Abstract:
Wireless Sensor Networks (WSNs) are critical in diverse applications such as environmental monitoring, healthcare, and military surveillance. However, their open nature and resource-constrained environment make them particularly vulnerable to security threats, especially Denial-of-Service (DoS) attacks. Real-time detection of such attacks is challenging due to the need for rapid response, dynamic network behavior, and limited computational and energy capabilities of sensor nodes. Traditional anomaly detection techniques often either overload the network or suffer from high false positive rates, making them unsuitable for deployment in real-world WSNs.

This research proposes a **hybrid detection framework** that combines **Fuzzy C-Means (FCM)** clustering, **Principal Component Analysis (PCA)**, and the **Random Forest** classifier to detect DoS attacks efficiently and accurately in real time. The system begins by applying FCM clustering to group nodes based on their communication behavior, which not only aids in localizing anomalies but also improves energy efficiency by reducing unnecessary inter-node communication and isolation.

To further optimize performance, PCA is employed to reduce the feature space by selecting the most informative variables, thus lowering computational complexity and enhancing processing speed. This step ensures that only significant behavioral metrics such as packet drop rate, transmission delay, and node throughput are used for further analysis.

Finally, the clustered and reduced feature data is passed to the Random Forest algorithm—a robust and interpretable machine learning model known for handling high-dimensional data and avoiding overfitting. The model accurately classifies whether a node is under DoS attack, leveraging decision trees trained on labeled data representing normal and malicious activities.

Extensive simulation results demonstrate that the proposed approach achieves a high detection rate, low false alarm rate, and optimal energy consumption, outperforming conventional methods. The hybrid model's adaptability and efficiency make it highly suitable for deployment in practical WSN environments requiring secure, real-time decision-making.

Keywords:
Wireless Sensor Networks, Denial-of-Service Attacks, Real-Time Intrusion Detection, Fuzzy C-Means Clustering, Principal Component Analysis, Random Forest Classifier, Energy-Aware Systems, Machine Learning