility and Andrews Plot," 2023.
18. S. Thapar and S. K. Sharma, "Attacks and security issues of mobile ad hoc networks," in Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India, 2019.
19. S. Rethinavalli and R. Gopinath, "Classification Approach based Sybil Node Detection in Mobile Ad Hoc Networks," International Journal of Advanced Research in Engineering and Technology, vol. 11, no. 12, pp. 3348–3356, 2020.
20. A. Chaudhary, V. N. Tiwari, and A. Kumar, "Analysis of fuzzy logic based intrusion detection systems in mobile ad hoc networks," BVICA M's International Journal of Information Technology, vol. 6, no. 1, p. 690, 2014.
21. M. Di Mauro, G. Galatro, G. Fortino, and A. Liotta, "Supervised feature selection techniques in network intrusion detection: A critical review," Engineering Applications of Artificial Intelligence, vol. 101, p. 104216, 2021.
22. A. Vasudeva and M. Sood, "Survey on sybil attack defense mechanisms in wireless ad hoc networks," Journal of Network and Computer Applications, vol. 120, pp. 78–118, 2018.

23. M. Aljabri, R. Zagrouba, A. Shaahid, F. Alnasser, A. Saleh, and D. M. Alomari, "Machine learning-based social media bot detection: a comprehensive literature review," Social Network Analysis and Mining, vol. 13, no. 1, p. 20, 2023.
24. N. Goyal and A. Gaba, "A review over MANET-Issues and Challenges," International Journal of Enhanced Research in Management & Computer Applications, vol. 2, pp. 2319–747116, Apr. 2013.
25. Z. Wei, H. Tang, F. R. Yu, M. Wang, and P. Mason, "Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning," IEEE Transactions on Vehicular Technology, vol. 63, no. 9, pp. 4647–4658, Nov. 2014, doi: 10.1109/TVT.2014.2313865.
26. A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," Cybersecur, vol. 2, no. 1, p. 20, Dec. 2019, doi: 10.1186/s42400-019-0038-7.
27. Anurag Das, "Cross Layer Design in Mobile Ad Hoc Networks: Issues and Solutions," 2018, doi: 10.13140/RG.2.2.16849.79200.
28. C. Shorten and T. M. Khoshgoftaar, "A survey on Image Data Augmentation for Deep Learning," J Big Data, vol. 6, no. 1, p. 60, Dec. 2019, doi: 10.1186/s40537-019-0197-0.
29. F. Emmert-Streib, O. Yli-Harja, and M. Dehmer, "Explainable artificial intelligence and machine learning: A reality rooted perspective," WIREs Data Mining Knowl Discov, vol. 10, no. 6, Nov. 2020, doi: 10.1002/widm.1368.
30. G. G. Gebremariam, J. Panda, and S. Indu, "Localization and Detection of Multiple Attacks in Wireless Sensor Networks Using Artificial Neural Network," Wireless Communications and Mobile Computing, vol. 2023, 2023.
31. Lim, M., Abdullah, A., & Jhanjhi, N. Z. (2020). Data fusion-link prediction for evolutionary network with deep reinforcement learning. International Journal of Advanced Computer Science and Applications, 11(6).
32. Alwakid, G., Gouda, W., Humayun, M., & Jhanjhi, N. Z. (2023). Diagnosing Melanomas in Dermoscopy Images Using Deep Learning. Diagnostics, 13(10), 1815.
33. Tayyab, M., Marjani, M., Jhanjhi, N. Z., Hashem, I. A. T., Usmani, R. S. A., & Qamar, F. (2023). A Comprehensive Review on Deep Learning Algorithms: Security and Privacy Issues. Computers & Security, 103297.
34. Pal, S., Jhanjhi, N. Z., Abdulbaqi, A. S., Akila, D., Almazroi, A. A., & Alsubaei, F. S. (2023). A hybrid edge-cloud system for networking service components optimization using the internet of things. Electronics, 12(3), 649.
35. Ponnusamy, V. (Ed.). (2016). Biologically-Inspired Energy Harvesting through Wireless Sensor Technologies. IGI Global.
36. Ponnusamy, V., Jung, L. T., Ramachandran, T., & Zaman, N. (2017, April). Bio-inspired energy scavenging in wireless ad hoc network. In 2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT) (pp. 1-5). IEEE.
37. Abbas, S. F., Shahzad, R. K., Humayun, M., Jhanjhi, N. Z., & Alamri, M. (2019). SOA Issues and their Solutions through Knowledge Based Techniques—A Review. Int. J. Comput. Sci. Netw. Secur., 19(1), 8-21.
38. Humayun, M., Jhanjhi, N. Z., Talib, M. N., Shah, M. H., & Suseendran, G. (2021). Cybersecurity for Data Science: Issues, Opportunities, and Challenges. Intelligent Computing and Innovation on Data Science: Proceedings of ICTIDS 2021, 435-444.

39. Kumar, P., Kumar, R., Aljuhani, A., Javeed, D., Jolfaei, A., & Islam, A. N. (2023). Digital twin-driven SDN for smart grid: A deep learning integrated blockchain for cybersecurity. Solar Energy, 263, 111921.
40. Mukherjee, D., Ghosh, S., Pal, S., Akila, D., Jhanjhi, N. Z., Masud, M., & AlZain, M. A. (2022). Optimized Energy Efficient Strategy for Data Reduction Between Edge Devices in Cloud-IoT. Computers, Materials & Continua, 72(1).
41. Hanif, M., Ashraf, H., Jalil, Z., Jhanjhi, N. Z., Humayun, M., Saeed, S., & Almuhaideb, A. M. (2022). AI-based wormhole attack detection techniques in wireless sensor networks. Electronics, 11(15), 2324.
42. Jabeen, T., Jabeen, I., Ashraf, H., Jhanjhi, N., Humayun, M., Masud, M., & Aljahdali, S. (2022). A monte carlo based COVID-19 detection framework for smart healthcare. Computers, Materials, & Continua, 70(2), 2365-2380.
43. Siddiqui, F. J., Ashraf, H., & Ullah, A. (2020). Dual server based security system for multimedia Services in Next Generation Networks. Multimedia Tools and Applications, 79, 7299-7318.
44. [44]Shahid,H.,Ashraf,H.,Ullah,A.,Band,S.S.&Elnaffar,S.Wormholeattackmitigationstrategiesandtheirimpact onwirelesssensornetworkperformance: Aliteraturesurvey. InternationalJournalofCommunicationSystems35, e5311(2022). URLhttps://onlinelibrary.wiley.com/doi/abs/10.1002/dac.5311. https://onlinelibrary.wiley.com/doi/pdf/10.1002/dac.5311.
45. Kaur, R., Verma, S., Jhanjhi, N. Z., & Talib, M. N. (2021, August). A comprehensive survey on load and resources management techniques in the homogeneous and heterogeneous cloud environment. In Journal of Physics: Conference Series (Vol. 1979, No. 1, p. 012036). IOP Publishing.
46. Alotaibi, A. F. (2021). A comprehensive survey on security threats and countermeasures of cloud computing environment. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(9), 1978-1990.
47. Al-Turjman, F. (Ed.). (2020). Drones in smart-cities: Security and performance. Elsevier.
48. Ponnusamy, V., Jung, L. T., Ramachandran, T., & Zaman, N. (2017, April). Bio-inspired energy scavenging in wireless ad hoc network. In 2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT) (pp. 1-5). IEEE.
49. Ponnusamy, V. (Ed.). (2016). Biologically-Inspired Energy Harvesting through Wireless Sensor Technologies. IGI Global.