

An efficient hybrid machine learning framework for wormhole detection in wireless sensor networks

Megha B. Patel *

*Department of Computer Engineering
Sankalchand Patel College of Engineering
Sankalchand Patel University
Visnagar 384315
Gujarat
India*

Manish M. Patel [†]

*Department of Information Technology
Sankalchand Patel College of Engineering
Sankalchand Patel University
Visnagar 384315
Gujarat
India*

Abstract

Wireless Sensor Networks (WSNs) are critical to IoT applications but remain highly vulnerable to wormhole attacks, which create covert tunnels between colluding attackers. This research proposes a hybrid intrusion detection framework combining K-Means clustering and Decision Tree classification for efficient and interpretable wormhole attack detection. Experimental evaluation on the publicly available “wormhole attack-Contr2” dataset (637,863 instances) achieved 98.86% accuracy, 97.12% precision, 98.45% recall, and 97.78% F1-score. Comparative analysis with SVM, KNN, Random Forest, standalone Decision Tree, and standalone K-Means demonstrates superior detection performance and computational efficiency, making the proposed framework suitable for resource-constrained WSN and edge environments.

Subject Classification (2020): 68T05, 68T07.

Keywords: Wireless sensor networks, Wormhole attack detection, K-means clustering, Decision tree, Hybrid machine learning, Intrusion detection system, Network security, Attack detection.

* E-mail: Patelmegha3110@gmail.com (Corresponding Author)

[†] E-mail: it43manish@gmail.com

1. Introduction

1.1 Background and Motivation

Wireless Sensor Networks (WSNs) support distributed sensing and communication in different applications. These networks consist of resource-constrained sensor nodes that communicate through multi-hop wireless links to forward sensed information toward a base station or gateway [1].

1.2 Wormhole Attack Threat Model

Wormhole attack is one of the most severe and difficult-to-detect security threat [2]. In a canonical wormhole attack scenario, two or more colluding malicious nodes establish a low-latency, high-bandwidth “tunnel” between geographically distant regions of the network [3], [4]. The basic wormhole attack scenario is illustrated in Figure 1.

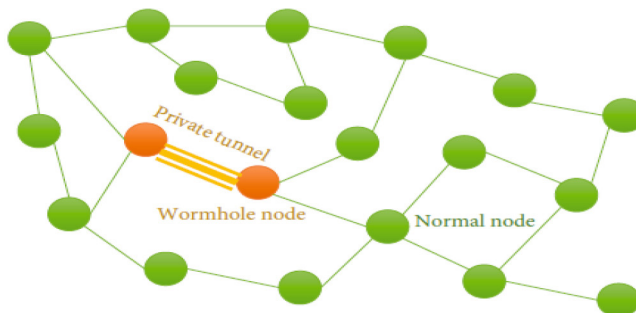


Figure 1

Wormhole attack with covert tunnel [5]

1.3 Research Motivation and Problem Statement

Traditional wormhole countermeasures may require synchronization, location information, specialized hardware, or high computational overhead [6]. Machine-learning-based IDS offer an alternative but may face many limitations [7-9].

2. Related Work

2.1 Traditional Wormhole Detection Approaches

Traditional wormhole countermeasures include packet-leash, localization, topology-based, and trust-based techniques [6], [8], [9].

2.2 Machine Learning for Intrusion Detection in WSNs

Machine learning has been widely used for intrusion detection in WSNs [10-13]. Supervised models such as SVM, KNN, Random Forest, and Decision Trees can classify network traffic as normal or malicious using extracted features [7], [14]. Alshehri [11] proposed a machine learning-based wormhole detection model for IoT and WSNs, achieving over 95% detection accuracy [11], [5].

2.3 Hybrid and K-Means-Based Approaches

Zaheer et al. [15] introduced a hybrid approach integrating K-Means clustering with Decision Tree classification. Wazid and Das [16] presented a K-Means-based hybrid intrusion detection approach for WSNs.

3. Proposed Methodology

3.1 System Architecture Overview

The proposed Hybrid K-Means–DT framework follows a two-stage intrusion-detection architecture comprising data preprocessing, K-Means clustering for structural feature extraction, Decision Tree classification for attack detection, and performance evaluation. The overall workflow is illustrated in Figure 2.

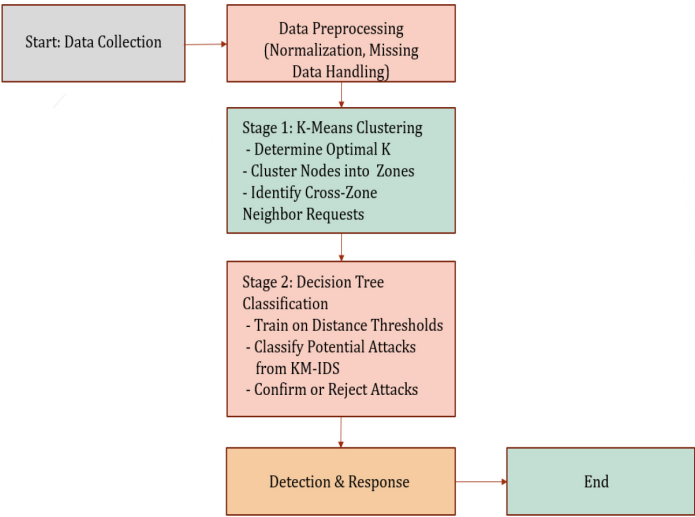


Figure 2
Proposed Method Flow chart

3.2 Stage 1: K-Means Clustering for Feature Enrichment

The optimal number of clusters was determined using the Elbow Method and Silhouette Analysis, resulting in $k=4$ with a silhouette score of 0.68. Following clustering, three types of structural information were incorporated into the feature representation: cluster assignment, distances from each instance to the four centroids, and relative cluster density. These derived attributes were combined with the 20 normalized original features to produce a 26-dimensional representation for subsequent classification.

3.3 Decision Tree Classification

Feature selection employs Gini impurity criterion for computational efficiency. Grid search combined with 5-fold cross-validation was used to tune the hyperparameters.

4. Experimental Setup

Experiments were conducted in Python 3.8 using scikit-learn, NumPy, and Pandas on an Intel Core i7 system with 32 GB RAM. The “wormhole attack-Contr2” dataset [17] was preprocessed using value imputation, label encoding, outlier treatment, Min-Max normalization, and Random Over-Sampling.

5. Results and Discussion

Table 1 presents comprehensive performance metrics for the proposed Hybrid K-Means-DT framework and all baseline models.

Table 1
Performance Comparison of Hybrid K-Means-DT and Baseline Models

Approach	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
SVM	97.02	94.41	95.12	94.76	12.0
KNN	98.24	96.05	96.83	96.44	13.0
Random Forest	99.18	97.54	98.11	97.82	10.0
Decision Tree	98.51	95.52	97.36	96.43	11.0
K-Means	89.04	84.25	87.61	85.89	20.0
Hybrid K-Means-DT	98.86	97.12	98.45	97.78	9.2

Figure 3 presents the accuracy of the proposed Hybrid K-Means-DT framework with the baseline models. Figure 4 compares the precision, recall, and F1-score of the evaluated models. The proposed method indicates balanced detection performance.

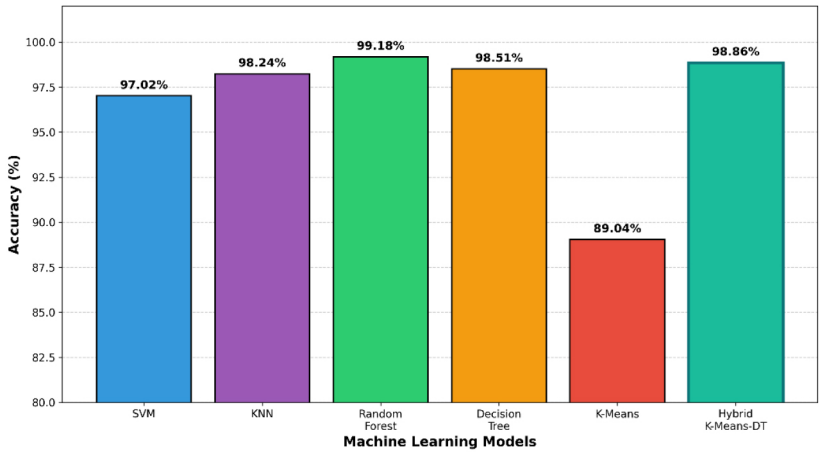


Figure 3
Accuracy Comparison

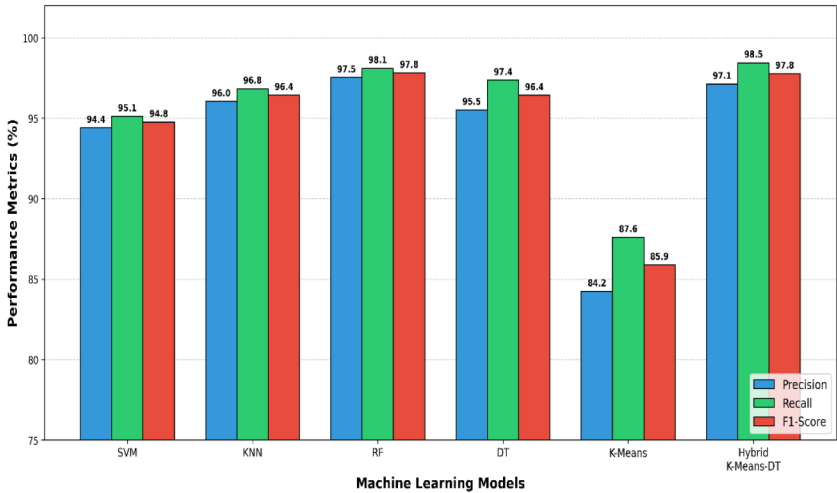


Figure 4
Precision, Recall, F1-Score Comparison

6. Conclusion and Future Work

K-Means-derived structural features were combined with an interpretable Decision Tree classifier, achieving 98.86% accuracy, 98.45% recall, and 9.2% FPR. The results demonstrate that the proposed architecture can provide competitive detection performance while maintaining computational efficiency and interpretable decision-making for WSN security applications. Future work will investigate multi-attack classification, online model adaptation, cross-protocol generalization, adversarial robustness, real-world WSN testbed evaluation, and energy-aware deployment.

References

- [1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Comput. Netw.*, vol. 38, no. 4, pp. 393–422 (2002), doi: 10.1016/S1389-1286(01)00302-4.
- [2] G. Farjamnia, Y. Gasimov, and C. Kazimov, "Review of the techniques against the wormhole attacks on wireless sensor networks," *Wireless Pers. Commun.*, vol. 105, no. 4, pp. 1561–1584 (2019), doi: 10.1007/s11277-019-06160-0.
- [3] M. Patel, A. Aggarwal, and N. K. Chaubey, "Detection of wormhole attacks in mobility-based wireless sensor networks," *Int. J. Commun. Netw. Distrib. Syst.*, vol. 21, no. 2, pp. 147–156 (2018), doi: 10.1504/IJCNDS.2018.094217.
- [4] M. Patel, A. Aggarwal, and N. K. Chaubey, "Analysis of wormhole attacks in wireless sensor networks," in *Recent Findings in Intelligent Computing Techniques*, P. Sa, S. Bakshi, I. Hatzilygeroudis, and M. Sahoo, Eds., *Advances in Intelligent Systems and Computing*, vol. 708, pp. 33–42. Singapore: Springer (2018), doi: 10.1007/978-981-10-8636-6_4.
- [5] 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. no. 2324 (2022), doi: 10.3390/electronics11152324.
- [6] 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 net-

- works based on post-wormhole actions,” *Sci. Rep.*, vol. 14, Art. no. 3428 (2024), doi: 10.1038/s41598-024-53938-9.
- [7] M. Patel and M. Patel, “A comparative analysis of machine learning models for enhancing wormhole attack detection in wireless sensor networks,” *J. Inf. Syst. Eng. Manage.*, vol. 10, no. 53s, pp. 317–327 (2025), doi: 10.52783/jisem.v10i53s.5893.
- [8] R. Garg, T. Gulati, and S. Kumar, “Range free localization in WSN against wormhole attack using Farkas’ lemma,” *Wireless Netw.*, vol. 29, pp. 2029–2043 (2023), doi: 10.1007/s11276-023-03279-8.
- [9] S. Javed, A. Sajid, T. Kiren, I. U. Khan, C. Dewi, F. Cauteruccio, and H. J. Christanto, “A subjective logical framework-based trust model for wormhole attack detection and mitigation in low-power and lossy (RPL) IoT-networks,” *Information*, vol. 14, no. 9, Art. no. 478 (2023), doi: 10.3390/info14090478.
- [10] S. Konatam, S. Nalluri, M. M. Malyala, H. Daiya, V. N. Kumar, and K. S. Raju, “A random forest-based method for effective and robust detection of wormhole attacks in wireless sensor networks,” in *Intelligent Computing and Communication, ICICC 2024, Lecture Notes in Networks and Systems*, vol. 1241, pp. 461–472. Singapore: Springer (2025), doi: 10.1007/978-981-96-1267-3_39.
- [11] A. H. Alshehri, “Wormhole attack detection and mitigation model for Internet of Things and WSN using machine learning,” *Peer J Comput. Sci.*, vol. 10, Art. no. e2257 (2024), doi: 10.7717/peerj-cs.2257.
- [12] R. Alghamdi and M. Bellaiche, “A cascaded federated deep learning based framework for detecting wormhole attacks in IoT networks,” *Comput. Secur.*, vol. 125, Art. no. 103014 (2023), doi: 10.1016/j.cose.2022.103014.
- [13] M. D. Kokate, A. Julian, R. Ramyadevi, M. Rele, G. I. Mary, and M. Vaithianathan, “Enhancing network security in wireless sensor networks through real-time intrusion detection systems,” *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 5-A, pp. 1743–1751 (2025), doi: 10.47974/JDMSC-2174.

- [14] D. Vaya and R. K. Saxena, "Security attack classification and performance analysis of machine learning algorithms over CSIC HTTP dataset," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 5-A, pp. 1569–1578 (2025), doi: 10.47974/JDMS-2155.
- [15] A. Zaheer, S. Tahir, M. F. Almufareh, and B. Hamid, "A hybrid model for botnet detection using machine learning," in *Proc. 2023 Int. Conf. Business Analytics Technol. Secur. (ICBATS)*, Dubai, United Arab Emirates (2023), pp. 1–8, doi: 10.1109/ICBATS57792.2023.10111161.
- [16] M. Wazid and A. K. Das, "An efficient hybrid anomaly detection scheme using K-means clustering for wireless sensor networks," *Wireless Pers. Commun.*, vol. 90, no. 4, pp. 1971–2000 (2016), doi: 10.1007/s11277-016-3433-3.
- [17] M. Z. Hussain, "Wormhole attack dataset (Version v2)," *Zenodo*, (2020), doi: 10.5281/zenodo.4312630.

Received June, 2026