Power System Technology
ISSN:1000-3673

Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

A Multi-Metric Trust-based Approach for Detecting Black Hole Attacks in Wireless Sensor Networks using K-Means Clustering

K. Kathirvel[1]* and S. Hemalatha[2]

[1]Research Scholar

*[1]kkathir.kandasamy@gmail.com[1]**

[2]Associate Professor

[2]hemalatha.s@kahedu.edu.in[2]

[1, 2] Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore-641 021, Tamilnadu, India

Abstract

In Wireless Sensor Networks (WSNs), securing communication against threats like blackhole attacks is essential for maintaining the integrity of the network. This paper proposes a system where the Cluster Head (CH) monitors and evaluates node behavior using manifold metrics: Packet Forwarding Behavior (PFB), Acknowledgment Ratio (AR), Reputation Score (RS), Cooperation Ratio (CR), and Energy Deviation (ED). These metrics help detect abnormal activities, especially packet dropping associated with blackhole attacks. The PFB measures how effectively a node forwards packets, while AR gauges the node's reliability in sending acknowledgments for forwarded packets. The RS is a long-term metric combining AR and PFB to track a node's trustworthiness over time. CR assesses a node's cooperative behavior with neighboring nodes, and ED evaluates energy usage, identifying anomalies in power consumption that could signal malicious activity. To classify nodes as either normal or potentially malicious (blackhole), a K-means clustering algorithm is employed. Nodes are grouped based on the five metrics into two clusters: one for normal nodes and another for suspicious nodes. The algorithm iteratively adjusts the cluster centroids using Euclidean distance until stable clusters are formed or a maximum number of iterations is reached. By applying this approach, the system effectively differentiates between normal and blackhole nodes, improving the security and resilience of WSNs against attacks. A proof of mathematical has proven the applicability of the proposed model. The simulation results shows better result compare with other existing models in terms of performance metrics. The proposed model has effectively detect the balckhole nodes compare with other models.

Keywords: Wireless Sensor Network, Security, Trust, Cluster head, K-means clustering

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

1. Introduction

In Wireless Sensor Networks (WSNs), ensuring secure and reliable data transmission is critical to maintaining overall network efficiency. These networks are frequently utilized in applications where real-time monitoring and communication are necessary, such as environmental observation, military operations, and healthcare monitoring (Alzubaidi, L et al., 2018). However, WSNs are highly susceptible to a variety of security threats, with blackhole attacks being one of the most severe. During a blackhole attack, malicious nodes deliberately drop packets instead of forwarding them, leading to substantial data loss and performance degradation across the network (Dharini, N et al., 2022). As a result, detecting and addressing these attacks is essential to maintaining the network's operational integrity. This paper introduces a multi-metric node evaluation approach, which allows a Cluster Head (CH) to observe and evaluate the behavior of nodes within its cluster. The system analyzes multiple parameters including Packet Forwarding Behavior (PFB), Acknowledgment Ratio (AR), Reputation Score (RS), Cooperation Ratio (CR), and Energy Deviation (ED). Together, these metrics serve to identify suspicious activities such as packet dropping, a hallmark of blackhole attacks. By tracking node behavior over time, the CH can detect and isolate malicious nodes, thus enhancing the security and stability of the network (Virendra, D et al., 2022). The figure 1 depicts the representation of wireless sensor networks.

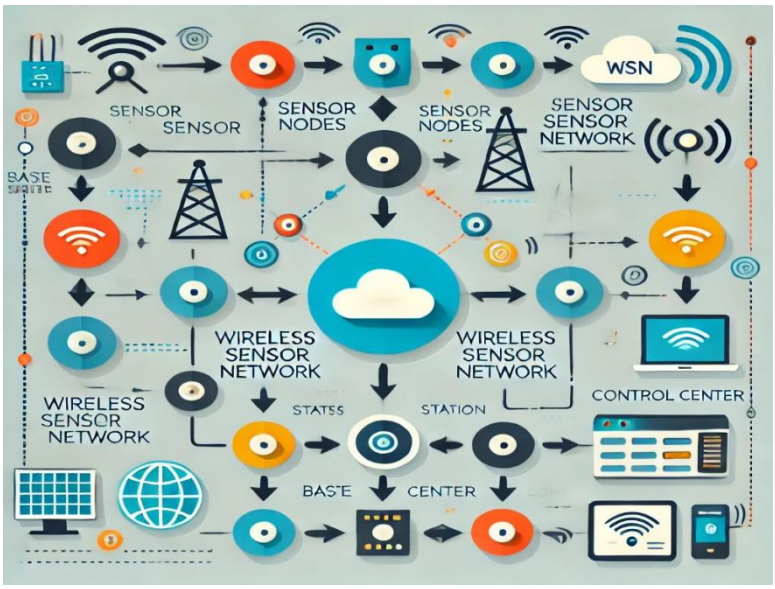

Figure 1. The Representation of Wireless Sensor Network

Blackhole attacks exploit the trust-based nature of WSN routing mechanisms. In these attacks, malicious nodes mislead others by falsely claiming the most efficient routes, only to discard data packets once received. This disruption leads to extensive data loss and deteriorates the overall network communication (Yoon, J et al., 2021, Zhang, H et al., 2019). Detecting these

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

attacks is challenging but crucial for preventing data inaccuracies and ensuring the success of mission-critical operations. If left unchecked, such attacks can compromise the network's reliability and diminish the quality of data gathered from the environment. The proposed detection strategy in this paper leverages a combination of short-term and long-term behavioral metrics to provide a comprehensive solution to detect blackhole attacks. By continually evaluating node performance, the Cluster Head can make informed decisions and take preventative actions, safeguarding the network from malicious activities and ensuring reliable packet transmission in WSNs (Liu, C et al., 2020).

The main goal of this research is to develop a robust and efficient multi-metric framework aimed at detecting malicious node activities, particularly blackhole attacks, in Wireless Sensor Networks (WSNs). The specific objectives are as follows:

- **Multi-Metric Evaluation Scheme**: To propose a method that uses multiple metrics such as Packet Forwarding Behavior (PFB), Acknowledgment Ratio (AR), Reputation Score (RS), Cooperation Ratio (CR), and Energy Deviation (ED) to continuously monitor and assess node performance.
- **Blackhole Attack Detection**: To identify and mitigate blackhole attacks by detecting nodes that fail to forward packets or drop them intentionally, preventing data loss and ensuring network integrity.
- **Anomaly Detection in Packet Forwarding**: To ensure the reliability of data transmission by integrating short-term and long-term behavioral data, identifying deviations from normal patterns, and detecting anomalies in node behavior.
- **Cooperation Verification**: To use the Cooperation Ratio (CR) for cross-verifying node interactions with neighbors, enabling the identification of unreliable or malicious nodes more comprehensively.
- **Energy Deviation Analysis**: To monitor node energy consumption using the Energy Deviation (ED) metric, helping to identify energy anomalies that may signal malicious actions like packet dropping or underperformance.
- **Network Security and Reliability**: To enhance the security and operational stability of WSNs by equipping the Cluster Head (CH) with a powerful mechanism to detect compromised nodes and prevent potential network failure.
- **Foundation for Future Enhancements**: To lay the groundwork for future developments, such as incorporating advanced machine learning techniques and collaborative intrusion detection systems, for detecting more sophisticated attacks in WSNs.

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

Through these objectives, the research aims to build a holistic framework to improve the security, reliability, and performance of WSNs by effectively identifying and addressing blackhole attacks in real time.

2. Background

2.1 Trust Management in WSN

In Wireless Sensor Networks (WSNs), where communication occurs over a shared medium, malicious nodes can exploit vulnerabilities to launch security attacks. The nodes in WSNs are typically constrained in terms of computational power, energy, memory, and bandwidth, making them particularly susceptible to such attacks, potentially rendering the network ineffective. Therefore, trust management is essential in WSNs to bolster security and ensure reliable network operation.

Trust plays a critical role in several network processes (Blaze, M et al., 1996). For instance, when routing, sensor nodes must identify which other nodes can be trusted to forward data. During the sensing process, nodes rely on neighboring nodes to validate measurements and detect anomalies. Trust also informs decisions related to data disclosure and key exchange, ensuring that only trusted nodes handle sensitive information. Trust management systems (TMS) offer lightweight solutions suitable for resource-constrained WSNs, ensuring improved network security without significantly affecting performance (Adnan, A et al., 2019). The concept of trust management was initially introduced by Blaze et al. in 1996 as a unified method for defining security policies and identifying trust relationships to facilitate secure authorization in distributed systems. Traditional authorization methods were insufficient in distributed environments, leading to the development of TMS to address these gaps by focusing on privileges and restrictions rather than individual identities (Niyato, D., et al., 2008).

In WSNs, nodes collaborate to provide network services such as data sensing and routing. Each node collects physical data and forwards it through other nodes toward a base station. Nodes can choose between prioritizing speed or conserving energy when transmitting data. Trust management is crucial in determining which nodes are most likely to perform specific tasks effectively and cooperatively (Rao, H et al., 2010). However, uncertainties arise from factors like data asymmetry (where a node lacks complete information about its peers) and opportunism (where nodes may pursue conflicting objectives). These uncertainties are exacerbated when some nodes are compromised or malfunctioning (Zhang, Z et al., 2019).

A Trust Management System helps mitigate uncertainty by using historical data to evaluate the trustworthiness of nodes. A node that has performed reliably in the past is likely to be trusted for similar tasks in the future. This enables nodes to coordinate with the most trustworthy peers, identifying faulty or malicious nodes and improving network reliability. Additionally, TMS can support other security mechanisms like privacy protection and key management by

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

enabling devices to exclude untrusted nodes from sensitive operations and secure key exchanges (Mahmoud, A. A et al., 2019).

2.2 The Impact of Blackhole Attacks in Wireless Sensor Networks (WSNs)

Wireless Sensor Networks (WSNs) are made up of distributed sensor nodes that collect and transmit environmental data to a central base station. These nodes often face limitations in terms of battery life, processing power, and memory. Deployed in environments like disaster zones, military fields, or healthcare settings, WSNs are susceptible to various security challenges. Among these, blackhole attacks stand out as particularly damaging (Akyildiz, I. F., et al., 2002). In a blackhole attack, a malicious node deceives neighboring nodes by claiming it has the shortest route to the base station. Once data is routed through it, the node drops the packets instead of forwarding them (Alcaraz, C et al., 2015). The effects of this attack include (Ding, Y et l., 2016, Khan, S. A et al., 2019, Kumar, A et al., 2018 and Nadir et al., 2018):

- **Data Loss**: When packets are dropped, the network suffers data loss, which disrupts critical real-time applications such as military surveillance and emergency monitoring.
- **Degraded Network Performance**: The attack hampers network performance by causing delays and requiring packet retransmissions, which drain energy and further strain the nodes' limited resources.
- **Compromised Network Integrity**: Blackhole nodes disrupt routing protocols, eroding trust in the network and making it harder for nodes to forward data reliably.
- **Increased Energy Consumption**: As affected nodes continue attempting transmissions, their energy resources are unnecessarily depleted, further reducing the lifespan of the network.
- **Cascading Failures**: If not detected early, the attack can escalate, leading to widespread network disruption as more nodes unknowingly forward data to the blackhole node.

Detecting and countering blackhole attacks is essential to ensure the security, efficiency, and longevity of WSNs.

2.3 K-Means Clustering in WSNs

The K-means clustering algorithm (Jain, A. K et al., 2010, Chaudhary, V et al., 2014, Xiao, Y et al., 2015 and Zhang, Y et al., 2016), a popular unsupervised learning method, can be effectively applied to WSNs for various purposes, including anomaly detection and efficient communication. The K means clustering algorithm has discussed in[]. The algorithm works by:

- **Initialization:** Choosing K initial centroids, representing cluster centers.
- **Assignment**: Assigning each node to the nearest centroid based on distance, typically using the Euclidean distance metric.

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

- **Update**: Recalculating the centroids based on the mean of nodes in each cluster.
- **Iteration**: Repeating the assignment and update steps until centroids stabilize.

In WSNs, K-means can be utilized to:

- **Optimize communication**: Nodes are clustered based on proximity or energy levels, reducing direct transmissions and saving energy.
- **Detect anomalies**: Nodes exhibiting abnormal behavior, like unusual energy consumption or packet forwarding patterns, can be grouped into separate clusters, helping to identify malicious nodes involved in attacks like blackhole activities.

By combining K-means clustering with metrics like Packet Forwarding Behavior (PFB) and Acknowledgment Ratio (AR), WSNs can enhance their defense against malicious attacks, improving overall network security and resilience.

3. Review of Literature

This section reviews various studies that address security challenges in Wireless Sensor Networks (WSNs), particularly in relation to trust, routing protocols, and security mechanisms. These studies explore diverse approaches to mitigating threats such as selective forwarding, eavesdropping, and malicious attacks within WSNs. Cao et al. (2021) developed an Identity-Based Encryption Algorithm (IIBE) to improve network security by simplifying the key generation process. Their solution reduces network traffic and overcomes several challenges associated with traditional encryption systems, including the management of public key certificates and key escrow issues. By eliminating the need for certificates, IIBE enhances efficiency while ensuring robust security.

Zhou et al. (2016) proposed a novel framework for WSNs consisting of three types of nodes: Cluster Heads (CHs), Inspector Nodes (INs), and Member Nodes (MNs). The INs monitor CH transmissions to prevent selective-forwarding attacks, while CHs relay packets from MNs and other CHs. This framework employs a reputation-based system to evaluate the behaviors of CHs and INs, calculating a composite reputation value (CRV) that accounts for forwarding rates, malicious node detection, and energy levels. The system not only improves security but also optimizes energy consumption, extending the network's operational lifetime. Haseeb et al. (2019) introduced the Energy-Aware and Secure Multi-Hop Routing (ESMR) protocol to improve both energy efficiency and multi-hop data security in WSNs. This protocol segments the network into inner and outer zones, creating clusters of nodes based on proximity. It enhances secure communication by using a secret-sharing mechanism to protect the data as it is transmitted between cluster heads and sink nodes. ESMR reduces vulnerabilities and ensures energy-efficient secure routing in multi-hop WSNs. Ourrouss et al. (2021) focused on combating malicious attacks through a bio-inspired trust management model, which integrates

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

the beta reputation system with Ant Colony Optimization (ACO). This model was applied to enhance the Dynamic Source Routing (DSR) protocol by identifying and isolating malicious nodes from the data forwarding process. The proposed system improves the robustness of the DSR protocol by ensuring that only trustworthy nodes participate in the routing process, thus preventing attacks like black hole and selective forwarding.

Majumder et al. (2023) proposed the CRYPTO-DSR protocol, a cryptography-based Dynamic Source Routing protocol designed to secure data transmission within WSNs. The protocol incorporates Johnson's algorithm for route computation and hash functions for secure packet transmission. By securing the data and routing path, CRYPTO-DSR strengthens the overall security of the WSN. This protocol also reduces the possibility of attacks targeting data integrity during transmission. Ali et al. (2020) introduced a data security method that utilizes a modified version of the Diffie-Hellman algorithm to reduce computational and response time while enhancing security. This method focuses on efficient generation of hash values for transmitted data, ensuring data integrity while improving processing efficiency. The approach is evaluated for its resilience to various attack vectors, ensuring that the protocol remains secure in a variety of scenarios. In WSNs, particularly in resource-constrained environments, implementing heavy security mechanisms like traditional cryptographic methods or blockchain can be challenging due to their high computational demands. These systems often require significant processing power, memory, and energy, which are not always available in WSN devices. Therefore, lightweight security solutions have gained significant attention. These solutions aim to balance security and resource efficiency, ensuring adequate protection against common security threats without overburdening the network's limited resources.

Research Gap

Although the aforementioned studies provide valuable insights into security challenges in WSNs, there are still several gaps that need to be addressed. One major gap is the need for security solutions that are both lightweight and capable of dealing with emerging security threats, such as black hole and selective forwarding attacks, without compromising network efficiency. Many existing solutions, while effective in specific scenarios, either focus on computationally expensive techniques or do not address the dynamic nature of WSNs effectively.Furthermore, while trust management models have been proposed, the integration of trust-based systems with routing protocols such as DSR, and their ability to adapt to dynamic changes in node behavior and network topology, remains underexplored. More research is needed to develop dynamic, scalable trust models that are lightweight and resource-efficient for WSNs, particularly for IoVT environments where vehicles continuously join and leave the network.

Lastly, there is a gap in exploring the integration of bio-inspired and machine learning-based methods with lightweight security protocols for real-time detection and mitigation of security

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

threats in WSNs. These approaches can potentially enhance the adaptability and accuracy of security mechanisms while ensuring minimal computational overhead, which is crucial for devices with limited resources.

In this context, the proposed research aims to fill these gaps by developing a lightweight, adaptive, and trust-based security model for WSNs and IoVTs, specifically focusing on the detection and mitigation of black hole attacks within the DSR routing protocol.

4. Proposed System

In a Wireless Sensor Network (WSN) designed to detect blackhole attacks, the following steps are assumed for initializing the network, along with the key assumptions for the described context.

4.1. Network Setup

- **Nodes:** The network consists of sensor nodes (N1, N2, N3, ..., Nn), deployed to monitor a specific area, collect data, and transmit it.
- **Cluster Formation:** The nodes are grouped into clusters, each managed by a Cluster Head (CH). The CH is responsible for overseeing the nodes within its cluster and aggregating their data.
- **Cluster Head (CH) Responsibilities**
  - Monitor the behavior of each node, including packet forwarding, acknowledgment, reputation score, cooperation with neighbors, and energy usage.
  - Detect abnormal behavior, such as potential blackhole attacks.

The Cluster Head (CH) assesses several metrics—Packet Forwarding Behavior (PFB), Acknowledgment Ratio (AR), Reputation Score (RS), Cooperation Ratio (CR), and Energy Deviation (ED)—for key purposes. First, this evaluation helps identify blackhole and other malicious nodes by tracking packet forwarding, acknowledgment, and energy usage trends. By analyzing these combined metrics, the CH can perform a thorough assessment of node behavior, distinguishing between temporary issues and consistent malicious activities. This approach enables the CH to create a trust profile for each node based on both historical and current behavior data, ensuring reliable data transmission throughout the network.

Additionally, monitoring multiple metrics minimizes the risk of false positives, resulting in more accurate decisions about node reliability. Tracking energy consumption helps identify abnormal patterns that may indicate packet dropping or malicious behavior. Finally, the CH checks node cooperation with neighbors using the Cooperation Ratio, which aids in identifying underperforming nodes. Overall, these evaluations help maintain the network's health by enabling early detection of issues and ensuring efficient, robust performance.

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

4.2 Packet Forwarding Behavior Calculation by Cluster Head

To assess the packet forwarding behavior of a node in a Wireless Sensor Network (WSN), particularly in the context of a potential blackhole attack, it is essential to evaluate the node's reliability in forwarding received packets over time. The objective is to determine whether the node consistently forwards packets or drops them, which may suggest malicious activity.

The Packet Forwarding Ratio (PFR) is calculated using the following formula:

$$Packet\ Forwarding\ Behaviour(PFR)_{CH}(t_i) = \frac{Packet_{forwarded}(t_i)}{Packet_{Received}(t_i)} \quad (1)$$

In the above equation,

$Packet_{forwarded}(t_i)$ be the number of packets forwarded by node i at time t

$Packet_{Received}(t_i)$ be the number of packets received by node i at time t.

The PFR can already take values between 0 and 1 if the number of packets forwarded is less than or equal to the number of packets received, assuming that the node forwards a portion of the packets it receives I,e $Packet_{forwarded}(t_i) \leq Packet_{Received}(t_i)$

We can define the Packet Forwarding Behavior (PFB) of a node iii as measured by the cluster head (CH) in a normalized way. The key points are:

- If the number of packets forwarded by a node is greater than or equal to the packets received, the behavior is capped at 1.
- If the node forwards no packets, the behavior is set to 0.
- If the node forwards half of the packets it receives, the behavior is 0.5.
- If no packets are received, the ratio is undefined, and we set the behavior to 0.

The Packet Forwarding Behavior (PFB) for node iii calculated by the cluster head (CH) is defined as

$$Packet\ Forwarding\ Behaviour_{CH}(t_i) = \begin{cases} 1, \text{if } Packet_{forwarded}(t_i) \geq Packet_{Received}(t_i) \\ 0, \text{if } Packet_{forwarded}(t_i) = 0 \text{ and } Packet_{Received}(t_i) > 0 \\ \frac{Packet_{forwarded}(t_i)}{Packet_{Received}(t_i)}, \text{if } 0 < Packet_{forwarded}(t_i) < Packet_{Received}(t_i) \\ 0, \text{if } Packet_{Received}(t_i) = 0 \end{cases} \quad (2)$$

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

If the number of packets forwarded is greater than or equal to the number of packets received i.e $\text{Packet}_{\text{forwarded}}(t_i) \leq \text{Packet}_{\text{Received}}(t_i)$ the PFR will be capped at 1**:**

If $\text{Packet Forwarding Behaviour}_{\text{CH}}(t_i) = 1$,the node is forwarding all the packets it receives.

$$\text{Packet Forwarding Behaviour}_{\text{CH}}(t_i) = \min\left(1, \frac{\text{Packet}_{\text{forwarded}}(t_i)}{\text{Packet}_{\text{Received}}(t_i)}\right) = 1$$

If no packets are forwarded by node i $\text{Packet}_{\text{forwarded}}(t_i)$=0, the Packet forwarding ratio becomes

$$\text{Packet Forwarding Behaviour}_{\text{CH}}(t_i) = \frac{0}{\text{Packet}_{\text{Received}}(t_i)} = 0$$

This means the node is not forwarding any packets.

Otherwise, the $\text{Packet Forwarding Behaviour}_{\text{CH}}(t_i) = 0.5$

If no packets are received by node I $\text{Packet}_{\text{Received}}(t_i)$=0 the ratio is undefined. In this case, a common approach is to set:

$$\text{Packet Forwarding Behaviour}_{\text{CH}}(t_i) = 0$$

By the way, a cluster head will calculate the Packet forwarding ratio of nodes which are in its control.

4.3 Acknowledgment-Based Monitoring Calculated by Cluster Head

The Acknowledgment Ratio (AR) measures the proportion of acknowledgment (ACK) packets received from a node in response to the data packets forwarded to it. When a cluster head (CH) monitors other nodes, especially in the presence of potential blackhole nodes, the AR becomes a key indicator of node reliability. Blackhole nodes usually drop packets and fail to send acknowledgments, resulting in a low AR for these nodes. Thus, a low AR can be a warning sign of malicious behavior, helping the CH identify unreliable or compromised nodes in the network.

The Acknowledgment Ratio (AR) for node i is:

$$Acknowledgment\ Ratio_{CH}(t_i) = \frac{Packet_{Acknowledgment}\ (t_i)}{Packet_{Sent}(t_i)}$$

(3)

The cluster head CH tracks the number of packets it sends to node i over time. This is denoted as$Packet_{Sent}(t_i)$.

The cluster head monitors how many ACK packets it receives from node iii in response to the packets sent. This is denoted as $Packet_{Acknowledgment}\ (t_i)$

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

The Acknowledgment Ratio (AR), like the previous metrics, already naturally lies between 0 and 1 because:

$$Packet_{Acknowledgment\ CH}(t_i)= \begin{cases} 1, \text{ if } Packet_{Acknowledgment}(t_i) \geq Packet_{Sent}(t_i) \\ \frac{Packet_{Acknowledgment}(t_i)}{Packet_{Sent}(t_i)}, \text{ if } 0 < Packet_{Acknowledgment}(t_i) < Packet_{Sent}(t_i) \\ 0, \text{ if } Packet_{Acknowledgment}(t_i) = 0 \text{ and } Packet_{Sent}(t_i) > 0 \\ 0, \text{ if } Packet_{Sent}(t_i) = 0 \end{cases} \quad (4)$$

If no acknowledgments are received,

$Packet_{Acknowledgment}(t_i) = 0$, Resulting in $Acknowledgment\ Ratio_{CH}(t_i) = 0$

If all packets sent are acknowledged,

$Packet_{Acknowledgment}(t_i) = Packet_{Sent}(t_i)$, Resulting in $Acknowledgment\ Ratio_{CH}(t_i) = 1$

If all packets sent are partially acknowledged,

$Packet_{Acknowledgment}(t_i) = 0$, Resulting in $Acknowledgment\ Ratio_{CH}(t_i) = 0.5$

4.4 Reputation Score (RS) by Cluster Head

To maintain and update a normalized reputation score for each node, the cluster head (CH) can apply a weighted formula that integrates the node's previous reputation score with its current behavior score. The current behavior score is derived from key metrics such as Packet Forwarding Behavior (PFB) and Acknowledgment Ratio (AR). This approach allows the CH to track changes in node behavior over time, ensuring that the reputation score reflects both historical performance and recent actions, providing a balanced and up-to-date assessment of node reliability.

$$\text{Reputation Score}_{CH(i+1)}(i) = \partial\ X\ \text{Reputation Score}_t(i) + \beta\ X\ \text{Current Behavior Score} \quad (5)$$

$\text{Reputation Score}_t(i)$ is the reputation score at time t, ∂ and β are weighting factors, and the current behavior score is based on metrics like packet forwarding and acknowledgment ratios. Behavior denotes, If a node's score steadily decreases over time, it indicates a history of malicious or unreliable behavior. To maintain and update a normalized reputation score for each node, the cluster head (CH) can use a weighted formula that combines the node's previous reputation score with its current behavior score, which is based on metrics such as Packet Forwarding Behavior (PFB) and Acknowledgment Ratio (AR).

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

$$\text{Current Behavior Score}_{CH(i+1)}(i) = w_1 . Packet_{Acknowledgment\ CH}(t_i) + w_2 . Packet\ Forwarding\ Behaviour_{CH}(t_i) \quad (6)$$

This formula (6) can be substituted in the above formula (5).

4.5 Cross-Verification with Neighboring Nodes by Cluster Head

To cross-verify the historical behavior of a node in a Wireless Sensor Network (WSN), the cluster head (CH) can assess the node's activity by comparing it with the behavior of neighboring nodes. This evaluation is based on the Cooperation Ratio (CR), which measures how consistently a node cooperates with its neighbors. By analyzing the CR, the CH can identify discrepancies in node behavior, detect signs of malicious activity, and ensure that each node is functioning as expected in relation to the broader network. This cross-verification process helps improve network reliability and security.

$$\Delta\text{Cooperation Ratio}_{CH}(t_i) = \text{Cooperation Ratio}_{neighbours}(\boldsymbol{t})\text{-}\ \text{Cooperation Ratio}_{neighbours}(\boldsymbol{ti}) \quad (7)$$

$\Delta\text{Cooperation Ratio}_{CH}(t_i)$is large, node i may be underperforming or behaving maliciously compared to its neighbors.

The Cooperation Ratio (CR) formula is:

$$\text{Cooperation Ratio}_{CH}(\boldsymbol{t_i}) = \frac{\boldsymbol{SC(t_i)}}{\boldsymbol{TC(t_i)}} \quad (8)$$

Where $0 \leq \text{Cooperation Ratio}_{CH}(t_i) \leq 1$ and deviations from the average neighbor CR can help the cluster head identify abnormal behavior.

$SC(t_i)$ refers to successful interactions or data transmissions that node i has completed with its neighbors (such as successful packet forwarding or acknowledgment exchanges).

$TC(t_i)$refers to the total number of interaction opportunities or data transmissions involving node i (both successful and failed).

4.6 Energy Calculation by Cluster Head

To identify potential blackhole attacks in a Wireless Sensor Network (WSN) through energy consumption analysis, the cluster head (CH) can utilize the Energy Deviation (ED) metric. This metric evaluates a node's actual energy usage against the expected consumption for normal packet forwarding activities. If a node exhibits significantly lower energy usage than anticipated, it may indicate packet dropping, suggesting malicious behavior such as a blackhole attack. By monitoring ED, the CH can effectively detect nodes that deviate from typical energy patterns, helping to safeguard the network against such threats.

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

$$\text{Energy Deviation}_{CH}(t_i) = 1 - \frac{\text{Actual Energy}(t_i)}{\text{Expected Energy}(t_i)} \quad (9)$$

$\text{Expected Energy}(t_i)$, the theoretical amount of energy that node i should consume is based on the number of packets it is expected to forward. This can be calculated by considering the total number of packets forwarded and the energy cost per packet.

$\text{Actual Energy}(t_i)$ This refers to the real amount of energy consumed by node i. If the node forwards fewer packets than expected, its actual energy consumption will be lower than the theoretical value. $\text{Expected Energy}(t_i)$ This refers to the real amount of energy consumed by node i. If the node forwards fewer packets than expected, its actual energy consumption will be lower than the theoretical value. This formula enables the cluster head to detect potential blackhole nodes by monitoring nodes that show unusually low energy consumption relative to their expected forwarding responsibilities. If a node consumes less energy than expected, it may be engaging in packet-dropping behavior, which is often associated with blackhole attacks.

This formula allows the cluster head to detect potential blackhole nodes by identifying those with unusually low energy consumption compared to their expected packet-forwarding responsibilities. When a node consumes less energy than anticipated, it may be involved in packet-dropping behavior, which is commonly linked to blackhole attacks. The following figure 2 shows the architecture of proposed model.

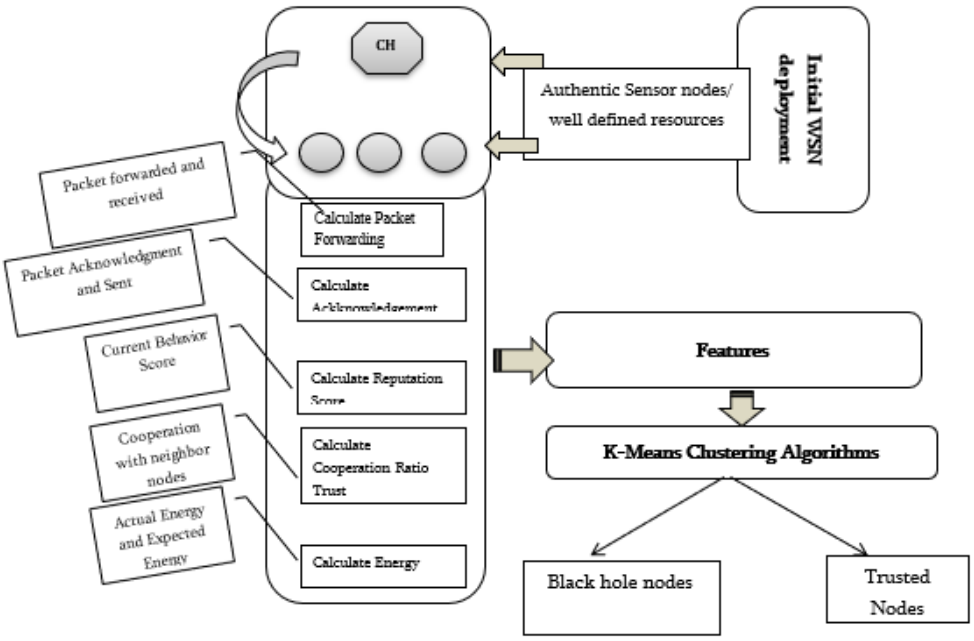

Figure 2. Architecture Diagram of the Proposed Model

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

The following algorithm depicts the calculation of various metrics by cluster head.

Algorithm1: Evaluation of Various Metrics by Cluster Head

```
Function evaluateNode(node):
    # Step 1: Calculate Packet Forwarding Behavior (PFB)
    PFB = calculatePacketForwardingBehavior(node)
    # Step 2: Calculate Acknowledgment Ratio (AR)
    AR = calculateAcknowledgmentRatio(node)
    # Step 3: Update Reputation Score (RS)
    RS = updateReputationScore(node, PFB, AR)
    # Step 4: Calculate Cooperation Ratio (CR)
    CR = calculateCooperationRatio(node)
    # Step 5: Calculate Energy Deviation (ED)
    ED = calculateEnergyDeviation(node)
    # Step 6: Store or return the metrics for the node
    Return (PFB, AR, RS, CR, ED)
End Function
Function calculatePacketForwardingBehavior(node):
    If node.Packets_Received(t) == 0:
        Return 0  # Undefined, set to 0
    Else If node.Packets_Forwarded(t) >= node.Packets_Received(t):
        Return 1  # Capped at 1
    Else If node.Packets_Forwarded(t) == 0:
        Return 0  # No packets forwarded
    Else:
        Return node.Packets_Forwarded(t) / node.Packets_Received(t)
End Function
Function calculateAcknowledgmentRatio(node):
```

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

```
    If node.Packets_Sent(t) == 0:
        Return 0  # Undefined, set to 0
    Else If node.Packets_Acknowledgment(t) >= node.Packets_Sent(t):
        Return 1  # All packets sent acknowledged
    Else If node.Packets_Acknowledgment(t) == 0:
        Return 0  # No acknowledgments received
    Else:
        Return node.Packets_Acknowledgment(t) / node.Packets_Sent(t)
End Function
Function updateReputationScore(node, PFB, AR):
    previousRS = node.ReputationScore(t)  # Previous reputation score
    currentBehaviorScore = (w1 * AR) + (w2 * PFB)  # Current behavior score
    newRS = alpha * previousRS + beta * currentBehaviorScore  # Update formula
    node.ReputationScore(t + 1) = newRS  # Update the reputation score for next time
    Return newRS
End Function
Function calculateCooperationRatio(node):
    successfulInteractions = node.Successful_Interactions(t)
    totalInteractions = node.Total_Interactions(t)
    If totalInteractions == 0:
        Return 0  # No interactions, set to 0
    Return successfulInteractions / totalInteractions
End Function

Function calculateEnergyDeviation(node):
    ActualEnergy = node.ActualEnergy(t)
```

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

```
    ExpectedEnergy = calculateExpectedEnergy(node) # Calculate based
on expected forwarding
    If ExpectedEnergy == 0:
        Return 0  # Avoid division by zero
    Return 1 - (ActualEnergy / ExpectedEnergy)  # Normalize the energy deviation
End Function
Function calculateExpectedEnergy(node):
    # This function calculates the expected energy based on packets expected to forward
    packetsForwarded = node.Packets_Forwarded(t)
    energyCostPerPacket = node.EnergyCostPerPacket
    Return packetsForwarded * energyCostPerPacket  # Expected energy calculation
End Function
# Main loop for cluster head to monitor nodes
For each node in cluster:
    (PFB, AR, RS, CR, ED) = evaluateNode(node)
    logNodeMetrics(node, PFB, AR, RS, CR, ED)  # Log the metrics for each node
End For
```

5. Identification of Black hole Attacks using K-Means Clustering Algorithms

To identify blackhole attacks in a Wireless Sensor Network (WSN) using the K-Means Clustering Algorithm, we can utilize several proposed metrics as features: Packet Forwarding Behavior (PFB), Acknowledgment Ratio (AR), Reputation Score (RS), Cooperation Ratio (CR), and Energy Deviation (ED). These metrics enable the cluster head (CH) to distinguish between benign and malicious (blackhole) nodes by grouping the nodes according to their behavioral patterns. Below is a detailed explanation, accompanied by an example.

Algorithm2: Identification of Blackhole Nodes

Step 1. INPUT:

- Node data with 5 features for each node: (PFB, AR, RS, CR, ED)
- Number of clusters k = 2 (for Normal Nodes and Blackhole Nodes)

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

- Maximum iterations (MAX_ITER)
- Convergence threshold (THRESHOLD)

Step 2. INITIALIZATION:

- Randomly select two nodes as initial centroids for Cluster 1 and Cluster 2:
  - Centroid_1 = (PFB_C1, AR_C1, RS_C1, CR_C1, ED_C1)
  - Centroid_2 = (PFB_C2, AR_C2, RS_C2, CR_C2, ED_C2)

The formula you mentioned is the Euclidean distance between two points in a 5-dimensional space. In this case, the two points represent:

Node i with its feature values: $\mathrm{PFB}_i, \mathrm{AR}_i, \mathrm{RS}_i, CR, \mathrm{ED}_i$

Centroid 1 with its feature values $\mathrm{PFB}_{c1}, \mathrm{AR}_{c1}, \mathrm{RS}_{c1}, CR_{c1}, \mathrm{ED}_{c1}$

Step 3. REPEAT until convergence or until MAX_ITER is reached:

- For each node i (where i = 1 to N for N nodes):
  - Calculate the Euclidean distance between node i and each centroid:

Node i with its feature values: $\mathrm{PFB}_i, \mathrm{AR}_i, \mathrm{RS}_i, CR, \mathrm{ED}_i$

Centroid 1 with its feature values $\mathrm{PFB}_{c1}, \mathrm{AR}_{c1}, \mathrm{RS}_{c1}, CR_{c1}, \mathrm{ED}_{c1}$

The Euclidean distance formula between these two points is given by:

$$Distance_1 = \sqrt{(PFB_i - PFB_{c1})^2 + (AR_i - AR_{c1})^2 (RS_i - RS_{c1})^2 (CR_i - CR_{c1})^2 (ED_i - ED_{c1})^2}$$

The formula for Distance_2 follows the same structure as the one for Distance_1, but with respect to Centroid 2 (C2). Here's the Euclidean distance formula for Distance_2:

$$Distance_1 = \sqrt{(PFB_i - PFB_{c2})^2 + (AR_i - AR_{c2})^2 (RS_i - RS_{c2})^2 (CR_i - CR_{c2})^2 (ED_i - ED_{c2})^2}$$

  - Assign node i to the closest cluster based on the minimum distance:
    - If Distance_1 < Distance_2, assign node i to Cluster 1 (Normal Nodes)
    - Else assign node i to Cluster 2 (Suspicious Nodes)
- After all nodes are assigned to clusters:
  - For each cluster (Cluster 1 and Cluster 2):
    - Recalculate the centroid by taking the mean of all nodes assigned to that cluster:

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

- Centroid_1 = (mean_PFB_Cluster1, mean_AR_Cluster1, mean_RS_Cluster1, mean_CR_Cluster1, mean_ED_Cluster1)

- Centroid_2 = (mean_PFB_Cluster2, mean_AR_Cluster2, mean_RS_Cluster2, mean_CR_Cluster2, mean_ED_Cluster2)

- Check for convergence:

- If the centroids' positions have not changed significantly (i.e., the change in position is less than THRESHOLD for both centroids), STOP.

- If the centroids have changed, repeat the process.

Step 4. OUTPUT:

- Final cluster assignments: Nodes in Cluster 1 are considered normal nodes, and nodes in Cluster 2 are considered suspicious (potential blackhole attackers).

6. Proof of Concept a Mathematical Example

Let's extend the example to 20 nodes with randomly assigned normalized feature values for Packet Forwarding Behavior (PFB), Acknowledgment Ratio (AR), Reputation Score (RS), Cooperation Ratio (CR), and Energy Deviation (ED). Here's a table 1 showing the features of 20 nodes.

Table 1. Sample Dataset with 20 features

ID	PFB	AR	RS	CR	ED
N1	0.9	0.88	0.85	0.92	0.1
N2	0.3	0.25	0.35	0.4	0.75
N3	0.85	0.87	0.88	0.9	0.08
N4	0.4	0.45	0.5	0.55	0.65
N5	0.78	0.8	0.82	0.84	0.12
N6	0.25	0.2	0.3	0.22	0.78
N7	0.95	0.92	0.9	0.94	0.05
N8	0.2	0.18	0.25	0.15	0.85
N9	0.87	0.89	0.9	0.88	0.07
N10	0.35	0.3	0.4	0.45	0.7
N11	0.82	0.85	0.87	0.88	0.1
N12	0.5	0.55	0.6	0.58	0.6
N13	0.18	0.15	0.2	0.25	0.88
N14	0.89	0.92	0.9	0.91	0.09

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

N15	0.27	0.22	0.3	0.2	0.8
N16	0.75	0.78	0.82	0.8	0.13
N17	0.92	0.94	0.91	0.93	0.06
N18	0.15	0.1	0.2	0.18	0.9
N19	0.8	0.82	0.85	0.83	0.12
N20	0.38	0.35	0.4	0.45	0.68

Step 1: Initialize Cluster Centroids

- Let's randomly select two initial centroids from the dataset:
  - Centroid 1: Node N1 = (0.90, 0.88, 0.85, 0.92, 0.10)
  - Centroid 2: Node N8 = (0.20, 0.18, 0.25, 0.15, 0.85)

Step 2: Compute Distances

We calculate the Euclidean distance between each node and the two centroids. Using the formula:

$$d(x_i - c_{k)}=\sqrt{(PFB_i - PFB_k)^2 + (AR_i - AR_k)^2(RS_i - RS_k)^2(CR_i - CR_k)^2(ED_i - ED_k)^2}$$

We can compute the distance between Node N3 and Centroid 1 as:

$$d(x_i - c_{k)}=\sqrt{(PFB_i - PFB_k)^2 + (AR_i - AR_k)^2(RS_i - RS_k)^2(CR_i - CR_k)^2(ED_i - ED_k)^2}$$

We can compute the distance between Node N3 and Centroid 1 as:

$$d(N_3 - c_{1)}=\sqrt{(0.85 - 0.90)^2 + (0.87 - 0.88)^2 + (0.88 - 0.85)^2 + (0.90 - 0.92)^2 + (0.08 - 0.10)^2}$$

$$= \sqrt{0.0025 + 0.0001 + 0.0009 + 0.0004 + 0.0004}$$

$$=\sqrt{0.0043}$$

=0.0655

Similarly, calculate the distance to Centroid 2.

Step 3: Assign Nodes to Clusters

Based on the computed distances, assign each node to the nearest centroid. Let's assign the nodes to the clusters as follows:

- Cluster 1 (Normal Nodes): N1, N3, N5, N7, N9, N11, N14, N16, N17, N19
- Cluster 2 (Suspicious Nodes): N2, N4, N6, N8, N10, N12, N13, N15, N18, N20

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

Step 4: Recomputed Centroids

Recalculate the centroids by averaging the feature values of the nodes in each cluster.

For Cluster 1**,** the new centroid would be the average of the feature vectors of all nodes in the cluster:

$$C1=\frac{1}{10}\left((0.90,088,0.85,0.92,0.10)+\cdots+(0.80,0.82,0.85,0.83,0.12)\right)$$

For Cluster 2, similarly average the nodes assigned to that cluster.

Step 5: Repeat Until Convergence

Repeat the distance calculation and reassignment of nodes until the cluster centroids stabilize, and the cluster memberships no longer change.

Final Cluster Assignments

- Cluster 1 (Normal Nodes): N1, N3, N5, N7, N9, N11, N14, N16, N17, N19.
  - These nodes have high PFB, AR, RS, and CR, with low ED.
- Cluster 2 (Suspicious Nodes): N2, N4, N6, N8, N10, N12, N13, N15, N18, N20.
  - These nodes exhibit lower PFB, AR, RS, and CR, with higher ED, indicating potential blackhole activity.

7. Trust Update Mechanism

- Use a trust update model where nodes' behavior is continuously evaluated over time. Trust scores are updated based on the observations of the node's forwarding behavior.
  - Trust Decay: Trust should decay over time if no recent interactions are recorded, allowing the network to quickly adapt to new conditions.
  - Trust Update Equation:

$$T_{t+1}(i)=(1-\gamma)X\ (T_i(i)+\gamma+New\ Classification\ of\ nodes$$

where γ is the trust decay factor, $T_i(i)$ is the trust score at time t, and New Trust Evidence is the score based on the latest interactions (e.g., forwarding ratios, acknowledgment).

8. Simulation Results and Discussion

To assess the performance of the proposed model in comparison to the traditional DSR routing protocol and the protocols presented by Virendra Dani et al. (2022) and N. Dharini et al. (2020), a detailed simulation was carried out using the NS3 Simulator tool. The evaluation focused on key performance metrics under varying conditions. In the simulation setup, a maximum of 100 nodes was involved, and blackhole nodes were introduced progressively, starting from 10% and increasing up to 80% over the simulation period. The parameters for the simulation are

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

outlined in Table 4.The traffic type was set to Constant Bit Rate (CBR), ensuring a steady flow of data, while the Nakagami propagation model was used to simulate realistic wireless communication conditions. Nodes moved according to the Random Waypoint mobility model, representing random movement patterns within the network. The medium access control (MAC) layer followed the 802.11 standard, and the communication took place over wireless channels. The data payload size for each packet was 512 bytes, and the simulation area covered 1000m x 1000m. The nodes' speed varied across several values: 5, 10, 15, 20, and 25 meters per second, and the data rate for transmission was set at 10.4 Mbps. These configurations allowed for a comprehensive analysis of the model's performance under different network conditions and attack scenarios.

Packet Dropping Ratio Analysis in the Presence of Black hole Attacks

Figure 3 depicts the effect of Black hole attacks on the packet drop rate in a Wireless Sensor Network (WSN). The graph clearly shows a direct relationship between the number of Black hole nodes and the packet drop rate, where an increasing number of attacks results in a corresponding rise in dropped packets. This pattern remains consistent over time, illustrating how Black hole attacks degrade network performance. The traditional DSR protocol, which lacks mechanisms to identify and defend against these attacks, is particularly vulnerable. As a result, the absence of security features in DSR contributes to the increased packet loss when Black hole nodes are present. This emphasizes the importance of incorporating advanced security strategies within WSNs to address these attacks. With proper detection and defense techniques, networks can minimize the impact of Black hole nodes, ensuring better performance and stability.

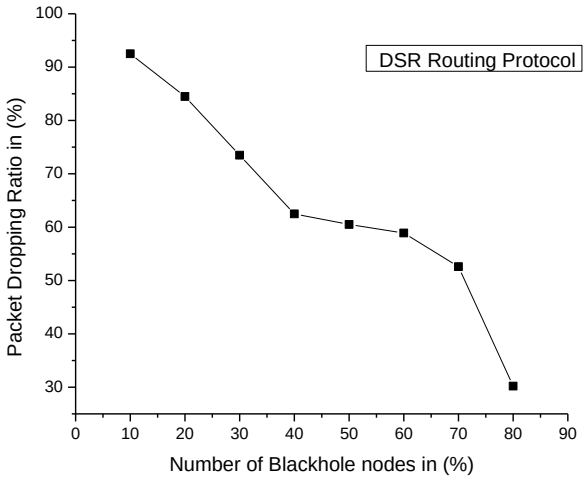

Figure 3. Influence of Black hole Attackers under Normal DSR Routing Protocol

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

Packet Delivery Ratio Analysis vs Black hole Attackers

Figure 4 presents a detailed analysis of how the packet delivery ratio (PDR) in a Wireless Sensor Network (WSN) is affected by the presence of Black hole attacks. In this study, we systematically increased the number of Black hole nodes at regular intervals to observe the corresponding changes in PDR. The results are telling: our proposed model consistently achieves a higher PDR compared to the traditional Dynamic Source Routing (DSR) protocol and the models introduced by Dharini et al. (2020) and Virendra et al. (2022). Even as the proportion of Black hole attackers escalates, our model maintains a significantly superior PDR, demonstrating its robustness against such malicious activities. This enhanced performance underscores the effectiveness of our approach in mitigating the adverse effects of Black hole attacks on packet delivery within WSNs. The key to our model's success lies in its integration of advanced detection and mitigation techniques. Specifically, we employ a multi-trust evaluation mechanism that considers a variety of Quality of Service (QoS) metrics: Packet Forwarding Behavior (PFB), Acknowledgment Ratio (AR), Reputation Score (RS), Cooperation Ratio (CR), and Energy Deviation (ED). By analyzing these metrics collectively, our model gains a comprehensive understanding of each node's behavior and trustworthiness.

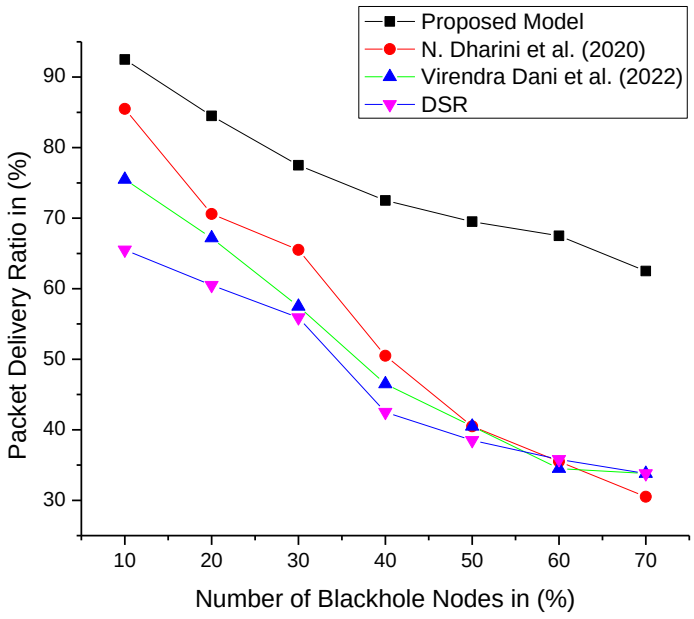

Figure 4. Packet Delivery Ratio Vs. No.of Blackhole Nodes

To further refine the detection process, we utilize the K-means clustering algorithm. This unsupervised machine learning technique groups nodes based on the evaluated QoS metrics, effectively distinguishing between normal and malicious behavior. As a result, Black hole nodes are identified and isolated more efficiently, which significantly reduces their impact on

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

the network's PDR. In contrast, the model proposed by Dharini et al. (2020) relies on a narrower set of metrics—packet count, energy levels, and Z-score calculations—to assess node trustworthiness. While this approach does offer some level of protection, it lacks the depth provided by our multi-metric evaluation, leading to a lower PDR than our model but still higher than that of the traditional DSR protocol and the model by Virendra et al. (2022).

Virendra et al.'s (2022) model focuses on Node Energy, Node Buffer Length, and Packet Drop metrics. This limited scope results in a weaker detection mechanism for Black hole attacks. The minimal set of parameters fails to capture the nuanced behaviors of malicious nodes fully, leading to a lower PDR compared to both our model and Dharini et al.'s approach. The traditional DSR protocol, devoid of any built-in security features, performs the worst among all, with a significantly reduced PDR as the number of Black hole attackers increases. Our model's incorporation of multiple QoS metrics and the K-means clustering algorithm facilitates a more nuanced and accurate evaluation of each node's reliability. For instance, PFB assesses how consistently a node forwards packets, while AR measures the ratio of acknowledgments received, indicating responsiveness. RS aggregates historical interactions to provide an overall trust score, CR evaluates the willingness of nodes to cooperate within the network, and ED monitors deviations in energy consumption that could signify malicious activity.

By analyzing these diverse metrics, our model can detect subtle anomalies in node behavior that single-metric models might overlook. The use of K-means clustering enhances this capability by grouping nodes with similar behaviors, making it easier to identify outliers indicative of Black hole attacks. This comprehensive approach not only improves the detection rate of malicious nodes but also minimizes false positives, ensuring that legitimate nodes are not wrongly penalized. The superior performance of our model, as evidenced by the consistently higher PDR in Figure 4, highlights the importance of a multifaceted security strategy in WSNs. Black hole attacks pose a significant threat to network integrity by selectively dropping packets, which can severely disrupt communication and data transmission. By effectively identifying and isolating these malicious nodes, our model safeguards the network's performance and reliability.

End to End Delay Analysis vs Black hole Attackers

The proposed model achieves significantly lower end-to-end delay compared to the models by Dharini et al. (2020) and Virendra et al. (2022) due to its advanced detection and mitigation techniques for Black hole attacks in Wireless Sensor Networks (WSNs). By employing a multi-trust evaluation mechanism using diverse Quality of Service (QoS) metrics—such as Packet Forwarding Behavior (PFB), Acknowledgment Ratio (AR), Reputation Score (RS), Cooperation Ratio (CR), and Energy Deviation (ED)—the proposed model quickly identifies malicious nodes, reducing packet loss and minimizing the need for retransmissions and route rediscoveries. In contrast, Dharini et al.’s model, which relies on simpler metrics like packet

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

count, energy levels, and Z-score, and Virendra et al.'s model, which uses Node Energy, Node Buffer Length, and Packet Drop, both have limited detection capabilities. This results in slower responses to Black hole attacks, leading to more packet loss, increased route rediscovery, and ultimately higher end-to-end delays. Moreover, the proposed model integrates the K-means clustering algorithm, which further enhances its ability to classify and isolate malicious nodes efficiently, a feature absent in both Dharini et al.'s and Virendra et al.'s models. The result is a more stable and efficient network, with the proposed model maintaining optimal routing and packet delivery performance even as the proportion of Black hole nodes increases, whereas the other two models experience higher delays due to their less comprehensive detection and mitigation strategies. The figure 4 depicts the end to end delay.

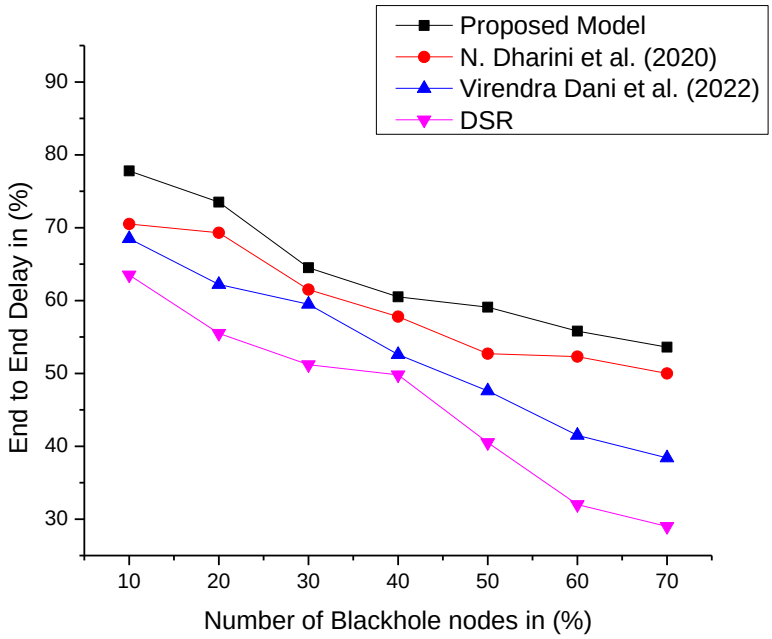

Figure 5. End to End Delay vs % Black hole Attackers

Routing Overhead vs Black hole Attackers

The routing overhead which is shown in figure 6 is significantly lower in the proposed model compared to the traditional DSR protocol and the models by Dharini et al. (2020) and Virendra et al. (2022) due to its more efficient detection, mitigation, and routing mechanisms in handling Black hole attacks in Wireless Sensor Networks (WSNs). One of the key factors contributing to reduced routing overhead is the proposed model's ability to quickly and accurately detect malicious nodes using a multi-trust evaluation system that incorporates metrics such as Packet Forwarding Behavior (PFB), Acknowledgment Ratio (AR), Reputation Score (RS), Cooperation Ratio (CR), and Energy Deviation (ED). These comprehensive metrics allow the

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

model to preemptively identify Black hole nodes, which minimizes the need for frequent route rediscoveries or adjustments. In contrast, models like those of Dharini et al. and Virendra et al. rely on fewer or more basic metrics, leading to slower detection of malicious activity and more reactive responses, which result in higher routing overhead due to increased route repairs and rediscoveries.

Additionally, the incorporation of the K-means clustering algorithm in the proposed model enhances its ability to classify nodes based on behavior patterns, allowing for proactive route adjustments that avoid compromised nodes. This clustering approach reduces the need for repetitive route maintenance or updates, which traditionally contribute to routing overhead. In contrast, the lack of such advanced clustering in the other models results in less efficient route management, further increasing overhead. By maintaining stable and secure routes, the proposed model reduces the amount of control messages required for route discovery and maintenance. Since Black hole nodes are isolated more efficiently, there are fewer instances where packets are dropped or routes fail, leading to a lower frequency of route rediscovery processes, which would otherwise contribute to higher routing overhead. As a result, the overall communication efficiency is enhanced, keeping the routing overhead minimal while maintaining optimal network performance.

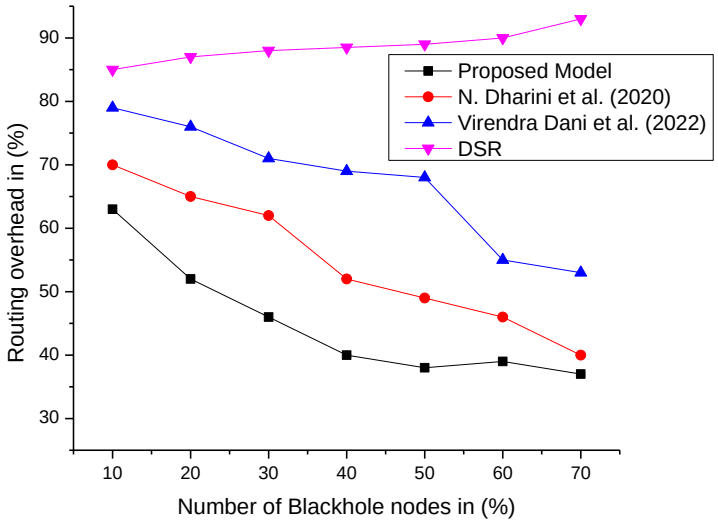

Figure 6. Routing Overhead vs % of Black hole Attackers

Detection Accuracy vs Black hole Attackers

The detection accuracy which is shown in the figure 7 in the proposed model is notably high due to its multi-faceted approach to evaluating node behavior and identifying Black hole

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

attacks in Wireless Sensor Networks (WSNs). The model employs a comprehensive multi-trust evaluation mechanism that incorporates several Quality of Service (QoS) metrics—such as Packet Forwarding Behavior (PFB), Acknowledgment Ratio (AR), Reputation Score (RS), Cooperation Ratio (CR), and Energy Deviation (ED)—to assess the reliability and trustworthiness of nodes. This wide range of metrics allows the model to detect subtle deviations in node behavior that might indicate malicious activity, leading to more accurate identification of Black hole nodes. Unlike models by Dharini et al. (2020) and Virendra et al. (2022), which rely on fewer or less comprehensive parameters like packet count, energy levels, Node Buffer Length, and Packet Drop, the proposed model's broader set of metrics provides a holistic view of node activity. By analyzing multiple aspects of node behavior, such as how well nodes forward packets (PFB), their acknowledgment patterns (AR), historical reputation (RS), willingness to cooperate (CR), and energy consumption anomalies (ED), the proposed model can more effectively distinguish between normal network variations and actual malicious behavior. This comprehensive analysis reduces false positives and false negatives, contributing to higher detection accuracy.

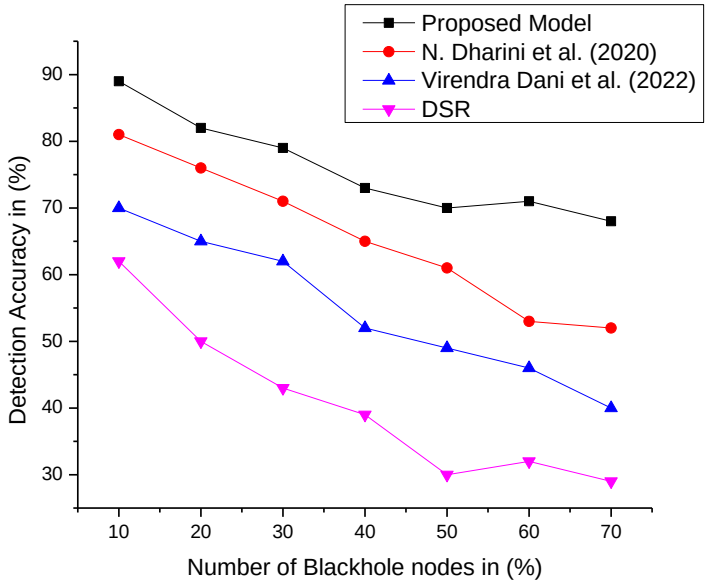

Figure 7. Detection Accuracy Vs. Number of Blackhole Nodes

Moreover, the proposed model's use of the K-means clustering algorithm significantly enhances its detection accuracy. K-means clustering allows the model to group nodes based on behavioral patterns derived from the QoS metrics. This machine learning technique helps the system classify nodes more accurately by identifying clusters of nodes that exhibit similar behaviors, making it easier to pinpoint outliers—those nodes behaving abnormally due to Black hole attacks. The clustering approach increases the precision of detecting malicious nodes

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

while reducing the likelihood of misclassifying legitimate nodes as malicious. In summary, the high detection accuracy of the proposed model stems from its multi-metric evaluation system and the application of K-means clustering, which together provide a detailed and precise understanding of node behavior. This multifaceted approach allows for the early and accurate identification of Black hole nodes, ensuring better network protection and fewer disruptions from undetected attacks.

9. Conclusion

In conclusion, securing communication in Wireless Sensor Networks (WSNs) against threats such as blackhole attacks is crucial for preserving the integrity and functionality of the network. This paper presents a robust system in which the Cluster Head (CH) actively monitors and evaluates node behavior through a set of critical metrics: Packet Forwarding Behavior (PFB), Acknowledgment Ratio (AR), Reputation Score (RS), Cooperation Ratio (CR), and Energy Deviation (ED). These metrics work collectively to identify abnormal activities, particularly those related to packet dropping that signify blackhole attacks.The employment of the K-means clustering algorithm allows for effective classification of nodes into two distinct groups—normal and suspicious—based on their behavior. By iteratively adjusting cluster centroids using Euclidean distance, the algorithm ensures accurate differentiation between benign and potentially malicious nodes. The mathematical proof provided demonstrates the applicability and validity of the proposed model, and the simulation results further highlight its superior performance compared to existing models.Overall, this approach enhances the security and resilience of WSNs by enabling timely detection and response to blackhole attacks, thereby ensuring more reliable communication and improved network performance. The findings underscore the effectiveness of using a multi-metric evaluation scheme in conjunction with clustering algorithms to bolster network security against evolving threats.

Future Enhancement

Future improvements could focus on expanding the node evaluation framework to include machine learning algorithms for predictive analysis, enabling more precise identification of emerging threats. Additionally, the implementation of real-time adaptive thresholds for metrics, based on the dynamics of the network, could further enhance detection efficiency. Expanding the system to facilitate cross-cluster cooperation and trust propagation would improve security across the network, allowing for distributed detection of malicious nodes in the WSN. Finally, incorporating energy-efficient strategies to optimize CH performance without sacrificing security could enhance the overall longevity and performance of the network. The rapid evolution of mobile computing and wireless networking technologies has led to a significant rise in the number of mobile users globally. This trend is central to the deployment of modern mobile ad-hoc networks and the provision of reliable communication services to users. However, ensuring dependable service is challenging due to limited resources

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

and complex network topologies. Trust protocols for mobile ad-hoc networks have emerged as a vital area of research in recent years, facilitating community-based mobile applications. Given the absence of central coordination and the shared nature of the wireless medium, achieving reliable communication in ad-hoc wireless networks is considerably more complex than in wired networks.

References

1. Adnan, A., & Yasin, M. (2019). Trust Management in Wireless Sensor Networks: A Survey. *IEEE Access*, 7, 75469-75489.
2. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. *IEEE Communications Magazine*, 40(8), 102-114.
3. Alcaraz, C., & Zeadally, S. (2015). Security in Wireless Sensor Networks: A Survey. *IEEE Communications Surveys & Tutorials*, 17(2), 903-925.
4. Ali, Shahwar, et al. "An efficient cryptographic technique using modified Diffie–Hellman in wireless sensor networks." *International journal of distributed sensor networks* 16.6 (2020): 1550147720925772.
5. Alzubaidi, L., & Zaidan, A. A. (2018). A survey of Wireless Sensor Networks security. *Journal of Network and Computer Applications*, 112, 22-37.
6. Blaze, M., Bleumer, E., & Strauss, M. (1996). The Role of Trust in Distributed Systems. *Proceedings of the 1996 IEEE Computer Society Workshop on Future Trends of Distributed Computing Systems*, 4-9.
7. Chaudhary, V., & Singh, S. (2014). Application of K-Means Clustering Algorithm in Wireless Sensor Networks. *International Journal of Computer Applications*, 98(13), 25-30.
8. Dharini, N., & Sharmila, M. (2020). Detection of Blackhole Attack in Wireless Sensor Networks using Trust Management. *International Journal of Computer Applications*, 975, 8887.
9. Ding, Y., & Liao, X. (2016). Research on Blackhole Attack in Wireless Sensor Networks. *International Journal of Computer Applications*, 139(9), 8-12.
10. Haseeb, Khalid, et al. "Secret sharing-based energy-aware and multi-hop routing protocol for WSN based WSNs." IEEE Access 7 (2019): 79980-79988.
11. Jain, A. K. (2010). Data clustering: 50 years beyond K-means. *Pattern Recognition Letters*, 31(8), 651-666.
12. Khan, S. A., & Iqbal, M. (2019). Impact of Blackhole Attack on Wireless Sensor Network. *International Journal of Engineering and Advanced Technology*, 8(5), 225-230.
13. Kumar, A., & Kumar, A. (2018). Mitigation Techniques for Blackhole Attack in Wireless Sensor Network: A Review. *Wireless Networks*, 24(7), 2337-2354.

Power System Technology
ISSN:1000-3673
Received: 06-02-2025 Revised: 15-03-2025 Accepted: 30-04-2025

14. Liu, C., & Yang, Y. (2020). A Trust-Based Approach to Secure Routing in Wireless Sensor Networks. *Future Generation Computer Systems*, 108, 885-895.
15. Mahmoud, A. A., & Hossain, M. S. (2019). A Novel Trust Management System for Wireless Sensor Networks. *International Journal of Information Security*, 18(3), 321-333.
16. Majumder, Sayan, Debika Bhattacharyya, and Subhalaxmi Chakraborty. "Mitigation of Sybil Attack in Mobile Ad Hoc Network Using CRYPTO-DSR: A Novel Routing Protocol." *International Journal of Intelligent Systems and Applications in Engineering* 11.4 (2023): 281-288.
17. Nadir, M. R., & Khan, A. (2018). A Comprehensive Review of Black Hole Attack in Wireless Sensor Network. *International Journal of Computer Applications*, 182(15), 18-25.
18. Niyato, D., & Hossain, E. (2008). Trust Management for Wireless Sensor Networks: A Survey. *Wireless Communications and Mobile Computing*, 8(9), 1153-1163.
19. Ourouss, Kaoutar, Najib Naja, and Abdellah Jamali. "Defending against smart grayhole attack within MANETs: A reputation-based ant colony optimization approach for secure route discovery in DSR protocol." *Wireless Personal Communications* 116 (2021): 207-226.
20. Rao, H., & Yang, C. (2010). A Trust-Based Framework for Data Gathering in Wireless Sensor Networks. *IEEE Transactions on Vehicular Technology*, 59(5), 2560-2570.
21. Virendra, D., & Saha, S. (2022). Enhanced Trust-Based Secure Routing for Wireless Sensor Networks. *IEEE Access*, 10, 20012-20027.
22. Xiao, Y., & Wang, W. (2015). K-means Clustering Algorithm and its Application in Wireless Sensor Networks. *Journal of Network and Computer Applications*, 57, 80-92.
23. Yoon, J., & Kim, H. (2021). Security and Performance Analysis of Wireless Sensor Networks against Blackhole Attacks. *Sensors*, 21(10), 3370.
24. Zhang, H., Wang, Y., & Xie, H. (2019). A Multi-Metric Evaluation Scheme for Secure Routing in Wireless Sensor Networks. *Ad Hoc Networks*, 85, 94-104.
25. Zhang, Y., & Wu, Q. (2016). A novel K-means clustering algorithm for wireless sensor networks. *International Journal of Distributed Sensor Networks*, 12(7), 1-12.
26. Zhang, Z., Wang, H., & Zhang, H. (2019). Trust-Based Security Protocols for Wireless Sensor Networks: A Survey. *IEEE Communications Surveys & Tutorials*, 21(4), 3565-3588.
27. Zhou, Hai, et al. "A security mechanism for cluster-based WSN against selective forwarding." Sensors 16.9 (2016): 1537.