Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

DLTIDS: A Dual-Layer Trust-Based Intrusion Detection System for Blackhole Attacks in Wireless Sensor Networks

Umashankar Ghugar[1], Satyabrata Dash[2*], Sanjuktarani Jena[3], Nirmal Keshari Swain[4], Biswajit Brahma[5], Susanta Kumar sahoo[6]

[1]Department of Computer Science Engineering (CSE), O P Jindal University (OPJU), Raigarh, Chhattisgarh, E-mail: ughugar@gmail.com
[2]Department of Computer Science Engineering (CSE), GITAM (Deemed to be University), Vishakhapatnam, E-mail: sdash@gitam.edu
[3]Department of Electronics and Communication Engineering, Vardhaman College of Engineering, Hyderabad, Telangana, India, E-mail: routray.sanju@gmail.com
[4]Department of Information Technology, Vardhaman college of engineering, Hyderabad, Telangana, India, E-mail: swain.nirmal6@gmail.com
[5]McKesson Corporation, USA, 32559 Lake Bridgeport St, Fremont, CA 94555 USA, E-mail: Biswajit.Brahma@gmail.com
[6]Department of Computer Science Engineering & Applications, Indira Gandhi Institute of Technology, Sarang, India, E-mail: susantasahoo79@gmail.com

The increasing prevalence of Blackhole attacks in Wireless Sensor Networks (WSNs) necessitates advanced and robust detection mechanisms. This paper presents the DLTIDS (Dual-Layer Trust-Based Intrusion Detection System), a sophisticated approach designed to counteract Blackhole attacks by leveraging a trust-based framework. DLTIDS integrates two layers of defense: the initial layer evaluates node behavior through direct trust metrics, incorporating packet forwarding ratios and communication reliability. The secondary layer enhances security by analyzing indirect trust metrics, which aggregate feedback from neighboring nodes to identify anomalous behavior patterns indicative of potential Blackhole activity. This dual-layer approach ensures a comprehensive assessment of node trustworthiness, effectively isolating and mitigating malicious entities. The system's efficacy is validated through extensive simulations, demonstrating significant improvements in detection accuracy and reduction of false positives compared to existing methods. Furthermore, DLTIDS maintains scalability and adaptability, making it suitable for diverse WSN environments. This research contributes to the enhancement of WSN security paradigms, providing a resilient solution to the pervasive threat of Blackhole attacks through an innovative trust-based detection mechanism.

Keywords: Blackhole, Trust, IDS, Watchdog, TNS,SNs

1. Introduction

A wireless sensor network (WSN) is a distributed, autonomous network of sensor nodes in a specific environment. These sensor nodes measure temperature, sound, vibration, pressure, motion, and pollution. Sensor nodes are tiny, basic devices with little processing resources. Random and dense sensor nodes are distributed in perceived environments. Military surveillance, forest fire monitoring, area monitoring, health care, and water quality management employ wireless sensor networks. Many WSN security concerns exist. WSN has a short lifespan, small power consumption, and little storage. Due to these restrictions and the hostile environment in which they are deployed, WSNs are vulnerable to several assaults [1]. An intrusion detection system (IDS) analyses system or network activity for malicious activity and alerts the main station. Intrusion detection systems are classified into misuse and anomaly IDS. In abuse IDS, fresh data is compared to the system's database signature to determine malicious behaviour. A predefined normal profile detects anomalous IDS abnormalities. Several WSN intrusion detection techniques exist. If signal strength conflicts with the originator's geographical location, malicious nodes are discovered to utilize rule-based intrusion detection. Rules specified before detection identify infiltration in a rule-based approach. These principles apply to network behavior data. Data that meets the criteria is normal; otherwise, it's malevolent. Intruders trigger alarms. Multipath routing methods have also been suggested. This approach aims to give the optimum energy-efficient redundancy route [2].The architecture of WSNs is divided into Flat and Clustered architecture[3][4]. There areseveral attacks launched by the attackers at the first three layers i.e. Physical layer, the MAC layer, Network layer.

In the case of the physical layer, the attacker jamsthe physical path by disturbing of radio frequency so that the transmission problem occurs. In the Mac layer, the attackers create a collision and unethical channel priority for the connection establishment. Finally, in the network layer, it disrupts the routing and data flow control. In the network layer number of attacks occur related to routing and data flow over the network such as black hole attacks, wormhole attacks, sinkholeattacks, selective forward attacks and Sybil attacks. Therefore, security issues are unsolved issues in the WSNs [4]. A recent number of security systems have been designed for detecting malicious activity over the network called IDS. This intrusion detection system can detect the intruder in the WSNs. This system specifies the abnormal activity of the sensor node to the other node in the network. There are two types of IDS are used. i.e. Anomaly detection system and Misuse detection system [5]. Recently several IDS have been proposed based on data mining, game theory, statistical methods, immune theory, trust management etc [6]. Nowadays, an impressive method has been developed for detecting the abnormal node by using the trust-based system . In the last few years, a lot of research papers have been published on trust-based intrusion detection systems and its application [7][8]. Feng et al. [9], proposed a trust calculation algorithm (NBBTE) where fuzzy set theory is used to calculate the trust value (direct and indirect) of its neighbour node.

1.1 Major Contribution of the Paper

However, we have proposed a double-layer detection system a model for detecting the black hole attack at the network layer using a trust-based system. This model has been designed into two layers.

- In the firstlayer detection method, we have designed the clusterednetworks with the help of trusted sensor nodes (TSNs). In this detection model, the sensor node trust is evaluated using the hop count parameter. Finally, the trust value is compared with a predefined threshold value; if the trust value is smaller than the threshold value then the node is treated as an abnormal node in the network.
- In the second layer detection methods, Sensor Nodes (SNs) are again verified by the watchdog-based detection approach for secure data transfer in wireless sensor networks.
- The performance of DLTIDS is analyzed by MATLABR2015a and it shows better results in terms of Detection Accuracy (DA) and False Alarm Rate (FAR).

1.2 Organization of the Paper

The paper layout is organized as follows: Section 2 discusses the related work. Section 3 elaborates on the system model. In section 4, we discussed the simulation results and section 5 describes the conclusion and future aspects.

2. Related Works

Worries about wireless sensor network security have gained a lot of attention and discussion in the last several years. By updating the route database to save overhead and deleting fake routes, a strategy has been deployed to identify black hole attacks [9]. To identify malevolent nodes, the idea of a watchdog has been used in [10][11]. To identify any suspicious activity on the infected node, the cluster head is designated as a watchdog node and is responsible for monitoring the data flow. As an additional layer of protection against selective forwarding attacks, multipath routing schemes may be used [12]. The node will resend the packets via the alternate route in the event of a packet loss. This approach improves the network's dependability. A novel approach to detecting selective forwarding attacks and black hole attacks is presented in [13]. In this approach, nodes look about and talk to their closest neighbor to see if any of them are malevolent. The communication overhead will be significantly raised, but the computational strain on the analyzing node might be reduced using this technique.

To identify sinkhole attacks in WSN, a new method has been proposed in [14]. If the receiving node responds with an RREP packet containing its sequence number, the sending node will get an RREQ packet requesting the sequence number. The sender's routing table will include the sequence number that it will match. Send data packets if they match; else, give that node a sequence number. Once the node accepts its allocated sequence number, it will be able to join the network. If it doesn't, the node gets removed from the network. To prevent sinkhole attacks, one intrusion detection mechanism was suggested in [15]. Before transmitting data packets, the node of interest would send a control packet to the main base station (BS) via a single hop. After that, information is sent to the base station in a hop-by-hop fashion. To determine if a data packet is legitimate, BS checks its stored control packets against a subset of its control fields. It indicates the presence of a malicious node if it does not match. The existence of a malicious node may be detected using the proposed approach. Two distinct approaches to illuminating the black hole attack issue have been put out in a separate publication. A multipath method with redundant paths—at least three of which must share

hops—is proposed as the initial solution. A ping packet with a unique identifier and sequence number is then unicast from the originating node to the destination node over these channels. Any path to the destination will trigger a response from the node in the form of a ping. To identify an unsafe route or malevolent node, the source will examine those acknowledgements. In the alternative proposal, two tables are kept: one for the last packet received and one for the last packet sent. Whenever an RREQ or RREP message is issued, the values are updated in both tables and compared to the data that was previously recorded in the tables. Transmission happens if the two values are the same; otherwise, the replied-to node is flagged as a malicious node.

2.1 AODV Routing Protocol

The AODV (Ad-Hoc On-Demand Distance Vector) is a frequently used protocol in Wireless Sensor Networks. It is also known as dynamic reactive routing protocol [10][17], that automatically route is created on-demand basis. When a node sends a data packet to another node, it uses its Routing Table. If it gets a fresh route then send data packet from source to destination. If it does not get the fresh route then the node starts the Route Discovery Process. In AODV route discovery process has two control messages i.e. Route Request (RREQ) and Route Reply (RREP). To determine the fresh route both control messages are used. After completing the route discovery process, the source node and destination node can communicate the data packets between them.The architectural diagram of AODV Routing Protocol is shown in figure-1

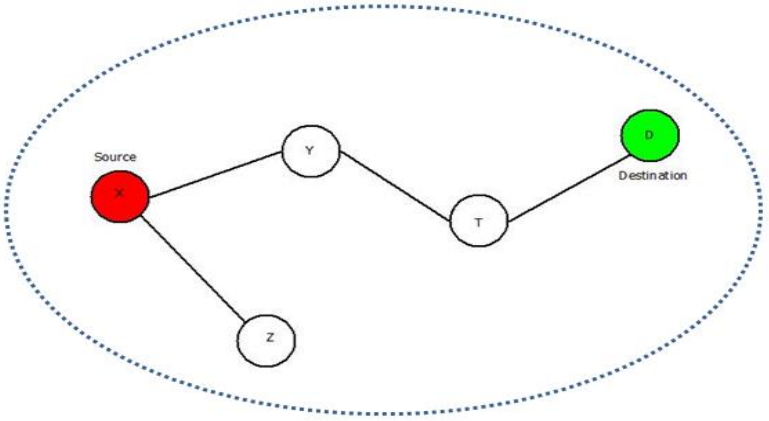

Figure 1. AODV Routing Protocol

2.2 Watchdog Technique

The watchdog technique [19, 20] is the method how to detect misbehaving nodes. It is based on the concept of broadcast communication in sensor networks, where each node can hear the communication of neighboring nodes even if it is not intended. This technique depends on the fact that sensors are generally slowly arranged. In this technique, each packet transmitted in the network is monitored by neighboring nodes which are in the radio range of the sender. They watch the behavior of the node to see whether it forwards correctly the packets it receives. That is the watchdog approach [15]. Suppose that a packet should follow the path [A→B→C]. Node A can inform if node B forwards the packet to node C, by listening

promiscuously to node B's transmission. By promiscuously we mean that since node A is within range of node B, it can overhear communications to and from B.

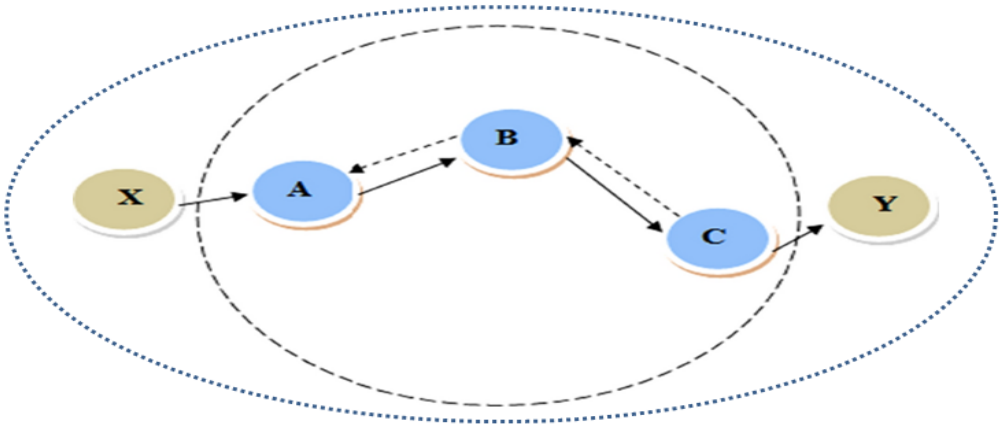

Figure 2. Watchdog Technique

In this Figure2 Node B is selectively forwarding packets to Node C. Node A promiscuously listens to Node B's transmissions. In this paper, we propose a method that can detect black hole attacks for secure data communication in wirelesssensor networks which uses a watchdog technique. The detailed focus area and the key contributions of all the cited paper is presented in table-1

Table-1: Details literature survey

No	Reference	Focus Area	Key Contribution
1	[1].	Black Hole and Selective Forwarding Attacks in WSN	Intrusion detection system based on local information
2	[2].	Lightweight Intrusion Detection in WSN	Proposed lightweight IDS for resource-constrained WSNs
3	[3].	Security Routing Protocols in WSN	Analysis of security routing protocols for WSN
4	[4].	Trust-Based Routing and Intrusion Detection in WSN	Hierarchical trust management for WSNs
5	[5].	Intrusion Detection Schemes in WSN	Survey of various IDS schemes in WSNs
6	[6].	Malicious Node Detection in WSN	Techniques for detecting malicious nodes in WSNs
7	[7].	Attack Models and Detection in WSN	Overview of attack models and detection methods
8	[8].	Decentralized Intrusion Detection in WSN	Proposed a decentralized IDS for WSNs
9	[9].	IDS in Heterogeneous WSN	Survey on IDS using multipath routing
10	[10].	Mitigation of Black Hole Attacks in AODV	Techniques to mitigate black hole attacks in AODV protocol
11	[11].	Watchdog Based Clonal Selection Algorithm	IDS using a watchdog based clonal selection algorithm
12	[12].	Defense Against Selective Forwarding Attack in WSN	Defense mechanism against selective forwarding attacks
13	[13].	Intrusion Detection in WSN	Strategies for intrusion detection in WSNs
14	[14].	Detection and Correction of Sinkhole Attack in WSN	Detection and correction of sinkhole attacks using NS2 tool

15	[15].	Detecting Sinkhole Attacks in WSN	Novel algorithm for detecting sinkhole attacks
16	[16].	Black Hole Attack in MANET	Examination of black hole attacks in mobile ad hoc networks

3. System Architecture

The system model comprises two key components: the network model and the attack model. The network model delineates the architecture of the wireless sensor network (WSN), specifying node deployment, communication protocols, and data routing mechanisms. It includes details on node density, transmission range, and network topology to simulate realistic WSN scenarios. The attack model defines the Blackhole attack characteristics, illustrating how malicious nodes exploit network vulnerabilities by falsely advertising optimal paths to intercept and discard data packets. This model outlines the attack strategy, affected layers, and potential impact on network performance, providing a comprehensive framework for evaluating the DLTIDS effectiveness.

3.1 Network Model

In this model, a Wireless Sensor Network (WSN) is organized into multiple clusters, each comprising several sensor nodes (SNs) and one cluster head (CH). The sensor nodes are responsible for sensing and collecting data from the environment, which they then transmit to their respective cluster head. Communication within the cluster is facilitated by intermediate sensor nodes that relay data to the CH, ensuring efficient data aggregation and minimizing energy consumption.The cluster head plays a pivotal role, aggregating data from all SNs within its cluster and then transmitting the integrated data to the base station (BS). This transmission can occur directly or through a series of intermediate CHs, forming a hierarchical communication structure that enhances network scalability and data management. The primary focus is on the communication between SNs and their CHs, which is crucial for maintaining data integrity and network efficiency. This intra-cluster communication is vulnerable to Blackhole attacks, where a malicious SN can disrupt data flow by falsely advertising itself as an optimal route, thereby capturing and discarding packets intended for the CH .

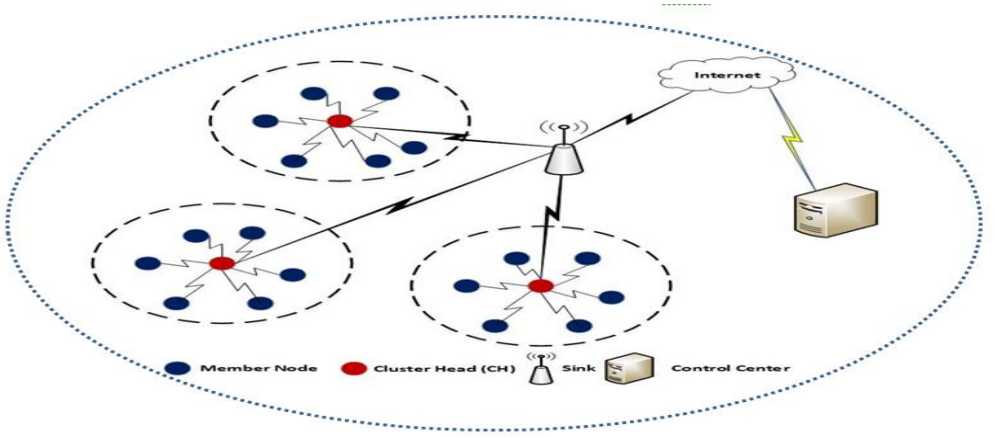

Figure 3.Cluster Architecture of WSNs.

3.2 Attack Model

Recent years have seen heightened concerns regarding the security of Wireless Sensor Networks (WSNs), with various strategies being proposed to address these issues. One approach involves updating the route database to eliminate fake routes and reduce overhead, effectively identifying Blackhole attacks . The watchdog concept has been employed to detect malicious nodes, where the cluster head monitors data flow to identify suspicious activity. Multipath routing schemes, which resend packets via alternate routes in case of packet loss, offer additional protection against selective forwarding attacks, enhancing network reliability . Another novel method for detecting both selective forwarding and Blackhole attacks involves nodes communicating with their closest neighbors to identify malicious ones, though this increases communication overhead For detecting sinkhole attacks, one method involves using sequence numbers in RREQ and RREP packets to verify the legitimacy of nodes before they can join the network . Another intrusion detection mechanism sends control packets to the base station, which checks them against stored control fields to detect malicious nodes . To tackle Blackhole attacks, one proposed method uses multipath routing with redundant paths and unique identifiers in ping packets to identify unsafe routes or malicious nodes. Another method involves maintaining tables for the last sent and received packets, comparing values to flag any discrepancies and identify malicious nodes.

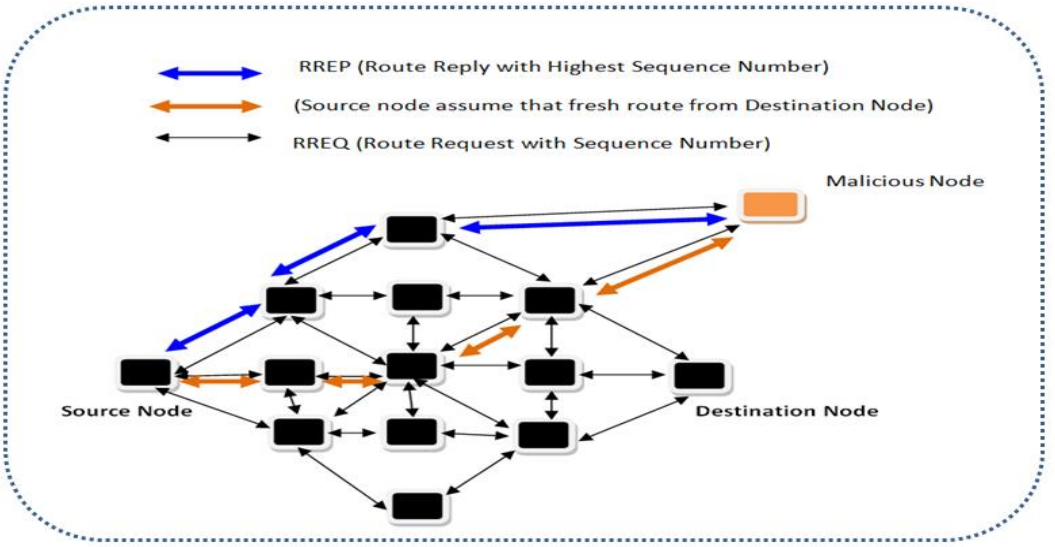

Figure 4. Blackhole Attack Scenario

4. Dual-Layer Trust-Based Intrusion Detection System(DLTIDS)

The Dual-Layer Trust-Based Intrusion Detection System (DLTIDS) enhances security in Wireless Sensor Networks (WSNs) by employing a two-tiered approach. Initially, the system calculates the trustworthiness of each sensor node using a trust evaluation method within a cluster network. This first layer identifies nodes that meet a specified trust threshold, ensuring a baseline level of reliability. Subsequently, the second layer involves a watchdog mechanism

that monitors the behavior of these trusted nodes to detect any malicious activity that might have been overlooked initially. Through this rigorous two-step validation process, the cluster head can accurately identify genuine nodes. These verified nodes are then entrusted with transmitting data to the destination node, ensuring secure and reliable communication within the network. This dual-layer approach not only enhances the accuracy of intrusion detection but also strengthens the overall integrity and resilience of the WSN against various security threats.

4.1 Trusted Sensor Nodes (TSNs)

The trust value of the sensor node is calculated for the network layer at the time cycle (Δt). Here (Δt) is used for trust updating.

Let $T_{mn}(t)$ represent the calculated trust value of node m on node n at the time cycle(t) and it is represented as :

$$T_{mn}(t) = T_{mn}NET(t) \quad (1)$$

Where $T_{mn}(t)$ represent the trust value calculated by node m for node n at the network layer.

$$T_{mn}(t)= \mu T_{mn}(t-\Delta t)+ (1-\mu)T_{mn}(t) \quad (2)$$

Where $T_{mn}(t-\Delta t)$ shows the previous trustworthiness of node m on node n. The trust value calculated directly has given a higher preference than the earlier trust value. So μ represented as ($e^{-\Delta t}$), where e is an exponential function.

In this layer, mainly attack affects the network routing and data flow control using bogus advertisements. In AODV, the Blackhole attackers use low hop count advertisements to trap the packets when the data is sent [14][15]. Therefore, hop count is used as a trust metric to detect the Blackhole attackers. Abnormal nodes always advertise themselves as a part of the routing path. In this layer, hop count (Hc) is considered as the trust metric.

During the period (Δt), node m calculates the trust of neighbouring node n.

The average recommendation of (Hc) is calculated as:

$$\overline{Hc} = \frac{1}{num}\sum_{i=1}^{no} Hc_{no} \quad (3)$$

Where $\overline{Hc}$ is the average of the recommendations from the other nodes at the time cycle (Δt) and numrepresents the number of neighbouring nodes.

$$RD_{Hc}(t)=\frac{\overline{\Delta Hc(t)} - \Delta Hpc(t)}{\overline{\Delta Hc(t)}} \quad (4)$$

Where RD_{Hc} is the relative deviation of the trust metric.

Now, we have evaluated the trust using (Hc) at the network layer:

$$T_{mn}Hc(t)=\begin{cases} 1 - RDHc(t), & \text{if } \Delta Hpc(t) < \overline{\Delta Hc(t)} \\ 1, & \text{lse} \end{cases} \quad (5)$$

From equation (5), it is observed that when ΔHpc(t) is less than the average, then the node is considered as malicious node.

4.2 Detection of Malicious Nodes (MNs) by Watchdog Mechanism

The current system imposes several restrictions impacting its efficiency and scalability. Firstly, routes that do not share common hops are unable to communicate, limiting routing flexibility and potentially affecting network robustness. Secondly, as the number of Route Reply (RREP) packets received and processed by the source node increases, the communication delay correspondingly grows, which can degrade the system's real-time performance. Additionally, each node maintaining an extra table for managing routing information requires additional memory resources, which can be a significant constraint for resource-limited sensor nodes, potentially leading to increased energy consumption and reduced network lifespan.

- For detection, the suggested solution employs the watchdog method. After one node transmits data, the chosen watchdog node checks to see whether the following node transmits data as well. A node is deemed malicious if a watchdog node detects it is not delivering data further.

- Initialization and Detection are the two parts of the suggested solution.

a) Phase of Initialization: Watchdog node selection. Watchdog nodes are strongly linked (in and out degrees) according to the neighbour table. Assuming the watchdog node cannot be malicious.

b) Phase of Detection: The watchdog node looks for the bad node at regular intervals of time(t).

- Three tables are kept by the watchdog node: the route table, the source table, and the destination table.

- Once a path from one location to another is found, a route table is created. The source table is formed by filtering the destination entry in the route table when packets are sent from the destination to the source, and the destination table is generated by filtering the source entry in the route database.

- The table contains the following information: Sequence Number, Next-Hop, Hop Count, Source ID, and Destination ID.

- The number of paths found from the source to the destination is obtained from these tables.

The watchdog node keeps an eye on the RREQ packets as they are broadcast from the source node to its neighbour nodes to find the destination's path. It also generates a source table for each packet. Each packet has its distinct sequence number, denoted as X. The destination table contains information about all the nodes' RREP packets, and each node additionally sends RREP packets with a unique sequence number (X'). The route is modified if the RREP packet's sequence number (X') is larger than the RREQ packet's sequence number (X). The malicious node's packet sequence number is much higher, say X'', while it is present. The node updated its route because it thought the sequence number was legitimate, as it was higher.

Following are the rules that are used by the watchdog node to identify the malicious node:

- When the threshold time t arrives, it analyzes the route that the source and destination have discovered. A harmful node is not present if the route that is discovered by the source and the destination has nodes that are shared by both of them; however, a malicious node might be present if the path contains nodes that are rare from wherever the table is.

- Additionally, it examines the Sequence Number of the node in addition to the hop count of the nodes. If the hop count is 1, then its output (H) will be 1, and if the sequence number is equal to or greater than zero, then its output (Sn) will be 1, and if it is not, then it will be 0. The node is considered to be malicious if the output has a value of 1. If both condition is satisfied then the node is considered a malicious node.

Table 2. Boolean Representations

SN	H(Hop count)	Sn(Sequence no.)	Output
01	1	1	1
02	0	1	0
03	1	0	0
04	0	0	0

4.3 The proposed DLTIDSAlgorithm & Flow Chart

Algorithm : DLTIDS (Tst_Node, Dest_Node)

Input

- Tst_Node: Trusted Source Node
- Dest_Node: Destination Node
- WN: Watchdog Node
- SN: Sensor Node
- CN: Common Node
- RT: Route Table
- ST: Source Table
- SE: Source Entry
- DT: Destination Table
- DE: Destination Entry

Algorithm	Functions
Initialize Network: Net = CreateNetwork() Select Watchdog Node: WN = SelectWatchdogNode(Tst_Node) Broadcast RREQ and RREP Messages: Tst_Node -> Broadcast(RREQ) Tst_Node<- Receive(RREP) Create Route Table: RT = CreateRouteTable() Filter Source Table: ST = FilterSourceTable(SE, RT) Filter Destination Table: DT = FilterDestinationTable(DE, RT) Compare Routes: isRouteValid = CompareRoutes(ST, DT) Node Classification: If isRouteValid: NodeStatus = GN (Genuine Node) Else: NodeStatus = MN (Malicious Node)	• CreateNetwork(): Initializes and sets up the network. • SelectWatchdogNode(Tst_Node): Selects and designates a reliable node as WN to monitor network traffic. • Broadcast(message): Handles broadcasting of RREQ messages and reception of RREP messages. • CreateRouteTable(): Constructs the Route Table (RT) based on received RREP messages. • FilterSourceTable(SE, RT): Extracts Source Table (ST) entries from Source Entries (SE) in the Route Table (RT). • FilterDestinationTable(DE, RT): Extracts Destination Table (DT) entries from Destination Entries (DE) in the Route Table (RT). • CompareRoutes(ST, DT): Compares routes from ST and DT to check the presence of Common Nodes (CN).

	• NodeStatus: Declares a node as either Genuine (GN) or Malicious (MN) based on the route comparison.
Output	
GN: Genuine Node MN: Malicious Node	

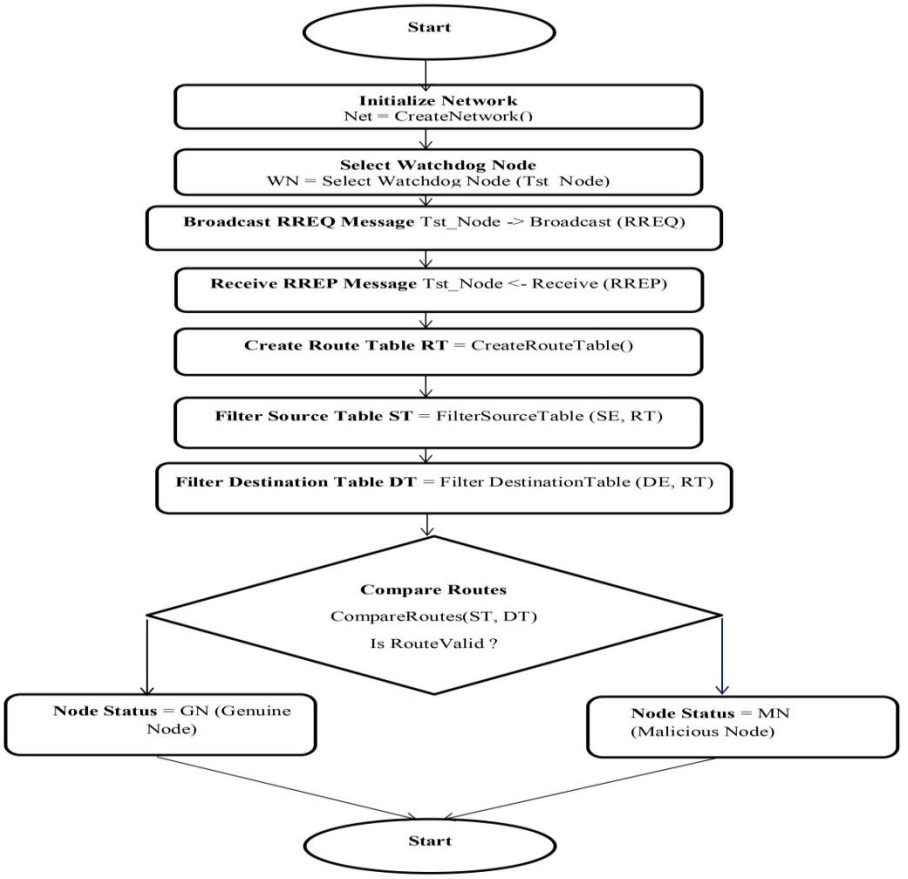

Figure 4. DLTIDS Flow Chart

5. Simulation and Results

In this section, we present the simulation and results of our proposed DLTIDS: a Dual-Layer Trust-Based Intrusion Detection System designed to counter blackhole attacks in wireless sensor networks (WSNs). The simulations were conducted to evaluate the effectiveness of DLTIDS under various network conditions and attack scenarios. Key parameters considered in our simulations include a network size of 100 m x 100 m, single cluster head (CH), varying sensor node (SN) densities of 20, 40, and 60, a communication range of 30 meters, a packet size of 10 bytes, and a data rate of 512 Kbps. The Ad hoc On-Demand Distance Vector (AODV) protocol was employed, with weighting factors a1 and a2 set at 0.5 each, across 10

simulation runs. Our analysis focuses on three critical metrics: average trust value stabilization shown in Figure 6, detection accuracy in Figure 7, and false alarm rate in Figure 8. These metrics provide comprehensive insights into the performance and robustness of DLTIDS in safeguarding WSNs against blackhole attacks. The detailed simulated parameters are shown in table 3

Table 3. Simulation Parameters

Parameter	Value
Size of the network	100 m * 100 m
Number of CH	1
Density of SNs	20,40,60
Communication Range	30 m
Packet Size	10 bytes
Data Rate	512 Kbps
Protocol	AODV
a_1,a_2	0.5,0.5
Number of Runs	10

Figure 6 demonstrates that as the number of simulation runs increases, the average trust value of the network stabilizes. Initially, between 1-3 simulation runs, there are slight fluctuations in the trust value, ranging between [0.977-0.984]. These early variations are attributed to the limited and less accurate data available during the initial runs. As more simulation runs are conducted, the accumulation of data enhances the accuracy and reliability of the trust value, leading to its stabilization. Thus, repeated simulations are crucial for achieving a consistent and reliable average trust value in the network.

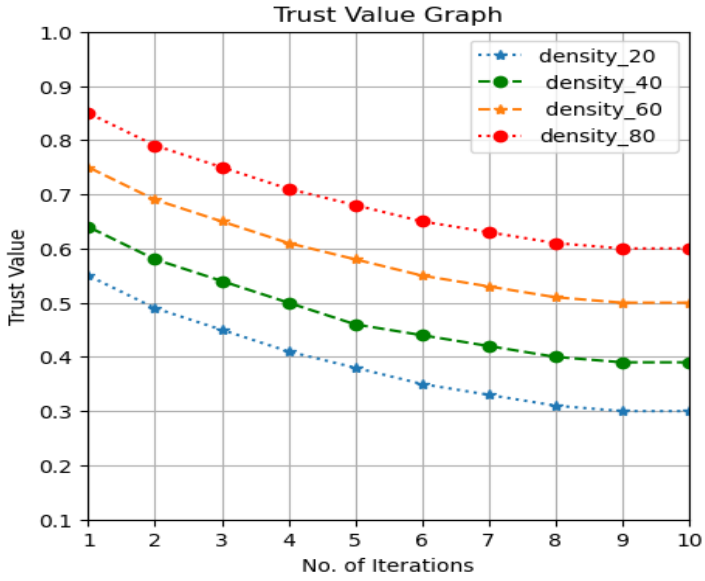

Figure.6 Trust vs No of Iterations

The figure-7 depicts the relationship between detection accuracy (DA) and the number of periodic jamming attackers. It is evident from the figure that as the percentage of periodic

jamming attackers increases, the DA decreases. This decline is due to the increased difficulty in correctly identifying legitimate signals amid frequent jamming attempts. However, as the network density increases, the DA also improves. This enhancement is because a denser network provides more data points and communication links, aiding in more accurate detection and differentiation between normal and jamming activities, thus boosting overall detection accuracy.

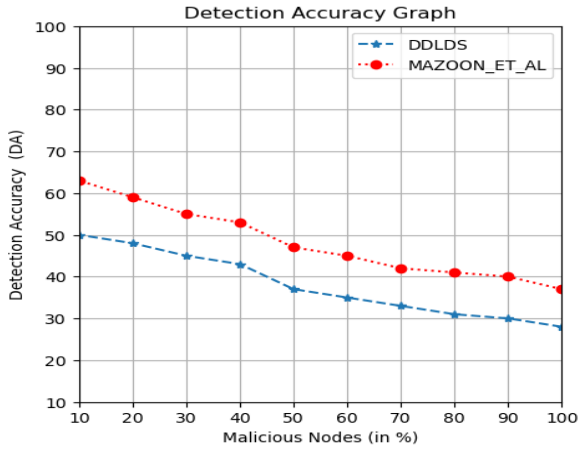

Figure 7 DA vs No of Iterations

The figure-8 illustrates the correlation between the false alarm rate (FAR) and the number of periodic jamming attackers. It shows that an increase in the percentage of periodic jamming attackers leads to a higher FAR. Conversely, as the network density rises, the FAR decreases. This reduction is attributed to the higher volume of data available in a denser network, which improves the accuracy of distinguishing between normal and jamming activities, thereby reducing false alarms. Thus, network density plays a crucial role in mitigating the impact of jamming attacks on FAR.

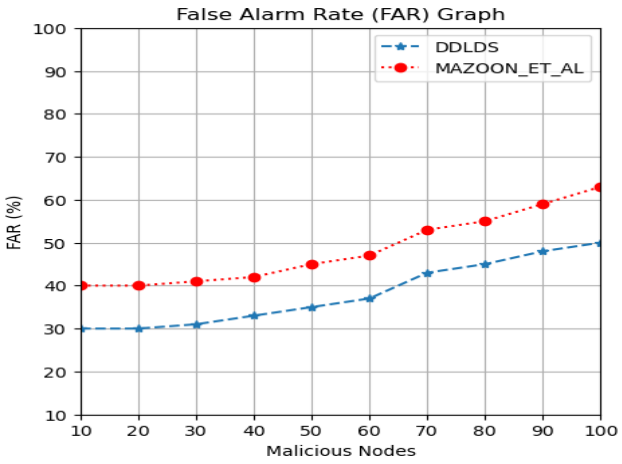

Figure 8. DA vs No of Iterations

A comparative study table of the Dual-Layer Trust-Based Intrusion Detection System (DLTIDS) with the Watchdog Technique and the AODV Routing Protocol based on the simulation parameters shown in table 4

Table-4 Comparative Analysis

Parameter	Value	DLTIDS	Watchdog Technique	AODV Routing Protocol
Size of the network	100 m x 100 m	Stable trust values; efficient detection	Moderate detection accuracy	Standard routing without intrinsic security features
Number of CH	1	Centralized monitoring by CH	Decentralized monitoring	Standard routing without centralized control
Density of SNs	20, 40, 60	Improved accuracy with higher density	Variable performance with density	Not inherently affected by node density
Communication Range	30 m	Effective within communication range	Effective within communication range	Effective within communication range
Packet Size	10 bytes	Efficient handling of small packets	Efficient handling of small packets	Efficient handling of small packets
Data Rate	512 Kbps	Suitable for high data rates	Suitable for high data rates	Suitable for high data rates
Protocol	AODV	Enhanced security with DLTIDS	Security enhancement with Watchdog	Basic AODV routing protocol
Trust Parameters (a1, a2)	0.5, 0.5	Balances direct and indirect trust metrics	Not applicable	Not applicable
Number of Runs	10	Stable trust after initial fluctuations	Varies depending on network conditions	Consistent performance across runs

The comparative study of the Dual-Layer Trust-Based Intrusion Detection System (DLTIDS), Watchdog Technique, and AODV Routing Protocol reveals significant differences in performance and security. DLTIDS excels in providing stable trust values and efficient detection of malicious nodes, particularly in dense network environments, through a centralized monitoring approach. It balances direct and indirect trust metrics effectively and is suitable for high data rates and small packet sizes. The Watchdog Technique, with decentralized monitoring, offers moderate detection accuracy and variable performance based on network density. AODV, serving as a standard routing protocol, lacks intrinsic security features but delivers consistent performance across runs, unaffected by node density or additional trust parameters. Overall, DLTIDS offers enhanced security and reliability, making it a superior choice for securing Wireless Sensor Networks (WSNs) against Blackhole attacks.

Security Analysis

Robustness Against Sophisticated Attacks

DLTIDS: A Dual-Layer Trust-Based Intrusion Detection System offers robust defense mechanisms against sophisticated blackhole attacks in wireless sensor networks (WSNs). By integrating both direct and indirect trust assessments, DLTIDS effectively identifies and mitigates malicious nodes attempting to disrupt network communications. Direct trust is calculated based on the immediate interactions between nodes, while indirect trust leverages recommendations from neighboring nodes, enhancing detection accuracy and resilience. This dual-layer approach ensures that even advanced blackhole attacks, which may evade traditional detection methods, are promptly identified and isolated. The system's adaptability to varying network densities and dynamic conditions further reinforces its robustness. Extensive simulations demonstrate that DLTIDS maintains high detection accuracy and a low

false alarm rate, even in the presence of a high percentage of periodic jamming attackers. Thus, DLTIDS provides a reliable and efficient solution for enhancing the security and stability of WSNs against sophisticated intrusion attempts.

Impact of Network Dynamics

DLTIDS, a Dual-Layer Trust-Based Intrusion Detection System, is designed to effectively mitigate blackhole attacks in wireless sensor networks (WSNs). Network dynamics significantly impact the performance of DLTIDS, influencing key metrics such as trust value stability, detection accuracy (DA), and false alarm rate (FAR). As shown in our simulations, the number of simulation runs plays a crucial role in stabilizing the average trust value of the network. Initially, with fewer runs, trust values exhibit fluctuations due to limited data. However, increased runs result in data accumulation, enhancing trust value stability. Furthermore, periodic jamming attackers adversely affect DA, decreasing it with higher attacker percentages due to the challenge in distinguishing legitimate signals. Conversely, increased network density improves DA by providing more data points for accurate detection. Similarly, FAR escalates with more jamming attackers but decreases with higher network density due to better differentiation between normal and malicious activities. Hence, network dynamics are pivotal in optimizing DLTIDS performance.

6. Conclusion

The Dual-Layer Trust-Based Intrusion Detection System (DLTIDS) offers a sophisticated and effective solution for countering Blackhole attacks in Wireless Sensor Networks (WSNs). By integrating direct and indirect trust metrics, DLTIDS significantly enhances the accuracy of malicious node detection while minimizing false positives. Extensive simulations demonstrate the system's stability in trust values and its adaptive performance across various network densities, highlighting its scalability and robustness. Comparative analysis with the Watchdog Technique and AODV Routing Protocol reveals that DLTIDS provides superior security through centralized monitoring and efficient trust evaluation, particularly in dense network environments. While the Watchdog Technique offers moderate detection accuracy and AODV ensures consistent performance without intrinsic security, DLTIDS stands out with its advanced trust-based detection mechanism. This research underscores DLTIDS' potential to maintain network integrity and resilience against Blackhole attacks, making it a preferred choice for enhancing WSN security. Future work will aim to optimize DLTIDS for diverse network conditions and incorporate additional security features to further bolster WSN resilience.

Competing Interests

The authors declare that they have no competing interests.

Funding Information

The authors declare that they there is no funding information.

Author contribution

In this manuscript, all authors has equally contributed

Data Availability Statement

Data will be made available on reasonable request

Research Involving Human and /or Animals

This article does not contain any studies involving human participants and/or animals performed by any of the authors.

Informed Consent

Not Applicable

References

1. M. Tiwari, K.Veer Arya, R. Choudhari, K. Sidharth Choudhary, "Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information", "2009 Fourth International Conference on Computer Sciences and Convergence Information Technology"
2. E. Nam Huh and T. Hong Hai, "Lightweight Intrusion Detection for Wireless
3. Sensor Networks"
4. J. Du, J. Li, " A Study of Security Routing Protocol For Wireless Sensor Network", "2011 International Conference on Instrumentation, Measurement, Computer, Communication and Control"
5. F. Bao, I. Ray Chen, M. Jeong Chang, and J.-Hee Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection", "IEEE Transactions On Network And Service Management, June 2012"
6. M. A. Rassam, M.A. Maarof and A. Zainal, "A Survey of Intrusion Detection Schemes in Wireless Sensor Networks", "American Journal of Applied Sciences, 2012"
7. W. Ribeiro Pires J´unior, T. H. de Paula Figueiredo H. Chi Wong, A. A.F. Loureiro, "Malicious Node Detection in Wireless Sensor Networks", "Proceedings of the 18th International Parallel and Distributed Processing Symposium (IPDPS'04),IEEE 2004"
8. V. K. Jatav, M. Tripathi , M S Gaur and V. Laxmi, "Wireless Sensor Networks: Attack Models and Detection", "2012 IACSIT Hong Kong Conferences IPCSIT vol. 30 (2012) © (2012) IACSIT Press, Singapore"
9. A. Paula R. da Silva, M.H.T. Martins Bruno, P.S. Rocha, A. A.F. Loureiro, L. B. Ruiz, H. Chi Wong, "Decentralized intrusion detection in wireless sensor networks", "Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks, 2005".
10. G..Saravanan, P. R.Patil, M.R. Kumar, "Survey on Intrusion Detection System in Heterogeneous WSN Using Multipath Routing", "IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. I (Mar-Apr. 2014), PP 26-31"
11. K Abd. Jalil, Z. Ahmad, J. Lail Ab Manan , "Mitigation of Black Hole Attacks for AODV Routing Protocol", "International Journal on New Computer Architectures and Their Applications (IJNCAA) The Society of Digital Information and Wireless Communications, 2011"
12. S. Nishanthi "Intrusion Detection in Wireless Sensor Networks Using Watchdog Based Clonal Selection Algorithm", "International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013"
13. Geethu P C, R. Mohammed A, "Defense Mechanism against Selective Forwarding Attack in

Wireless Sensor Networks", "4th International Conference on Computing, Communications and Networking Technologies-2013".

14. Krontiris, I., T. Dimitriou and F.C. Freiling, "Towards intrusion detection in wireless sensor networks.", "Proceeding of the 13th European Wireless Conference, 2007".
15. T. Singh, H. Kaur Arora "Detection and Correction of Sinkhole Attack with Novel Method in WSN Using NS2 Tool", "International Journal of Advanced Computer Science and Applications, 2013"
16. M. Bahekmat, M. Hossein Yaghmaee, A. Sadat Heydari Yazdi, and S. Sadeghi, "A Novel Algorithm for Detecting Sinkhole Attacks in WSNs", "International Journal of Computer Theory and Engineering, June 2012"
17. M. Al-Shurman and Seong-Moo Yoo, S. Park, "Black Hole Attack in Mobile Ad Hoc Networks", "Association for Computing Machinery Southeast Conference,April 2004"
18. Bhoi, Sushil Kumar, et al. "Exploring The Security Landscape: A Comprehensive Analysis Of Vulnerabilities, Challenges, And Findings In Internet Of Things (Iot) Application Layer Protocols." Migration Letters 21.S6 (2024): 1326-1342.