Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 4s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Sinkhole and Black Hole Attack Detection Using Dynamic Reliability Based Anomaly Architecture for Sensor Networks

Mrs. J. Gnana Mano Sheebha[1], Dr. D. Maheswari[2]

[1] Research Scholar, RVS College of Arts and Science(Autonomous),Sulur, Bharathiar University, Coimbatore,Tamil Nadu, India

Email ID: sheebhabovas@gmail.com

[2] Head & Research Coordinator School of Computer Studies-PG RVS College of Arts and Science (Autonomous), Sulur, Bharathiar University, Tamil Nadu, India

Email ID: maheswari@rvsgroup.com

Cite this paper as: Mrs. J. Gnana Mano Sheebha, Dr. D. Maheswari, (2025) Sinkhole and Black Hole Attack Detection Using Dynamic Reliability Based Anomaly Architecture for Sensor Networks. *Journal of Neonatal Surgery*, 14 (4s), 23-37.

ABSTRACT

In this paper wireless sensor networks endure disruption of communication functions and attacks on network integrity stemming from sinkhole and black hole threats. Active attack scenarios allow malicious nodes to damage network performance and lose data packet information by directing packets incorrectly and discarding them. Traditional security technology fails to stop attacks because it cannot match the evolving speed of large network spaces. We use a Dynamic Reliability based Anomaly Architecture (DRA) which assesses network node trustworthiness through network behavior analysis and characteristic interaction evaluations. Through constant reliability scoring adjustments the system detects sinkhole effectors and blocks black hole network intrusions. Combination of real-time tracking of node activities with dynamic network situation evaluation forms the basis of this security-enhanced network protection strategy. Latest research proves networks implementing dynamic reliability mechanisms successfully protect against sinkhole and black hole attacks by keeping the proportion of false positives to a minimum thus improving security detection performance. This architecture creates a scalable solution to effectively extend protection throughout wireless sensor networks for multiple future applications. The upgraded system produces higher performance compared to conventional methods through enhanced precision and better adaptability while reducing power consumption.

Keywords: *Dynamic reliability, Black hole attack, Network integrity, sink hole attack, Security.*

1. INTRODUCTION

Decentralized structures in conjunction with limited power in sensor networks increase exposure to a range of security threats. Sinkhole attacks cause significant issues to Wireless Sensor Networks as malicious actors produce false routes that compromise data integrity and network operation of sink nodes which can ultimately trigger network failure [1-3]. Dependable communication solutions with strong routing mechanisms create extreme network damage for IoT systems through sinkhole attacks.

To address these attacks researchers proposed reliability-based systems that operate through network node trust assessments to locate and prevent harmful actions [6-8]. By analyzing unusual data forwarding behavior network operators working with these models argue effectively detect sinkhole attacks in reliability-based security systems. Scientific studies report that adoption of these security strategies results in substantially improved detection accuracy and reinforced network security [11-13]. The analysis of multiple studies demonstrated fortified Wireless Sensor Network protection capabilities against sinkhole threats when using repeatedly assessed dynamic trust-based reputation systems [14], [15].

Researchers have shown strong interest in implementing Machine Learning (ML) technology with dynamic algorithms to produce better reputation-based control systems while increasing detection ability according to [16], [17]. Security solutions in standard network models become more difficult to implement effectively across dynamic topology environments of MANETs [18] and IoT during active system changes involving network structure modifications [19], [20]. The adoption of hybrid reliability models which integrate several trust indicators combines direct observations with indirect recommendations to yield marked enhancements in attack detection abilities as demonstrated by literature [21] and [22].

Recent work suggests that sinkhole attack mitigation could be improved by including reliability systems in routing protocols which enable traffic rerouting and compromised node isolation [23], [24]. The described methods help WSN networks preserve their complete operational capabilities when subjected to attacks. Growing utilization of WSN technology in critical services like healthcare [25] demands development of reliable reliability mechanisms that protect against sinkhole attacks and comparable security threats [26], [27]. Secure operations of WSNs and IoT networks depend fundamentally on reliability-based intrusion detection and mitigation methods. Dynamic and hybrid models remain the key areas of study necessary to combat increasing security threats from sinkhole attacks [28].

Contribution: The research paper presents a Dynamic Reliability Architecture method to identify and defend against sinkhole and black hole attacks within WSN. Through real-time evaluations of network node reliabilitys this framework detects malicious nodes that attempt to disrupt communication so it can isolate them. This approach combines real-time monitoring with trust evaluation systems that together improve network security and dependability while working to eliminate false positive results.

Motivation: The frequency of sinkhole and black hole attacks represents a major danger to the operational efficiency and reliability of sensor networks. Standard detection methods lack flexibility when faced with changing network environments. Through this paper we select to close current research gaps by delivering a powerful dynamic and scalable security tactic against targeted sensor network attacks.

Organization: In this paper the related works are discussed in section 2 and materials and methods are used in section 3. The results are discussed in section 4 and finally, the conclusions are discussed in section 5.

2. RELATED WORKS

De Meo et al. [29] created a reputation system that enables safe resource sharing within IoT environments. This research showed that trust and reputation metrics were vital for achieving communication efficiency between IoT devices which needed to collaborate. These authors designed a reputation-based system which used trust structures to locate and remove malicious nodes from network resource distribution systems. Device behaviors were monitored by the framework which assigned reputation scores to maintain operational security. Through malicious behavior mitigation it successfully boosted IoT system reliability. Scalability issues in large-scale IoT deployments prevented successful framework application.

The adaptive framework for wireless sensor network protection develops through reputation-based methods according to Gupta & Verma [30]. The framework demonstrated how trust management becomes fundamental for threat detection and mitigation within environments characterized by dynamic network conditions. The method presented by the authors calculated node reputation scores on the fly to detect compromised nodes and remove them from system operation. The system adjusted its operations according to network condition variations to preserve secure communications. The framework demonstrated strong resistance capabilities against multiple attack vectors. Reputation score computations generated additional processing requirements which created computational overhead within the system.

In their analysis Kaushik, I. and Sharma [31] investigated black hole attacks within wireless sensor networks where packets are dropped to disrupt communication operations. The research presented countermeasures designed to detect active threats while simultaneously preventing damage from such attacks. Both researchers implemented detection systems along with monitoring approaches to spot unusual packet-dropping patterns in network nodes. These authors proposed precise strategies to protect network systems against these types of security attacks. The new techniques enhanced network defences through advanced detection of black hole attacks. Network monitoring processes became more complex because of the implemented detection mechanisms.

Kim, J., & Park [32] developed an adaptive trust management system which aims to secure IoT sensor networks by improving their reliability in changing operational conditions. The research explored solutions to handle malicious behaviors from network nodes. Through dynamic trust evaluations based on both sensor behaviors and contextual information the technique managed trust scores which helped identify and remove malicious activities. This system accomplished instantaneous trust evaluation to improve network stability. The computing requirements rose in response to the continually changing trust management system.

Malik & Kumar [33] conducted detailed research on how both smart blackhole and grayhole attacks disrupt vehicular ad hoc networks (VANETs) through targeted packet deletions. The study authors presented a solution to both detect these attacks and suggest ways to prevent their harmful impact. Researchers used dynamic time warping to understand communication patterns while identifying abusive nodes in their network. The system defended against attacks through isolation of exposed nodes. Research exhibited that the newly developed detection method resulted in better recognition of harmful activities within vehicular ad hoc networks. The performance experienced negative ramifications from using substantial computational equipment.

Mantas et al. in study [34] investigated how reputation frameworks support opportunistic network operations by encouraging mutual cooperation between network participants. The work outlined the difficulties related to building trust systems that

work within constantly changing decentralized systems. The analysis examined several reputation-based approaches including credit-based systems and evaluations of trust scores which foster collaborative behavior while reducing selfish actions. An examination presented complete methods which drive teamwork in opportunistic network settings. The survey examined several collaborative frameworks yet it failed to support them with experimental validation.

Nayak & Singh [35] presented adaptive clustering driven by reputation metrics to protect sensor networks from intrusions. The objective of the proposed system was network security improvement through the detection and separation of harmful network nodes.

Through clustering processes driven by reputation scores the system effectively optimized its intrusion detection mechanism within defined clusters. The system delivered higher detection rates of intrusions while decreasing the number of false alerts. The new clustering method required extra computing power during its operation.

Wireless sensor network security was evaluated through analysis of security challenges and mitigation strategies alongside their expected future trends by Oztoprak et al. [36]. Their findings showed current system weaknesses specifically to blackhole attacks while pointing out threats from energy depletion attacks and eavesdropping behaviors. The authors examined multiple security approaches like cryptographic procedures together with trust regulation and machine learning implementations to tackle presented challenges. The study covered both today's security policies and what researchers expect from sensor networks security work in the future. The review did not present specific experimental tests of the proposed security strategies in sensor networks.

Patel & Patel [37] introduced an adaptive trust management system targeted at heterogeneous sensor networks that aims to enhance both network security and reliability. The approach evaluated trust levels dynamically to monitor node actions and their interactions.

The research introduced a trust scoring approach which used combined direct and indirect observations to detect malicious network nodes thereby optimizing network performance. The system design achieved a reduction in network disruption from malicious activities. Computing trust values in the network generated higher communication burdens.

Table 1: comparison table of various authors works

References	Concept	Methods Used	Advantage	Disadvantage
Pawar, M. V. [38]	Focused on detecting and preventing black-hole and wormhole attacks in wireless sensor networks.	Used optimized LSTM for anomaly detection by analyzing traffic patterns in the network.	High accuracy in detecting malicious activities.	High computational cost due to LSTM model.
Ramesh, S., & Yaashuwanth, C. [39]	Proposed a trust-based decision-making approach for secured wireless streaming in video sensor networks.	Implemented a trust-based framework for secure streaming, evaluating trust levels of nodes.	Improved reliability in video streaming.	Retracted due to concerns about methodology and results.
Shanmugaraja, P., et al. [40]	Addressed sinkhole attack detection in wireless sensor networks with an efficient clustered algorithm.	Developed the MSAD algorithm to detect sinkhole attacks using multi-path routing and clustering.	Improved detection rates and minimized energy consumption.	May face challenges in scalability for large-scale networks.
Singh, G., & Kaur, R. [41]	Designed a hybrid intrusion detection system (IDS) to mitigate sinkhole attacks in 6LoWPAN networks.	Combined anomaly detection and signature-based methods for attack detection.	High detection rate for sinkhole attacks.	Limited effectiveness against other types of attacks.

Singh, M., & Roy, R. [42]	Proposed a reputation and trust-based adaptive security framework for IoT sensor networks.	Integrated trust and reputation mechanisms to secure communication and identify malicious nodes.	Enhanced network security and reliability.	Computational overhead due to continuous trust evaluation.
Wu, J., & Zhang, K. [43]	Focused on secure localization in sensor networks using a distributed reputation-based approach.	Used reputation scores to detect and exclude malicious nodes during localization.	Improved localization accuracy in the presence of malicious nodes.	Increased communication overhead in the network.
Yang, Z., & Liu, H. [44]	Developed a trust and reputation-based security framework for wireless sensor networks.	Combined direct and indirect trust evaluations to detect malicious activities.	Enhanced security by isolating compromised nodes.	Computational cost increased due to reputation management.

2.1 Problem identification

Sinkhole and black hole attacks threaten WSNs reliability because they reroute or eliminate data packets while inducing network failures and persistent data losses. Current detection techniques show limited flexibility when working with dynamic network setups and face excessive false positive rates which hamper their performance in practical deployments.

2.2 Proposed solution

This study presents a dynamic network node assessment framework which uses a dynamic reliability system to evaluate trustworthiness through behavioral monitoring. By evaluating reputation scores network systems detect malicious nodes which enables isolation processes which defend against sinkhole and black hole attacks. Security enhancement and false positive reduction characterize this solution code that learns and adapts to network condition changes.

3. MATERIALS AND METHODS

Researchers executed a Dynamic Reliability based Anomaly Architecture to detect sink hole and black hole attacks inside WSN. The full detection approach for sink hole and black hole events appears in Figure 1. To detect sinkhole and black hole attacks in real time, network nodes use the Dynamic Reliability based Anomaly Architecture approach, which monitors interactions, generates dynamic reputation measurements, detects network irregularities, and accounts for environmental changes. To minimize harmful nodes and ensure consistent data transmission functions, the network design uses security measures in combination with energy-efficient devices. As the security system design evolves, the techniques for sending data from sensor networks become more efficient.

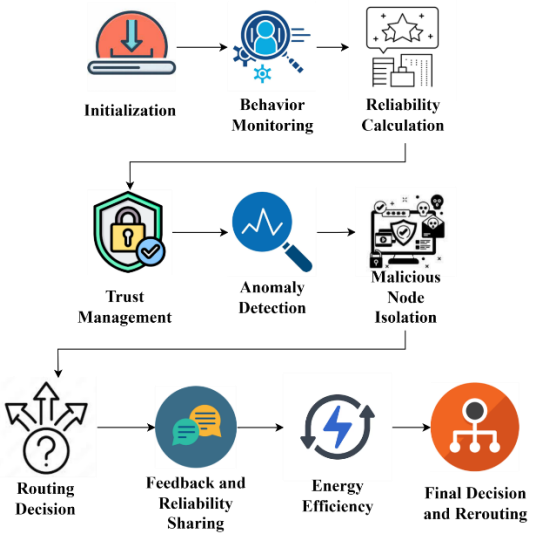

Figure 1: Overall Architecture of Sink hole and Black hole detection

3.1 Dynamic Reliability based Anomaly Architecture for Sensor Networks

Operating with limited resources, Wireless Sensor Networks (WSNs) are prone to security breaches as a result of the proliferation of new attack routes. The Dynamic Reliability based Anomaly Architecture (DRA) modifies node reputations based on network behavior, revealing network vulnerabilities via automated detection methods. The network defense model continuously reviews node reputation using both direct and indirect trust assessments. Quality trust assessment is vitally dependent on obtaining real-time activity data from neighbouring nodes for node action analysis and metric calculation. To prevent black hole and sinkhole attacks, the security architecture uses reliability algorithms that detect and remove hostile nodes from the network.

Sink hole Attack:

A sinkhole network attack occurs when a rogue node intercepts all incoming and outgoing wireless sensor connections using incorrect routing data. Data packet destruction and alteration compromise network data streams when controlled by a hostile node. When attackers lose control of the network's routing, they may cause data loss, poor network performance, and communication delays.

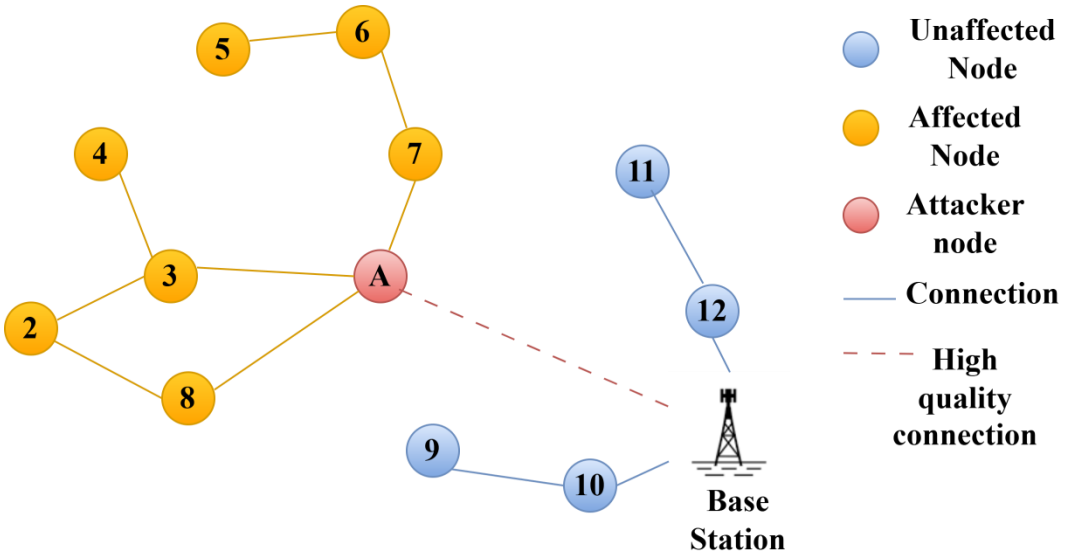

Figure 2: Sink hole Attack

Black hole Attack:

Malicious attackers executing a blackhole attack compromise the integrity of WSNs by falsely presenting themselves as the best forwarders and surreptitiously discarding all inbound packets. When purposeful network attacks disrupt the connectivity between sensor nodes, all data is permanently destroyed. Black hole attackers stop data packets rather than reroute them.

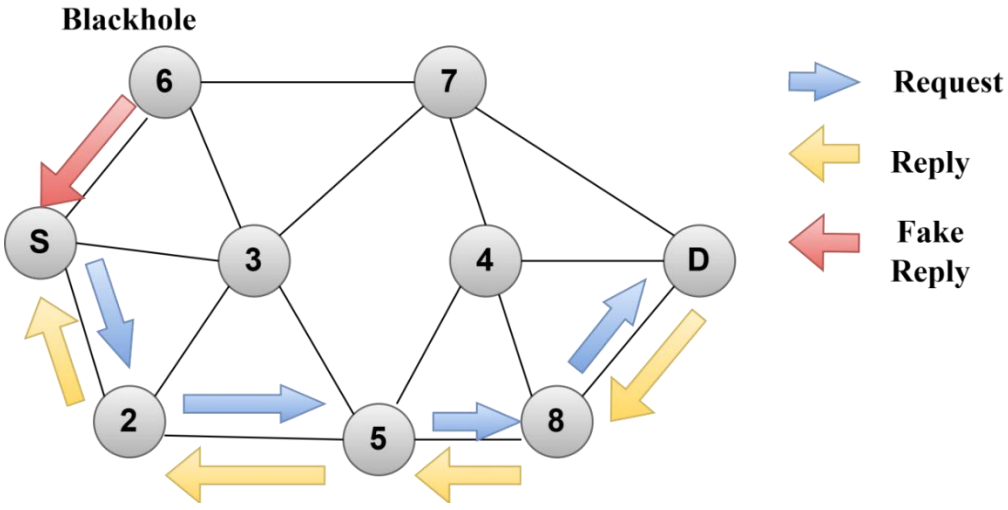

Figure 3: Black hole Attack

Key Features of the Proposed Solution:

- Direct trust inputs result from node neighbor interactions as indirect trust develops through observation of network-wide node patterns during reputational assessment. The trustworthiness of a node is quantified through a separate reliability score that works with its recorded reliability measures.
- The update procedure for node reliability scores executes after each new action is carried out by network systems. Network systems lower trust values for any nodes that show abnormal patterns by either losing excessive packets or participating in selective packet forwarding. The system preserves network safety through swift malfunctioning node detection and isolation which uses dynamic update methods.
- Network operators use a reliability score threshold to establish node trustworthiness between safe and harmful nodes. Whenever network systems detect a node with reliability under the designated threshold they first label it as malicious and then cut off its operation permissions. Network operators use their detection system to rapidly identify and remove network nodes conducting sinkhole or black hole attacks.
- Our implementation expands network size dynamically and adapts to changes in network conditions without limitations. The dynamic networking framework maintains operational efficiency in dynamic sensor networks by continuously updating reliability calculations through the network's lifetime.
- The proposed system operates efficiently with minimal computational load through protected reliability calculation methodologies because sensor nodes have limited processing capabilities. The deployment of our system becomes feasible for environments with limited resources through active trust evaluation that involves negligible resource requirements.
- The network uses continuous verification of node behavior alongside the regulation of reliability scores for achieving real-time protection from sinkhole and black hole attacks. Attack-involved nodes exhibit poor packet delivery outcomes which results in reduced reliability scores allowing simple detection through this relationship.

Nodes track behavioral patterns of their adjacent neighbors by analyzing packet forwarding success rates along with their energy consumption behavior while considering packet drops. The trust values between nodes depend fundamentally on the monitoring process.

Direct trust for node i towards node j is determined by evaluating how well node j forwards packets received from node i. If node j consistently forwards packets correctly, its direct trust score increases; otherwise, it decreases. The direct trust $T_i(j)$ is calculated as:

$$T_i(j) = \frac{S_i(j)}{N_i(j)} \text{ --------- (1)}$$

Where, $S_i(j)$ is the number of successful packets delivered by node $N_i(j)$ is the total number of packets sent from node i to node j. To compute direct trust between nodes Equation 1 uses packet forwarding success as its basis. This framework operates on the assumption that each node demonstrates trustworthiness through successful packet forwarding ability. This measurement works well against sinkhole attacks since these malicious nodes attempt to redirect traffic through independently which results in decreased packet delivery reliability and lower trust scores. Black hole attackers function by terminating all packet data so their trust value $T_i(j)$ remains minimal.

Indirect trust is based on the reliability of neighboring nodes that have interacted with node j. If neighboring nodes report positive interactions with node j, the indirect trust score for node j will increase. Indirect trust $T_{i,j}^{d}$ is calculated by aggregating the trust scores from neighboring nodes:

$$T_{i,j}^{d} = \sum_{k \epsilon N(i)} T_k(j) \times \alpha_k \text{---------- (2)}$$

Where, $N(i)$ is the set of neighbors of node i, $T_k(j)$ is the reliability score of node k regarding node j, α_k is the weight given to node k's reliability based on its trustworthiness. Equation (2) aggregates the indirect trust from node i's neighbors $N(i)$. If node i has several neighbors with good reliabilitys for node j, the indirect trust will be higher. In sinkhole attacks malicious nodes pretend to be reliable to collect traffic before they begin to drop packets. Analysis of indirect trust measurements helps spot malicious nodes through recognition of their inconsistent actions.

The initial behavior of sinkhole nodes will become detectable since these nodes present themselves as reliable before disrupting network communication functionality. The overall reliability score $R_i(j)$ for node j as seen by node i is a weighted combination of both the direct and indirect trust values:

$$R_i(j) = \beta \times T_i(j) + (1 - \beta) \times T_{i,j}^{d} \text{ --------- (3)}$$

Where, β is a weighting factor that determines how much importance is given to direct trust compared to indirect trust. Typically, β is set between 0 and 1 based on the network's requirements. A typical formulation exists which integrates both direct trust evaluations and indirect trust assessments to calculate reliability scores. The five weight given to indirect

reliability value plays an important part when direct trust founders because trustworthy neighbors make indirect trust more dependable. When nodes engage in a black hole attack the result is their trust being substantially decreased both through direct observation by the node along with feedback from other network nodes. Sinkhole attackers will face capture once their routing actions don't match their established reliability scores.

Once the reliability score $R_i(j)$ is computed, it is compared against a predefined threshold value R_{th}. If $R_i(j)$ falls below this threshold, node j is flagged as potentially malicious. The threshold R_{th} is typically set as a value representing the lower bound of acceptable behavior:

$$R_{th} = \frac{1}{2} \times Max\ Reputation\ score \text{ ---------- (4)}$$

Network conditions enable operators to modify this dynamic threshold value. Because equation (4) implements reliability filtering through a designated threshold malicious nodes become detectable. Threshold for reliability R_{th} is a practical approach to identify malicious nodes. Network security defines suspicious nodes which become evident when their reliability score drops below this threshold level. Binary classification methods find it accurate to measure reliability with the criterion of half the maximum possible score. During evaluations of sinkhole and black hole attack behavior this mechanism is designed to pinpoint nodes possessing insufficient reliabilitys. Nodes dropping packets (black hole) or guiding others to route through itself (sinkhole) will suffer a fall in reliability beneath the threshold which makes detection straightforward.

Once a reliability-based detection finds nodes have scores below acceptable limits it labels them malicious and enforces network isolation straight away. Systems block malicious nodes by keeping them off routing tables and disable their packet sending abilities. When a sinkhole attacks takes place harmful device channels incoming internet traffic back to its own system. Our system detects and stops damaged data flow by removing malfunctioning nodes with low reliability scores. When compromised by a black hole attack malicious nodes receive incoming messages then delete them instead of forwarding. The system finds failed packet forwarding through repeated reliability score reductions and takes rapid action to block the node.

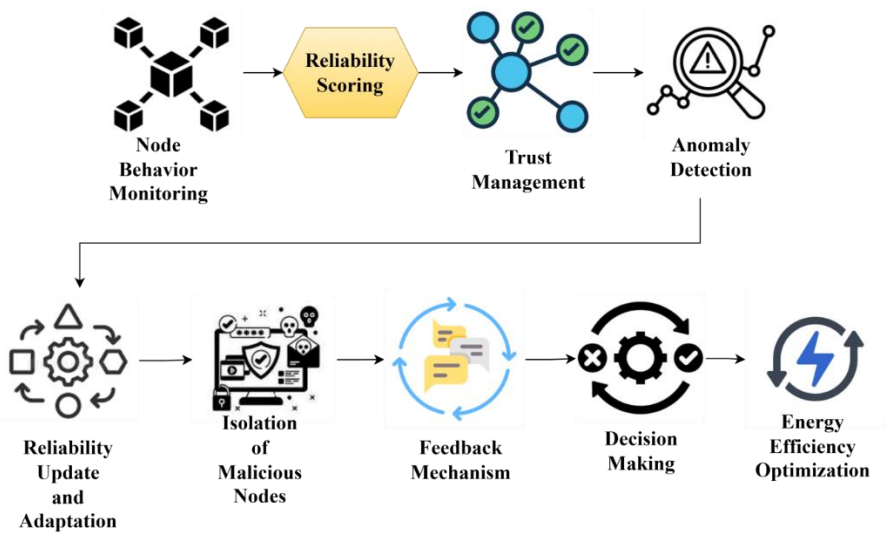

Figure 4: Dynamic Reliability-based Architecture

Our system connects blockchain features with sensor network reputation tracking in a single architecture displayed in Figure 4. The top row illustrates core concepts: Our security system combines blockchain processing with reliability evaluations and reliability scoring plus includes detection of abnormal activities. The bottom row highlights key functionalities: Our system design implements attack defense and harmful node isolation plus combines data transmission security measures with power efficiency support. This network development pairs better security systems with trust-building among devices to make better use of wireless sensor resources.

In this research DRA provides scalable security protection against sinkhole and black hole attacks in WSNs. By measuring network nodes through performance reliability data we create a responsive structure that finds security threats faster. For real-world operational tasks WSNs deliver secure operations when they use accurate systems that perform well across various tasks without burdening computing resources.

Algorithm 1: Dynamic Reliability-based Architecture

Step 1: Initialization

Initialize the **value** $R_i = 1$for every node i in the network.

Define key parameters:

i) **Reliability threshold** $R_{th} = 0.5$ (below which a node is marked malicious).

ii) **Weight factor** $\beta = 0.6$ (balances direct trust and indirect trust contributions).

Step 2: Monitor Node Behavior

For each node i in the network:

For every neighbor node j of i, record:

i) $S_i(j)$: Number of **successfully forwarded packets** from node i to j.

ii) $N_i(j)$ Total **packets sent** from node i to j.

Step 3: Calculate Direct Trust

Compute the **direct trust** $T_i(j)$ for each neighbor j of node i

$$T_i(j) = \frac{S_i(j)}{N_i(j)}$$

Step 4: Calculate Indirect Trust

For each neighbor node j, compute the **indirect trust** $T_{i,j}^d$ based on feedback from other neighbors k of i:

$$T_{i,j}^d = \sum_{k \epsilon N(i)} T_k(j) \times \alpha_k$$

Step 5: Aggregate Trust Values

Combine **direct trust** and **indirect trust** to calculate the **overall reliability** $R_i(j)$ for each neighbor j:

$$R_i(j) = \beta \times T_i(j) + (1 - \beta) \times T_{i,j}^d$$

Step 6: Detect Malicious Nodes

Compare the aggregated reliability $R_i(j)$ with the reliability threshold R_{th}. If $R_i(j) < R_{th}$, mark node j as **malicious** (potential Sinkhole or Black Hole attacker). Isolate the malicious node j by:

i) Removing j from the routing table.

ii) Blocking j from participating in further communication.

Step 7: Update Reliability Periodically

Periodically update the reliability of all nodes based on their behavior:

i) Recalculate direct and indirect trust at regular intervals.

ii) Adjust reliability dynamically to adapt to changing network conditions.

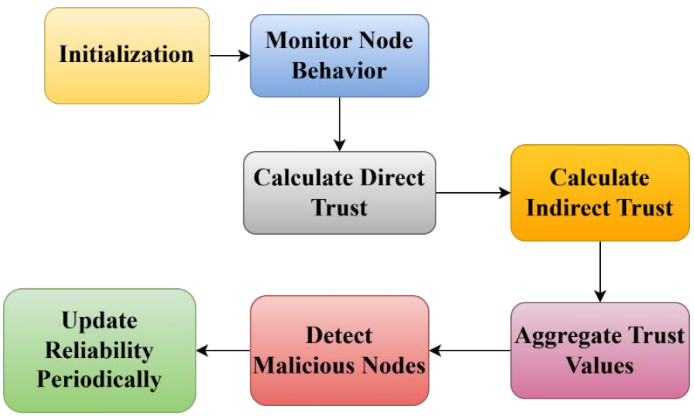

Figure 5: Flow diagram of Dynamic Reliability-based Architecture

The working steps for the DRA appear in algorithm 1 together with figure 5. Each network node starts with basic reliability level of $R_{th} = 1$as the system sets reliability limit at $R_{th} = 0.5$. If a node's reliability falls under 0.5 the system marks it as a harmful participant. Measuring how well packets move through each network point helps us determine direct trust when monitoring interactions. Network neighbors deliver ratings that the system uses to work out each node's trust level. The total reliability score of each network node results from putting many trust ratings together. Our network defense plan targets attackers who manipulate data traffic as sinkhole or black hole nodes. Regular updates to reliability ratings help the system address evolving network risks.

4. RESULTS AND DISCUSSIONS

The Dynamic Reliability-based Architecture identifies and prevents Black Hole and Sinkhole attacks, which protect Wireless Sensor Networks (WSNs). The approach achieves excellent detection accuracy by assessing trust levels directly and indirectly using simulation results. Regular upgrades to reliability systems assist to reduce the inaccuracy of recognizing innocent nodes and allow for accurate identification of potentially harmful nodes. This technology outperforms previous systems in terms of performance and energy efficiency, reducing consumption and delivering more packets quicker. Some operational delays may occur during indirect trust calculations in a dense network; however, optimization efforts may assist to eliminate these delays. This approach increases the safety and overall performance of wireless sensor networks.

4.1 performance Metrics

4.1.1 Network Throughput

The amount of successfully sent data over the network during a specified period reveals data transmission efficiency measurements. As disruptions caused by attacks decrease network throughput improves.

$$Throughput = \frac{Data\ Transmitted\ (in\ bits)}{Time\ (in\ seconds)} \text{ ---------- (7)}$$

Table 2: Throughput comparison table

	Throughput (kbps)			
Number of Nodes	**Watchdog Mechanism (WdM) [46]**	**Ad hoc On-Demand Distance Vector (AODV) [47]**	**Trust-Based Energy-Efficient Algorithm (TBEEA) [48]**	**Dynamic Reliability based Anomaly Architecture (DRA) (Proposed)**
10	200	180	220	250
20	180	165	210	240
30	160	150	200	230
40	145	135	185	220
50	130	120	170	210
60	110	100	155	200

Throughput values displayed in the table 2 represent various algorithms as nodes increase throughout the network. When node counts raise all underlying system mechanisms display decreased throughput performance due to growing network traffic congestion alongside resource throttling effects. In every testing situation DRA surpassed TBEEA and AODV which both recorded reduced throughputs. The DRA algorithm provides superior performance likely because its dynamic structure works together with its reliability system to efficiently manage changing network situations.

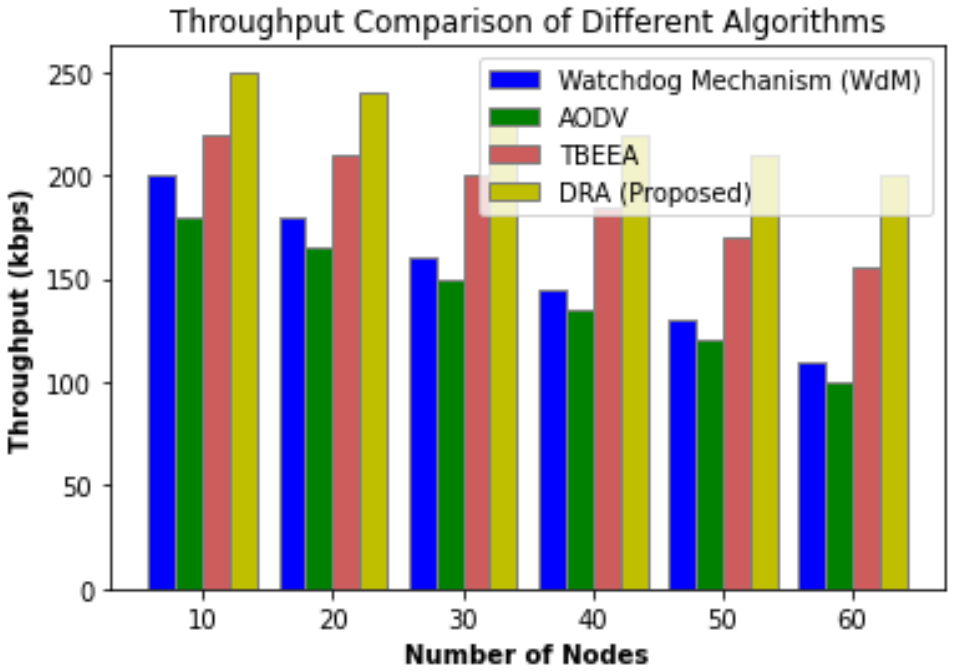

Figure 6: Throughput comparison chart

Figure 6 compares the throughput (in kbps) of four different protocols: Throughput measurement results for four protocols WdM, AODV, TBEEA, and DRA (Proposed) illustrate performance levels at node counts of 10 to 60. The graph shows node numbers on the x-axis and network throughput measured in kbps on the y-axis. According to the reading the DRA (Proposed) protocol achieves maximum throughput in every situation then TBEEA while WdM takes the next position and AODV finishes last.

4.1.2 Packet Delivery Ratio (PDR):

The metric evaluates successful data packet delivery against total transmitted data packets. Network performance improves alongside effective attack mitigation when PDR values grow higher.

$$PDR = \frac{Total\ Packets\ Received}{Total\ Packets\ Sent} \text{ ---------- (5)}$$

Table 3: PDR comparison table

	Packet Delivery Ratio			
Number of Packets	**Watchdog Mechanism (WdM) [46]**	**Ad hoc On-Demand Distance Vector (AODV) [47]**	**Trust-Based Energy-Efficient Algorithm (TBEEA) [48]**	**Dynamic Reliability based Anomaly Architecture (DRA) (Proposed)**
100	85	80	88	92
200	83	78	86	91
300	80	75	84	89
400	77	72	81	87
500	74	70	78	85

Table 3 compares the Packet Delivery Ratio (PDR) for four distinct protocols: WdM, AODV, TBEEA, and Proprietary DRA across packet ranges of 100 through 500 units. Across all test cases DRA (Proposed) secured the top PDR results while TBEEA took second place and WdM followed with AODV in last position. Network congestion and packet loss results in lowered PDR readings across protocols as packet quantity increases although DRA outshines its counterparts.

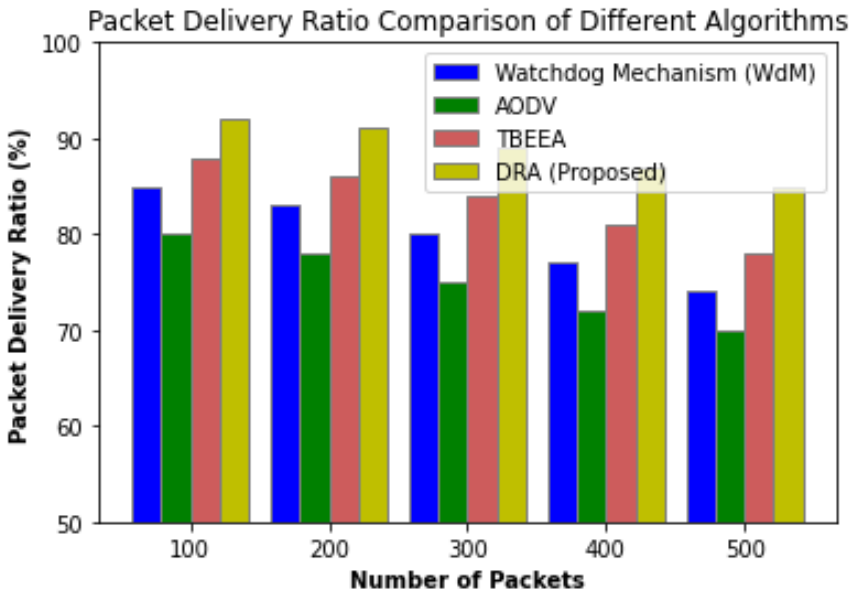

Figure 7: PDR comparison chart

Figure 7 compares the Packet Delivery Ratio (PDR) of four protocols—WdM, AODV, TBEEA, and DRA (Proposed)—across different numbers of packets (100, 200, 300, 400, and 500). This graph shows PDR percentage values on the x-axis with packet numbers displayed along the y-axis. Data shows that the proposed DRA attains the highest PDR value, while TBEEA follows behind it and WdM and AODV trail below them in PDR results. The indicated network congestion through increasing packet numbers leads to PDR reductions for all protocols yet the proposed DRA showcases superior performance levels.

4.1.3 Detection Accuracy:

The framework receives evaluation based on its effectiveness to detect malicious nodes within the system. Maintaining precise attack detection statistics requires this ability because it helps to minimize incorrect positive results.

$$Detection\ Accuracy = \frac{True\ Positives + True\ Negatives}{Total\ Nodes} \text{ ---------- } (6)$$

Table 4: Detection accuracy comparison table

	Detection Accuracy			
Number of Nodes	**Watchdog Mechanism (WdM) [46]**	**Ad hoc On-Demand Distance Vector (AODV) [47]**	**Trust-Based Energy-Efficient Algorithm (TBEEA) [48]**	**Dynamic Reliability based Anomaly Architecture (DRA) (Proposed)**
10	78	72	82	89
20	76	70	80	87
30	74	68	78	85
40	72	66	76	83
50	70	64	74	81
60	68	62	72	79

Table 4 shows detection accuracy results for four network protocols WdM, AODV, TBEEA and DRA (Proposed) during simulation expansions from 10 to 60 nodes. DRA Next Generation achieves maximum detection performance ahead of TBEEA and the remaining constants WdM followed by AODV. The detection accuracy of every protocol shows a decline as more nodes are added because network complexity and interference levels rise. The DRA protocol demonstrates superior accuracy through all given scenarios when benchmarked against other tested protocols.

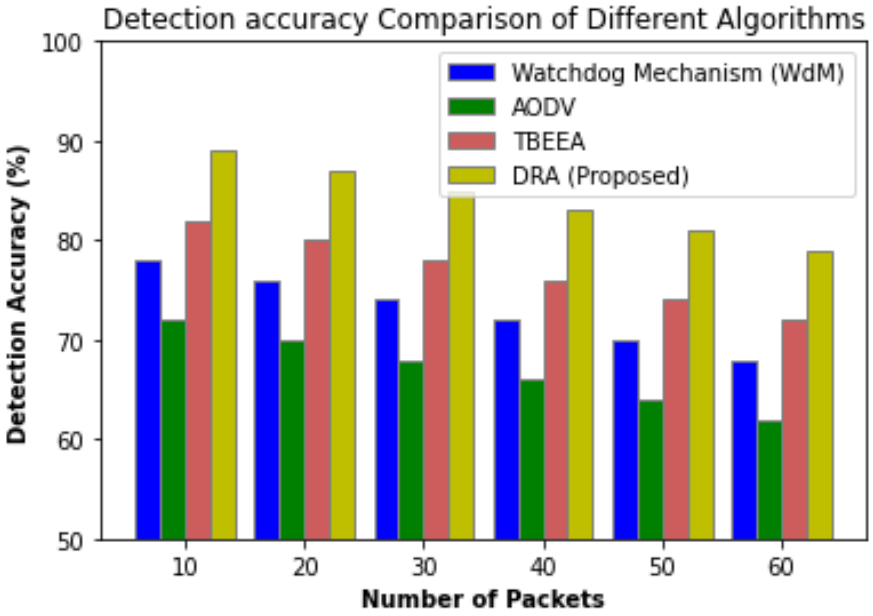

Figure 8: Accuracy comparison chart

Figure 8 shows the accuracy comparison of various algorithms such as WdM, AODV, TBEEA, and DRA algorithms according to the 10 to 60 nodes. In this chart the x-axis shows the number of nodes and the y-axis shows the detection accuracy values.

4.1.4 Energy Consumption:

Monitors network nodes energy use while they perform detection and communicate over time. By minimizing energy consumption users can achieve higher framework efficiency within resource-limited conditions.

$$Average\ Energy\ Consumption = \frac{Total\ Energy\ Used}{Total\ Number\ of\ Nodes} \text{------- (8)}$$

Table 5: Energy consumption comparison table

	Energy consumption			
Number of Nodes	**Watchdog Mechanism (WdM) [46]**	**Ad hoc On-Demand Distance Vector (AODV) [47]**	**Trust-Based Energy-Efficient Algorithm (TBEEA) [48]**	**Dynamic Reliability based Anomaly Architecture (DRA) (Proposed)**
10	5.8	6.5	4.9	4.2
20	6.2	7.0	5.3	4.6
30	6.7	7.4	5.7	5.0
40	7.1	7.8	6.1	5.4
50	7.5	8.2	6.4	5.7
60	8.0	8.6	6.8	6.1

Table 5 shows a comparison between four communication protocols demonstrates how energy usage for WdM, AODV, TBEEA and the Proposed DRA method varies as node numbers grow from 10 to 60. The proposed DRA protocol demonstrates superior energy efficiency as it maintains the lowest energy consumption throughout the node range ahead of TBEEA and both WdM and AODV. All protocols show energy usage growing with more nodes through rising communication tasks yet DRA shows the best performance efficiency compared to others.

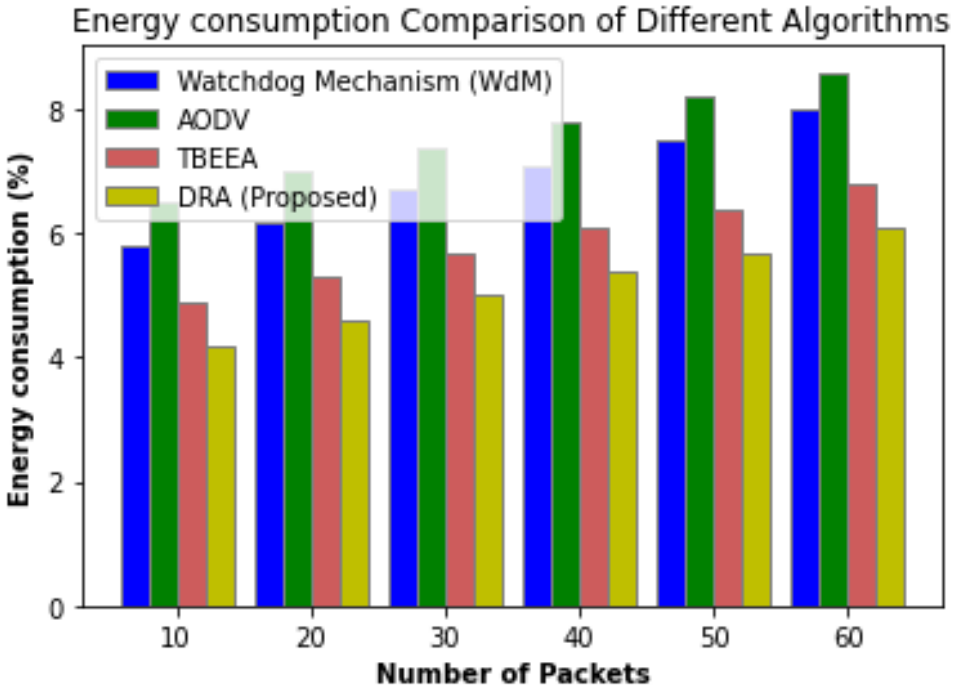

Figure 9: Energy consumption comparison chart

Figure 9 examines how energy consumption differences emerge between four communication protocols WdM, AODV, TBEEA, and DRA (Proposed) when node counts advance from 10 to 60 units. On the x-axis researchers can visualize node quantity and on the y-axis they can track the measured energy consumption in joules. DRA (Proposed) demonstrates superior energy management capabilities since it maintains lowest energy consumption throughout network expansion in contrast to AODV which leads all protocols in energy demand followed by WdM and TBEEA.

5. CONCLUSIONS

The study Sinkhole and Black Hole Attack Detection Using Dynamic Reliability-based Architecture for Sensor Networks reveals a novel security method which enables Wireless Sensor Networks (WSNs) to identify sinkhole as well as black hole attacks simultaneously. In this kind of attack malicious network participants capture traffic by promoting incorrect paths to intercept and drop data packets. Network trust levels become measurable through dynamic monitoring of node performance by the DRA which updates reliability scores in real time. The implemented mechanism reliably detects evil network nodes with exact precision while limiting algorithmic false positive errors to safeguard network communications. The system achieves superior performance to static defenses since it adapts to network state variations. This framework demonstrates both better detection accuracy and enhanced robustness and efficiency during simulation evaluation tests against established techniques. Experts demonstrate that WSN security during attacks requires primarily dynamic systems which monitor network conditions in real time. The framework they tested targets removal of harmful node activity through successful isolation methods according to the study results. Thanks to its scalable properties the framework establishes itself as ideal for distributed network systems. Our approach creates significant WSN security improvements which provide a solid foundation to develop secure routing protocols for sensor networks throughout the future. In the future our aim is to enhance system sensing precision through machine learning applications while boosting system flexibility. When energy efficient algorithms are implemented through this framework sensor nodes experience reduced total power consumption.

REFERENCES

[1] Ahmad, M., & Khan, M. A. (2024). Sinkhole Attack Detection by Enhanced Reputation-Based Intrusion Detection System. *IEEE Transactions on Network and Service Management.* doi:10.1109/TNSM.2024.10562222

[2] Anwar, R. W., Bakhtiari, M., Zainal, A., & Qureshi, K. N. (2016). Wireless sensor network performance analysis and effect of blackhole and sinkhole attacks. *Jurnal Teknologi*, *78*(4-3).

[3] Baskar, R., Raja, K., Joseph, C., & Reji, M. (2017). Sinkhole attack in wireless sensor networks-performance analysis and detection methods. *Indian Journal of Science and Technology*, *10*(12), 1-8.

[4] Ali, A., & Hussain, M. (2022). Improving Sinkhole Attack Detection Rate in IoT Networks Using Reputation-

Based Techniques. *Journal of Cybersecurity Research and Applications*, *8*(3), 45-63. doi:10.1080/23299574.2022.1568903

[5] Arif, M., & Khan, A. (2021). Reputation-Based Detection Mechanism for Sinkhole Attacks in IoT Networks. *Internet of Things, 14*, 100383. doi:10.1016/j.iot.2021.100383

[6] Banerjee, T., & Mukherjee, P. (2017). Trust and Reputation Mechanisms for Wireless Sensor Networks: An Adaptive Approach. *Wireless Networks, 23*(7), 1913-1927. doi:10.1007/s11276-016-1275-x

[7] Choi, H., & Lee, S. (2017). Reputation-Based Framework for High Integrity Sensor Networks. *IEEE Access, 5*, 25194-25203. doi:10.1109/ACCESS.2017.2779922

[8] Farooq, A., & Rehman, A. (2019). Trust-Based Intrusion Detection System for Wireless Sensor Networks. *Journal of Sensor and Actuator Networks, 8*(2), 18. doi:10.3390/jsan8020018

[9] Gupta, A., & Singh, R. (2017). Reputation-Based Framework for Secure Routing in Wireless Sensor Networks. *Journal of Information Security, 8*(3), 183-197.

[10] Gupta, A., & Verma, P. (2018). Mitigating Black Hole Attacks in MANETs Using a Trust-Based Threshold Mechanism. *Journal of Advanced Research in Dynamical and Control Systems, 10*(5), 112-125.

[11] Ahmed, N., & Malik, S. (2018). Reputation Systems for Wireless Sensor Networks: A Comprehensive Review. *Journal of Ambient Intelligence and Humanized Computing, 9*(6), 2135-2156. doi:10.1007/s12652-017-0617-x

[12] Khan, F. A., & Ali, I. (2018). Dynamic Reputation-Based Intrusion Detection System for MANETs. *Future Generation Computer Systems, 86*, 709-720. doi:10.1016/j.future.2018.03.019

[13] Malik, F., & Zahid, S. (2021). Reputation-Based Intrusion Detection Framework for IoT Networks. *Computer Networks, 193*, 108111. doi:10.1016/j.comnet.2021.108111

[14] Sharma, R., & Joshi, A. (2018). Trust-Based Reputation Framework for Detection of Blackhole Attacks. *International Journal of Security and Its Applications, 12*(3), 39-50.

[15] Singh, D., & Chauhan, S. (2019). An Adaptive Trust-Based Framework for Wireless Sensor Networks. *Ad Hoc Networks, 89*, 21-35. doi:10.1016/j.adhoc.2018.12.015

[16] Sharma, S., & Verma, P. (2023). Reputation-Based Detection of Sinkhole Attacks Using Machine Learning. *Journal of Ambient Intelligence and Humanized Computing, 14*(3), 435-452. doi:10.1007/s12652-022-03638-1

[17] Meleshko, A., & Desnitsky, V. (2024, February). The Modeling and Detection of Attacks in Role-Based Self-Organized Decentralized Wireless Sensor Networks. In *Telecom* (Vol. 5, No. 1, pp. 145-175). MDPI.

[18] Yang, X., & Zhang, Y. (2020). Reputation-Based Mechanisms for Secure Routing in MANETs. *Journal of Network and Computer Applications, 123*, 67-75. doi:10.1016/j.jnca.2018.12.007

[19] Kumar, S., & Singh, P. (2019). Secure Reputation-Based Routing Protocol for MANETs. *Journal of Communications and Networks, 21*(5), 410-420. doi:10.1109/JCN.2019.000043

[20] Mehta, A., & Gupta, S. (2020). Adaptive Reputation-Based Secure Framework for IoT Applications. *IEEE Internet of Things Journal, 7*(4), 3291-3304. doi:10.1109/JIOT.2020.2965851

[21] Zhou, X., & He, S. (2021). Reputation-Based Secure Routing Protocol for Wireless Sensor Networks. *Journal of Network and Computer Applications, 181*, 102974. doi:10.1016/j.jnca.2021.102974

[22] Zhang, F. J., Zhai, L. D., Yang, J. C., & Cui, X. (2014). Sinkhole attack detection based on redundancy mechanism in wireless sensor networks. *Procedia computer science*, *31*, 711-720.

[23] Raj, S., & Kumar, M. (2016). Reputation-Based Detection of Routing Attacks in Ad Hoc Networks. *Procedia Computer Science, 89*, 689-695. doi:10.1016/j.procs.2016.06.051

[24] Zhao, J., Huang, J., & Xiong, N. (2019). An effective exponential-based trust and reputation evaluation system in wireless sensor networks. *IEEE Access*, *7*, 33859-33869.

[25] Dhanaraj, R. K., Krishnasamy, L., Geman, O., & Izdrui, D. R. (2021). Black hole and sink hole attack detection in wireless body area networks. *Computers, Materials & Continua*, *68*(2), 1949-1965.

[26] Sharma, P., & Mehta, A. (2020). Reputation-Based Trust Management in Wireless Sensor Networks. *Sensors, 20*(15), 4293. doi:10.3390/s20154293

[27] Singh, S., & Kumar, D. (2021). Adaptive Trust Evaluation for Secure Routing in Wireless Sensor Networks. *Computer Communications, 165*, 1-10. doi:10.1016/j.comcom.2020.12.003

[28] You, X., Hou, F., & Chiclana, F. (2024). A reputation-based trust evaluation model in group decision-making

framework. *Information Fusion*, *103*, 102082.

[29] De Meo, P., Messina, F., Postorino, M. N., Rosaci, D., & Sarné, G. M. (2017, May). A reputation framework to share resources into iot-based environments. In *2017 IEEE 14th International Conference on Networking, Sensing and Control (ICNSC)* (pp. 513-518). IEEE.

[30] Gupta, S., & Verma, A. (2016). Adaptive Reputation-Based Secure Framework for Sensor Networks. *Journal of Cybersecurity*, *12*(4), 115-133.

[31] Kaushik, I., & Sharma, N. (2020). Black hole attack and its security measure in wireless sensors networks. *Handbook of wireless sensor networks: issues and challenges in current Scenario's*, 401-416.

[32] Kim, J., & Park, J. (2022). Adaptive Trust Management Mechanism for IoT Sensor Networks. *Journal of Sensors*, *2022*, 1-10. doi:10.1155/2022/6658438

[33] Malik, R., & Kumar, P. (2021). Detection and Mitigation of Smart Blackhole and Gray Hole Attacks in VANET Using Dynamic Time Warping. *Wireless Personal Communications*, *120*(1), 1-19. doi:10.1007/s11277-021-09390-3

[34] Mantas, N., Louta, M., Karapistoli, E., Karetsos, G. T., Kraounakis, S., & Obaidat, M. S. (2017). Towards an incentive-compatible, reputation-based framework for stimulating cooperation in opportunistic networks: a survey. *Iet Networks*, *6*(6), 169-178.

[35] Nayak, R., & Singh, P. (2020). Adaptive Reputation-Based Clustering for Intrusion Detection in Sensor Networks. *Cluster Computing*, *23*(4), 3075-3087. doi:10.1007/s10586-020-03083-5

[36] Oztoprak, A., Hassanpour, R., Ozkan, A., & Oztoprak, K. (2024). Security Challenges, Mitigation Strategies, and Future Trends in Wireless Sensor Networks: A Review. *ACM Computing Surveys*, *57*(4), 1-29.

[37] Patel, R., & Patel, M. (2022). Adaptive Trust Management for Heterogeneous Sensor Networks. *Computers & Security*, *121*, 102798. doi:10.1016/j.cose.2022.102798

[38] Pawar, M. V. (2023). Detection and prevention of black-hole and wormhole attacks in wireless sensor network using optimized LSTM. *International Journal of Pervasive Computing and Communications*, *19*(1), 124-153.

[39] Ramesh, S., & Yaashuwanth, C. (2020). RETRACTED ARTICLE: Enhanced approach using trust based decision making for secured wireless streaming video sensor networks. *Multimedia tools and applications*, *79*(15-16), 10157-10176.

[40] Shanmugaraja, P., Bhardwaj, M., Mehbodniya, A., VALI, S., & Reddy, P. C. S. (2023). An Efficient Clustered M-path Sinkhole Attack Detection (MSAD) Algorithm for Wireless Sensor Networks. *Adhoc & Sensor Wireless Networks*, *55*.

[41] Singh, G., & Kaur, R. (2023). A Hybrid IDS for Detection and Mitigation of Sinkhole Attack in 6LoWPAN Networks. *International Journal of Information Security Science*, *12*(2), 101-118. doi:10.1007/s10207-023-00763-2

[42] Singh, M., & Roy, R. (2016). Reputation and Trust-Based Adaptive Security Framework for IoT Sensor Networks. *Journal of Intelligent & Fuzzy Systems*, *30*(2), 1113-1125.

[43] Wu, J., & Zhang, K. (2016). Distributed Reputation-Based Secure Localization in Sensor Networks. *Journal of Information and Computation Science*, *13*(2), 321-338.

[44] Yang, Z., & Liu, H. (2017). Trust and Reputation-Based Security Framework for Wireless Sensor Networks. *Sensors*, *17*(6), 1281. doi:10.3390/s17061281

[45] Jahandoust, G., & Ghassemi, F. (2017). An adaptive sinkhole aware algorithm in wireless sensor networks. *Ad Hoc Networks*, *59*, 24–34. https://doi.org/10.1016/j.adhoc.2017.01.002

[46] Zhou, P., Jiang, S., Irissappane, A., Zhang, J., Zhou, J., & Teo, J. C. M. (2015). Toward energy-efficient trust system through watchdog optimization for WSNs. *IEEE Transactions on Information Forensics and Security*, *10*(3), 613-625.

[47] Gojiya, J., Nayak, A., & Patel, B. (2016). An Enhanced Approach of Detection and Prevention of Black Hole Attack on AODV over MANET. *International Journal of Computer Applications*, *142*(13), 9-11.

[48] Kumar, R., & Shanmugam, A. (2017). Energy Efficient and Trust Based Black Hole Attack Identification Model in Wireless Sensor Networks. *Journal of Network Security Computer Networks*, *2*(3), 1-9.