International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(4s) 2026 pp. 37-47
https://doi.org/10.70917/ijcisim-2026-2491
Article

A Trust-Weighted Stacking Ensemble Framework for Wormhole Attack Detection in Wireless Sensor Networks

Megha B. Patel[1*], Manish M. Patel[2]

[1] Sankalchand Patel College of Engineering, Sankalchand Patel University, Visnagar-384315, India.
Email: patelmegha3110@gmail.com
[2]Sankalchand Patel College of Engineering, Sankalchand Patel University, Visnagar-384315, India
Email: it43manish@gmail.com

Abstract: Wireless Sensor Networks (WSNs) are extensively employed in smart monitoring, healthcare, industrial automation and agriculture. However, due to the open communication environment and limited resources, they are quite vulnerable to routing attacks such as wormhole attacks. Current detection approaches are primarily based on hardware support, topological assumptions, or single-model learning techniques, which impair their scalability and adaptability. In this paper, we present a novel architecture called Adaptive Trust-Weighted Ensemble with Dynamic Feature Fusion (ATWEDF) for wormhole attack detection in WSNs. The proposed approach uses classifiers such as Random Forest, XGBoost and Support Vector Machine to provide behavioural, communication and verifier trust signals. A correlation-based dynamic feature fusion mechanism is utilized to encourage discriminative feature representation and Logistic Regression meta-learner performs adaptive trust-weighted stacking for final classification. The studies have been performed on Wormhole attack-Contr2 v2 dataset which consists of 637,862 records with 20 input features. The experimental findings reveal that ATWEDF obtains 99.75%, 99.83%, 99.84%, 99.83% and 0.55% for Accuracy, Precision, Recall, F1-score and False Positive Rate respectively which is better than the existing baseline models. The results confirm that trust-weighted stacking with correlation-driven feature fusion is an effective and reliable solution for wormhole attack detection in WSNs.
Keywords: Wireless Sensor Network, Wormhole Attack, Intrusion Detection, Stacking ensemble, Trust-Weighted learning, Feature fusion, Random Forest, Support Vector Machine, XGBoost, Logistic regression meta-learner.

1. Introduction

Wireless Sensor Networks (WSNs) are developing as one of the most promising enabling technologies for smart environments and real-time monitoring applications. Wireless Sensor Network (WSN) is a network of large number of sensor nodes [1] that collaborate to monitor and collect data and then communicate this data through wireless communication channels to central monitoring stations. Wireless Sensor Networks (WSN) are extensively used in healthcare systems, military surveillance, smart agriculture, industrial automation, environmental monitoring, intelligent transportation systems, disaster management applications because of its low deployment cost, scalability and distributed sensing capability [1][2].

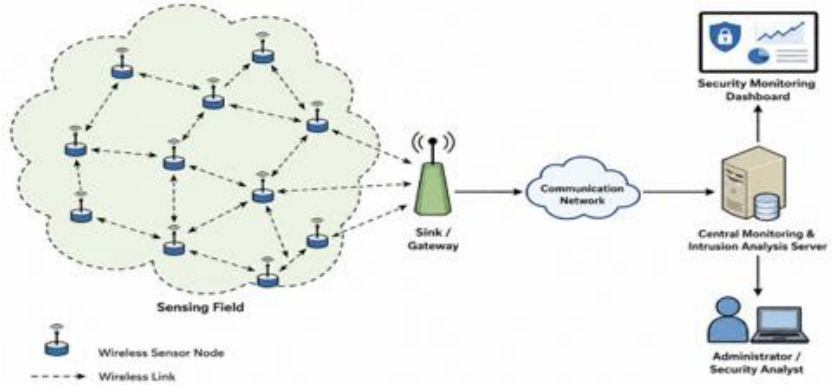

Fig. 1. Generic wireless sensor network topology for centralized monitoring and intrusion analysis

WSN has several advantages but has severe security concerns due to restricted computational resources, limited energy supply, decentralized routing and open wireless communication. These constraints make WSNs as very vulnerable to various attacks such as sinkhole attacks, Sybil attacks, selective forwarding attacks, blackhole attacks, denial-of-service attacks, and wormhole attacks [1][2][15]. Among the most dangerous and difficult to detect attacks in the routing layer are wormhole attacks.

A wormhole attack is an attack in which two or more malicious nodes [1] work together to establish a low latency tunnel between two distant areas of the network and replay routing messages to alter the perception of the topology within the network. Hence, the normal sensor nodes incorrectly consider the malicious path as the quickest communication path. This leads to traffic rerouting, path distortion, packet loss, network congestion and degraded data transfer [3][4]. Wormhole attacks are unlike many classic attacks in that they are not always associated with the change of packets and may be difficult to detect using typical cryptography-based approaches.

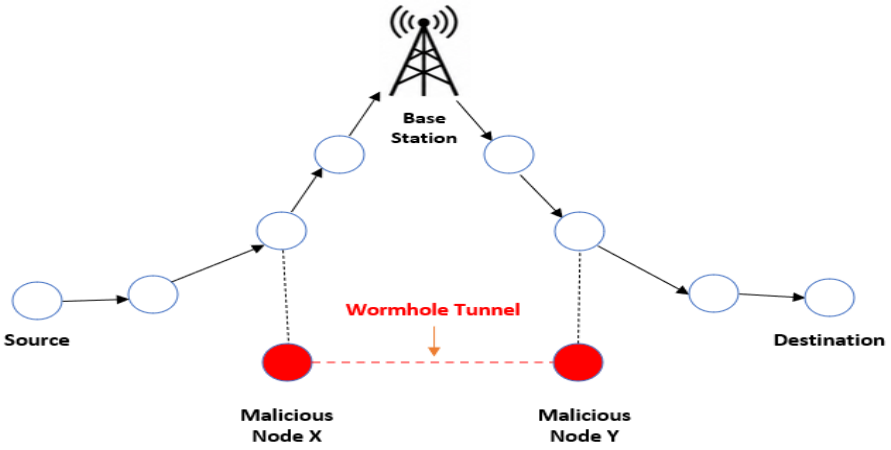

Fig. 2. Conceptual wormhole attack scenario in wireless sensor network

Several classic wormhole detection approaches are offered such as packet leash, time synchronization, geographical localization, hop-count, watchdog and cryptographic authentication [1][5]. However, most of these solutions require additional hardware support, precise clock synchronization, localization devices or protocol-specific assumptions, which increases the complexity in deployment and processing overhead.

Recent developments in Artificial Intelligence (AI), Machine Learning (ML) and Deep Learning (DL) [1] have vastly enhanced intrusion detection ability in Wireless Sensor Networks. ML-based intrusion detection systems should not substantially rely on handcrafted rules or hardware assumptions to automatically learn traffic behaviour patterns and identify abnormal routing activities [6][10]. Existing machine learning-based solutions are constrained by a dependence on a single model, inadequate feature optimization, insufficient calibration of trust, and limited generalization to a broad spectrum of attack behaviours.

To overcome these limitations, this research presents ATWEDF, an Adaptive Trust-Weighted Ensemble with Dynamic Feature Fusion for wormhole attack detection in Wireless Sensor Networks. The proposed method consists of the trust-aware stacking meta-learning based on the combination of Random Forest, XGBoost and Support Vector Machine classifiers and a correlation-driven feature fusion to improve the detection reliability by reducing the false alarms.

The key contributions of this work are summarized as follows:

1. Wormhole attack detection in WSNs is proposed based on a trust-weighted stacked ensemble framework.
2. To enhance discriminative feature representation, a correlation-based dynamic feature fusion mechanism is proposed.
3. Probabilistic trust signals generated by Random Forest, XGBoost, and SVM are fused through Logistic Regression meta-learning.
4. The proposed ATWEDF framework is evaluated using the Wormhole attack-Contr2 v2 dataset and achieves better performance compared to conventional machine learning approaches.
5. The proposed framework provides a significant reduction of false positive rates with high detection accuracy and robustness.

The rest of this paper is organized as follows:

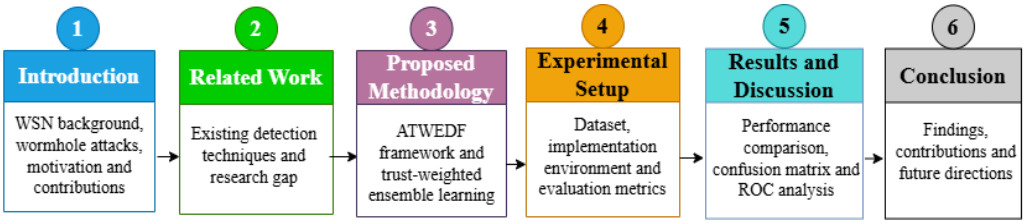

Fig. 3. Paper Organization

2. Related Work

2.1. Machine Learning-Based Wormhole Detection in WSNs

The machine learning approaches have proven crucial in the detection of wormhole attack in Wireless Sensor Networks. Shaon and Ferens [3] proposed an ANN based wormhole attack detection system, which can perform better than the Support Vector Machine and Logistic Regression classifiers without any additional hardware assumptions. They demonstrated the applicability of supervised learning to attack detection at routing layer.

To improve path selection under wormhole attack conditions, Harpal et al. [4] proposed a watchdog- and clustering-based mechanism. The approach they adopted used routing behaviour analysis to detect suspicious communication paths in WSN environments.

Alshehri [8] proposed a hybrid SVM and Deep Neural Network framework for the detection of wormhole attack in IoT and WSN environments. The study showed that hybrid deep learning models can successfully learn complex attack patterns and enhance the classification performance.

Abdullah et al. [9] developed a wormhole attack detection system based on LSTM for agricultural monitoring applications. They achieved a detection accuracy of almost 99%. They proved the effectiveness of temporal deep learning architectures for attack classification.

Almalki and Alajmani [10] investigated various machine learning classifiers for wormhole attack detection and concluded that XGBoost is the best approach in their evaluation environment based on the IoT.

Despite the promising results of these studies, most existing approaches mainly focus on single-model learning and do not consider trust-aware ensemble learning and dynamic feature fusion.

2.2. Trust- and Correlation-Based Intrusion Detection Approaches

Trust management and correlation analysis have become an important research direction of Wireless Sensor Network intrusion detection. Lai et al. [5] proposed a correlation based malicious node identification mechanism using temporal, spatial and event-based relationships among sensor nodes. Their work showed that correlation aware intrusion detection can enhance the reliability of malicious node identification as compared to traditional trust scoring based approaches.

Zhang et al. [6] proposed a wormhole attack detection mechanism based on Bayesian classification and node similarity. Their framework integrates shortest path hop count analysis and node pairs similarity to mitigate energy consumption and enhance suspicious node coverage.

These studies show the necessity of relational and correlation-aware security analysis. However, they do not consider correlation-driven feature fusion in a stacked machine learning framework.

2.3. Feature Selection and Lightweight IDS Frameworks

Feature selection is important to increase the performance of intrusion detection and to reduce the computational overhead [13]. Subbiah et al. [7] presented an intrusion detection system utilizing Boruta feature selection and Random Forest classifier. They found that feature tuning can considerably increase the classification performance of WSN intrusion detection.

Jabor et al. [14] presented a lightweight intrusion detection framework based on blockchain and machine learning for Wireless Sensor Networks. They tried to decrease computing overhead and have a good detection capability.

These studies illustrate the importance of feature optimization and designing lightweight IDSs. However, the current techniques do not employ correlation-weighted representations for dynamic feature fusion.

2.4. Real-Time and Behavioral Wormhole Detection Mechanisms

Similarly, behaviour and real-time based detection techniques have been investigated to counter wormhole attack as well. Bhatti et al. [11] presented a detection and isolation approach based on post-wormhole activity to identify malicious routing behaviour without requiring additional hardware support.

Zhukabayeva et al. [12] suggested a real-time anomaly detection system for WSNs, which can identify wormhole and sinkhole attacks in cyber-physical sensor environments. They noticed that wormhole attack has a considerable impact on routing behaviour, delay characteristics and stability of the network.

While these methodologies give practical insights into the behaviour of wormholes, they do not have the trust-aware stacked learning and correlation-driven feature fusion.

2.5. Research Gap and Motivation

Existing wormhole attack detection systems are mostly based on static trust evaluation, single model machine learning, heuristic routing analysis or protocol assumptions. Current researches do not combine synchronously:

- Trust-aware stacked ensemble learning
- Correlation-based dynamic feature fusion
- Adaptive meta-learning-based trust calibration
- Probabilistic synthesis of evidence across several models

This research gap inspires the proposed ATWEDF framework which combines trust-weighted stacking and dynamic feature fusion to improve reliability of wormhole attack detection while minimizing the false positive rate.

3. Proposed Methodology

3.1. Overview of ATWEDF Framework

The proposed framework is named ATWEDF (Adaptive Trust-Weighted Ensemble with Dynamic Feature Fusion). The framework is designed as a centralized intrusion detection architecture suitable for sink side or gateway level security monitoring in Wireless Sensor Networks.

The ATWEDF framework is composed of three major stages:

1) Base Trust Model Training
2) Dynamic feature fusion
3) Trust weighted stacking ensemble learning

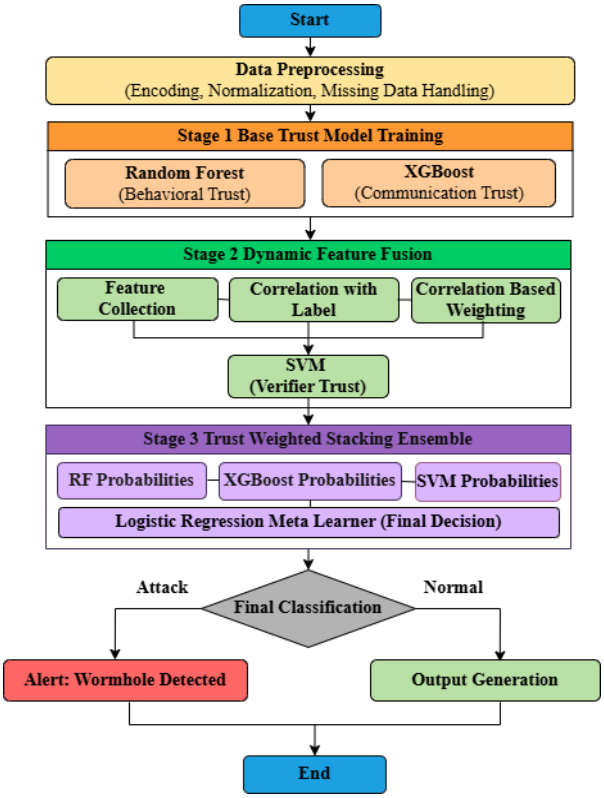

Fig. 4. Proposed ATWEDF framework architecture

3.2. Stage 1: Base Trust Model Training

In the first stage, trust-aware attack predictions are generated by training Random Forest (RF) and XGBoost (XGB) on the pre-processed dataset.

Let the training dataset be represented as:

$$D = \{(x_i, y_i)\}_{i=1}^{N} \quad (1)$$

where x_i is the feature vector for the ith network instance, and y_i is the binary class label.

The trust outputs produced by the base models are defined as:

$$T_{RF} = P_{RF}(y = 1|x) \quad (2)$$

$$T_{XGB} = P_{XGB}(y = 1|x) \quad (3)$$

where T_{RF} and T_{XGB} are Behavioural Trust and Communication Trust respectively.

These trust signals provide further evidence on the possibility of wormhole activity, which is subsequently combined with the verifier trust generated during the Dynamic Feature Fusion stage.

3.3. Stage 2: Dynamic Feature Fusion

The Pearson correlation analysis is performed between each input feature and the target attack label.

The Pearson correlation coefficient is computed as:

$$r_i = \frac{\mathrm{Cov}(X_i, Y)}{\sigma_{X_i}\sigma_Y} \quad (4)$$

The resulting correlation values are normalized to get adaptive feature weights:

$$W_i = \frac{|r_i|}{\sum_{j=1}^{m}|r_j|} \quad (5)$$

Compared to traditional feature-selection techniques that discard weak features, the proposed framework keeps all available features and adjusts their influence according to the strength of their correlation.

The weighted feature representation is calculated as:

$$X_w = X \odot W \quad (6)$$

Then it provides the weighted feature matrix to a Support Vector Machine (SVM) as a verifier model and produces another trust signal:

$$T_{SVM} = P_{SVM}(y = 1|X_w) \quad (7)$$

This verifier trust offers an independent assessment of attack probability by using correlation-enhanced feature representations.

3.4. Stage 3: Trust-Weighted Stacking Ensemble Learning

In the final phase, the trust outputs generated by Random Forest, XGBoost and SVM are fused through a trust-weighted stacking ensemble framework.

The trust-feature matrix is defined as follows:

$$M = [T_{RF}, T_{XGB}, T_{SVM}] \quad (8)$$

where M is behavioural, communication and verifier trust information.

The stacking meta-learner is a Logistic Regression classifier. The probability of wormhole attack is estimated as:

$$P(y = 1|M) = \sigma(\beta_0 + \beta_1 T_{RF} + \beta_2 T_{XGB} + \beta_3 T_{SVM}) \quad (9)$$

The final classification decision is acquired as,

$$\hat{y} = \begin{cases} 1, & P(y = 1|M) \geq 0.5 \\ 0, & \text{otherwise} \end{cases} \quad (10)$$

The trust-weighted stacking technique can adaptively fuse evidence, and can exploit the complementing strengths of various models to improve overall detection reliability.

4. Experimental Setup

4.1. Dataset Description

Experiments are carried out using the Wormhole attack-Contr2 v2 dataset obtained from Zenodo DOI: 10.5281/zenodo.15821959 [16]. The dataset was built for the purpose of wormhole intrusion detection in Wireless Sensor Networks.

Table 1. summary of the dataset characteristics

Parameter	Value
Dataset Name	Wormhole attack-Contr2 v2
Total Records	637,862
Input Features	20
Class Labels	Binary
Attack Instances	485,718
Normal Instances	152,144

Parameter	Value
Protocol Coverage	AODV and ICMP
Domain	Wireless Sensor Networks

4.2. Implementation Environment

The proposed ATWEDF framework was implemented in Google Colab using the python language. The experimental approach comprises data pre-processing, feature standardization, correlation analysis, dynamic feature weighting, trust model training, stacking ensemble learning and performance evaluation.

Model training and testing was performed using stratified 80:20 train-test split to retain the original class distribution. Before training the SVM verifiers, we applied correlation-based feature weighting. We used Logistic Regression as meta-learner in stacking.

Table 2. Hyperparameter Configuration

Component	Setting
Random Forest	n_estimators = 200
XGBoost	n_estimators = 200
XGBoost	max_depth = 6
XGBoost	learning_rate = 0.05
Linear SVM	C = 1.0, max_iter = 3000
Logistic Regression	C = 1.0, max_iter = 1000
Cross Validation	3-fold
Train-Test Split	80:20

These parameter selections are determined empirically to balance classification performance, computational efficiency and generalization capacity.

4.3. Evaluation Metrics

Performance of the proposed wormhole attack detection model was evaluated based on Accuracy, Precision, Recall, F1-Score, False Positive Rate (FPR) and ROC-AUC [7]. These metrics provide a comprehensive assessment of the classification efficiency of the model and its capability to distinguish between attack and normal traffic [8][10].

- **Accuracy**

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{11}$$

- **Precision**

$$Precision = \frac{TP}{TP + FP} \tag{12}$$

- **Recall**

$$Recall = \frac{TP}{TP + FN} \tag{13}$$

- **F1-Score**

$$F1\text{-}Score = \frac{2 \times Precision \times Recall}{Precision + Recall} \quad (14)$$

- **False Positive Rate**

$$FPR = \frac{FP}{FP + TN} \quad (15)$$

- **ROC-AUC**

The Area Under Curve (AUC) is a metric used to evaluate the separability of classifiers.

5. Results And Discussion

5.1. Comparative Performance Analysis

Table 3 shows the comprehensive performance metrics of the proposed ATWEDF framework and all the baseline models.

Table 3. Comparative Performance Analysis

Approach	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
SVM	92.95	96.83	93.81	95.30	9.80
KNN	97.12	97.76	98.47	98.11	7.20
Random Forest	98.35	98.57	99.27	98.92	4.60
Decision Tree	98.74	98.79	99.57	99.18	3.90
XGBoost	99.25	99.28	99.74	99.51	2.30
Naive Bayes	92.30	94.34	95.62	94.98	18.30
K-Means	83.36	92.36	85.19	88.63	22.50
ATWEDF	99.75	99.83	99.84	99.83	0.55

The proposed ATWEDF framework achieved the best performance in all evaluation measures. Compared to the single baseline classifier XGBoost, ATWEDF obtained superior accuracy, precision, recall, F1-score and ROC-AUC with a considerable reduction of false positive rates. The false positive rate is reduced from 2.30% to 0.55% demonstrating the efficiency of trust-weighted stacking and correlation driven feature fusion.

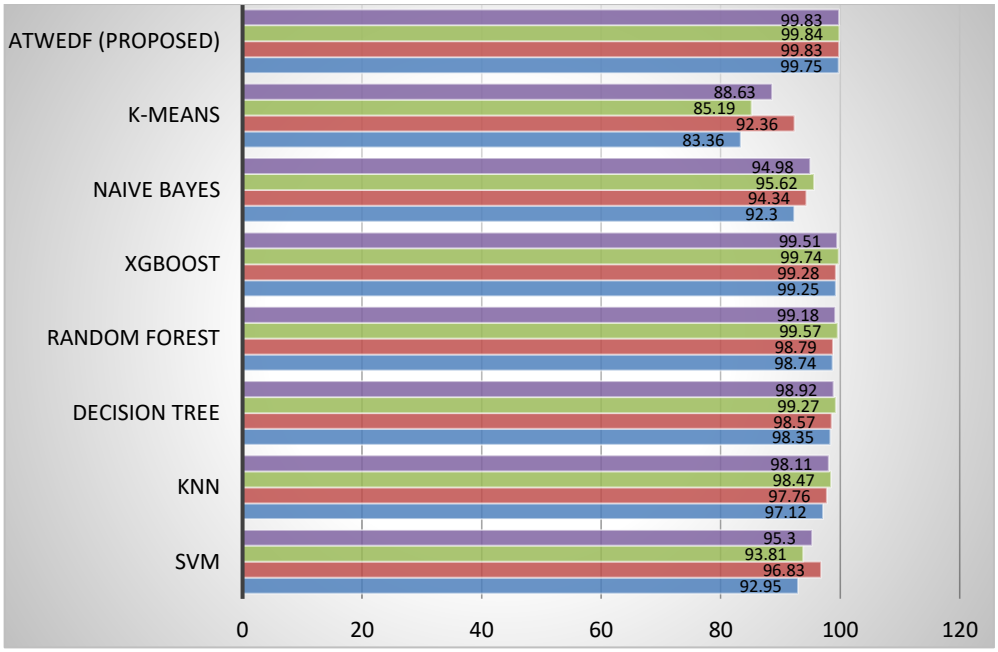

Fig. 5. Accuracy, Precision, Recall and F1-Score Comparison of ATWEDF and Baseline Models

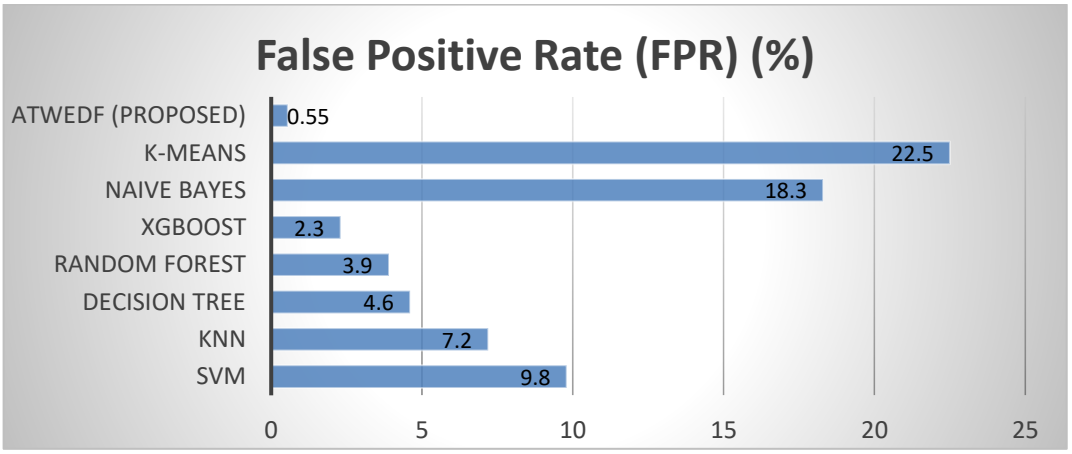

Fig. 6. False Positive Rate Comparison of ATWEDF and Baseline Models

5.2. *Classification and ROC Analysis*

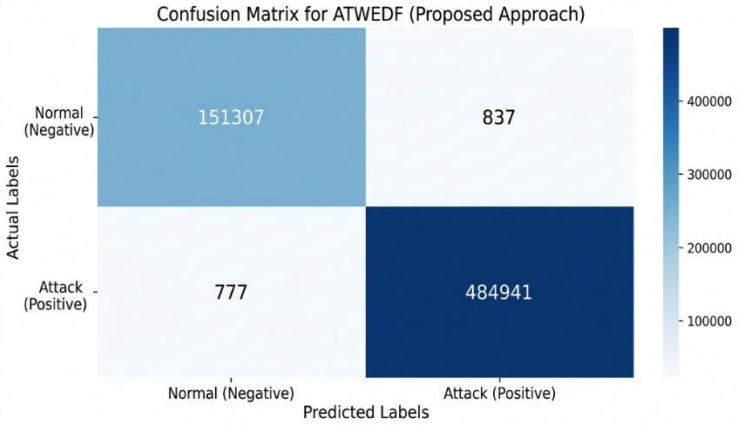

Fig. 7. Confusion Matrix of the Proposed ATWEDF Framework

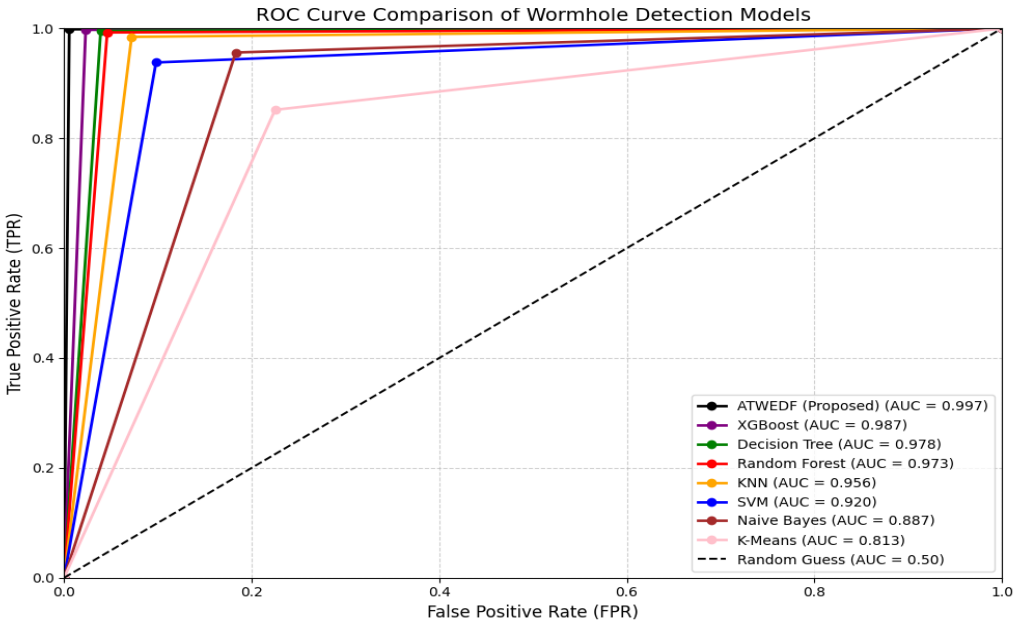

Fig. 8. ROC Curve Comparison of ATWEDF and Baseline Models

The confusion matrix obtained by the proposed ATWEDF framework is shown in Figure 7. The high concentration of correctly classified instances along the principal diagonal indicates a good classification capability with few misclassification errors. The ROC performance of the evaluated models is shown in Figure 8. The proposed framework achieved AUC value of 0.997 which is an excellent value indicating the class separability and robust detection performance over different decision threshold.

5.3. Discussion

The good performance of ATWEDF can be attributed to the complementary advantages of the three-stage framework.

- Random Forest is good at capturing nonlinear routing behavior.
- XGBoost enhances hard-example refinement via gradient boosting.
- SVM is a verifier branch with correlation-weighted feature.
- Logistic Regression learns trust weights adaptively from classifier behavior.

Unlike traditional trust models based on handcrafted reputation scores, the proposed framework learns the trust in a dynamic way by fusing probabilistic evidence. Experimental results show that correlation-driven feature weighting can significantly improve error calibration and false alarm suppression.

6. Conclusion

In this paper, we propose Adaptive Trust-Weighted Ensemble with Dynamic Feature Fusion (ATWEDF) for wormhole attack detection in Wireless Sensor Networks. The proposed framework combines Random Forest, XGBoost and Support Vector Machine classifiers by employing trust-aware stacked meta-learning and correlation-driven feature fusion. Experimental evaluation on the Wormhole attack-Contr2 v2 dataset demonstrated that ATWEDF obtains superior intrusion detection performance with 99.75% accuracy, 99.83% precision, 99.84% recall, 99.83% F1-score, 0.55% false positive rate, and 0.997 ROC-AUC.

The proposed framework outperformed the conventional machine learning approaches significantly with low false alarm rates. The study validates the effectiveness of the proposed solution in terms of trust-weighted stacking and dynamic feature fusion for detection of attack in routing layer in Wireless Sensor Networks.

Future work will focus on:

- Real time deployment in resource constrained WSNs
- Lightweight optimization for edge-based intrusion detection
- Multi-attack classification

- Integration of federated learning
- Cross-dataset generalization analysis.

References

1. M. Hanif, H. Ashraf, Z. Jalil, N. Z. Jhanjhi, M. Humayun, S. Saeed, and A. M. Almuhaideb, “AI-Based Wormhole Attack Detection Techniques in Wireless Sensor Networks,” Electronics, vol. 11, no. 15, art. 2324, 2022.
2. A. Oztoprak, R. Hassanpour, A. Ozkan, and K. Oztoprak, “Security Challenges, Mitigation Strategies, and Future Trends in Wireless Sensor Networks: A Review,” ACM Computing Surveys, vol. 57, no. 4, art. 104, 2024.
3. M. N. A. Shaon and K. Ferens, “A Computationally Intelligent Approach to the Detection of Wormhole Attacks in Wireless Sensor Networks,” Advances in Science, Technology and Engineering Systems Journal, vol. 2, no. 3, pp. 302–320, 2017.
4. Harpal, G. Tejpal, and H. Kaur, “Wormhole Attack Detection from Wireless Sensor Networks Using Machine Learning Techniques,” International Journal of Mechanical Engineering and Technology, vol. 10, no. 10, pp. 302–314, 2019.
5. Y. Lai, L. Tong, J. Liu, Y. Wang, T. Tang, Z. Zhao, and H. Qin, “Identifying malicious nodes in wireless sensor networks based on correlation detection,” Computers & Security, vol. 113, art. 102540, 2022.
6. Z. Zhang, Z. Zeng, W. Yang, and F. Wu, “Wormhole attack detection method based on node pair similarity, shortest path hop count, and Bayesian classification algorithm in wireless sensor networks,” Journal of Wireless Communications and Networking, vol. 2026, art. 29, 2026, doi: 10.1186/s13638-025-02564-8.
7. S. Subbiah, K. S. M. Anbananthen, S. Thangaraj, S. Kannan, and D. Chelliah, “Intrusion Detection Technique in Wireless Sensor Network using Grid Search Random Forest with Boruta Feature Selection Algorithm,” Journal of Communications and Networks, vol. 24, no. 2, pp. 264–273, 2022.
8. A. H. Alshehri, “Wormhole attack detection and mitigation model for Internet of Things and WSN using machine learning,” PeerJ Computer Science, vol. 10, art. e2257, 2024.
9. A. Abdullah, A. N. A. Albaihani, B. Osman, and Y. Omar, “Detecting Wormhole Attack in Environmental Monitoring System for Agriculture using Deep Learning,” Journal of Advanced Research in Applied Sciences and Engineering Technology, vol. 51, no. 2, pp. 153–176, 2025.
10. M. Almalki and S. Alajmani, “Machine Learning-Based Detection of Wormhole Attacks in IoT Networks Using Classification Models,” International Journal of Recent Technology and Engineering, vol. 14, no. 1, 2025.
11. D. S. Bhatti, S. Saleem, A. Imran, H. J. Kim, K.-I. Kim, and K.-C. Lee, “Detection and isolation of wormhole nodes in wireless ad hoc networks based on post-wormhole actions,” Scientific Reports, vol. 14, art. 3428, 2024.
12. T. Zhukabayeva, L. Zholshiyeva, Y. Mardenov, A. Buja, S. Khan, and N. Alnazzawi, “Real-Time Detection and Response to Wormhole and Sinkhole Attacks in Wireless Sensor Networks,” Technologies, vol. 13, art. 348, 2025.
13. A. Sirisha and K. S. Sri, “Cluster head based dual level node authentication model with node pattern analysis for intrusion detection in wireless sensor networks using machine learning,” Discover Computing, vol. 29, art. 45, 2026.
14. M. S. Jabor, A. S. Azez, J. C. Campelo, and A. Bonastre, “A Lightweight IDS Based on Blockchain and Machine Learning for Detecting Physical Attacks in Wireless Sensor Networks,” Sensors, vol. 26, art. 1961, 2026.
15. S. Asare and W. P. Rey, “Review of Intrusion Detection Algorithms for Mitigating Sinkhole Attack on LEACH Protocol in Wireless Sensor Network,” International Journal of Computer Networks and Applications, vol. 13, no. 2, 2026.
16. Wormhole attack-Contr2 v2 Dataset, Zenodo DOI: 10.5281/zenodo.15821959.