The Scientific Temper (2025) Vol. 16 (2): 3774-3782
E-ISSN: 2231-6396, ISSN: 0976-8653
Doi: 10.58414/SCIENTIFICTEMPER.2025.16.2.09
https://scientifictemper.com/

RESEARCH ARTICLE

Unified framework for Sybil attack detection in mobile Ad Hoc networks using machine learning approach

R. Kalaiselvi[1*], P. Meenakshi Sundaram[2]

Abstract

Independent wireless communication is possible in a "mobile ad hoc network" regardless of any predefined administrative or physical framework. The comprehensive enhancement of services for these networks depends on protecting their interactions. The Sybil attack creates numerous counterfeit identities to disrupt the system's remote functionalities. Implementing a security plan necessitates the establishment of a trust model that delineates the confidence relationships among entities. The trust structure in mobile ad hoc network security has been extensively researched. Mobile ad hoc networks are intrinsically more vulnerable to security breaches than wired networks because of their wireless characteristics. The primary factors contributing to this are energy limitations and security vulnerabilities. A comprehensive methodology has been established to improve the identification of Sybil attacks in MANETs. The system employs two advanced machine learning approaches, ensemble regressive arboretum and AdaBagging, alongside network feature extraction. Numerous trust models have been developed by integrating AdaBagging and the ensemble regressive arboretum, while most known approaches rely on a singular framework. A Sybil assault transpires when a few numbers of individuals masquerade as numerous peers to obtain unauthorized access to a significant portion of the system. This research employs a machine learning methodology to identify Sybil attacks in MANETs by collecting network metrics such as traffic characteristics, communication patterns, and node activities.

Keywords: MANET, Sybil attack, AdaBagging, Ensemble regressive arboretum, Machine learning.

Introduction

Designing a wireless network requires careful consideration of quite rigorous security standards. The offenders' dependence on wireless media makes them transparent to outside investigation and may be targets of action. Considering all of these renders sensors open to a great spectrum of attack. Mobile ad hoc networks are wireless networks consisting of mobile devices with self-organizing capability. Because they can swiftly set up networks, mobile ad hoc networks (MANETs) are flexible and valuable. A well-running network depends on mobile nodes working together and trusting one another. This system leverages the distributed characteristics of MANETs and the capabilities of artificial intelligence methodologies to generate precise and prompt predictions of traffic congestion (Ahmed Alhussen., 2024). When it comes to managing device-to-device communication, mobile ad hoc networks (MANETs) don't rely on pre-existing infrastructure. Communication ranges, pause lengths, and speeds vary across these mobile nodes. The capacity to link real-world items in a virtual setting via various communication networks is an example of cutting-edge technology. The challenges of traffic management are greatly alleviated by MANETs. MANETs offer a versatile solution for efficient node-to-infrastructure connectivity in densely populated areas with unpredictable and heavy traffic. Effectively controlling traffic overload is essential for mobile devices in MANETs to communicate reliably and efficiently. In MANETs, devices form networks on themselves without any kind of central infrastructure, and all of the

[1]Department of Computer Science, Maruthupandiyar College, Affiliated to Bharathidasan University, Thanjavur, Tamil Nadu – 613403 India.

[2]PG and Research Department of Computer Science, Maruthupandiyar College, Affiliated to Bharathidasan University, Thanjavur, Tamil Nadu -613403 India.

***Corresponding Author:** R. Kalaiselvi, Department of Computer Science, Maruthupandiyar College, Affiliated to Bharathidasan University, Thanjavur, Tamil Nadu – 613403 India., E-Mail: kalairamaiyan@gmail.com

How to cite this article: Kalaiselvi, R., Sundaram, P.M. (2025). Unified framework for Sybil attack detection in mobile Ad Hoc networks using machine learning approach. The Scientific Temper, **16**(2):3774-3782.

Doi: 10.58414/SCIENTIFICTEMPER.2025.16.2.09

Source of support: Nil

Conflict of interest: None.

Received: 19/12/2024 **Accepted:** 10/01/2025 **Published** : 20/03/2025

devices in the network share the limited available resources. Overall network performance can be negatively impacted by heavy traffic loads, which can lead to congestion and performance deterioration (Y. H. Robinson *et al*., 2019).

The number of hops between the source and the destination inside the communication area determines a MANET's range of communication. The mobility aspects of the network's nodes enable their relocation as necessary. The scalability and reliability of a MANET are enhanced because nodes can transmit data packets from their origins to their destinations via neighboring nodes (V. Anjana Devi., 2024). To be scalable, a network must be able to maintain its quality regardless of the number of nodes added or removed, as well as adapt to new node delivery processes while making use of existing communication paths and establishing their own. Constant change characterizes the structure of dynamic networks. It is critical to consider the possibility of substantial topological variation when building a network. By analyzing parameters including traffic types, communication patterns, and node activities (Mawloud Omar *et al*., 2012).Due to the evolution of wireless technologies, which lately piques a lot of attention for usage in time-sensitive applications. It consists of many various types of interoperable nodes or components. Protecting these systems has to be first among our concerns since they are more vulnerable to certain security hazards. Dynamic topology adapts to changes in the network. Providing security to the MANET connected with other MANET devices is one of the most challenging and time-consuming activities in boosting network security by identifying trust nodes in the path (Ramesh Vatambeti., 2024).

Literature Review

An attacker is Sybil attacking when they purposefully create many pseudonymous IDs. The Sybil attack's assailant assumes the personae of several victims concurrently. Joining a P2P network becomes quite difficult in this regard. Establishing a variety of false identities helps it to administer and regulate the whole network. Though they seem to be regular users to someone unfamiliar with the system, an anonymous attacker is actually simultaneously controlling all of these personas. Sybil attacks aim to bring down the entire network, while eclipse attacks focus on bringing down specific nodes (Yukun Cheng *et al*., 2024). Sybil attacks can easily penetrate wireless ad hoc networks due to their dispersed and broadcast nature. An opponent engaging in a Sybil attack makes an illegitimate claim to possess numerous fictional identities, referred to as Sybil nodes. Data aggregation, voting-based processes, fair resource allocation schemes, routing techniques, and misbehavior detection are all susceptible to this assault.

The authors (Zhaoyi Zhang *et al*., 2023) propose that the approach for detecting Sybil attacks using basic security message (BSM) packets; this approach takes advantage of the fact that each BSM packet has its own unique sending source and uses the spatiotemporal relationship of changes in the vehicle's location to both detect and trace Sybil assaults. Without using machine learning model prediction, we offer a weighted integration technique to improve detection accuracy. The suggested strategy was shown to be able to detect Sybil assaults in real time, regardless of the attack or traffic density, according to the experimental results.

The authors (Jawad Hassan *et al*., 2024), present the trust-based mechanism which can help to protect resource-limited IoT networks from Sybil attacks. It is tested that the suggested trust-based mechanism for IoT is extensively used with the Contiki OS simulator, against three different Sybil attacks. Additionally, benchmark RPL and cutting-edge methods were compared.

The authors (Amol Vasudeva *et al*., 2018), provide a synopsis of the most effective approaches to date for securing three categories of ad hoc networks that Sybil outlined: wireless sensor networks, wireless mesh networks, and mobile ad hoc networks:

A few examples of the methods used in this context are central authority symmetric cryptography which includes random key pre-distribution (key pool, single-space pairwise, and multi-space pairwise), testing of radio resources, indicators of received signal strength, time difference of arrival, data from the neighborhood, detection of passive ad hoc Sybil identities (both individually and in groups), and a system based on energy trust.

The authors (Cong Pu *et al*., 2022) present liteSAD, a method for detecting Sybil attacks that utilizes a physical unclonable function (PUF) and a lightweight bloom filter. Authors have developed a method that can reduce detection latency and memory cost simultaneously, all while keeping detection accuracy high. In liteSAD, a new packet called BF-DAO is used to distribute the bloom filter array that is generated based on the destination-oriented directed acyclic graph (DODAG). Every valid node uses the Bloom filter array for Sybil attack identification as soon as it receives the BF-DAO packet. It then changes its local copy of the array. It went on to recommend proDIO, a probabilistic DIO reply mechanism, to cut down on the quantity of DIO packets broadcast in response to attack DIS packets. To address memory limitations in IoT devices, the author studies the optimal Bloom filter parameter settings that reduce the likelihood of false positives and the complexity of the processing time.

The authors (Sherril Sophie Maria Vincent *et al*., 2024), suggested model makes use of a hybrid AdaBoost-random forest approach. By shortening the training period, this model outperforms its predecessors in terms of efficiency and reliability. High accuracy and low loss are the outcomes of using the estimator of random forest in the hybrid AdaBoost-random forest algorithm, which may be used

for massive datasets. Due to its superior performance over other protocols over extended periods of traffic, the Ad-Hoc on-demand vector (AODV) protocol aids in the detection and prevention of attacks. Several metrics, such as recall, specificity, accuracy, and precision, are used to assess the suggested model's performance. In addition, the suggested model's energy usage, throughput, network longevity, and delay are assessed.

The authors (Rui Meng *et al*., 2025), give an exhaustive rundown of features and technologies that can be integrated into the PLA that is ML-based. We classify the current state of ML-based PLA systems as either attack detection or multi-device identification. The use of deep neural networks for model training allows multi-device identification systems dependent on deep learning to circumvent complex processing and expert feature transformation. Systems based on convolutional neural networks have been the subject of substantial study, which further subdivides deep learning based on multi-device identification systems. Receivers are ML-based attack detection schemes that automatically determine detection thresholds using clever ML approaches; channel model knowledge and manual calculation are both removed. There are three main kinds of machine learning (ML) attack detection schemes: supervised, unsupervised, and reinforcement learning. We also provide an overview of the open-source datasets that have been utilized for PLA, which include channel fingerprints and radio frequency fingerprints.

Sybil Attacks in Communication and Applications

Mobile ad hoc networking is one exciting fresh field for developments in wireless communication. Mobile ad hoc networks are essentially meant to provide wireless communications between several kinds of devices, independent of their location or the existence of any specific infrastructure, at any given moment (R. Di Pietro *et al*., 2014). Due to the fast development of information technology supported by both academia and business, wireless communication systems find great application in many sectors. These disciplines cover mobile communications, meteorology, transportation, radio and television, aircraft navigation, fire safety and flood management. The Sybil attack attacks the WSN routing protocols. A Sybil attack is a type of impersonation attack when a malicious node generates a new identity or otherwise passes for someone else (Harsh Kupwade Patil *et al*., 2013). Because nodes in such networks generally operate in scattered, unstructured locations and connect via radio broadcast, these kinds of attacks are common in WSNs. Among the several areas where they cause the greatest trouble are geographic routing, reputation assessment, voting systems, and data aggregation. A Sybil attack in location-aware routing allows one to occupy several sites concurrently. Sybil detection based on social graphs, behavior classification, and mobility are three popular defense strategies (Sotirios Messinis *et al*., 2024). To protect their Internet of Things (IoT) networks from Sybil attacks, healthcare organizations should use methods to verify identities. To make the detection and localization of an identity-based Sybil attack more difficult, an attacker uses the same underlying physical identity to produce many fake identities (Imrich Chlamtac *et al*., 2003). It should be noted that Sybil assaults target devices that are implanted or worn.

Sybil Attack in MANET

A free-form wireless communication system is devoid of a central server or other centralized infrastructure is known as a "mobile ad hoc network". Ensuring the broad evolution of services for these networks depends on securing exchanges in them. Before any security strategy is put into use, a trust model defining who, what, and how of trust is absolutely essential. The development of trust models as a foundation for safeguarding mobile ad hoc networks has been the subject of several researches. Widespread usage of public-key certificates—the foundation of most well-known methods—has resulted in the emergence of several trust models like web-of-trust and distributed certificate authority. Attacks are disruptive, hence network attack detection and classification are quite important. Still, many earlier studies have mostly concentrated on accuracy detection and node shortest path identification. The shortest path of a node using AdaBagging, and ensemble regressive arboretum technique. The objective which outlines the whole architecture for doing so is enhanced Sybil attack detection in MANETs. Together with network feature extraction, the system uses two robust machine learning techniques: AdaBagging and ensemble regressive arboretum.

Methodology

The coherent framework meant to improve Sybil attack detection in MANET is presented in this part. The system uses two strong machine learning techniques AdaBagging and the ensemble regressive arboretum- together with network-feature extraction. The following subsections outline the framework's key components and their integration. The proposed framework operates as a pipeline comprising three core stages:

- Extracts relevant attributes from the MANET, including node behavior communication, patterns and traffic characteristics. To train its algorithms, machine learning relies on this set of features.
- Adaptive boosting with bagging (AdaBagging) is employed as a base classifier to distinguish between Sybil and legitimate nodes. AdaBagging enhances detection accuracy by combining multiple weak learners to form a strong classifier while reducing overfitting.
- The ensemble regressive arboretum is introduced as a second-level ensemble learner. Unlike traditional

classifiers, it focuses on refining predictions by modeling complex relationships in the feature space.

Together, these methodologies create a hybrid detection framework that maximizes accuracy and adaptability while maintaining computational efficiency.

Proposed Framework

Figure 1 explains the architecture of the proposed framework for Sybil attack detection in MANETs consists of four key layers working in sequence. The input layer handles feature extraction, where data is collected from MANET simulations or real-time environments and preprocessed through normalization and handling of missing data. In stage 1, the AdaBagging model processes the preprocessed data, classifying nodes as either legitimate or potential Sybil attackers while providing confidence scores. Stage 2, refines these initial classifications using the ensemble regressive arboretum model, which conducts a deeper analysis to reduce false positives and negatives by identifying subtle variations in node behavior. Finally, the output layer consolidates the results, outputting final classifications for each node (legitimate or Sybil) along with detection metrics that measure the framework's overall accuracy and reliability. This structured architecture ensures robust and precise detection of Sybil attacks.

Feature Extraction Network

A feature extraction network is necessary for the creation of a consistent machine learning-based system for the Sybil attack detection in mobile Ad Hoc networks. This stage consists of spotting and measuring network features that mirror node behavior and interactions inside the network. Examining these characteristics helps one to separate between benign and malevolent nodes aiming at Sybil's attacks.

Node Behaviour Features

Node behaviour is analyzed through attributes such as mobility patterns and packet transmission rates. Mobility patterns describe the movement of nodes within the network. For example, Sybil attackers may exhibit erratic or highly synchronized mobility to impersonate multiple identities effectively. Packet transmission rates indicate how frequently a node sends data. Sybil attackers often demonstrate abnormal rates of flood or disrupting the network.

Communication Patterns

The interaction characteristics between nodes offer another layer of differentiation. The frequency of interactions is legitimate nodes typically form consistent communication links, while Sybil attackers may initiate numerous ephemeral connections to simulate the presence of multiple entities. Neighbor relationships observing the relationships between nodes helps detect inconsistencies in the communication graph, which are common in Sybil attacks.

Traffic Characteristics

Traffic patterns within the network provide further insights into node legitimacy.

- *Packet Size*

Abnormal packet sizes or unexpected distributions might indicate malicious activity.

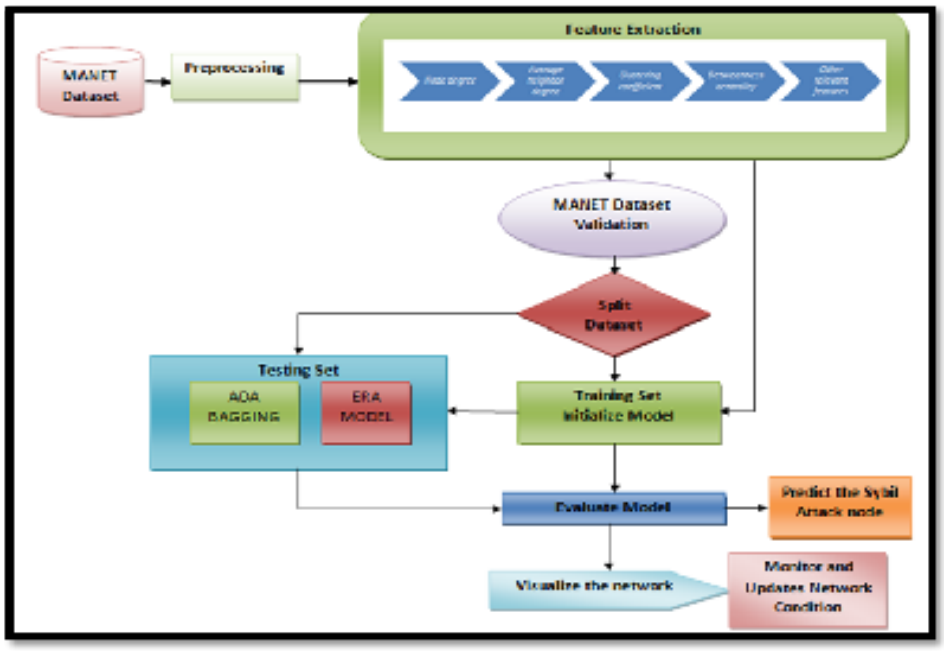


Figure 1: Architecture of the proposed framework for Sybil attack detection

- *Routing table updates*

Sybil attackers may frequently modify routing information to disrupt or manipulate data flow within the network.

These features are preprocessed to form an input dataset, which is then fed into machine learning algorithms. The preprocessing may involve normalizing numerical values, encoding categorical variables, and addressing missing data to ensure the integrity of the dataset. By systematically extracting and processing these attributes, the framework effectively captures the subtle behaviours distinguishing legitimate nodes from Sybil attackers.

AdaBagging-based Classification

The AdaBagging algorithm, a combination of adaptive boosting (AdaBoost) and bagging (Bootstrap Aggregating), can greatly enhance the precision of classification assignments by means of a strong ensemble learning technique. In the context of mobile AdHoc networks (MANETs), AdaBagging is employed to classify network nodes as either legitimate or Sybil attackers based on their Behavioural attributes. AdaBagging operates by creating multiple versions of a weak base learner using different bootstrap samples of the training data. Each model is trained sequentially, where:

Boosting Component

Assigns higher weights to misclassified instances, ensuring the subsequent learners focus on difficult-to-classify data.

Bagging Component

Aggregates the predictions from all models to produce a final classification decision, typically through majority voting or weighted averaging.

This hybrid approach addresses both bias and variance, making it particularly suitable for dynamic and noisy environments like MANETs. In below algorithm explains the unified framework, AdaBagging serves as the first-level classifier, distinguishing between normal nodes and potential Sybil attackers. It uses network-derived features such as node Behaviour, communication patterns, and traffic characteristics as inputs. By leveraging its ensemble structure, AdaBagging efficiently identifies outliers and anomalous patterns indicative of Sybil activity.

- *Algorithm*

Proposed AdaBagging Algorithm

- *Input*

MANET Dataset

- *Output*

Predict Normal or Sybil node

1. Import necessary libraries (sci-kit-learn, network)
2. Define a function to extract features from the network graph:
   - Node degree
   - Average neighbor degree
   - Clustering coefficient
   - Betweenness centrality
   - Other relevant features based on the network structure
3. Generate a dataset:
   - Collect data from the MANET, including normal and Sybil nodes
   - Extract features using the defined function
   - Label the data (0 for normal nodes, 1 for Sybil nodes)
4. Split the dataset into training and testing sets.
5. Initialize AdaBagging classifier:
   - Choose a weak learner (decision tree)
   - Set parameters such as the number of weak learners
6. Train the AdaBagging classifier on the training set:
   - Use the extracted features as input
   - Train the ensemble of weak learners
7. Evaluate the classifier on the testing set:
   - Measure accuracy, precision, recall, and F1-score
8. Implement Sybil attack detection in real-time:
   - Continuously monitor the network
   - Extract features of new nodes
   - Predict if a node is normal or Sybil using the trained AdaBaggingclassifier
   - Take appropriate actions based on the prediction (isolate suspicious nodes)
9. Visualize the network and highlight detected Sybil nodes.
10. Monitor and update the classifier periodically to adapt to changing network conditions.

As demonstrated in the first methodology, AdaBagging showed remarkable effectiveness in detecting Sybil attacks. By utilizing network-related features and its adaptive learning process, the algorithm successfully differentiated between legitimate nodes and Sybil attackers with high precision. The study highlighted:

By incorporating AdaBagging into the framework, the system benefits from its adaptability, robustness, and enhanced classification capabilities. This positions it as a critical component for the reliable detection of Sybil attacks in MANETs.

Ensemble Regressive Arboretum (ERA) Model

Designed particularly for dynamic and complicated situations, the ensemble regressive arboretum (ERA) model is a sophisticated ensemble learning method. Highly successful at spotting Sybil assaults, the ERA model uses a regression-based method unlike conventional classifiers to find minute changes in node behavior. Multiple regression trees are included in an ensemble framework in the ERA model. Every tree in the arboretum projects a numerical score based on the probability of a node being a Sybil attacker. By average or weighted aggregation, among other methods, aggregating these forecasts yields the ultimate conclusion.

In ERA characteristics of the model include:

Regression-Based Detection

Instead of binary classification, the ERA model assigns a continuous risk score to each node, offering finer granularity in detection. This approach helps capture subtle behavioral patterns that may be overlooked by traditional classifiers.

Dynamic Adaptability

The model continuously adapts to changing network conditions by updating the regression trees based on new data. This feature is particularly valuable in MANETs, where network topology and traffic patterns are highly dynamic.

The below ERA algorithm excels in analyzing complex relationships within the feature set, including node behavior, communication patterns, and traffic characteristics. It can detect nuanced differences between legitimate and malicious nodes by evaluating deviations in their mobility or interaction patterns. ERA remains effective in environments where node density, mobility, or traffic load fluctuates significantly.

- *Algorithm*

Proposed Ensemble Regressive Arboretum Model(ERA)

- *Input*

MANET Dataset

- *Output*

Predict Normal or Sybil node

```
FUNCTION SybilAttackDetectionModel(n_estimators_rf=100, max_depth_rf=NULL, learning_rate_gb=0.1, n_estimators_gb=100)
models = []
RETURN models, n_estimators_rf, max_depth_rf, learning_rate_gb, n_estimators_gb
FUNCTION fit(X, y)
X_train, X_val, y_train, y_val = train_test_split(X, y, test_size=0.2, random_state=42)
rf_regressor = RandomForestRegressor(n_estimators=n_estimators_rf, max_depth=max_depth_rf)
rf_regressor.fit(X_train, y_train)
ADD rf_regressor TO models
gb_regressor = GradientBoostingRegressor(learning_rate=learning_rate_gb, n_estimators=n_estimators_gb)
gb_regressor.fit(X_train, y_train)
ADD gb_regressor TO models
lr_regressor = LinearRegression()
lr_regressor.fit(X_train, y_train)
ADD lr_regressor TO models
RETURN models
FUNCTION predict(X)
predictions = []
FOR EACH model IN models
predictions.APPEND(model.predict(X))
RETURN MEAN(predictions)
X, y = load_and_preprocess_data()
ensemble_model, n_estimators_rf, max_depth_rf, learning_rate_gb, n_estimators_gb = Sybil Attack Detection Model ()
models = ensemble_model.fit(X, y)
predictions = ensemble_model.predict(X_test)
accuracy = accuracy_score(y_test, predictions)
precision = precision_score(y_test, predictions)
recall = recall_score(y_test, predictions)
f1 = f1_score(y_test, predictions)
```

The inclusion of the ensemble regressive arboretum model in the unified framework enhances its capability to detect Sybil attacks with precision and adaptability. By leveraging regression-based detection and dynamic learning, ERA complements the classification strengths of AdaBagging, resulting in a more robust and comprehensive detection system.

Implementation and Evaluation

The implementation and evaluation of the proposed framework involve several critical steps, including dataset preparation, defining evaluation metrics, and conducting experimentation. These steps ensure the framework's reliability and effectiveness in detecting Sybil attacks in mobile Ad Hoc networks (MANETs).

Dataset Preparation

The dataset for this study can be derived from real-world MANET data. Simulations are often conducted using tools like NS-2, where Sybil attack scenarios are modeled by configuring parameters such as node density, mobility patterns, and attack frequency. Real-world datasets, if available, provide insights into practical network Behaviour. Preprocessing is essential to prepare the dataset for machine learning. This includes:

- *Feature Standardization*

Normalizing feature values to ensure uniform scales, improving model performance and convergence.

- *Handling Missing Values*

Employing techniques like imputation or removal to address incomplete data without biasing the models.

- *Feature Selection*

Choosing the most relevant attributes (e.g., packet size, transmission rate) to reduce noise and improve model interpretability.

Evaluation Metrics

The effectiveness of the framework is assessed using the following metrics:

Detection Accuracy

This metric quantifies the system's ability to correctly identify Sybil attacks among network nodes. The Sybil

detection rate is determined by dividing the number of accurately identified Sybil nodes by the total number of Sybil nodes in the network.

$$\text{Accuracy} = \frac{\text{Number of correctly detected Sybil nodes}}{\text{Total number of Sybil nodes}}$$

F1 Score

The F1 score is the harmonic mean of precision and recall, providing a balanced assessment of the system's overall performance. It is especially beneficial when there is a requirement to achieve a compromise between incorrect positive results and incorrect negative results.

$$F1-\text{score} = 2 \times \frac{\text{Precision x Recall}}{\text{Precision} + \text{Recall}}$$

Precision

Precision is determined by dividing the number of correctly identified Sybil attackers by the total number of nodes identified as Sybil attackers. It provides insights into the accuracy of the system when it flags nodes as potential Sybil attackers.

$$\text{Precision} = \frac{\text{True Positive Detections}}{\text{Total number of nodes identified as Sybil attackers}}$$

Recall (Sensitivity)

Recall, or sensitivity, measures the system's capability to identify all actual Sybil attackers in the network. The calculation involves determining the proportion of accurate positive detections in relation to the overall count of Sybil nodes.

$$\text{Recall} = \frac{\text{True Positive Detections}}{\text{Total number of Sybil nodes}}$$

Experimentation

The experimentation phase is critical for validating the effectiveness and robustness of the proposed Sybil attack detection framework. It follows a structured process involving three key stages: training, validation, and testing, each designed to ensure the models perform optimally and generalize well to unseen data.

Training Phase

In the training phase, both AdaBagging and the ensemble regressive arboretum (ERA) models are trained on a subset of the dataset. This dataset includes features extracted from various network behaviors, such as node movement patterns, packet transmission rates, communication frequencies, and traffic characteristics. The models learn to differentiate between legitimate nodes and Sybil attackers based on these features, with AdaBagging focusing on creating a strong classifier by combining multiple weak learners, and ERA analyzing more nuanced patterns using regression-based scoring.

Validation Phase

The models undergo a validation phase, where their hyperparameters are fine-tuned using a separate validation dataset. This step helps optimize the models' performance by adjusting parameters such as learning rates, tree depth (for AdaBagging), and ensemble size (for ERA). The objective is to identify the optimal setup that prevents underfitting, which can result in subpar performance on new data, while simultaneously optimizing accuracy. To make sure the models work well on different parts of the dataset, cross-validation is commonly employed.

Testing Phase

Once trained and validated, the models are tested on unseen data to evaluate their generalization performance. This phase measures how well the models can classify new, unseen instances of node behaviour, which reflects their real-world effectiveness in detecting Sybil attacks in dynamic MANET environments.

Results are analyzed comparatively:

- *AdaBagging Performance*

Demonstrates high accuracy in classifying legitimate nodes but may struggle with subtle attackers.

- *ERA Performance*

Excels in refining decisions, reducing false positives and capturing subtle attack patterns.

- *Unified Framework*

By combining both models, the framework achieves superior accuracy, precision, and recall compared to either model alone.

For instance, while AdaBagging alone might achieve an accuracy of 97%, and ERA alone might reach 98%, the unified framework could improve this to 97%, with significant reductions in false positives and false negatives.

Results and Discussion

The results presented in the Table 1 offer a detailed comparison of the performance metrics for AdaBagging and the ensemble regressive arboretum (ERA) model during both the training and testing phases with hold-out validation. The models' efficacy in detecting Sybil attacks in MANETs may be understood by examining the performance metrics, which include recall, accuracy, precision, and F1-score (Figure 2).

AdaBagging Performance

In the training phase, AdaBagging demonstrates strong performance with an accuracy of 96.88 and 96.82% precision, showing its ability to correctly classify both legitimate nodes and Sybil attackers. During testing (with

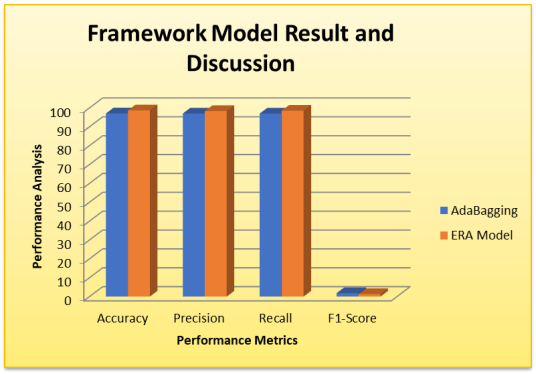
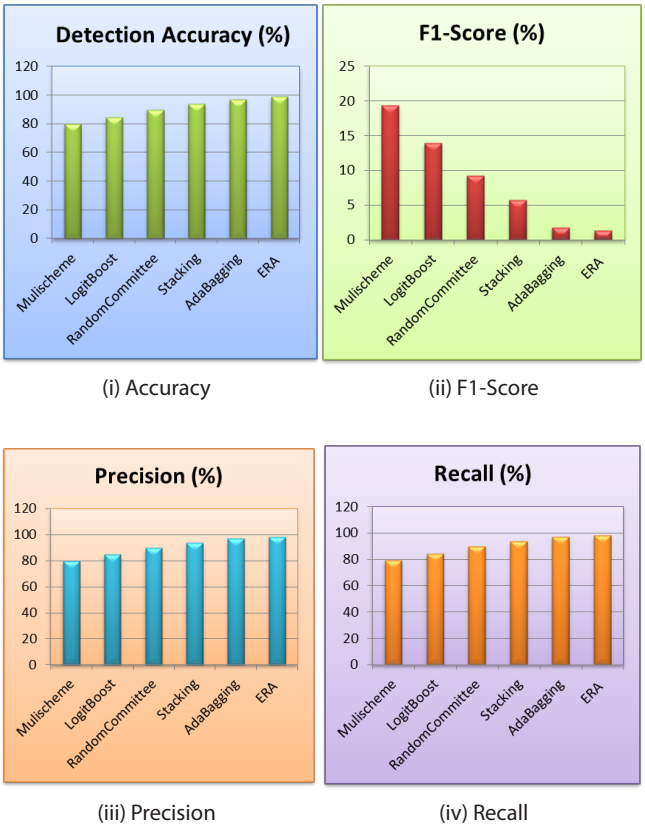


Figure 2: Framework model result and discussion

30% hold-out validation), the accuracy slightly increases to 97.07%, and precision remains high at 97.02%. The recall for AdaBagging is also strong, at 96.75% in the training phase and 97.00% in testing, indicating the model's ability to detect most Sybil attackers. However, the F1-score, which balances precision and recall, shows a relatively low value of 2.30% in training and 1.80% in testing. This suggests that while AdaBagging is effective at identifying Sybil attackers, its performance may not be as balanced, with a potential bias towards precision, causing it to miss some true positive Sybil nodes.

ERA Model Performance

The ERA model shows slightly better performance than AdaBagging across all metrics. In the training phase, the ERA model achieves an accuracy of 98.26%, which increases to 98.72% in testing, highlighting its strong capability to generalize on unseen data. Precision and recall for the ERA model also perform better than AdaBagging, with precision reaching 98.14% in training and 98.29% in testing, and



(i) Accuracy (ii) F1-Score

(iii) Precision (iv) Recall

Figure 3: Comparative analysis of various machine learning algorithms

recall improving to 98.43 and 98.54%, respectively. This indicates that ERA is more adept at detecting Sybil attacks while maintaining a balance between false positives and false negatives. However, the F1-score for ERA is lower than AdaBagging, with a value of 1.69% in training and 1.32% in

Table 1: Unified framework model result and discussion

Performance Metrics	*AdaBagging model*		*Ensemble regressive arboretum model (ERA Model)*	
	Training phase hold-out validation (70%)	*Testing phase hold-out validation (30%)*	*Training phase hold-out validation (70%)*	*Testing phase hold-out validation (30%)*
Accuracy	96.88	97.07	98.26	98.72
Precision	96.82	97.02	98.14	98.29
Recall	96.75	97.00	98.43	98.54
F1-Score	2.30	1.80	1.69	1.32

Table 2: Comparative analysis with proposed framework

	Detection accuracy (%)	*F1-Score (%)*	*Precision (%)*	*Recall (%)*
Mulischeme	79.68	19.30	79.59	79.32
LogitBoost	84.53	13.93	84.46	84.40
RandomCommittee	89.75	9.23	89.69	89.58
Stacking	93.87	5.67	93.40	93.47
AdaBagging	97.07	1.80	97.03	97.00
ERA (%)	98.72	1.32	98.29	98.54

testing. This reduction in the F1-score suggests that while ERA excels in accuracy and recall, it may slightly struggle with achieving a perfect balance between precision and recall, leading to more false positives.

Comparative analysis with other models

From Table 2, it is evident that ERA outperforms all other models in terms of detection accuracy, precision, and recall. AdaBagging also shows strong results, with high precision and recall but a slightly lower F1 score. While models like RandomCommittee and stacking also show competitive performance, they do not achieve the same level of accuracy as AdaBagging or ERA. These findings underline the effectiveness of ensemble-based models, particularly AdaBagging and ERA, in providing accurate and reliable Sybil attack detection in MANETs (Figure 3).

Conclusion

Particularly during testing, which is necessary to evaluate performance in the real world, the comparison of the two models shows that the ERA model beats AdaBagging in terms of memory, accuracy, and precision. Improved testing accuracy indicates that ERA can generalize effectively on unknown data. Hence proving its resilience in dynamic contexts like MANETs. Both models, however, show rather good performance; the unified framework might use the advantages of each method to enhance output even more. The F1 scores indicate that both models, while strong in overall detection, may benefit from additional fine-tuning or post-processing steps to improve the balance between precision and recall. This could involve further model optimization or hybrid techniques to refine the detection of Sybil attacks, especially in more challenging scenarios. While the ERA model shows superior performance in terms of accuracy, precision, and recall, AdaBagging still offers reliable performance and may be more computationally efficient. Combining the strengths of both models into a unified framework could offer enhanced performance for detecting Sybil attacks in MANETs, making the system both accurate and robust in various network conditions.

Ethical approval

None of the writers have ever conducted research involving human subjects, and none of that work appears in this paper.

Acknowledgment

Their insightful criticism and recommendations greatly improved the text, and we are grateful to the Editor, Associate Editor, and Reviewers for their work.

References

Ahmed Alhussen, and Arshiya S. Ansari. (2024). Real-Time Prediction of Urban Traffic Problems Based on Artificial Intelligence-Enhanced Mobile Ad Hoc Networks (MANETS), Computers, Materials and Continua, 79(2), Pages 1903-1923.

Amol Vasudeva., Manu Sood. (2018). Survey on sybil attack defense mechanisms in wireless ad hoc networks, Journal of Network and Computer Applications, 120, Pages 78-118.

Anjana Devi, V., Vithya Ganesan., Sri Anima Padmini, V., Shriman k.arun. (2024). An energy efficient routing establishment (EERE) mechanism for MANET-IoT security, Franklin Open, 8.

Cong Pu., Kim-Kwang Raymond Choo. (2022). Lightweight Sybil Attack Detection in IoT based on Bloom Filter and Physical Unclonable Function, Computers & Security, 113.

Di Pietro, R., Guarino, S., Verde, N.V., Domingo J, -Ferrer. (2014). Security in wireless ad-hoc networks – A survey, Computer Communications, 51, Pages 1-20.

Harsh KupwadePatil, Thomas M. Chen. (2013). Chapter 16 - Wireless Sensor Network Security, Computer and Information Security Handbook (Second Edition), Pages 301-322.

Harold Robinson, Y., Golden Julie, E., Krishnan Saravanan., Le Hoang Son., Raghvendra Kumar., Mohamed Abdel-Basset. (2019). Link-Disjoint Multipath Routing for Network Traffic Overload Handling in Mobile Ad-hoc Networks, IEEE Access,7, Pages 143312-143323.

Imrich Chlamtac, Marco Conti., Jennifer J.-N. Liu. (2003). Mobile ad hoc networking: imperatives and challenges, Ad Hoc Networks, 1(1), Pages 13-64.

Jawad Hassan., Adnan Sohail., Ali Ismail Awad., M. Ahmed Zaka. (2024). LETM-IoT: A lightweight and efficient trust mechanism for Sybil attacks in Internet of Things networks, Ad Hoc Networks, 163.

Mawloud Omar., Yacine Challal., Abdelmadjid Bouabdallah. (2012). Certification-based trust models in mobile ad hoc networks: A survey and taxonomy, Journal of Network and Computer Applications, 35(1), Pages 268-286.

Ramesh Vatambeti., Srihari Varma Mantena., K.V.D. Kiran., Srinivasulu Chennupalli., M Venu Gopalachari. (2024). Black hole attack detection using Dolphin Echo-location-based machine learning model in MANET environment, Computers and Electrical Engineering, 114.

Rui Meng., Bingxuan Xu., Xiaodong Xu., Mengying Sun., Bizhu Wang., Shujun Han., Suyu Lv., Ping Zhang. (2025). A survey of Machine Learning-based Physical-Layer Authentication in wireless communications, Journal of Network and Computer Applications, 235.

Sherril Sophie Maria Vincent., N. Duraipandian. (2024). Detection and prevention of sinkhole attacks in MANETS based routing protocol using hybrid AdaBoost-Random forest algorithm, Expert Systems with Applications, 249.

Sotirios Messinis., Nikos Temenos., Nicholas E. Protonotarios., Ioannis Rallis., Dimitrios Kalogeras., Nikolaos Doulamis. (2024). Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review, Computersin Biology and Medicine, 170.

Yukun Cheng., Xiaotie Deng., Yuhao Li., Xiang Yan. (2024). Tight incentive analysis of Sybil attacks against the market equilibrium of resource exchange over general networks, Games and Economic Behaviour, 148, Pages 566-610.

Zhaoyi Zhang., Yingxu Lai., Ye Chen., Jingwen Wei., Yuhang Wang. (2023). Detection method to eliminate Sybil attacks in Vehicular Ad-hoc Networks, Ad Hoc Networks, 141.