Wireless Networks
https://doi.org/10.1007/s11276-022-02917-x

ORIGINAL PAPER

An energy aware secure three-level weighted trust evaluation and grey wolf optimization based routing in wireless ad hoc sensor network

R. Isaac Sajan[1] · V. Bibin Christopher[1] · M. Joselin Kavitha[2] · T. S. Akhila[3]

Accepted: 26 January 2022

Abstract
Due to the widespread application of wireless sensor networks in fields such as healthcare, the battlefield, etc., security has become a prime concern for transmitting information without any data manipulation. For this concern, we introduce a Three-Level Weighted Trust evaluation-based Grey Wolf Optimization (3LWT-GWO) approach for the effective detection of misbehaving nodes and provide an optimal secure route through trusted nodes for delivering the data securely to the destination. The proposed model is categorized into three phases: (a) trust-based clustering, (b) cluster head selection, and (c) optimal data routing. Initially, the sensors are deployed randomly in the region in which the nodes have the initial same energy. Then the clustering of nodes is performed in the first phase by computing the Overall Trust Score (OTS) for each node based on the factors like direct trust, indirect trust, energy trust, Long-term neighbor Recommendation Trust, authentication trust, and link quality trust. This OTS helps to identify unsafe nodes. After the identification of unsafe nodes, clustering is performed. In the second stage, the weight of each node is calculated based on the residual energy, node distance, and energy. Then the node that has the highest weight is nominated as Cluster Head. Next, optimal routing is performed based on the GWO algorithm by computing the Trust Satisfactory degree, distance, energy, and delay. Based on the estimated route, the packet is delivered from the source node to the destination. The performance of the 3LWT-GWO method delivers better results when compared with the prevailing techniques in terms of energy consumption, throughput, network lifetime, accuracy, detection rate, and delay.

Keywords Wireless sensor network · Security · Optimization · Routing · Flooding attack · Trust · Clustering

1 Introduction

Wireless ad hoc sensor network, which is a self-organized type of wireless network includes the various sensing terminals to monitor the environmental conditions, troop deployment, agricultural management, industrial applications, etc. [1]. The network is ad hoc when it does not depend on the preexisting architecture, including routers in wired infrastructure or access points. Instead, the nodes connected are treated as the routers in the network [2]. The tremendous growth in ad hoc networks has pushed the network to be adopted in several wireless applications. To perform data communication, the sensor nodes deployed require energy from their batteries. The larger consumption of energy from the node not only weakens the battery lifespan but also degrades the network performance. Thus, energy-efficient routing techniques are needed to assist in the proper routing of data packets to their destination [3–5].

Security is a potential area of research to facilitate secure data communication among the nodes in an ad hoc environment [6]. Ad hoc Wireless sensor networks (WSN) are most vulnerable to Denial of Service (DoS) attacks and a lot of research has been adopted to improve survivability. A DoS attack depletes the node batteries and limits the

✉ R. Isaac Sajan
isaacsajanr.001@gmail.com

[1] Department of Computer Science and Engineering, Ponjesly College of Engineering, Nagercoil 629003, India

[2] Electronics and Communication Engineering, Marthandam College of Engineering and Technology, Kanyakumari, India

[3] Electronics and Communication Engineering, Mar Phraem College of Engineering and Technology, Kanyakumari, India

Published online: 16 February 2022

availability of network resources by generating unwanted traffic on the network [7]. Vampire attacks are more hazardous and not-protocol specific, even the authenticate user can't predict there is an attack or prevent the malicious activities [8, 9]. The compromised node can alter the entire network structure and can actively perform authentication processes with their neighbors which have no way to differentiate between trusted and fraudulent nodes. There are two classifications of vampire attacks that include attacks on stateless protocols and stateful protocols [10]. The attacks on the stateless routing protocol include stretch and carousel attacks. In the stretch attack, an adversary generates a long route instead of the data transmission taking place on the shortest path. In a carousel attack, the attacker sends the packet through a series of loops such that the specific node appears in the route several times [11]. For the second category, stateless routing protocols know the topology and its state already, so the data forwarding is done based on the stored path. Two categories of stateless routing are malicious discovery and directional antenna attacks. In a directional antenna attack, the packet is redirected unnecessarily and wastes more energy while a malicious discovery attack occurs at route discovery initiated by any node by wrongly calming topology change. These types of attacks rapidly drain a large amount of energy and exhaust the battery life soon.

WSNs have a wide range of applications, ranging from indoor placement in the workplace to outdoor deployment on a tactical battlefield. These networks, however, are prone to a variety of security risks due to their deployment in remote places. If the network is used for other applications, such as in military warfare, the situation becomes even more serious. Node failure is also highly likely in such circumstances because of the resource limits of the sensor nodes. To make this technology usable in realistic environments, certain application criteria must be met. Because of the operation's secrecy and the hostile territory's inaccessibility, it is not always possible to manually restore the energy of the power-constrained sensor equipment throughout the operation.

Due to the self-configuring nature, the nodes are susceptible to various types of security attacks that affect the routing [12]. The attacks caused by malicious nodes disturb the data routing, temporal or permanently stop the communication exchange, and distract the functioning of the network. Cryptography-based security models are not enough for the unique characteristics and challenges that occur in open networks [13]. Although strong cryptographic techniques can provide authentication and integrity, it fails when the authenticated compromised nodes have easy access to the information and secret keys due to insider attacks. Trust-based security has recently emerged as an attractive complement for cryptography which provides a successful relationship and improves security among the nodes [14]. In trust-based approaches, the future actions are predicted based on the previous node behavior and make an effective decision in the detection of malicious nodes. If the node is detected, then the specific node gets isolated and the neighboring nodes are alerted to cooperate with them for data delivery, aggregation, or any other processing functions. Trust-based neighbor selection is also a powerful approach for validating the neighbor nodes and thereby enhancing the privacy and reliability of data transmission [15, 16].

Many recent studies [17–20] have examined malicious node detection and data security in WSN by applying the trust-based paradigm. Trust-based routing algorithms have now been acknowledged as a successful method in recent years and have been employed in a number of research papers to detect malicious nodes [17–20]. To detect malicious nodes, the majority of these studies rely on the indirect and direct trust of nodes. Each node's direct trust is based on the node itself, while its indirect trust is based on its neighbors. Furthermore, Opportunistic Routing (OR) is a newly popular method for protecting WSN [21]. When compared to standard routing protocols, this technology conducts routing operations via the optimal route. OR efficiently transforms weak links into strong ones, providing several advantages over standard transmissions [22]. The fundamental characteristic of OR is that it creates routes depending on the selection of more trustworthy nodes, which are more likely to succeed in routing [23].

Numerous trust-based approaches were presented earlier to overcome the misbehavior attacks on the network. Several challenges are faced in designing the robust trust model [9, 18, 24, 25]. Most of the models do not consider the data forwarding issues caused by poor link quality, faulty nodes, and higher congestion levels. Also, the optimized end-to-end route is determined based on the trusted neighbors and eliminates energy factors. Even though the combination of trust and energy factors are considered in some of the routing models, they do not address the node misbehavior attack [26]. Several secure data aggregation schemes have also been introduced by various researchers [27–30]. Some approaches incur high computational overhead, while trust data exchange may lead to false reporting attacks and minimize the trust rate for the authorized node.

According to existing research works, a single or many factors, such as distance, energy, or power consumption, and connectivity determine the next hop in a routing algorithm. Also, due to the open nature of the wireless network, nodes are vulnerable to various threats, including vampire and flooding attacks. These attacks decrease the energy level of the sensor nodes and prevent the forwarding of data packets. Also, the proper balancing of energy

and security is needed to overcome the unwanted energy depletion of the nodes. It has been demonstrated that selecting nodes based on a variety of factors increases network performance. As a result, recognizing numerous criteria might help nodes in a decentralized and dispersed network make more accurate selections. Since WSNs have features similar to open systems, trust-based procedures established for open systems can be used for WSNs. Current trust-based procedures for WSNs are primarily concerned with security measures such as identifying malicious nodes. However, other factors of trust and reputation in WSNs must be explored without jeopardizing the resources. These concerns motivate us to develop secure and energy-efficient protocol that facilitate real-time data monitoring in environments such as area surveillance and military applications where there is limited opportunity to change recharge or recharge batteries. A Three-level trust evaluation-based weighted Grey wolf optimization algorithm (3LT-WGWO) is developed in this paper by employing more trust factors and security measures for the detection and isolation of compromised nodes.

1.1 The contributions made in this paper are as follows:

- The security is enhanced by computing Direct Trust (DT), Indirect trust (IT), Energy Trust (ET), Long-term neighbor Recommendation Trust, Authentication Trust, and Link quality Trust for each node.
- The indirect trust measure is improved by adding packet reception trust, identical packet trust, and availability trust.
- The three-level trust satisfactory degree is evaluated and a Valid Trust Certificate (VTC) is issued by the BS only for the trusted nodes.
- The energy consumption is reduced by choosing the most efficient transmitting path by using GWO algorithm.
- The proposed method is evaluated by comparing its performance with the existing techniques in terms of residual energy, throughput, delay, detection rate, detection accuracy, energy efficiency, effectiveness, and communication cost.

The remaining sections of this paper are as follows: In Sect. 2, the review of recent papers are delivered, Sect. 3 provides the introduced 3LWT-GWO methodology, Sect. 4 provides the obtained results and comparative analysis, and Sect. 5 gives a brief conclusion of the paper.

2 Related work

Some of the recent approaches modeled in the trust-based secure data transmission and their limitations are listed below.

Yousefpoor et al. [27] proposed a secure data aggregation method in which intra cluster data aggregation, inter-cluster data aggregation, and data transmission are the three steps of this technique. A Fuzzy Scheduling System (FSS) is used to manage the data transmission rate the member nodes during the intra-cluster data aggregation phase. An aggregation tree is built between the cluster head nodes during the inter cluster data aggregation phase. Hasheminejad et al. [28] introduced an aggregation model based on reliable trees. In this method, the sensor nodes are arranged into a binary tree in the suggested technique. Then, using a shared key, aggregation requests are validated, and if the request is accepted, the aggregate phase starts. The error created along the way is discovered hop by hop in the suggested approach, which uses dynamic generator polynomial size. In the event of an error, a retransmission request will be issued to the previous hop. In addition, intermediary nodes perform aggregating functions on the received packages, which reduces the quantity of data transmitted through the network. However, due to the detection of error by hop by hop, the delay in data transmission is increased.

A safe data aggregation approach based on star and tree architectures is proposed by Naghibi et al. [29]. This network is organized into four equal sections geographically, with each part forming a stable star structure. Each node is allocated a parent for data transmission in the Secure Hybrid Structure Data Aggregation (SHSDA) technique. The lightweight symmetric encryption is used to increase data security, and a key is exchanged between each parent node and its offspring. The encrypted data is transmitted from leaf nodes to parent nodes, and through a star structure, it eventually reaches the root. The data is then sent to the base station by a tree structure. Their suggested technique outperforms other methods in terms of flexibility, throughput, packet delivery rate, data delivery latency, and average energy consumption. However, the detection rate is very low. For WSNs, Sharifi et al. [30] proposed a hierarchical routing and data aggregation approach. The network is clustered according to the suggested technique, and some nodes are chosen as cluster heads. A tree is constructed inside backbone-tree nodes after creating a rendezvous region. Through cluster head and backbone-tree nodes, the aggregated data is delivered to the sink. This method has high packet delivery rates, low consumption of energy, and low latency. However, it is not effective against malicious attacks.

For secure transmission, trust-based models are vital in selecting trusted neighbors. AlFarraj et al. [31] discussed an Activation-Function identification of genuine nodes. This model involves two phases, including direct trust assessment and additive metric assessment. At first, the shortest path is estimated based on Dijkstra's algorithm and then the direct trust of the nearby nodes is estimated on the basis of energy as well as trust measures. If the estimated path trust value is larger than the mediate node trust score, then the sequence of the path is estimated. In the second phase, the source nodes preserve the reliable path based on the regression factor credentials and refinement process. Here, two metrics such as path probability and risk assessment metrics are considered. During routing, three steps like path detection, maintenance, and replacement are performed for the transmission by a reliable node.

For the detection of malicious attacks, Terence and Purushothaman [32] presented a Warning Message Counter method (WMC) that identifies the malicious nodes in WSN. Here, the nodes are categorized into (1) sensor nodes, which sense and forward data to the destination, and (2) monitor nodes, which identify the compromised node under its region. For each node, the neighbor list is generated based on broadcasting the hello message, and then the route is discovered with the shortest path based on beacon messages. The destination node sends the acknowledgment message to the source node after receiving the packet. During data dissemination, packet dropping is detected based on the WMC approach. Here, the warning count status is periodically updated in the monitor table. By comparing with the threshold value, the monitor node determines the compromised nodes and sends its list to other nodes in its region. Thus, if a node contains malicious nodes as its neighbors, it discards the node and reconstructs the route by triggering route discovery for data broadcast.

For the network security issues that occurred due to the wormhole and black hole attacks by the presence of malicious nodes, Gomathy et al. [33] introduced a Heterogeneous Cluster-Based Routing (HCBS) mechanism in WSN. Initially, the sensor nodes positioned on the field are clustered and the packet transmission is performed between the base station and cluster. During transmission, the node which is constantly monitoring the transmitting data is considered a malicious node. The node is detected as malicious when the trust factor is less than the MAC Address Translation. The detection efficiency of this model is 96%, which achieves a better energy consumption rate.

A Secure optimal route selection and attack detection are solved in terms of optimization algorithms by Isaac and Jasper [34] who designed a Secured Atom Search Routing (SASR) model. At the first stage, CHs are nominated by the threshold-based energy level and form the clusters. Then, the knowledge base sited in the base station monitors the malicious activity using the invasion discovery system. The data collected from the cluster heads is stored by the KB, and the interference engine generates the rules for the detection process. Next, trust verification is performed to ensure the node's trust in transmitting the data securely to the next node. When the packet transmitted is not received at a specific time interval, then the node trust is calculated for all member nodes by the CH. If the malicious behavior is detected, then an alert message is delivered along with its ID and location to the CH for the isolation of the malicious node. Further, the optimal route selection is performed by the SASR algorithm that considers trust, energy, delay, and distance factors for finding the secured data path for data transmission.

For secure communication and to defend against black hole attacks, Elmahdi et al. [35], modified an ad-hoc on-demand multipath distance vector model. This approach finds the route based on the route discovery process that solves the problem of a link failure in ad hoc networks. During the route discovery process, when the link fails, another route is selected based on the route stored previously. The messages are classified into multiple paths and forwarded to the destination with the shortest distance. An Enhanced Homomorphic Encryption (EHC) is introduced which uses the additive and multiplicative properties of large prime numbers in the generation of the secret key. The encryption scheme is categorized into three main stages, including key generation, encryption, and decryption algorithms. At the final stage of reception, the encrypted parts with the duplicate messages and ID identified are discarded.

To achieve security and energy-intended routing, Kumar et al. [36] presented a security-based Data-Aware Routing Protocol (SDARP) that balances security and prolongs the network lifetime. This model comprises two phases, including Optimal CH and energy-efficient routing. In the first stage, the cluster is molded depending upon the hop distance and total nodes in the network. After the clustering process, CH is selected based on mobility, stability, node capacity, and signal strength. If more than two CHs are elected, then optimal selection of CHs is initiated. The data collected from all the Member Nodes (MN) and nodes that have high pack drops are not considered in future data transmission. For enhancement of the data gathering ratio, the fuzzy algorithm is utilized in the cluster model. In the next phase, energy-aware routing is combined with data security in terms of encryption, and the decryption process is computed to obtain authentication and data integrity.

In terms of security concerns, trust management is a vital factor that evaluates the trust score for the recognition of malevolent users in the WSN. Selvi et al. [18] discussed An Energy-Aware Trust-Based Secure Routing (EATSRA)

algorithm to address the security issues in WSN. This model estimates trust metrics such as residual energy, signal strength, node behavior, and packet delivery ratio. Here, the overall trust factor is estimated between the neighboring nodes to identify the malicious node and isolate it from the network. Also, a random way mobility model is applied to select CH with a low mobility factor. Next, the spatial–temporal constraints are utilized with a decision tree algorithm to select the best-secured path to forward the data to the destination (Table 1).

3 Proposed 3LWT-GWO Methodology

The 3LWT-GWO Methodology has three phases: (a) trust-based clustering, (b) Cluster Head selection, and (c) optimal data routing. Initially, the node is deployed randomly in the network region in which the nodes have the initial same energy.

3.1 Trust-based clustering

Each node stores the Node_ID, next hop_ID, transmitter node ID, and receiver ID. The trust establishment is performed based on the trust score. The estimation of individual trust for each node is listed as follows;

1. Direct Trust (DT)

In order to identify false nodes, each sensor node observes the behavioral patterns of its fixed neighbors. Each behavioral pattern is considered to express the trust of the node. Various trust metrics are integrated to compile the overall trust score. The direct trust score is computed solely based on personal observation.

Specifically, node a will measure the reliability of node b. At time t, the direct trustworthiness of node b is estimated by node a if they are one-hop neighbors. In this case, direct observation results are gathered by node a to evaluate node b. The reliability of a node can be assessed based

Table 1 Summary of the existing trust-based routing schemes

Author	Technique used	Features	Type of attack	Advantages	Disadvantages
Yousefpoor et al. [27]	FSS	Data aggregation	Traffic analysis and eavesdropping attacks	High network lifetime and packet delivery ratio	Computational complexity is high
Hasheminejad et al. [28]	Tree based model	Data aggregation, reliable routing	–	Low energy consumption, high reliability	High delay
Naghibi et al. [29]	SHSDA	Secure data aggregation	Denial of service attack	High flexibility, throughput, and packet delivery rate	Detection rate is very low
Sharifi et al. [30]	Tree and rendezvous based routing	Data aggregation and hierarchical routing	–	high packet delivery rates, low consumption of energy, and low latency	not effective against malicious attacks
AlFarraj et al.[31]	AF-TNS	Trusted neighbors are selected for secure transmission	Node misbehavior attack	Simpler decision making	Trust factor is low
Terence and Purushothaman [32]	WMC	Detects the malicious node	Black hole, gray hole, and sink hole attack	Computational overhead is low	Detection rate is low
Gomathy et al. [33]	HCBS	To perform trust-based secure routing	Black hole and wormhole attack	Detection efficiency is high	High data loss and delay
Isaac and Jasper [34]	SASR	Optimal route selection and secure routing	Carousal, and stretch attack	Knowledge intrusion system reduces the computational complexity	Delay is high
Elmahdi et al. [35]	Modified AOMDV	Intrusion is avoided from the malicious nodes	Black hole attack	PDR is high	Computational complexity is high
Kumar et al. [36]	SDARP	Fuzzy data gathering enhances the data gathering ratio	Worm hole, sink hole attack	Energy efficiency is high	Security is not at the satisfied level
Selvi et al. [18]	EATSRA	Trust scores are estimated for the detection of malicious nodes	DoS attack, Sybil attack, flooding attacks	PDR, delay performance is good	Intrusion detection rate is low

on direct trust by analyzing various factors. These include the following factors:

- Packet reception trust:

If node a checks node b, then the measure of Packets Received (PR) is the specified number of acknowledgments (ACK) transmitted by node b. This measure will not be greater than the ratio of node b. According to the variation of the ratio, node a can tell if node b has malicious behavior. Assuming that the ratio of packets received changes over a series of time periods (t_b, t_{b-1}) and there is no significant difference, then node b is trustworthy.

$$PR_{a,b}(t) = \frac{PR_{a,b}(t) - PR_{a,b}(t-1)}{PR_{a,b}(t) + PR_{a,b}(t-1)} \tag{1}$$

- Identical packet trust:

Due to the wireless environment, it is likely that the same packets may be obtained from various sources, i.e., they may be either directly received from the sender or they may be received from some other node for forwarding. However, it is comprehended that each packet sent by a node has a reference period and can be properly recognized regardless of how likely the whole packet is identical.

$$IPT_{a,b}(t) = \frac{PK_{a,b}(t)}{PK_{a,b}(t) + RD_{a,b}(t)} \tag{2}$$

where $PK_{a,b}(t)$ signifies the required number of transmitted packets and SF$ij(t)$ signifies the redundant number of transmitted packets.

- Availability trust:

Node a sends a HELLO message to node b to check if the packet can be transmitted to node b. If node a gets a HELLO-ACK message from node b, it is assumed that node b is available. The availability trust of the neighboring nodes is computed using Eq. (3).

$$AT_{a,b}(t) = \frac{PAK_{ab}(t)}{PAK_{ab}(t) + NPAK_{ab}(t)} \tag{3}$$

where $PAK_{ab}(t)$ signifies the number of acknowledged packets and $NPAK_{ab}(t)$ signifies the number of packets that are not acknowledged.

$$DT(t) = PR_{a,b}(t) + IPT_{a,b}(t) + AT_{a,b}(t) \tag{4}$$

2. Indirect Trust (IT)

A node that relies on advice provided by neighbors to build an idea about the behavioral patterns of other nodes is called an indirect trust. The trust estimation is performed at a certain time period, which is called a cycle or round. The indirect trust computes the trust of a particular node by neighbor trust degree using Eq. (5).

$$IT(t) = \frac{1}{NE}\sum_{d=1}^{NE} DT(t) \tag{5}$$

where NE denotes the nearby nodes and DT indicates the direct trust score computed by the nearby nodes.

3. Energy Trust (ET)

The power consumption of the genuine node usually has a stable value in the network. However, malicious activities that perform DoS attacks will devour more energy faster than conventional nodes.

Energy is depleted when a data packet is transmitted or received or when a sensor is overhearing traffic from neighboring sensors. The power consumption of a node can be calculated using the subsequent equations:

The loss of energy during the transmission process is determined using Eq. (6).

$$EN_{trx} = \begin{cases} EN_{rt} * e + e * * di^2\, \varepsilon_{fs} & di < di_0 \\ EN_{rt} * e + e * * di^4\, \varepsilon_{mp} & di \geq di_0 \end{cases} \tag{6}$$

where di is the separation distance, e signifies the total number of bits, $di_0 = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}}$, EN_{rt} indicates the energy that is necessary to activate the receiver or transmitter.

The essential energy needed to receive 'e' bits of packets is computed using Eq. (7).

$$EN_{rec} = EN_{rt} * e \tag{7}$$

The total depleted energy or consumed is computed using Eq. (8).

$$EN_{con} = EN_{trx} + EN_{rec} \tag{8}$$

The residual energy can be determined using Eq. (9).

$$EN_{rd} = EN_{\text{int}} - EN_{con} \tag{9}$$

where EN_{int} indicates the initial energy of the sensor.

Based on the above equations, the energy trust of a node can be computed using Eq. (10).

$$ENT = \begin{cases} 0, & EN_{rd} < EN_{thr} \\ 1 - EN_{cons} & else \end{cases} \tag{10}$$

4. Long-term neighbor Recommendation Trust (LNRT)

Only the third-party nodes which have a high priority degree predicted by the outlier detection approach are treated as trusted recommenders. Most of the time it is not possible to have direct communication between the subject and the target node. During these cases, the subject node gets advice from the consultant for trust evaluation. However, it is questionable whether the information that

the subject node obtains is accurate or not. Therefore, it is necessary to estimate the reliability of the recommender to decide whether the information received is true or not. The reliability of the recommender is predicted using Eq. (11).

$$RT = \left| RS_{nei(b)} - RS_{avg(b)} \right| \tag{11}$$

where $RS_{nei(b)}$ indicates the score of node b received from the neighboring node and $RS_{avg(b)}$ indicates the average score of node b.

5. Authentication Trust

The trustworthiness or quality of any node in the WSN is determined to prevent the network from DoS attacks. A DoS attack involves temporary or permanent disruptions to network channels. So, to ensure the reliability of a node, a fixed number of packets are sent and returned by the same sensor node.

For instance, assume two nodes 'a' and 'b' where node 'a' needs to find the trustworthiness of node 'b'. The node 'a' transmits a set of packets (hello) to 'b'. The node 'b' accepts the packets and sends them back to 'a'. If the sum of packets delivered and received by 'a' is equivalent, then node 'b' is trustable.

$$AT = \frac{Pfd_a}{\Pr d_a} \tag{12}$$

where Pfd_a signifies the sum of packets forwarded by node 'a' and $\Pr d_a$ signifies the sum of packets received by node 'a'.

6. Link quality Trust

For this trust, a threshold level is fixed for the best link to identify the misjudging nodes among normal nodes. The trust is used to find the node that the highest level of link quality in terms of less time consumption and high connectivity (Fig. 1).

The distance between the two sensors a and b can be given as

$$dis(s_a, s_b) = \sqrt{(x_a - x_b)^2 + (y_a - y_b)^2} \tag{13}$$

Based on Eq. (13), the link quality of two sensors can be computed using Eq. (14).

$$LQT = \begin{cases} 1, & if \ \ dis(s_a, s_b) \le Rn_{com} \\ 0, & otherwise \end{cases} \tag{14}$$

where Rn_{com} signifies the communication range of the sensor.

The overall trust score is computed using Eq. (15).

$$OTS = DT + IT + ET + LNRT + AT + LQT \tag{15}$$

3.2 Weighted trust CH selection

To avoid the selection of a malicious node as CH, it is necessary to elect a CH that is reliable and efficient. The CH is elected depending on the weight of the node. This weight is determined based on some measures such as distance, trust, and energy.

1. Distance

It is best to select the node that is positioned in the middle of the cluster. The distance between nodes a and the center o with location (a_x, a_y) and (o_x, o_y) is computed using Eq. (16).

$$d(a, o) = \sqrt{(a_x - o_x)^2 + (a_y - o_y)^2} \tag{16}$$

The sensor that is positioned near the cluster center has the highest possibility to become CH.

2. Trust

Trust is a significant metric in this model since it is better to choose a trusted node with less power than an unreliable node with higher power levels. At the time of the first round of voting, each node has a similar initial trust score. The conduct of the sensor nodes may change over time during the next round. Moreover, when determining the weights of nodes, a higher preference is given to the trusted node. Therefore, higher weights are allocated for the trust metric. This is because the nodes with high trusted scores have greater chances of being selected as CH when compared to sensor nodes with lower trust scores. The trust of each node is determined using Eq. (15).

3. Energy

CH does more tasks than CMs. Thus, the sensor with the maximum residual energy level is elected as CH. Each sensor computes its energy weight according to Eq. (17). Then it combines its ID along with the weight and sends a voting message to the neighboring sensors. The sensor node that has the highest weight transmits a message signal. Each sensor waits for time 't' which signifies the competition period before the sensor expresses itself as CM or CH. The competition period should not be too minimum or too long in order to avoid the consumption of more energy.

$$EN_{rd} = EN_{\text{int}} - EN_{con} \tag{17}$$

$$Wt_{(CH)} = \alpha * d(a, u) + \beta * OTS + \gamma * EN_{rd} \tag{18}$$

At the beginning of the process, the nodes do not belong to any clusters. To create a cluster, each node sends a "Hello" packet to its neighbors. Once a node gets this packet, it updates the data with its weight value. The nodes then compare this weight value with others. If the weight of

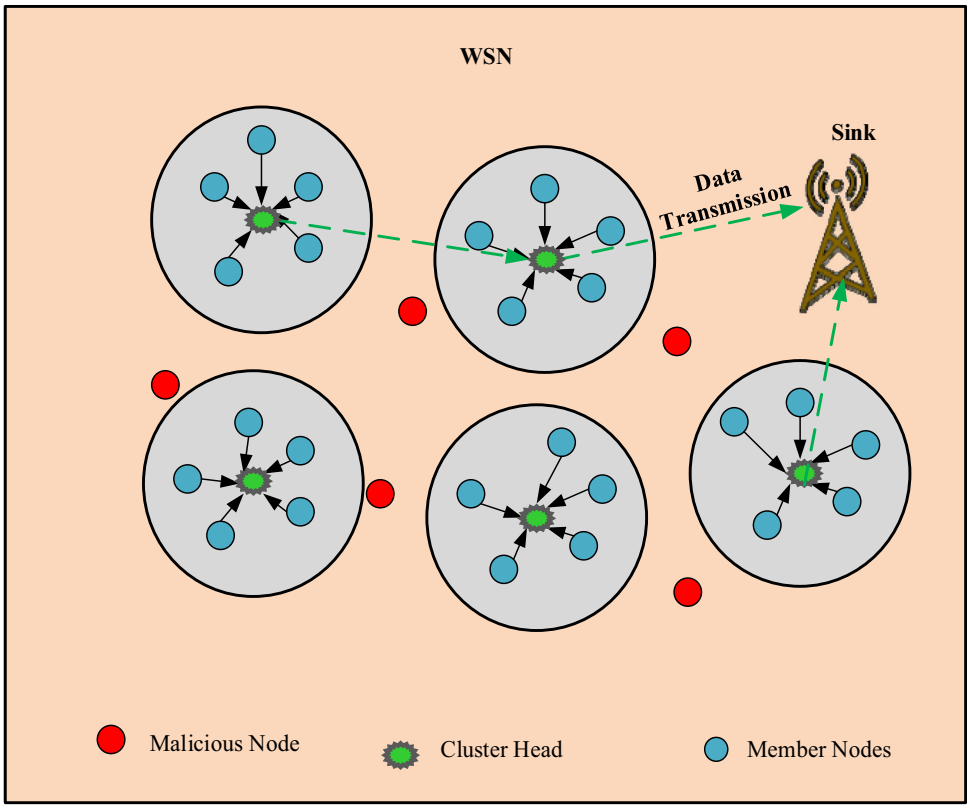

Fig. 1 Cluster formation and CH selection

the node is lower than other nodes, then it waits for an "INVITE" from other nodes that consider themselves as CH. All nodes wait for a time 't' to get an invitation from CH. If the node does not receive any INVITE messages within the provided time period, then it declares itself as CH.

3.3 Optimal data routing

During data transmission, two processes are performed, (1) 3 Level TSD evaluation, and, (2) optimal route selection.

1. 3 Level Trust Satisfactory Degree (3L-TSD) evaluation for Flooding node Detection based on trust validation

Before transmitting the data, the trust validation is performed on three levels that include MN–MN, MN-CH, and CH-BS. Then, the TSD is computed by the base station based on the OTS and $Wt_{(CH)}$. Next, the BS issues the Valid Trust Certificate (VTC) for the only trusted nodes and isolates the misbehaving nodes. Thus, the nodes that hold VTC are only considered in the optimal routing stage. Figure 2 illustrates the optimal secure routing path via trusted nodes established by the proposed model.

2. Optimal route selection

For the selection of the optimal path, we introduce a weighted GWO algorithm that considers factors like TSD, distance, energy, and delay. To improve the search, the high convergence rate and high coverage weight are updated to identify the location of the prey. The proposed algorithm holds the social hierarchy, encircling the prey, hunting, and attacking prey stages to construct the optimal path to catch the prey (destination node). Then the routing path is updated for each node to reach the destination. Based on the best fitness measure obtained from the attacking activity, the optimal route is discovered for data transmission.

Gray wolves are called apex hunters and are placed at the topmost position of the food chain. Typically, the total number of wolves in a group varies from 5 to 12. The front-runners, also termed as alphas, have a female and a male. Alpha is largely accountable for creating verdicts regarding sleeping areas, hunting, waking times, and more. The decision of the Alpha is then uttered to the group. Nevertheless, some forms of behavioral democracy have also been witnessed, in which Alpha trails the other wolves in the group. The Alpha is the most dominant one because his or her commands must be followed by the other wolves. Amusingly, the Alpha is not only the most powerful candidate present in the group but also the finest in controlling the group.

Beta holds the second position in the series of grey wolves. They support Alpha in making decision or some other actions. Beta is considered the most competitive to

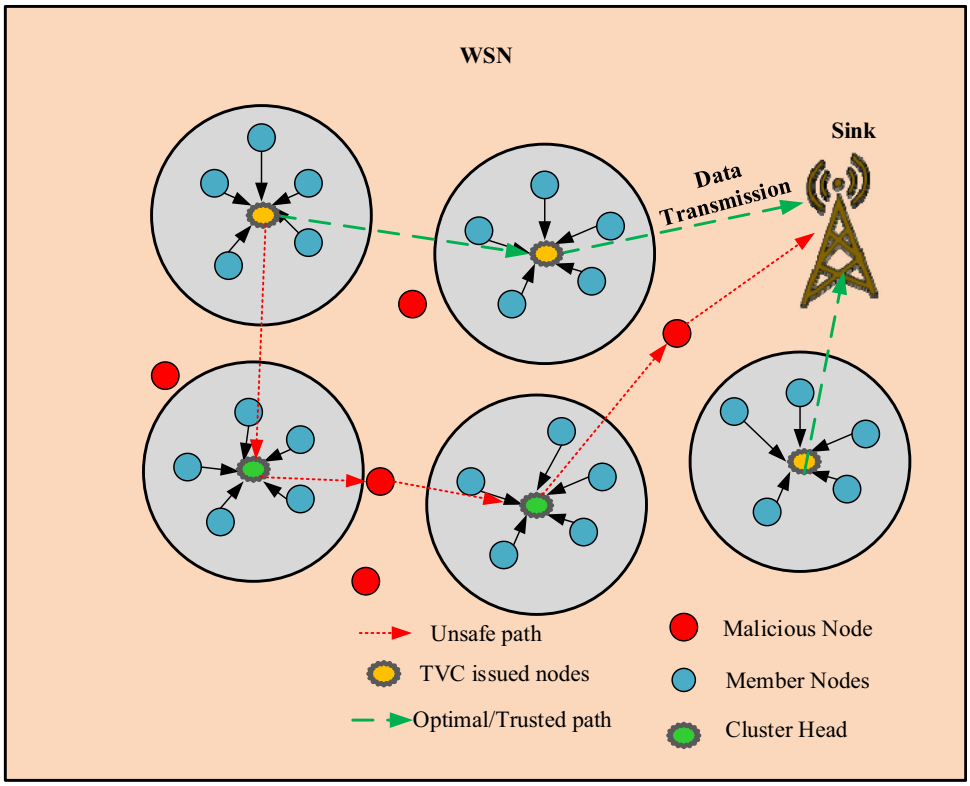

Fig. 2 Flood node detection and optimal route selection phase

become an alpha if an alpha wolf becomes old or dies, and it can be either female or male. The beta wolf follows the commands of Alpha and manages other low-grade wolves. It has the duty to act as a consultant for the alpha and also act as an instructor for the group. They enforces the alpha's rules within the group and criticizes the alpha.

The lowermost grey wolf is named the omega. This type is submissive to all other ruling wolves. These wolves are the last ones indorsed to consume the food. It appears that omega wolves are not an essential factor in the group. However, it has been perceived that the entire group faces inner struggles and complications when omega is lost. This is because of the cruelty and displeasure of all wolves by the omegas. In certain circumstances, the omega also acts as the babysitter in the group.

If the wolf is neither an omega, beta, nor alpha, then they are termed delta. Caretakers, scouts, hunters, seniors, and sentinels participate in this group. Scouts are accountable for monitoring the borders of the terrain and cautioning the other wolves in the event of danger. Sentinels guard and assure protection for the group. Elderly qualified wolves are beta or alpha. Hunters assist betas and alphas when searching for targets and deliver food to the group. Ultimately, the caretaker is liable for taking care of the fragile, sick, and injured wolves.

The main stages that involve gray wolve's hunting strategy are as follows:

- Search, chase, and proximity to prey.
- Chasing, circling, and harassing the animal until it stays still.
- Attacking the prey.

The hunting and social hierarchy of the wolves are mathematically derived using the following steps:

1. Social hierarchy

In GWO, we assume that the optimal solution is alpha (a). As a result, the following two best solutions are termed beta (b) and delta (d), whereas the remaining solution candidates are named omega (x). The hunting in the GWO method is led by a, b, and d. The rest of the x wolves in the group go behind these three wolves.

2. Fitness evaluation

The fitness is evaluated for each node using the formula given in Eq. (19).

$$f(x) = \frac{1}{4}[\alpha D_{des} + \beta T_{tot} + \gamma D + \delta E_{res}] \tag{19}$$

where α, β, γ, and δ represents the weight values such that,$\alpha + \beta + \gamma + \delta = 1$. D_{des} indicates the distance to the destination, T_{tot} indicates the total trust, D denotes delay, and E_{res} indicates remaining energy. The weights of D_{des} and D are provided with lower weight values and the weights of T_{tot} and E_{res} are provided with higher weight

values. The weight value of α is given as 0.05, β as 0.45 and γ as 0.05 and δ as 0.45. After computing the fitness using Eq. (19), the source node transfers the packet to the next-hop neighboring sensor with the best fitness.

3. Surrounding the prey

During hunting, the gray wolves form a circle around the prey. This is mathematically represented in Eq. (20).

$$\vec{M} = \left|\vec{L} \,.\, \vec{W}_{pt(t)} - \vec{W}_{(t)}\right| \tag{20}$$

$$\vec{W}_{(t+1)} = \vec{W}_{pt(t)} - \vec{J} \cdot \vec{M} \tag{21}$$

where $\vec{J}$ and $\vec{L}$ indicates the coefficient vector, t represents the present iteration, $\vec{W}$ represents the grey wolf's location vector, and $\vec{W}_{pt}$ indicates the location vector of the prey. The vector $\vec{J}$ and $\vec{L}$ is computed using Eqs. (22) and (23).

$$\vec{J} = 2\vec{j}.Rn_{(1)} - \vec{j} \tag{22}$$

$$\vec{L} = 2.Rn_{(2)} \tag{23}$$

where $Rn_{(1)}$ and $Rn_{(2)}$ indicates the random vectors whose value lies in between [0, 1], and as the iteration progresses, the value of $\vec{j}$ dwindles from 2 to 0.

4. Hunting

Gray wolves have the skill to know where to find wild animals and surround the prey. The chase is typically led by Alpha. However, Beta and delta may also join the hunt at times. But in a visual space, there is no idea regarding the position of the prey. Therefore, to model the hunting characteristics of gray wolves in mathematical form, delta, beta, and alpha are assumed to be more knowledgeable regarding the possible position of the prey. Thus, the first three finest solutions currently available are stored and other affiliate wolves are guided to renew their location depending on the status of the best search agents. This criterion is expressed in Eqs. (24–30).

$$\vec{M}_a = \left|\vec{W}_a \,.\vec{L}_1 + \vec{W}\right| \tag{24}$$

$$\vec{M}_b = \left|\vec{W}_b \,.\vec{L}_2 + \vec{W}\right| \tag{25}$$

$$\vec{M}d = \left|\vec{W}_d \,.\vec{L}_3 + \vec{W}\right| \tag{26}$$

$$\vec{W}_1 = \vec{W}_a - \vec{J}_1 \,.\, \vec{M}_a \tag{27}$$

$$\vec{W}_2 = \vec{W}_b - \vec{J}_2 \,.\, \vec{M}_b \tag{28}$$

$$\vec{W}_3 = \vec{W}_d - \vec{J}_3 \,.\, \vec{M}_d \tag{29}$$

$$\vec{W}_{(t+1)} = \frac{\vec{W}_1 + \vec{W}_2 + \vec{W}_3}{3} \tag{30}$$

It is perceived that the last location will be in a space inside a circle that is decided by the location of delta, alpha, and beta. In simple terms, the delta, alpha, and beta compute the location of the prey, and the rest of the wolves randomly renew their status around the prey.

5. Confronting prey (exploitation)

The gray wolves terminate the hunt by attacking the victim as soon as it stops stirring. The mathematical model to reach the prey is represented by the parameters $\vec{j}$ and $\vec{J}$. Here, $\vec{J}$ signifies a random value between $[-j,j]$. The location of the next search agent will be between the prey's location and the current location when the range of $\vec{J}$ is [−1, 1].

6. Searching prey (exploration)

Grey wolves habitually explore based on the location of the delta, beta, and alpha. The search argent diverges to the food source when the value of $\vec{J}$ is less than 1 or greater than 1. This mathematically signifies the Grey wolf's exploration process. In the reliability model, a node pays attention to its fixed neighbors to appraise the reliability of these nodes. A node can detect and compare the resources of an adjacent node through direct interactions. When accurate observation is done, a comprehensive history of trust can be obtained by a node. This historical data contains information about the node's connectivity and trustworthiness. Moreover, trust is evaluated on a regular basis with a set time period and trust value is determined based on the manner in which the packets are forwarded. The procedure takes place until the more efficient and safe route to the destination is found. The choice of intermediate nodes is determined in accordance with the reliability (fitness) of the nodes. The flowchart for the GWO algorithm is provided in Fig. 3.

4 Experimental result and performance analysis

The proposed 3LWT-GWO method is simulated on the MATLAB platform and its performance is estimated under flooding attacks in terms of energy consumption, detection accuracy, detection rate, delay, and throughput.

4.1 Evaluation metrics

The metrics used for verifying the performance of the proposed 3LWT-GWO method are given as follows:

(i) Throughput: The number of successfully delivered records in the allotted time is termed throughput and is given in bits per second.

$$THR = \frac{Pk_{del}}{t} \tag{31}$$

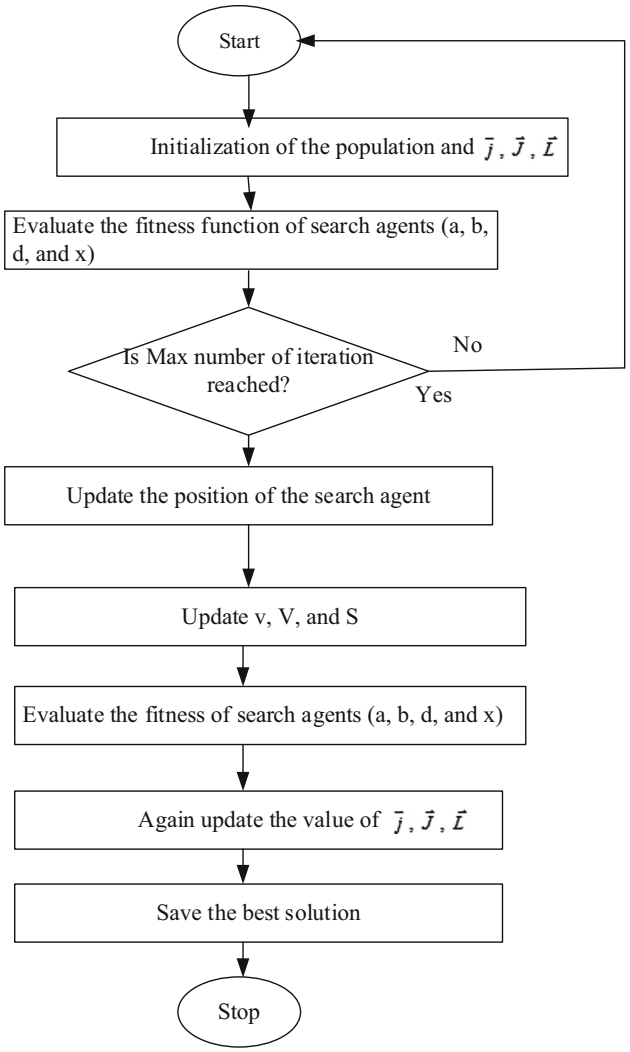

Fig. 3 Flowchart for GWO algorithm

where Pk_{del} denotes the sum of delivered packets and t signifies the time period.

(ii) Delay: The time spent waiting for the data packet to arrive at its destination is termed as delay. It is computed using Eq. (32).

$$DLY = \frac{T_{avr} - T_{snd}}{q} \tag{32}$$

where q indicates the number of connections, T_{avr} signifies the time of arrival, and T_{snd} is the time at which the packet was sent.

(iii) Energy: The total energy consumed is equivalent to the sum of energy dissipated during reception and transmission of packets. This is found using Eq. (33).

$$EN_{con} = EN_{trx} + EN_{rec} \tag{33}$$

where EN_{trx} indicates the energy dissipated during transmission and EN_{rec} indicates the energy dissipated during the reception.

(iv) Detection Rate: It is the successful detection of malevolent nodes present in the network and is computed using Eq. (34).

$$DR = \frac{D_{mal}}{ACT_{mal}} \times 100 \tag{34}$$

where D_{mal} indicates the detected number of malicious sensors and ACT_{mal} denotes the actual number of malicious sensors.

(v) Detection accuracy: This term signifies the relation between actual results and the predicted outcome. It is computed using Eq. (35).

$$D_{acc} = (TP + TN)/(TP + TN + FP + FN) \tag{35}$$

where TP and TN represent true positive and true negative respectively, and FP and FN represent false positive and false negative respectively.

4.2 Simulation setup

The performance of the 3LWT-GWO technique is verified on the MATLAB platform by setting up 100 sensors in 100 m × 100 m area. Each node has a communication range of 30 m, 0.01 J transmission energy, 0.01 J receiving energy, and initial energy of 1 J. The sink is positioned at (100, 10), the antenna type is Omnidirectional (CR-OMN2409) that has a frequency bandwidth of 2.4 GHz, and the data packet size is taken as 512 bytes, and the simulation time is 500 s. The attack is performed by flooding the node with RREQ packets. The other simulation parameters are listed in Table 2.

4.3 Result analysis

The 3LWT-GWO routing method is compared with the recent techniques such as SASR [34], AF-TNS [31], Modified AOMDV [35], SDARP [36], and EATSRA [18].

The lifetime of the WSN depends on the energy depleted during the transmission of the data. Figure 4 provides the analysis conducted for determining the remaining energy of the nodes by changing the number of mischievous sensors from 10 to 50%. The results of the proposed 3LWT-GWO are then compared with the recent techniques like SASR [34], AF-TNS [31], Modified AOMDV [35], SDARP [36], and EATSRA [18]. The remaining energy when 10% malicious nodes for the proposed 3LWT-GWO and the existing techniques SASR [34], AF-TNS [31], Modified AOMDV [35], SDARP [36], and EATSRA [18] are 98%,97%, 95%, 94.5%, 91%, and 88% respectively. However, when the number of malicious

Table 2 Parameters of the network

Parameters	Value
Compared methods	AF-TNS [31], SASR [34], Modified AOMDV [35], SDARP [36], and EATSRA [18]
Network area	$100m \times 100m$
Location of the base station	(100,10)
Sensors in the network	100
CH's communication range	50 m
Member node's communication range	30 m
Sensor node's initial energy	1.0 J
ε_{mp}	0.0013 pJ/bit/m^2
ε_{fs}	10 pJ/bit/m^2
E_{elec}	50 nJ/bit
Malicious nodes	10 to 50
Receiving and transmission energy	0.01 J
Data packet size (bytes)	500

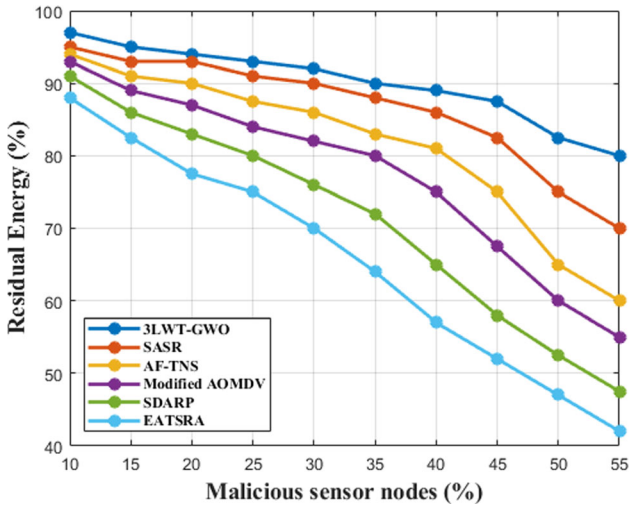

Fig. 4 Energy Consumption analysis by deploying mischievous nodes from 10 to 50%

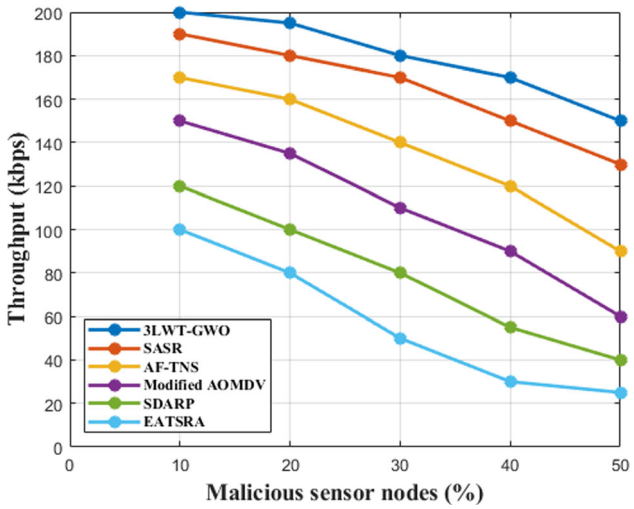

Fig. 5 Throughput analysis by deploying malicious nodes from 10 to 50%

nodes is increased, the residual energy is also decreased. When the network is deployed with 55% of malicious nodes, the EATSRA method has the lowest residual energy of 43% among the existing techniques, whereas the proposed method has the highest residual energy of 80%. From the results, it is evident that the proposed 3LWT-GWO method has more residual energy even under the presence of several malicious nodes. This is due to the elimination of flooding attack nodes that cause a severe drop in energy.

The throughput of the proposed 3LWT-GWO method is analyzed in Fig. 5. Here, the throughput declines as the number of anti-nodes rises. But, the presented 3LWT-GWO method has considerably higher throughput compared with the existing SASR [34], AF-TNS [31], Modified AOMDV [35], SDARP [36], and EATSRA [18] methods. In the event of malicious attacks, the findings clearly indicate that the proposed 3LWT-GWO algorithm has a greater average throughput than other methods. The throughput of the SASR [34], AF-TNS [31], Modified AOMDV [35], SDARP [36], and EATSRA [18] methods under the presence of 50% malicious nodes is 130 kbps, 90 kbps, 60 kbps, 40 kbps, and 22 kbps respectively. The collected findings demonstrate that the proposed routing algorithm outperforms the current routing methods with high throughput of 148 kbps. Since the existing methods are unable to effectively detect the malicious nodes, more packets may be lost during the routing process. Malicious sensors are identified and packet losses are reduced in the proposed 3LWT-GWO algorithm. However, since the

nodes have a higher risk of connection failure, the existing methods have a lower throughput than the proposed 3LWT-GWO algorithm.

Figure 6 presents the outcome obtained for the delay analysis under 10% to 50% of malicious nodes. Here, delay signifies the time interval taken for a source node to deliver the packet to the final destination. Existing methods such as SASR [34], AF-TNS [31], Modified AOMDV [35], SDARP [36], and EATSRA [18] have longer end-to-end packet transfer delays than the proposed 3LWT-GWO method. Even though the delay seems to increase as the number of malicious sensors increases, the proposed 3LWT-GWO method has taken less time (0.019 s) to deliver the packets than the rest of the methods like AF-TNS (0.055 s), SASR (0.049 s), Modified AOMDV (0.043 s), SDARP (0.035 s), and EATSRA (0.022 s). The existing techniques have a longer delay than the proposed 3LWT-GWO method due to the increased likelihood of connection failure. The delay analysis demonstrates data is transmitted more quickly with the proposed 3LWT-GWO method with an average delay of 0.092 s. This is due to the optimal and shortest route selection by the GWO algorithm.

The results obtained by analyzing the detection rate under the presence of malicious nodes are presented in Fig. 7. This outcome depicts that when the network has 10% malicious nodes, the detection rates of all the methods are similar. But when the malicious sensors is gradually raised, the detection rate of the methods declines. The detection rate of all the existing methods such as SASR [34], AF-TNS [31], Modified AOMDV [35], SDARP [36], and EATSRA [18] has higher detection rate of 100%. When the malicious sensors are raised to 50%, the detection rate of the existing SASR [34], AF-TNS [31], Modified AOMDV [35], SDARP [36], and EATSRA [18] are reduced to 90%, 85%, 80%, 75%, and 70% respectively. However, the detection rate of the proposed 3LWT-GWO method is 93%. The experimental findings demonstrate that the proposed 3LWT-GWO algorithm's effectiveness in detecting malicious nodes is promising. The reason for the increased detection rate is due to the ability to detect malicious nodes during the clustering and routing processes.

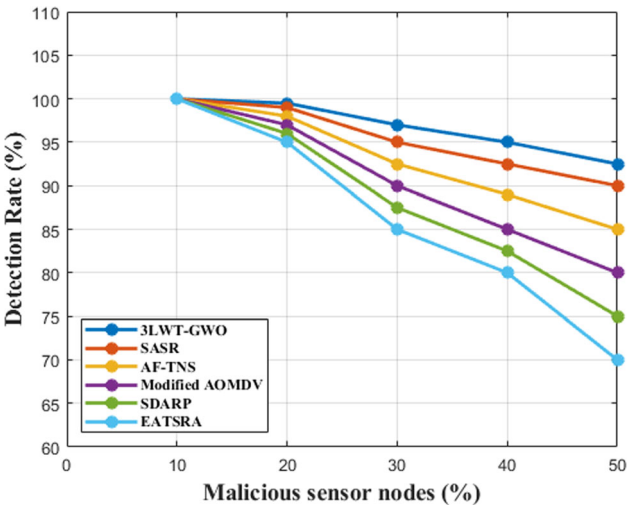

Fig. 7 Detection rate analysis by deploying malicious nodes from 10 to 50%

Figure 8 showcases the comparative results obtained for accuracy by varying the number of anti-nodes. Here, the accuracy of the 3LWT-GWO is perceived to be greater than other algorithms like SASR [34], AF-TNS [31], Modified AOMDV [35], SDARP [36], and EATSRA [18]. Among the existing algorithms, EATSRA shows poor

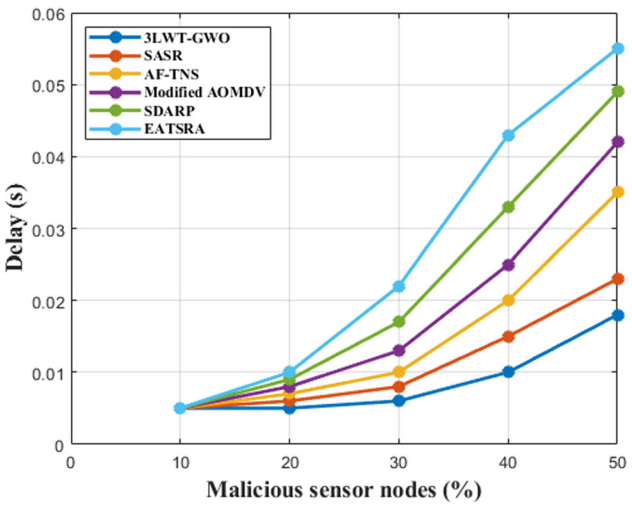

Fig. 6 Delay analysis by deploying mischievous nodes from 10 to 50%

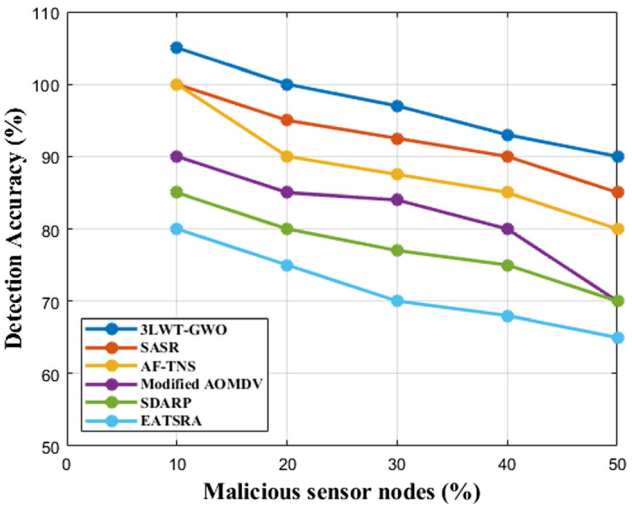

Fig. 8 Detection accuracy analysis by deploying mischievous nodes from 10 to 50%

accuracy results of 65%, whereas the accuracy of the proposed method is 90%. This is because, the combination of various trust measures in the proposed 3LWT-GWO algorithm like direct trust, indirect trust, energy trust, long-term neighbor recommendation trust, authentication trust, and link quality trust helps to detect and separate anti-nodes from the network.

Figure 9 signifies the efficiency analysis conducted for the proposed and the existing methods. The energy efficiency is increased as the number of nodes is increased. When the proposed method is compared with the existing methods, the energy efficiency of the proposed 3LWT-GWO algorithm is above 70% which is higher than the rest of the existing methods like SASR [34], AF-TNS [31], Modified AOMDV [35], SDARP [36], and EATSRA [18]. The SASR algorithm has the second best results (62%) followed by SASR [34], AF-TNS [31], Modified AOMDV [35], SDARP [36], and EATSRA [18]. Also, as the number of nodes are increased, the energy efficiency is also increased. The improved efficiency of the proposed method is due to the optimal route selection based on trust, distance, delay, and energy by the GWO algorithm.

The effectiveness of the proposed algorithm as given in Fig. 10 is determined based on the number of alive sensor nodes as the number of rounds is increased. As the number of rounds is increased, the number of alive sensors are decreased. However, the proposed 3LWT-GWO algorithm has more number of alive nodes compared to the existing algorithms. The number of alive nodes for the proposed 3LWT-GWO algorithm drops to zero after 3000 rounds whereas the number of alive nodes for the existing SASR algorithm drops to zero after 2500 rounds. The algorithm that is less effective is EATSRA in which the energy of all the nodes are depleted within 700 rounds. The trust based clustering, trust based CH selection, and the optimal routing selection in the proposed algorithm eliminates the nodes that cause flooding attack. This increases the number of rounds.

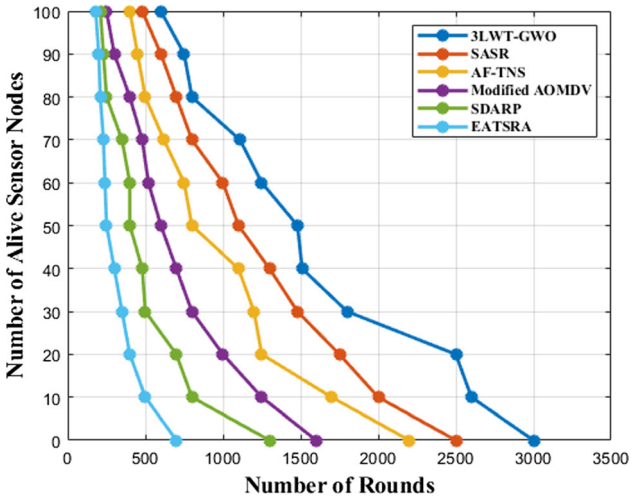

Fig. 10 Effectiveness analysis

The communication cost analysis of the proposed method is provided in Fig. 11. The analysis results show that the cost of the proposed method is very low compared to other existing algorithms. Communication cost is the number of messages a node has to handle in order to deliver the message and perform trust evaluation. The communication cost is determined by varying the trust threshold value. Based on the analysis, it is perceived that the communication cost of the proposed method is low compared to the existing techniques. Whereas EATSRA has the highest communication cost among all the methods. The communication cost for the existing methods are high because of the encryption and decryption process. Whereas, the communication cost of the proposed 3LWT-

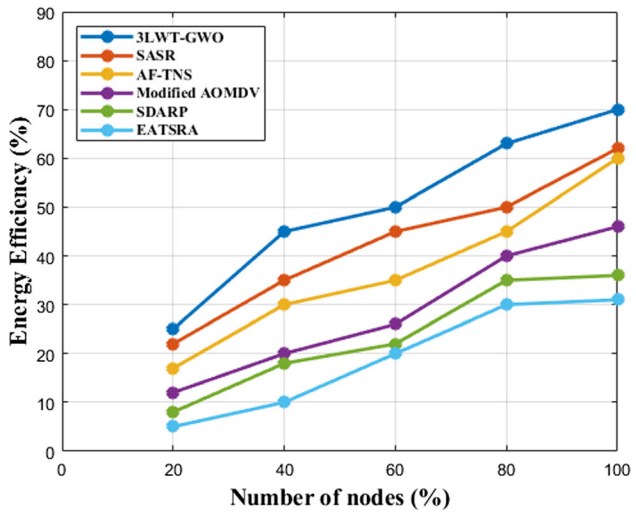

Fig. 9 Efficiency analysis

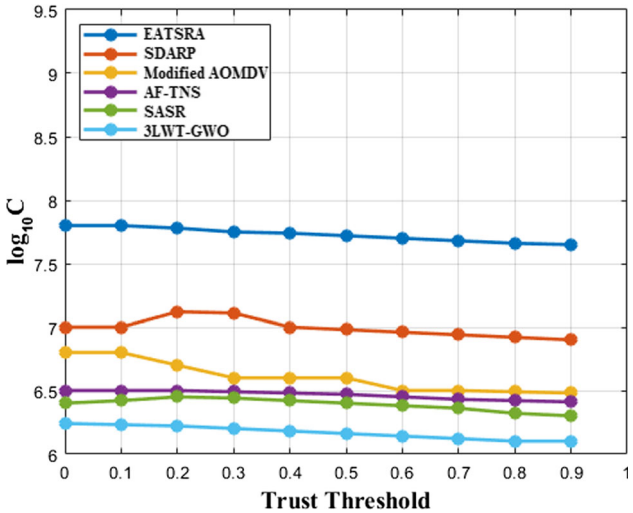

Fig. 11 Communication cost analysis

GWO algorithm is reduced since the proposed method does not use any key management/ encryption algorithms.

5 Conclusion

In any communication network, data security is the most stressed issue. However, it is a difficult task on WSN. Among the several kinds of attacks, flooding is one of the prime factors that depletes more energy and causes service denial. Security in this kind of network can be attained by introducing a proper routing technique. Therefore, this paper presents a novel 3LWT-GWO routing method to eliminate the mischievous nodes and transfer the data packet through a reliable path. The proposed 3LWT-GWO routing method has three stages: (a) trust-based clustering, (b) Cluster Head selection, and (c) optimal data routing. The trust-based cluster formation and CH selection at the first two stages provide added security to the network and the optimal route selection by the GWO algorithm at the third stage helps to tract the most reliable and efficient route for transferring the data. The superiority of the proposed 3LWT-GWO routing method is analyzed by comparing it with the prevailing well-known recent techniques. Based on the outcomes, it is proven that the 3LWT-GWO routing method outperforms other methods in terms of throughput, delay, energy consumption, accuracy, and detection ratio. This protocol can be applied to ground surveillance systems to warn military commanders by collecting data from targets of interest in hostile areas. Such missions often pose a high level of risk for humans. As a result, the military's capacity to launch unmanned surveillance missions using WSN is hugely beneficial. A surveillance system must be able to get the present location of a vehicle with acceptable precision in order to successfully detect, classify, and track it. This protocol collects the data, blocks the malicious nodes, and sends the data to a remote base station via an optimal path. Future work may focus on developing the optimization technique with faster convergence. Also, we will try to improve the data aggregation process by employing techniques like watermarking and digital signatures to assure data integrity.

Acknowledgements Not applicable.

Authors contribution All the authors have participated in writing the manuscript and have revised the final version. All authors read and approved the final manuscript.

Funding There is no funding for this study.

Declarations

Conflict of interest Authors declares that they have no conflict of interest.

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

Consent to participate There is no informed consent for this study.

Consent for publication Not applicable.

References

1. Shahbaz, A. N., Barati, H., & Barati, A. (2021). Multipath routing through the firefly algorithm and fuzzy logic in wireless sensor networks. *Peer-to-Peer Networking and Applications, 14*(2), 541–558.
2. Desai, R., Patil, B. P., & Sharma, D. P. (2017). Routing protocols for mobile ad hoc network: A survey and analysis. *Indonesian Journal of Electrical Engineering and Computer Science, 7*(3), 795–801.
3. Aadil, F., Raza, A., Khan, M. F., Maqsood, M., Mehmood, I., & Rho, S. (2018). Energy aware cluster-based routing in flying ad-hoc networks. *Sensors, 18*(5), 1413.
4. Mosavifard, A., & Barati, H. (2020). An energy-aware clustering and two-level routing method in wireless sensor networks. *Computing, 102*(7), 1653–1671.
5. Hajipour, Z., & Barati, H. (2021). EELRP: Energy efficient layered routing protocol in wireless sensor networks. *Computing*, *103,* 2789–2809.
6. Rani, A., & Kumar, S. (2017). A survey of security in wireless sensor networks. In *2017 3rd international conference on computational intelligence and communication technology (CICT)* (pp. 1–5). IEEE.
7. Yadav, K. S., & Tamboli, M. (2017). Defending against path-based denial of service attack in wireless sensor network. In *International conference on examination in modern technology and engineering (ICEMTE)* (Vol. 5, No. 3, pp. 46–51).
8. Panda, S. N. (2018). GPS hash table based location identifier algorithm for security and integrity against vampire attacks. In M. U. Bokhari, N. Agrawal, & D. Saini (Eds.), *Cyber security* (pp. 81–89). Springer.
9. Isaac Sajan, R., & Jasper, J. (2021). A secure routing scheme to mitigate attack in wireless adhoc sensor network. *Computers and Security, 103*, 102197.
10. Kumari, R., & Sharma, P. K. (2018). A silver-coated scheme for detection and prevention against vampire attack in wireless sensor network. In V. Janyani, M. Tiwari, G. Singh, & P. Minzioni (Eds.), *Optical and wireless technologies* (pp. 547–555). Springer.
11. Sharma, M. K., & Joshi, B. K. (2017). Detection and prevention of vampire attack in wireless sensor networks. In *2017 International conference on information, communication, instrumentation and control (ICICIC)* (pp. 1–5). IEEE.
12. Mittal, N., Singh, S., Singh, U., & Salgotra, R. (2021). Trust-aware energy-efficient stable clustering approach using fuzzy type-2 Cuckoo search optimization algorithm for wireless sensor networks. *Wireless Networks, 27*(1), 151–174.
13. Hamsha, K., & Nagaraja, G. S. (2019). Threshold cryptography based light weight key management technique for hierarchical WSNs. In *International conference on ubiquitous communications and network computing* (pp. 188–197). Springer.
14. Labraoui, N., Gueroui, M., & Sekhri, L. (2016). A risk-aware reputation-based trust management in wireless sensor networks. *Wireless Personal Communications, 87*(3), 1037–1055.

15. Malik, S. K., Dave, M., Dhurandher, S. K., Woungang, I., & Barolli, L. (2017). An ant-based QoS-aware routing protocol for heterogeneous wireless sensor networks. *Soft computing, 21*(21), 6225–6236.
16. Fang, W., Zhang, W., Yang, W., Li, Z., Gao, W., & Yang, Y. (2021). Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks. *Digital Communications and Networks, 7*, 470–478.
17. Khan, T., Singh, K., Abdel-Basset, M., Long, H. V., Singh, S. P., & Manjul, M. (2019). A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks. *IEEE Access, 7*, 58221–58240.
18. Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Nehemiah, H. K., & Kannan, A. (2019). An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. *Wireless Personal Communications, 105*(4), 1475–1490.
19. Shahidinejad, A., & Barshandeh, S. (2020). Sink selection and clustering using fuzzy-based controller for wireless sensor networks. *International Journal of Communication Systems, 33*(15), e4557.
20. Gilbert, E. P. K., Baskaran, K., Rajsingh, E. B., Lydia, M., & Selvakumar, A. I. (2019). Trust aware nature inspired optimised routing in clustered wireless sensor networks. *International Journal of Bio-Inspired Computation, 14*(2), 103–113.
21. Lyu, C., Zhang, X., Liu, Z., & Chi, C. H. (2019). Selective authentication based geographic opportunistic routing in wireless sensor networks for Internet of Things against DoS attacks. *IEEE Access, 7*, 31068–31082.
22. Kumar, N., & Singh, Y. (2017). Trust and packet load balancing based secure opportunistic routing protocol for WSN. In *2017 4th International conference on signal processing, computing and control (ISPCC)* (pp. 463–467). IEEE.
23. Bangotra, D. K., Singh, Y., Selwal, A., Kumar, N., Singh, P. K., & Hong, W. C. (2020). An intelligent opportunistic routing algorithm for wireless sensor networks and its application towards e-healthcare. *Sensors, 20*(14), 3887.
24. Habib, M. A., Saha, S., Razzaque, M. A., Mamun-Or-Rashid, M., Hassan, M. M., Pace, P., & Fortino, G. (2020). Lifetime maximization of sensor networks through optimal data collection scheduling of mobile sink. *IEEE Access, 8*, 163878–163893.
25. Fang, W., Zhang, W., Chen, W., Pan, T., Ni, Y., & Yang, Y. (2020). Trust-based attack and defense in wireless sensor networks: A survey. *Wireless Communications and Mobile Computing, 2020*, 1–20.
26. Mehmood, G., Khan, M. Z., Waheed, A., Zareei, M., & Mohamed, E. M. (2020). A trust-based energy-efficient and reliable communication scheme (trust-based ERCS) for remote patient monitoring in wireless body area networks. *IEEE Access, 8*, 131397–131413.
27. Yousefpoor, E., Barati, H., & Barati, A. (2021). A hierarchical secure data aggregation method using the dragonfly algorithm in wireless sensor networks. *Peer-to-Peer Networking and Applications, 14*, 1–26.
28. Hasheminejad, E., & Barati, H. (2021). A reliable tree-based data aggregation method in wireless sensor networks. *Peer-to-Peer Networking and Applications, 14*(2), 873–887.
29. Naghibi, M., & Barati, H. (2021). SHSDA: Secure hybrid structure data aggregation method in wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing, 12*, 1–20.
30. Sharifi, S. S., & Barati, H. (2021). A method for routing and data aggregating in cluster-based wireless sensor networks. *International Journal of Communication Systems, 34*(7), e4754.
31. AlFarraj, O., AlZubi, A., & Tolba, A. (2018). Trust-based neighbor selection using activation function for secure routing in wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing*, *2018,* 1–11.
32. Terence, J. S., & Purushothaman, G. (2019). A novel technique to detect malicious packet dropping attacks in wireless sensor networks. *Journal of Information Processing Systems, 15*(1), 203–216.
33. Gomathy, V., Padhy, N., Samanta, D., Sivaram, M., Jain, V., & Amiri, I. S. (2020). Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks. *Journal of Ambient Intelligence and Humanized Computing, 11*(11), 4995–5001.
34. Isaac Sajan, R., & Jasper, J. (2020). Trust-based secure routing and the prevention of vampire attack in wireless ad hoc sensor network. *International Journal of Communication Systems, 33*(8), e4341.
35. Elmahdi, E., Yoo, S. M., & Sharshembiev, K. (2020). Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks. *Journal of Information Security and Applications, 51*, 102425.
36. Kumar, K. V., Jayasankar, T., Eswaramoorthy, V., & Nivedhitha, V. (2020). SDARP: Security based Data Aware Routing Protocol for ad hoc sensor networks. *International Journal of Intelligent Networks, 1*, 36–42.

R. Isaac Sajan was born in Kanyakumari, India, in 1984. He received his B.E., M.E., and Ph.D degrees in Computer Science and Engineering from Anna University, Chennai, India, in 2006, 2008 and 2021. Currently he is working as an Associate Professor in Department of Computer Science and Engineering, Ponjesly College of Engineering, Nagercoil, India. His-current research interests include Wireless Sensor Networks, Mobile Computing, Cloud Computing, Wireless Communications in general and Artificial Intelligence.

V. Bibin Christopher was born in Kanyakumari, India, on April 5,1985. He received his B.E. degree in Electrical Engineering 2006. He received his M.E and Ph.D degree in Computer Science and Engineering from Anna University, Chennai, India, in 2009 and 2021. Currently he is working as an Associate Professor in Ponjesly College of Engineering, Nagercoil, India. His current research interests include Wireless Sensor Networks, Mobile Computing, and Network Security.

M. Joselin Kavitha received her B.E. degree in Electronics and Communication Engineering and M.E. degree in Communication System from Anna University, India, in 2008 and 2010 respectively. She is an assistant professor in Marthandam College of Engineering and Technology, India. Her research interests are Wireless Sensor Networks, Wireless Communication and VLSI Design.

T. S. Akhila received her B.E. degree in Electronics and Communication Engineering and M.E. degree in Embedded System Technologies from Anna University, India, in 2009 and 2011 respectively. She is an assistant professor in Mar Ephraem College of Engineering and Technology, India. Her research interests are Wireless Sensor Networks, Wireless Communication, VLSI Design and Embedded System.