Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7766303

OTSAR: AN OPTIMAL TRUSTED SECURITY AWARE ROUTING TECHNIQUE FOR WWIRELESS SENSOR NETWORK USING EFFICIENT CLUSTERING APPROACH

Vasanthamma G[1], Dr.R.Balakrishna[2]
[1]Associate Professor, Dept of CSE, PDIT, Hospet & Research Scholar,Dept of CSE,RRCE,VTU, gvasreddy@gmail.com
[2]Professor & Principal , Dept of CSE, Rajarajeswari College of Engineering, Bangalore -74, rayankibala@gmail.com

Abstract
Secure routing is essential in wireless sensor networks (WSNs) because these networks are frequentlypositioned in antagonisticsurroundings where security threats such as node compromise, tampering, and eavesdropping can occur. Secure routing is necessary to protect the WSN against malicious attacks that can compromise the discretion, honesty, and accessibility of the data transmitted in the nets. Thus, the need for secure routing is crucial to ensure the reliable and secure operation of WSNs in numerousrequests such as military investigation, healthcare monitoring, and environmental monitoring, among others.In this study, we propose a technique called Optimal Trusted Security Aware Routing (OTSAR) for Wireless Sensor Networks (WSN) that ensures secure data transfer between nodes through intermediate nodes. To achieve this, we first introduce the Laplacian Grey Wolf Optimization (LGWO) algorithm for load-balanced clustering based on node information such as location and mobility. Next, we use the Improved Kernel Ridge Regression (IKRR) algorithm to calculate the trust degree of each node in the cluster and select the cluster head (CH). The routing is then performed through highly trusted intermediate CHs to ensure secure data transmission and defend against internal attacks. We appraise the presentation of the proposed OTSAR technique finished various imitation scenarios and compare the results with existing state-of-the-art routing schemes to demonstrate its effectiveness.

Keywords: trust degree, secure routing, energy efficiency, clustering, cluster head

1. Introduction

A network of inexpensive, small sensor nodes known as a wireless sensor network (WSN) are equipped with sensors, processing capabilities, and wireless communication interfaces [1][2]. These nodes are typically distributed in a geographic area and communicate with each other to gather data about the environment, such as infection, moistness, light, and sound. The information gathered by the sensor hubs utilized for a variability of submissions, counting environmental nursing, industrial automation, healthcare, and military surveillance [3]. WSNs are often used in situations where traditional wired networks are impractical or impossible to deploy, such as in remote areas or harsh environments. Security in WSN refers to the protection of the data and communiqué exchanged amongst the nodes in the net from unauthorized access, modification, and destruction. Due to the open wildlife of wireless communication, WSNs are susceptible to numeroussanctuary threats such as snooping, data meddling, node capture, and denial-of-service occurrences [4]. Thus, ensuring the security of WSN is critical to maintaining the concealment, truthfulness, and accessibility of the data transmitted over the net [5].

Different security mechanisms [6][7] are encryption, authentication, key management, and interruption detection/prevention schemes are employed to protected the WSNs. Secure routing in WSN refers to the procedure of choosing and establishing a secure path for data broadcastfrom a network's source node to its terminus node while maintaining the confidentiality, integrity, and availability of the transmitted data. It involves ensuring that the data is not intercepted or modified by an attacker during transmission and preventing attacks such as data injection, eavesdropping, and tampering. Secure routing schemes [8] use cryptographic techniques and authentication mechanisms to establish secure communication between nodes and prevent unauthorized access to the network. The problem in secure routing is to find a safe and efficient path among the source and terminus nodes in a WSN, while ensuring data confidentiality, integrity, and availability, and also preventing unauthorized access, tampering, and other security attacks. Secure routing faces many challenges are limited resources, dynamic network topology, unreliable communication links, and malicious attacks from inside or outside the network. These challenges make it difficult to design and implement secure routing protocols that provide end-to-end security and preserve network resources [9].

Trusted routing [10] is a technique in WSNs that aims to ensure the secure and reliable transfer of data between sensor nodes through intermediate nodes, called cluster heads (CHs). In trusted routing, nodes that have been deemed trustworthy are chosen as CHs, and routing is performed through these highly trusted nodes to safeguard the secure and dependable transfer of data. The trustworthiness of a node is typically based on factors such as its history of successful data transfers, its battery level, and its location within the network. By using trusted routing techniques, WSNs can defend against internal attacks and ensure that sensitive data is securely transmitted.Trusted routing also has some drawbacks, such as: Trusted routing algorithms [11] can be complex and difficult to implement, requiring significant computational resources and expertise. As the size of the network grows, it becomes increasingly difficult to manage and maintain trust relationships between nodes, which can reduce the scalability of the system. Trusted routing algorithms can introduce additional overhead, such as the need for nodes to exchange trust information, which can increase communication and computation costs. Trusted routing can be vulnerable to attacks that target the trust management mechanisms, such as false or malicious information being introduced into the network, or nodes being compromised or impersonated [12]. There is currently no widely accepted standard for trusted routing in WSNs, which can make it difficult to develop interoperable and secure systems.

The Trust-based Co-operative Authentication Bitmap Routing Protocol (TCABRP) [13].Energy Optimized Secure Routing [14] A Summary Trust Estimation Model for Malica Node Identification and Isolesal The Routing Protocol uses a multi-facting strategy that considering a node and the remaining energy length and path length. Biostimulation and trust-based C Select Based C Selection Applicable for WSN. Each node is designed and used the Bat optimization algorithm (BOA) [15] to select from and a trust-level to calculate the trust level. WSN is supported by the multi-objective ant-colony optimization (SRPMA) secure routing protocol [16]. The multi-objective routing algorithm known as the ant colony algorithm was developed as a multi-objective routing algorithm as two optimization goals and trustworthy of the root lanes information with two objective activities. The reliable and secure scheme [17] uses data packets to select a node and the double-guarantee scheme for WSNs to select a node. Reliable Energy and Aware Security routing (ESRT) Scheme [18] Retaining a

reliable environment and separate the nodes of misfortune. Activation Function Based Trusted Neeber Class (AF-TNS) [19] The resource-manager is used for resource-managed WSNs to improve network security. To find physical layer attacks in the WSN, the tampering and tampering Attack (SBTN-TC) [20] is used a security technology that uses a reliable node.

Our contributions.The proposed OTSAR technique for WSN is designed to ensure secure data transfer between nodes through the intermediate nodes in a WSN network. Here is a brief description of the proposed OTSAR technique:

1. Load balanced clustering: The first step is to efficiently cluster the nodes based on their location and mobility using the Laplacian Grey Wolf Optimization (LGWO) algorithm, which ensures balanced load distribution among the clusters.
2. Trust computation: Once the clusters are formed, the trust grade of each node in the cluster is calculated using the Improved Kernel Ridge Regression (IKRR) algorithm. This computation helps in identifying the trusted nodes in the cluster which will become the Cluster Head (CH).
3. Secure data transmission: The routing procedure is approved out through the highly trusted intermediate CHs, which ensures secure data transmission and defends against internal attacks. This technique ensures that data is securely transferred between the foundation and the terminus through the trusted intermediate nodes.
4. Performance evaluation: Finally, the presentation of the planned OTSAR technique is appraised through unalike simulation situations, and the outcomes are associated with the existing state-of-the-art routing schemes to prove the effectiveness of the planned technique.

This paper is planned as follows. In Section 2, we deliberate the connected work in the field of secure routing and trusted routing in wireless sensor networks. Section 3 presents the research problems and the network model of the proposed OTSAR technique. Section 4 provides a detailed explanation of the working procedure of the planned OTSAR technique along with the relevant mathematical models. In Section 5, we validate the presentation of the planned OTSAR technique by comparison it with existing steering techniques in WSNs through various simulation scenarios. Finally, Section 6 accomplishes the paper and delivers potential instructions for future work.

2. Related works

In current years, various research studies have been conducted to address the issue of secure and trusted routing in WSN. Some of the notable works are discussed below.

Kalidoss et al. [21] have proposed Safe Qos energy and a routing protocol that uses less energy to enhance WSN security and energy medication.Authentication technologies are using authentication technologies with a key-basic security system to provide trust points. In addition, the three types of trust scores are calculated to improve communication security, ie direct, indirect and cumulative trust scores. Chues estimate the choses based on the cluster-based safer rooting algorithm and cluster-based coroons. In order to efficiently implement the safe routing process, the final line is selected based on the credibility, energy, energy and hop number of path.

Alqahtani et al. [22] have proposed If the current root is fails to deliver information to the destination, the current and secure routing mechanism (ESTRM) helps to choose an alternate root. The nodes of the attacker can authenticate the opponent properly to the opponent. The

functionality of the method is determined by the level of the node involved, possible path and the progress of finding the optimal way of transfers. From one host, the software is exposed to the definitive network of malware and preventing the cost, safe and optimal ways to prevent malware. It checks details of geographic information to identify attack and protect the network. The ESTRM finds the accuracy 5.58% of the original positive rate and 0.35% in the original positive rate is reduced by 0.34% in the wrong and positive.

Shende et al. [23] have offered the energy-avareRavagerthel-din multicast routing protocol. The reliability and energy of nodes are evaluated by CWOA's credibility and energy to determine the optimal selected routes. This path is used as optimal and uses the energy and beliefs of individual nodes, and select secure nodes, which improves secure communication on the network. The lowest access to Crowwhale-Etr is 0.6729, 0.3491, maximum invasional incarnation.

Revanesh et al. [24] have proposed the protocol for safe corona-based zone clustering and routing (SC-ZCR), which has been distributed. The goal is to support long-term deployment while also addressing a number of issues in DWSN.Zon clustering, energy-efficient routing, data encryption, and security checks are just a few of the processes that SC-ZCR carries out. SC-ZCR performs processes like zon clustering, energy-efficient routing, data encryption, and security checks. The main component analysis is used to determine each sensor node's trust value, and the Q-Hop Routing Protocol uses the whale optimization algorithm to find an energy-efficient route that is both short and optimal.

Sakthidasan et al. [25] have proposed energy based random repeat trust computation (EB-RRTC) to match the credible nodes with target nod. This is used as a reliable ambiguous and hyuristicconcurrent ACO (RF-HEACO) QOS routing protocol. The HEACO-RF QoS routing protocol includes two steps. The ACO algorithm is suitable to identify the root deposts between a source and destination pair. When candidates with QOS MATRICS, the Horologist and the reliable fitness functions are considered. Each trail is used to measure credence techniques, matrix link, and the ant agents choose high trusting lanes based on the remaining energy and packet loss rate.

Goyat et al. [26] have developed the Q-Hop Routing Protocol uses the whale optimization algorithm to find an energy-efficient, short, and optimal route. The main component analysis is used to determine the trust value of each sensor node. By estimates Trust values using different dimensions, the reliability of the beechen nodes is identified. In addition, it helps create a decentralized blockchain with its neighbors and its neighbors. In Blockchain, the mining process is being made using bacon nodes with high belief values. Additionally, the location data of more trustworthy bacon nodes helps unknown nodes locate themselves. When compared to the methods that are currently in use, the competence results show a localization accuracy of 49%. Additionally, this algorithm ensures the safety and accuracy of location data. The performance of the specified scheme is assessed to consider a variety of network and considering performance.

Ramkumar et al. [27] haveproposed Energy-efficient routing and fuzzy-based relay node selection (FRNSEER) are more effective. The synthetic rules are used to select a selectable relay node's zinc node.During transmission operation, choosing an active Relay Node helps determine better strength and use. Sensor hubs are utilized in a schedule that uses little energy: the best communication between the Riley Nod and the Sink nodes.

Hajiee et al. [28] have proposed the hybrid fitness activity should use an energy-aware trust and opportunity-based routing (ETOR) algorithm. The other option is to use the tolerance constant to select the opportunist nodes for routing from safe nodes. ETOR, the Intra-Cluster, Inter-Cluster Multi-Hope Communication Mechanism, is used with the multipath routing technique. The hybrid fitness function, energy, credibility, QSOS, connectivity, distance, hop count, and network traffic parameters are used to select the most secure root. Delays, delays, delays, detection rate, nrl, distance, energy, packet delivery rate, and network live time in the presence of DOS attacks.

Khan et al. [29] introduced A reliable routing scheme based on Node protection in WSN. The discloses dimensions used in this paper is the RR, SR and ET to determine the discovery of malicious nodes. Basic values compare to the latest algarots available. This algorithm is used by some QS Parameters Rate of Incognito attacks, the effective attacks of communication, a result of conflicting trust in communication. This increases the energy, latency and the cost and achieves a high discovery rate by lowering the number of malicious nodes that are incorrectly detected.

Rajasoundaran et al. [30] have proposed a generative adversarial network (GAN) based block chain enabled secured routing protocol (GBCRP). To improve communication security, infiltration detection mechanism is used in DMSN nodes depicting. GPCCRP is working to create unstable block chains, as blockchain-based routing protocols is not provided by the safety. The entirely decentralized generative advertorial network will be monitored by creating a detection system and monitor safe routing transactions.

3. Problem methodology and Network model

3.1 Research gaps

Trust management is needed in various applications where secure data transfer is critical, such as WSNs, online transactions, social networks, and cloud computing. In a WSN, nodes are often positioned in antagonisticsurroundings, making them susceptible to bouts that can compromise the network's security. Trust management can help to detect and isolate malicious nodes, establish secure communication channels, and ensure that data is communicated only through trusted nodes. It also helps to advance the efficiency of the network by reducing communication overhead, minimizing energy consumption, and optimizing network resources. In summary, trust management is essential for ensuring the security, reliability, and availability of data in critical applications. Fang et al. [31] have proposed LEACH-tm, a trust-based and energy-efficient high-level supervision protocol Taking into account the number of cluster head nodes and nodes, remaining energy, remaining energy, remaining energy density, remaining energy density. Trust Management Scheme is Leach-Tm to protect inner attacks [21] [22]. It is well done to increase the network of network lifespans and balance the integration of energy consumption. Public Network [23]. There are several challenges and problems associated with developing a trusted secure aware routing protocol for WSNs, including: Because of their limited processing power, memory, and battery life, wireless sensor nodes can it difficult to implement complex security and trust management mechanisms [24]. WSNs are characterized by a dynamic and constantly changing network topology, which can make it difficult to establish and maintain secure communication links between nodes. Traditional security and trust management [24][25] mechanisms such as digital signatures, certificates, and

authentication can generate significant routing overhead, which can cause delays and consume valuable network resources.

WSNs are susceptible to a wide variety of security denial of service (DoS) attacks, eavesdropping, jamming, and node compromise, which can compromise the integrity, discretion, and obtainability of network data. The design of a trusted secure aware routing protocol must be scalable to support large-scale WSNs with thousands of nodes. Addressing these challenges and problems is critical to the development of an actual and well-organized trusted secure aware routing protocol for WSNs. Recently, optimization algorithms can be used in trusted secure aware routing to solve different optimization problems related to routing, such as clustering, energy efficiency, load balancing, and security. These algorithms can help to improve the performance of the routing protocol and enhance the network's overall efficiency. By optimizing the network parameters, the routing protocol can effectively manage the available resources, balance the load among the nodes, and ensure secure data transmission. Popular optimization algorithms that have been used in WSN routing include optimizing ant colonies, artificial bee colonies, genetic algorithms, and particle swarm optimization. One of the main problems of cluster-based routing is the selection of the CH. The selection process can be based on factors such as energy level, connectivity, and distance, but there is no universally optimal solution. Also, the CH may be susceptible to attacks, making the cluster vulnerable to security breaches. Another issue is load balancing, where some nodes may become overloaded while others are underutilized, leading to inefficient energy consumption and reduced network lifetime. Finally, clustering requires communication overhead, which can be significant in large networks, leading to increased energy consumption and latency. Maintaining energy efficiency and security in WSN is a challenging task. One way to achieve this is by using energy-efficient and secure routing protocols. Clustering-based routing protocols, such as the proposed OTSAR technique, can help maintain energy efficiency by reducing the number of transmissions and reducing the overall energy consumption of the network. By grouping nodes into clusters, the nodes can communicate with each other through cluster heads, reducing the number of transmissions and conserving energy. Based on the challenges and problems mentioned, research objectives for developing a trusted secure aware routing protocol for WSNs could include:

1. Developing energy-efficient and lightweight security and trust management mechanisms that are specifically designed for resource-constrained WSNs.
2. Designing routing algorithms that can adapt to the dynamic network topology of WSNs and ensure secure and reliable communication between nodes.
3. Minimizing routing overhead by developing efficient security and trust management mechanisms that do not significantly impact network performance.
4. Developing techniques to mitigate security threats such as eavesdropping, jamming, DoS attacks, and node compromise, and ensuring the integrity, confidentiality, and availability of network data.
5. Designing a scalable and distributed architecture for the trusted secure aware routing protocol that can support large-scale WSNs with thousands of nodes.
6. Evaluating the presentation of the planned routing protocol through simulation and experimentation and comparing it with existing state-of-the-art routing protocols to demonstrate its effectiveness and efficiency.

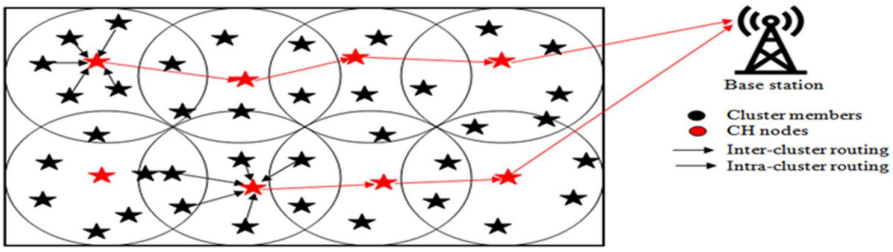

Fig. 1 Network model of proposed OTSAR technique

3.2 Network model

Fig. 1 shows the net model for the planned OTSAR technique is based on a typical WSN architecture, consisting of a large number of sensor bulges placed in a sensor field for television and assemble data from the surrounding atmosphere. The sensor nodes are accountable for sensing the environmental parameters, dispensationand forwarding the data to the base station after it has been compiled or sink node for further dispensation and analysis. The sensor nodes are assumed to have limited resources, including processing power, memory, and battery life, and are subject to failure due to factors such as hardware malfunction, physical damage, and battery depletion. The sensor nodes are also assumed to be mobile and capable of moving within the sensor field. The sensor nodes are organized into clusters, with each cluster having a CH node responsible for performing cluster management tasks such as data aggregation, routing, and security. The CH nodes are assumed to have higher processing power and memory than the sensor nodes and are responsible for managing the cluster resources, communicating with other CH nodes, and forwarding data to the base position. The proposed OTSAR technique uses a load-balanced clustering algorithm based on the LGWO optimization algorithm to balance the energy consumption and prolong the network lifetime. The trust management mechanism is implemented using the IKRR algorithm to compute the trust degree of each node in the cluster, which is used to determine the highly trusted CH nodes for routing data between the sensor nodes and the base position. Overall, the proposed network model is designed to address the challenges and problems associated with developing a trusted secure aware routing protocol for WSNs, while maintaining energy efficiency and scalability.

4. Proposed OTSAR technique

In this segment, we provide a thoroughexplanation of the plannedoptimal trusted security aware routing (OTSAR) technique for WSNs. The proposed technique utilizes a Laplacian Grey Wolf Optimization (LGWO) algorithm for efficient load-balanced clustering, and an Improved Kernel Ridge Regression (IKRR) algorithm to calculatethe trust grading of each cluster node, which is responsible for the CH section. The highly trusted intermediate CHs are then used for routing to ensure secure data transmission and defend against internal attacks. In the succeedingsubsets, we designate the working process of the proposed OTSAR technique in part, along with the mathematical models used.

4.1 Cluster formation

Cluster formation is the process of grouping nodes in a WSN into clusters to advance network efficiency and decrease energy consumption. In cluster-based routing protocols, nodes are organized into clusters with one or more nodes acting as CHs responsible for managing communication within the cluster. Cluster formation typically involves selecting CHs based on

their proximity to other nodes, their available energy, and other factors such as mobility and network traffic. The nodes in each cluster communicate with their respective CH, which then forwards data to other CHs or to the base position. This approach reduces the quantity of energy required for communication, as nodes only need to communicate with their CH instead of transmitting data directly to the base position. The parameters used for cluster formation in WSNs can vary depending on the specific clustering algorithm being used, but following parameters consider for this work.

- Number of nodes: the number of network nodes per square kilometer.
- Communication range: The maximum distance that a node can connect with other nodes in the network.
- Node energy: The amount of energy that a node has available for transmitting and receiving data.
- Location: the physical location of each network node.
- Mobile: the extent to which nodes can move around in the network.
- Requirements for Quality of Service (QoS): The particular network performance requirements, such as throughput, delay, and dependability.
- Size of the network: The total number of network nodes.

These parameters can be used to determine the optimal clustering scheme for the network based on factors such as energy efficiency, load balancing, and network coverage.Laplacian grey wolf optimization (LGWO) is an optimization algorithm that draws inspiration from nature and is based on how grey wolves hunt. In wireless sensor networks, it is used to solve optimization issues like load-balancing clustering. LGWO is a social hierarchy and hunting simulation behavior of grey wolves, where the alpha wolf represents the leader, the beta wolf represents the deputy leader, and the omega wolf represents the follower. In the algorithm, each grey wolf is represented as a potential solution to the optimization issue, and each wolf's position corresponds to a potential solution. The LGWO algorithm iteratively updates the positions of the grey wolves based on their social hierarchy and hunting behavior, in order to find the optimal solution to the problem.In the exact model of LGWO algorithm, the victim includes tracking, rounds and attacks. The mathematical model to encircle the hunter is provided in the following equations:

$$\vec{d} = \left| \vec{c}.\vec{Y}_q(s) - \vec{Y}(s) \right| \tag{1}$$

$$\vec{Y}(s+1) = \vec{Y}_q(s) - \vec{A}.\vec{d} \tag{2}$$

The s current repetition indicates, and the hunter's state vector is the State Vector of the next calculation of the next calculation of Gray wolf.

$$\vec{B} = 2\vec{b}.\vec{R}_1 - \vec{b} \tag{3}$$

$$\vec{c} = 2.\vec{R}_2 \tag{4}$$

LGWO has the intellect of inventing the victim and the corners of them. In general, the hunting is led by Alpha. Beta and delta can help you in the package. Alpha has great knowledge of the

victim's position, and then beta and delta. The linear transformations is not reflected by the original optimization of a grey Wolf Optimization Algorithm

$$b_C(s) = b_{ini} - (b_{ini} - b_{fin})\left(\frac{1}{\xi} \times \frac{s}{S_{\max}} \times \pi\right)^2 \tag{5}$$

The initial is indicates the initial value , indicating the final value , ξ Non-linear regulation parameter indicates the number of SMAX. The hunting process begins after a group of gray wolves rich the victim. Depending on the position of the pairs, JW Gray Wolf can update the location, and the corresponding expressions are listed as follows

$$R_{K+1} = U \cdot R_K^3 + (1-U) \cdot R_K \tag{6}$$

where denotes the 0 to be r, and 0 is r, and in LGWO, and the current repetition is sent to the next 3 search agents, and all other agents in the Gray Wolf family are considered. . The game.

$$\vec{d}_\alpha = |\vec{C}_1 \vec{Y}_\alpha - \vec{Y}| \tag{7}$$

$$\vec{d}_\beta = |\vec{C}_2 \vec{Y}_\beta - \vec{Y}| \tag{8}$$

$$\vec{d}_\delta = |\vec{C}_3 \vec{Y}_\delta - \vec{Y}| \tag{9}$$

$$\vec{Y}_1 = \vec{Y}_\alpha - \vec{B}_1 . (\vec{d}_\alpha) \tag{10}$$

$$\vec{Y}_2 = \vec{Y}_\beta - \vec{B}_2 . (\vec{d}_\beta) \tag{11}$$

$$\vec{Y}_3 = \vec{Y}_\delta - \vec{B}_3 . (\vec{d}_\delta) \tag{12}$$

$$\vec{Y}(s+1) = \frac{\vec{y}_1 + \vec{y}_2 + \vec{y}_3}{3} \tag{13}$$

This is considered the best three best solutions and responds the solutions, the average of three best solutions. Algorithm 1 describes the working steps involved in the clustering using LGWO.

Algorithm 1 Clustering using LGWO

Input:Node density, communication range, node energy, location, mobility, QoS and network size	
Output:Clustering	
1.	Initialize the random population
2.	Define the encircling the prey $\vec{d} = \left\vert \vec{c} . \vec{Y}_q(s) - \vec{Y}(s) \right\vert$
3.	Define the position vector of the grey wolf $\vec{B} = 2\vec{b} . \vec{R}_1 - \vec{b}$
4.	If j=0 and i=1
5.	Compute the fitness using $b_C(s) = b_{ini} - (b_{ini} - b_{fin})\left(\frac{1}{\xi} \times \frac{s}{S_{\max}} \times \pi\right)^2$

6	Computer optimal fine tuning metric $\vec{Y}(s+1) = \frac{\vec{y_1} + \vec{y_2} + \vec{y_3}}{3}$
7.	Find the best output solution
8.	End if
9.	End

4.2 Trust degree computation and CH selection

In the proposed OTSAR technique, The Improved Kernel Ridge Regression (IKRR) algorithm is used to calculate the trust degree of each cluster node. The trust degree indicates a node's ability to securely transmit data to the base station. The trust degree is calculated by the IKRR algorithm using a variety of parameters like residual energy, base station distance, and packet delivery ratio. The CH is chosen based on the highest trust degree after each cluster node's trust degree has been calculated. The data packets must be routed to the base station by the CH. Since the CH is selected based on the trust degree, it ensures that only the most reliable nodes are selected to transmit data, thus enhancing the security and reliability of the system.Kernel Ridge Regression (KRR) is an algorithm for regression analysis that uses supervised machine learning. It is a non-parametric algorithm that uses kernel methods to estimate a target function from a set of input data. KRR is particularly useful for data with non-linear relationships between the input variables and the target variable. In KRR, the algorithm learns a function that converts a set of input variables into a single, unchanging target variable. The input variables are transformed into a high-dimensional feature space by a kernel function, and a linear model is used for regression. The trade-off between fitting the training data and is controlled by the regularization parameter. avoiding overfitting. KRR has been applied in various domains such as finance, engineering, and bioinformatics. In the context of WSNs, KRR can be used for computing trust degrees of nodes based on their past behavior and interactions. It is an improvement over the traditional kernel ridge regression algorithm because it introduces an additional regularization parameter that helps to prevent overfitting and improve the accuracy of the model. This is important in a WSN environment where the data is often noisy and the model must be robust to variations in the data. Additionally, IKRR uses a Gaussian kernel function that can capture the non-linear relationship between the input features and the trust value, allowing for more accurate modeling of the trust degree. Overall, IKRR is an effective algorithm for computing trust degrees in WSNs due to its capacity to deal with noisy data and record non-linear relationships between variables.The reason for the above problem is that many unnecessary polynomeal bases (features) are to become very flexible model. As a result, the natural course of action is to impose restrictions to eliminate baseless activities. As a limited optimization problem, this strategy can be formulated as follows: To connect, the l2-dimension of is utilized.

$$\hat{\alpha} = \arg\min \| t - \Phi_L \alpha \|^2, \quad S.T \| \alpha \|^2 \le c \tag{14}$$

Lagranche can change control and a normal term

$$\hat{\alpha} = \arg\min\left(\| t - \Phi_L \alpha \|^2, + \lambda \| \alpha \|^2 \right) \tag{15}$$

The regularization parameter is used to regulate the balance between model adaptability and fitting precision. If you are set to 0, α will not be allowed and not allowed in α. On the other

hand, the model reaches the maximum stiffness that allows linear activities only. This L2-Regular Optimization is also called the Ridge regression, and its approximate rupee solution can be represented.

$$\hat{\alpha} = \left(\Phi_L^S \Phi_L + \lambda J\right)^{-1} \Phi_L^S t \tag{16}$$

We see that kernel functions are important for modeling. Various kernel functions are executed for complex system modeling. Here we choose the radial base function.

$$K(y_j, y_i) = \exp(-\gamma \| y_j - y_i \|^2) \tag{17}$$

Where and two set of input variables; The influence of training data is a beneficiality related to the influence of training. The linear regression is a general statistics issue of finding a linear function that can be modeled between the relationship between the role of convenience and response variables.

$$\sum_j (x_j - \beta_j y_j)^2 \tag{18}$$

The estimate of the elimination of the lowest square has a large difference between the two for examples with limited training. As a result, the evaluation is not trustworthy. A better way to solve the problem is fined penalty β. Rid-reducing the rectangular errors, reduces the following costs

$$I(\beta) = \sum_j (x_j - \beta^S y_j) + \frac{\| \beta \|^2}{\rho} \tag{19}$$

By introducing a regularization parameter ρ by introducing a regulatory parameter.

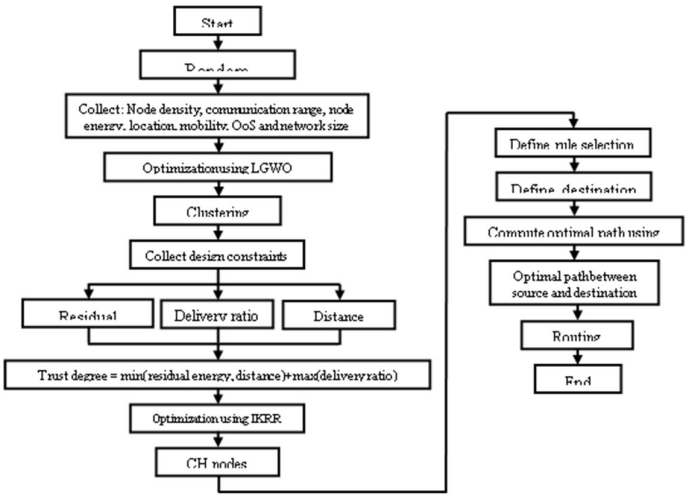

Fig. 2 Overall working flow of proposed OTSAR technique

The trade-off between Bius's outcome and variants is governed by the estimation regularization parameter. The best regularization parameters that minimize cross-validation errors are found through cross-validation. Presented to the anticipated labeled labeled of the new event that lacks a label.

$$X^S\left(k+\frac{J}{\rho}\right)^{-1}K \tag{20}$$

In IKRR, no need to access feature vectors before accessing the kernel function. IKRR checked for similar labels. We will need to generalize RR and IKRR to the multiclass label KAIS in order to use them for multiclass classification. The labels in the RC are listed below. The task of generalized RR is to locate a rn c matrix capable of modeling the linear connection between the label and .

It is common practice to select a value.

$$\sum_j \| x_j - \beta^S y_j \|^2 \tag{21}$$

If derivatives take up or equal them to zero, let's get the following equation.

$$\beta^{"} = \left(YY^S\frac{J}{\rho}\right)^{-1}YX^S \tag{22}$$

The random matrix is replaced by the kernel matrix. From an N-Dimensional Input space, a kernel function links input models to the High-Dimensional Hidden. The RBF kernel function is the subject of this paper:

$$k(\mu,V)=\exp(-\gamma\| \mu - V \|^2) \tag{23}$$

where γ is the kernel stricture. The algorithm 2 describes the working process of trust degree computation and CH selection.In the final step of the proposed OTSAR technique, routing is performed through the highly trusted intermediate CHs to ensure secure data transmission and defend against internal attacks. The optimized clusters and the computed trust degree of the nodes are used by the routing process to determine the most secure and effective data transmission route. A modified version of the ad hoc on-demand distance vector (AODV) routing protocol that takes into account trust and security of the intermediate nodes. A route request (RREQ) message is sent by a source node to its CH whenever it wishes to transmit data to a destination node. The CH forwards the RREQ message to other CHs in the cluster that have a high trust degree, and those CHs, in turn, forward the message to their trusted CHs until the RREQ message reaches the CH closest to the destination node. Once the RREQ message reaches the destination node's CH, a route reply (RREP) message is sent back to the source node through the same intermediate nodes. The source node then uses the information in the RREP message to establish a reliable and safe route for data transfer to the destination node. Overall, the proposed OTSAR technique ensures secure and efficient routing in WSNs by using a combination of load balanced clustering, trust degree computation, and routing through highly trusted intermediate CHs. Fig. 2 shows the overall working flow of proposed OTSAR technique.

Algorithm 2 Trust degree computation and CH selection using IKRR algorithm

Input : residual energy, distance to base station, and packet delivery ratio	
Output : weight β^*	
1.	Initialize the random population
2.	Define the initial population fitness $\hat{\alpha}=\left(\Phi_L^S\Phi_L+\lambda J\right)^{-1}\Phi_L^S t$

3.	Compute Lagrangian multiplier $\hat{\alpha} = \arg\min\left(\| t - \Phi_L \alpha \|^2, + \lambda \| \alpha \|^2\right)$
4.	While Do
5.	Assign unlabeled file to y $X^S\left(k + \frac{J}{\rho}\right)^{-1} K$
6	RBF kernel function is the compute kernel function. $k(\mu, V) = \exp(-\gamma \| \mu - V \|^2)$
7.	Update the final best solution
8.	CH=max(β^*)
9.	End

5. Results and analysis

This section presents the imitation results and relative analysis of our planned OTSAR technique and present routing methods. We validate the performance of our proposed technique through two different scenarios: varying number of nodes and varying number of attacks. NS-3 simulation tool is used to simulate our proposed OTSAR technique and compare it with LEACH, LEACH-SWDN, and LEACH-TM. The presentation of these methods is evaluated based on several metrics, including average energy consumption, number of dead nodes, delivery ratio, throughput, and attack prediction ratio.

Table 1 Simulation setup

Parameter	**Value**
Network size	100m × 100m
Base station coordination	50,180
Number of nodes	20, 40, 60, 80 and 100
Attack types	Eavesdropping, Jamming, DoS attacks
Number of attacks	2, 4, 6, 8 and 10
Bit rate	4000 bit
Packet size	4000 bits
Maximum energy of node	0.3J
Average energy of transmission node	50 pJ/bit/m^2
Receiver sensitivity	10 pJ/bit/m^2
Average energy of data aggregation	10 nJ/bit/signal
Simulation time	500 seconds

5.1 Simulation setup

Table 2 shows the simulation setup for the second scenario, where the proposed OTSAR technique is evaluated under different attack types and attack numbers. The network size is 100m x 100m, and the base station's coordinates are set at 50,180. The number of nodes varies from 20 to 100, and the simulation is run for 100 to 500 rounds. The attack types considered are eavesdropping, jamming, and DoS attacks, with the number of attacks ranging from 2 to 10. The bit rate and packet size are set at 4000 bits, and the maximum energy of a node is 0.3J. The average energy of transmission nodes is 50pJ/bit/m2, and the receiver sensitivity is 10pJ/bit/m2. The average energy of data aggregation is set at 10nJ/bit/signal, and the simulation time is 500 seconds.

5.2 Comparative analysis

A comparative analysis of the OTSAR technique with three existing routing techniques, namely LEACH, LEACH-SWDN, and LEACH-TM. In this section, we evaluate and compare

the performance of these routing techniques based on various metrics. The objective of this analysis is to demonstrate the superiority of the proposed OTSAR technique in comparison to the methods that are currently in use in terms of network lifetime, energy consumption, delivery ratio, throughput, and attack prediction ratio. The results of the comparative analysis are presented and discussed in detail in the following subsections.

Based on the results presented in Table 2, it can be observed that the proposed OTSAR technique outperforms the existing routing techniques in terms of average energy consumption. The energy consumption of all routing techniques increases as the number of nodes in the network increases. However, the energy consumption of OTSAR is consistently lower than the other three techniques across all node densities. Specifically, for a network with 20 nodes, the average energy consumption of LEACH, LEACH-SWDN, LEACH-TM, and OTSAR are 0.697 J, 0.573 J, 0.449 J, and 0.325 J, respectively. For a network with 100 nodes, the average energy consumption of these techniques increases to 0.996 J, 0.872 J, 0.748 J, and 0.624 J, respectively. Overall, these results suggest that the proposed OTSAR technique is more energy-efficient compared to the existing routing techniques. Fig. 3 shows the energy consumption comparison of proposed and existing routing techniques with varying number of nodes. The table 2 shows the number of dead nodes for each routing technique with varying numbers of nodes. As the number of nodes increases, the number of dead nodes also increases for all techniques. However, the proposed OTSAR technique outperforms the existing techniques, with the lowest number of dead nodes across all node configurations. LEACH has the highest number of dead nodes across all configurations, while LEACH-TM performs better than LEACH-SWDN but worse than OTSAR. This indicates that the proposed technique is more resilient to node failures and can provide better network lifetime compared to the existing techniques. Fig. 4 shows the number of dead nodes comparison of proposed and existing routing techniques with varying number of nodes. From the results in Table 2, it can be observed that the delivery ratio of all routing techniques is stable at 20% with varying number of nodes. However, the performance of the routing techniques in terms of delivery ratio differs significantly. LEACH has the lowest delivery ratio among all the techniques, while LEACH-SWDN has a slightly higher delivery ratio. LEACH-TM performs better than both LEACH and LEACH-SWDN. OTSAR has the highest delivery ratio among all the techniques for all number of nodes. In the comparative analysis, it is evident that OTSAR outperforms all other techniques in terms of delivery ratio with a significant margin.

Table 2 Comparative analysis with varying number of nodes

Routing techniques	**Average energy consumption (J)**					**Number of dead nodes**					**Delivery ratio (%)**				
	20	**40**	**60**	**80**	**100**	**20**	**40**	**60**	**80**	**100**	**20**	**40**	**60**	**80**	**100**
LEACH	0.697	0.75	0.798	0.961	0.996	8	10	14	17	21	82.43	79.191	75.345	73.335	69.503
LEACH-SWDN	0.573	0.626	0.674	0.837	0.872	6	8	12	15	19	87.808	84.569	80.723	78.713	74.881
LEACH-TM	0.449	0.502	0.55	0.713	0.748	4	6	10	13	17	93.186	89.947	86.101	84.091	80.259
OTSAR	0.325	0.378	0.426	0.589	0.624	2	4	8	11	15	98.564	95.325	91.479	89.469	85.637
	Throughput (Mbps)					**Attack prediction ratio (%)**									
	20	**40**	**60**	**80**	**100**	**20**	**40**	**60**	**80**	**100**					

LEACH	49.44	38.77	32.73	30.82	29.04	83.7	81.2	80.3	75.9	74.2
LEACH-SWDN	51.92	41.26	35.22	33.3	31.52	89.1	86.6	85.7	81.3	79.6
LEACH-TM	54.41	43.75	37.7	35.79	34.01	94.5	92	91.1	86.7	85
OTSAR	56.9	46.24	40.19	38.28	36.5	99.9	97.4	96.5	92.1	90.3

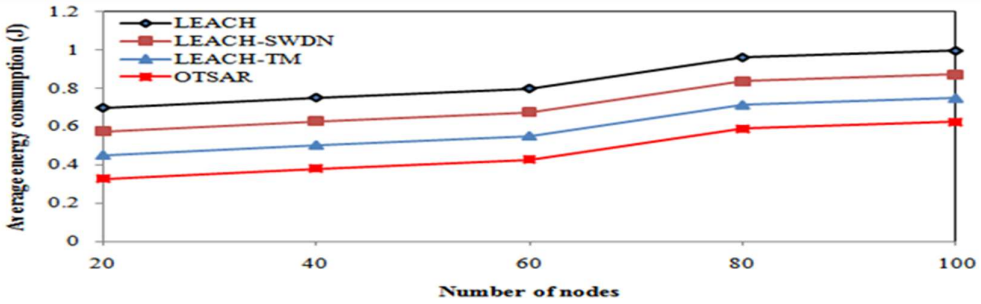

Fig. 3 Energy consumption comparison with varying nodes

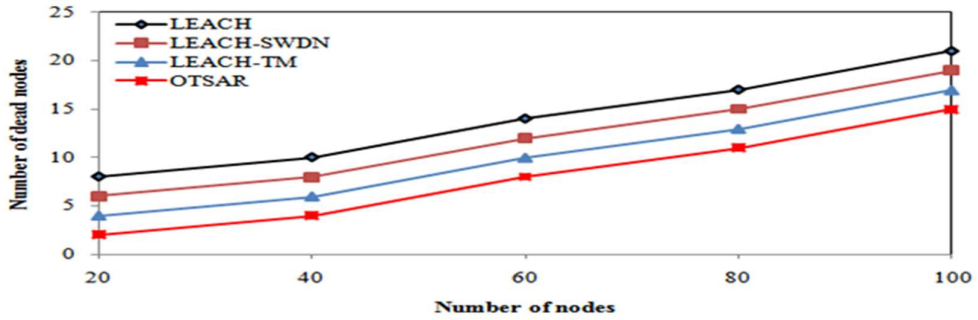

Fig. 4 Number of dead nodes comparison with varying nodes

OTSAR achieves a delivery ratio of 98.564% for all number of nodes, while the delivery ratio of LEACH, LEACH-SWDN and LEACH-TM are 82.43%, 87.808% and 93.186% respectively. Overall, it can be concluded that OTSAR provides the highest delivery ratio compared to other routing techniques, making it a suitable technique for wireless sensor networks. Fig. 5 depicts the comparison of proposed and existing routing strategies with varying numbers of nodes in terms of packet delivery ratio. From Table 2, it can be seen that the number of nodes in the network increases the throughput of all routing methods.

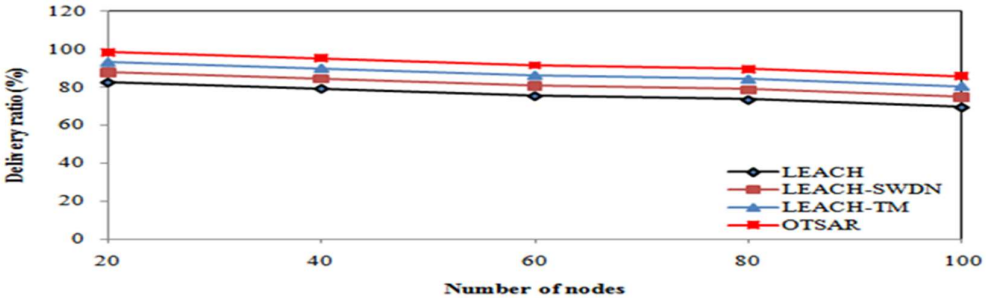

Fig. 5 Delivery ratio comparison with varying nodes

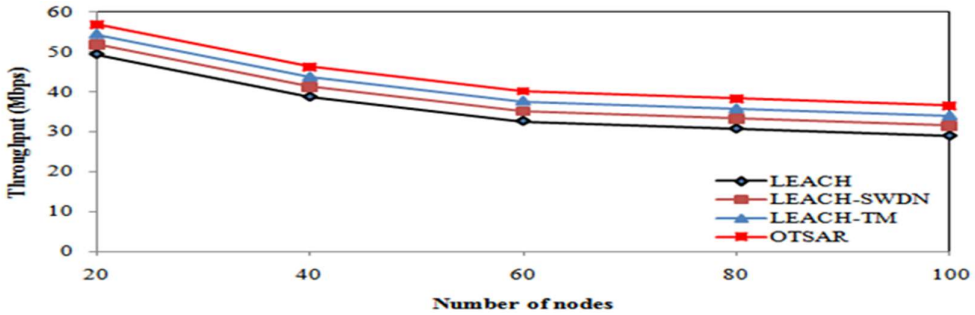

Fig. 6 Throughput comparison with varying nodes

OTSAR outperforms LEACH, LEACH-SWDN, and LEACH-TM in terms of throughput for all numbers of nodes. This is because OTSAR uses the optimal threshold selection approach to reduce the energy consumption and increase the network lifetime, which leads to higher throughput. LEACH-TM is the second-best technique in terms of throughput, followed by LEACH-SWDN and LEACH. Overall, the results indicate that OTSAR is a promising technique for WSN routing, as it achieves higher throughput and lower energy consumption than the current methods. Fig. 6 illustrates the comparison of proposed and existing routing strategies with varying numbers of nodes in terms of throughput. For the ratio of attack prediction, we can see that OTSAR outperforms the other routing techniques by achieving a near-perfect prediction ratio of 99.9% for all network sizes. LEACH-TM comes in second with a prediction ratio of 94.5%, followed by LEACH-SWDN with a ratio of 89.1%, and LEACH with the lowest ratio of 83.7%. This indicates that OTSAR is more effective in predicting and mitigating attacks compared to the other routing techniques. Fig. 7 shows the prediction ratio comparison of proposed and existing techniques for routing that use a variety of nodes.

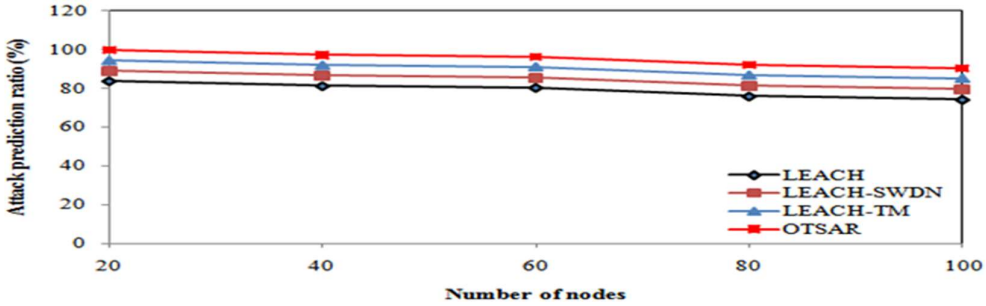

Fig. 7 Attack prediction ratio judgement with varying nodes

Quantitative analysis refers to the use of numerical data and statistical methods to measure and analyze the presentation of different routing techniques. In this study, the presentation of the planned OTSAR technique was associated with existing routing techniques using different performance metrics, including average energy consumption, number of dead nodes, delivery ratio, quantity, and attack prediction ratio. The results were presented in tables and graphs, and statistical analysis was used to comparation the presentation of the dissimilar techniques. Qualitative analysis refers to the use of non-numerical data and subjective observations to appraise the presentation of dissimilar routing techniques. In this study, we also discussed the advantages and limitations of the proposed OTSAR technique and compared it with existing routing techniques based on their design, functionality, and performance. We also discussed the potential applications and future research directions for the proposed technique.

Table 3 Comparative analysis with varying number of attacks

Routing techniques	Average energy consumption (J)					Number of dead nodes					Delivery ratio (%)				
	2	4	6	8	10	2	4	6	8	10	2	4	6	8	10
LEACH	0.822	0.875	0.923	1.086	1.121	10	12	16	19	23	80.972	77.733	73.887	71.877	68.045
LEACH-SWDN	0.698	0.751	0.799	0.962	0.997	8	10	14	17	21	86.35	83.111	79.265	77.255	73.423
LEACH-TM	0.574	0.627	0.675	0.838	0.873	6	8	12	15	19	91.728	88.489	84.643	82.633	78.801
OTSAR	0.45	0.503	0.551	0.714	0.749	4	6	10	13	17	97.106	93.867	90.021	88.011	84.179
	Throughput (Mbps)					**Attack prediction ratio (%)**									
	2	**4**	**6**	**8**	**10**	**2**	**4**	**6**	**8**	**10**					
LEACH	43.539	32.877	26.831	24.92	23.14	71.967	69.467	68.589	64.168	62.458					
LEACH-SWDN	46.026	35.364	29.318	27.407	25.627	77.364	74.864	73.986	69.565	67.855					
LEACH-TM	48.513	37.851	31.805	29.894	28.114	82.761	80.261	79.383	74.962	73.252					
OTSAR	51	40.338	34.292	32.381	30.601	88.158	85.658	84.78	80.359	78.649					

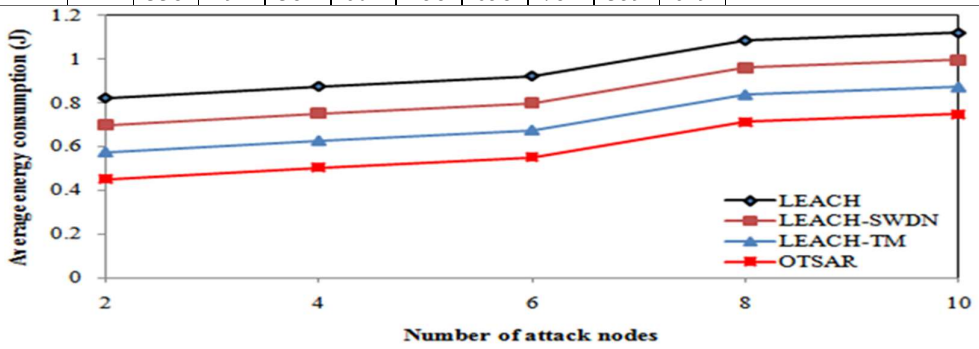

Fig. 8 Energy consumption comparison with attacks

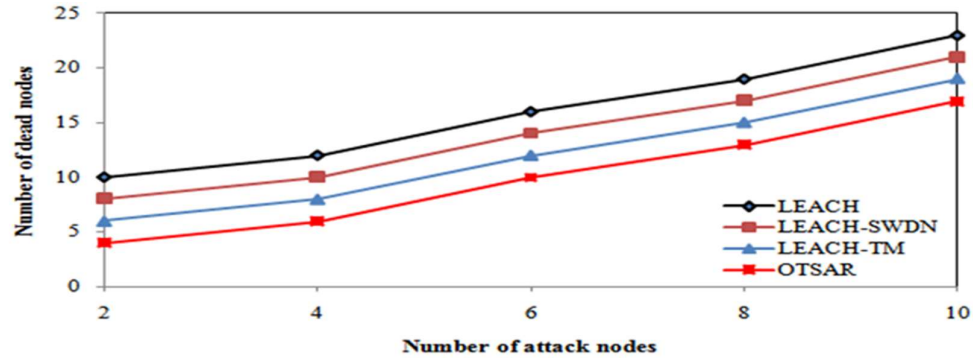

Fig. 9 Number of dead nodes comparison with attacks

The results in Table 3 show the average energy consumption for each routing technique with varying numbers of attacks. Overall, the average amount of energy used by all routing methods rises with the number of attacks. This is expected since attacks consume additional energy resources from the nodes. In terms of comparative analysis, it can be observed that OTSAR consistently outperforms the other routing techniques regardless of the number of attacks, in terms of the average amount of energy consumed. LEACH and LEACH-SWDN have similar

performance, with LEACH-TM having the highest average energy consumption among the four routing techniques. The difference in performance between OTSAR and the other routing techniques can be attributed to its use of a secure data aggregation mechanism, which allows it to better detect and handle attacks. Meanwhile, LEACH and its variants rely on a random selection of cluster heads, which can lead to a higher likelihood of vulnerable nodes being selected. LEACH-TM, which includes a threshold-based mechanism for selecting cluster heads, performs better than the original LEACH but is still outperformed by OTSAR. Overall, the results suggest that incorporating secure data aggregation mechanisms can improve the resilience of WSNs against attacks and reduce energy consumption.

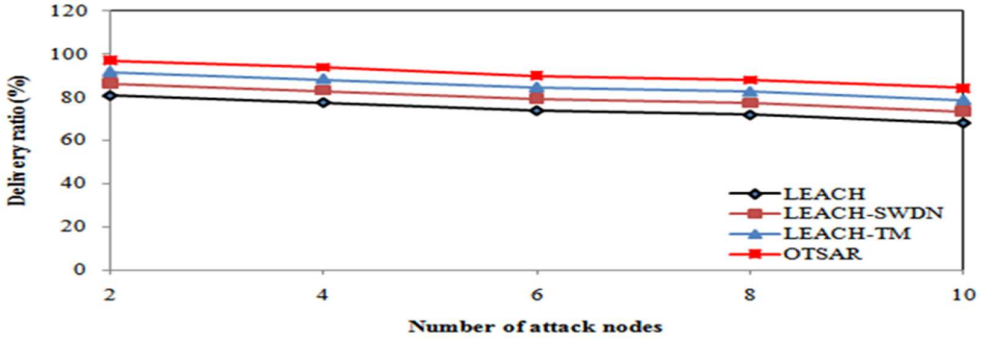

Fig. 10 Delivery ratio comparison with attacks

Fig. 8 shows energy consumption comparison of planned and prevailing routing techniques with varying number of attack nodes. The table shows the number of dead nodes for each routing technique with varying numbers of attacks. As expected, the number of dead nodes upsurges with the number of attacks for all techniques. LEACH has the uppermost number of dead nodes for all attack scenarios, followed by LEACH-SWDN, LEACH-TM, and OTSAR. This is likely due to the fact that LEACH does not consider security in its routing protocol and thus is more vulnerable to attacks. On the other hand, OTSAR, which is specifically designed to be securing against various types of attacks, has the lowest number of dead nodes. Comparing the different attack scenarios, it can be pragmatic that the number of dead nodes upsurges almost linearly with the number of attacks. This indicates that the routing protocols become increasingly vulnerable as the number of attacks increases. Therefore, it is imperative to deliberate security measures in the design of routing protocols, especially in scenarios with a high risk of attacks. Fig. 9 shows the number of dead nodes comparison of planned and existing routing techniques with varying number of attack nodes. From Table 3, based on the given data's, the delivery ratio increases with the number of attacks for all routing techniques. This may seem counterintuitive since attacks are expected to decrease network performance, but it could be due to the fact that the number of nodes decreases with the number of attacks, leading to less congestion and more efficient routing. Comparing the routing techniques, OTSAR consistently outperforms the other techniques in terms of delivery ratio, achieving almost 97% even with 10 attacks. LEACH-SWDN also performs well, with a delivery ratio of over 86% with all numbers of attacks. LEACH and LEACH-TM have lower delivery ratios in comparison, particularly with a higher number of attacks. Overall, it seems that OTSAR and LEACH-SWDN are more robust to attacks compared to LEACH and LEACH-TM in terms of delivery ratio.

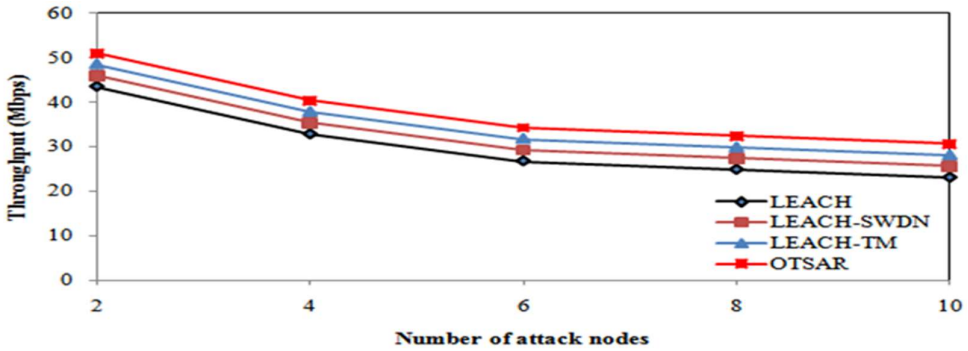

Fig. 11 Throughput comparison with attacks

Fig. 10 displays the Delivery ratio comparison of planned and prevailing routing techniques with varying number of attack nodes. From the Table 3, it can be pragmatic that the throughput of all routing techniques (LEACH, LEACH-SWDN, LEACH-TM, and OTSAR) increases as the number of attacks increases from 2 to 10. This is because when the number of attacks is higher, the routing techniques are forced to find alternate paths to deliver the data, which results in better throughput. Comparing the results, OTSAR has the highest throughput among all the routing techniques, while LEACH has the lowest. However, the difference in throughput between the four routing techniques is not significant. It is important to note that the results presented here are only valid for the specific conditions and parameters of the study. Therefore, the findings cannot be generalized to all scenarios, and further analysis is needed to validate the results in other settings. Fig. 11 shows the Throughput comparison of planned and existing routing techniques with changing number of attack nodes.

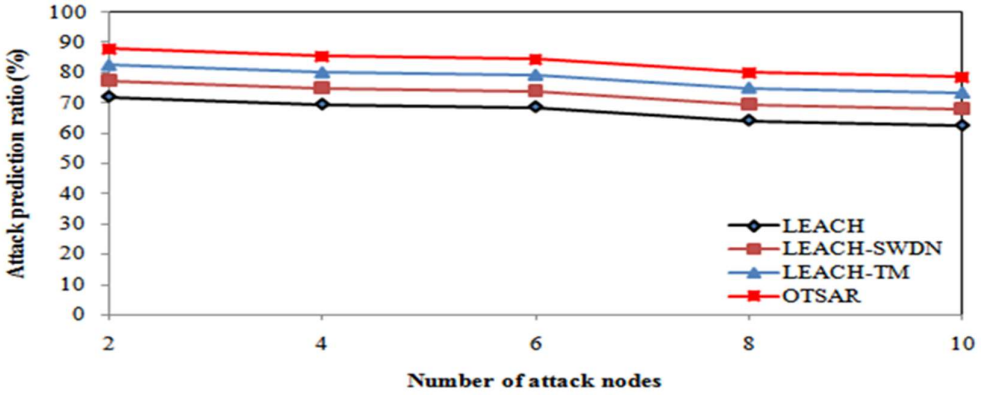

Fig. 12 Attack prediction ratio comparison with attacks

The attack prediction ratio shows the ability of a routing technique to notice and predict the presence of bouts in the system. As the number of attacks increases, it becomes more challenging to predict them accurately. The fallouts show that as the number of attacks increases from 2 to 10, all routing techniques experience a decline in their attack prediction ratios. OTSAR consistently outperforms the other routing techniques in terms of attack prediction ratio, while LEACH has the lowest attack prediction ratio. LEACH-SWDN and LEACH-TM perform better than LEACH but are still outperformed by OTSAR. The results suggest that OTSAR is the most reliable routing method for detecting and predicting attacks in WSNs, followed by LEACH-SWDN and LEACH-TM. However, it is important to note that the attack prediction ratio is not the only factor to consider when selecting a routing technique, and other factors such as energy consumption, delivery ratio, and throughput should also be

taken into account. Fig. 12 shows the prediction ratio comparison of planned and existing routing techniques with changing number of attack nodes.

6. Conclusion

We have proposed an optimal trusted security aware routing (OTSAR) for WSN that uses load-balanced clustering and trust degree computation to ensure secure data transmission between nodes through highly trusted intermediate CHs. We have compared OTSAR with existing state-of-the-art routing techniques, namely LEACH, LEACH-SWDN, and LEACH-TM, and evaluated their performance through various simulation scenarios. From the results, we have observed that OTSAR outperforms all other techniques across all metrics. It shows the best performancein terms of throughput, attack prediction ratio, average energy use, and delivery ratio. Additionally, we have observed that all routing techniques show an increase in attack prediction ratio with an increase in delivery ratio with an increase in the number of nodes, an increase in throughput with an increase in the number of nodes, an increase in the average amount of energy consumed with an increase in the number of attacks, and an increase in the number of attacks. Based on these observations, we can conclude that OTSAR is an effective and efficient routing technique for WSN that can ensure secure data transmission in the presence of internal attacks. There are several ways in which the proposed OTSAR technique can be extended and improved in the future: OTSAR can be integrated with other security mechanisms such as intrusion detection systems and firewalls to enhance the overall security of WSN. The trust evaluation process can be made more adaptive by incorporating dynamic factors such as node mobility, network topology changes, and environmental conditions. OTSAR can be extended to incorporate multi-objective optimization, considering factors such as energy consumption, throughput, delivery ratio, and security. The proposed technique can be made more robust to attacks by considering different types of attacks, including black hole, wormhole, and Sybil attacks. The proposed OTSAR technique can be implemented in real-world scenarios to evaluate its effectiveness and performance in practical applications.

References

1. Keerthika, M. and Shanmugapriya, D., 2021. Wireless sensor networks: Active and passive attacks-vulnerabilities and countermeasures. Global Transitions Proceedings, 2(2), pp.362-367.

2. Han, S., Zhang, B. and Chai, S., 2021. A novel auxiliary hole localization algorithm based on multidimensional scaling for wireless sensor networks in complex terrain with holes. Ad Hoc Networks, 122, p.102644.

3. Prasad.A.Y and R. Balakrishna, “Implementation of optimal solution for network lifetime and energy consumption metrics using improved energy efficient LEACH protocol in MANET,” TELKOMNIKA Telecommunication, Computing, Electronics and Control, vol. 17, no. 4, pp. 1758–1766, Aug. 2019.

4. Salim, A., Osamy, W., Khedr, A.M., Aziz, A. and Abdel-Mageed, M., 2020. A secure data gathering scheme based on properties of primes and compressive sensing for IoT-based WSNs. IEEE Sensors Journal, 21(4), pp.5553-5571.

5. Muzammal, S.M., Murugesan, R.K. and Jhanjhi, N.Z., 2020. A comprehensive review on secure routing in internet of things: Mitigation methods and trust-based approaches. IEEE Internet of Things Journal, 8(6), pp.4186-4210.

6. Prasad.A.Y and R. Balakrishna, "A generic algorithmic protocol approaches to improve network life time and energy efficient using combined genetic algorithm with simulated annealing in MANET," International journal of intelligent unmanned systems, vol. 8, no. 1, pp. 23–42, 2020.
7. Yu, D., Kang, J. and Dong, J., 2021. Service attack improvement in wireless sensor network based on machine learning. Microprocessors and Microsystems, 80, p.103637.
8. Mazumdar, N., Nag, A. and Singh, J.P., 2021. Cache-aware mobile data collection schedule for IoT enabled multi-rate data generator wireless sensor network. Sustainable Computing: Informatics and Systems, 31, p.100583.
9. Dong, M., Li, H., Yin, R., Qin, Y. and Hu, Y., 2021. Scalable asynchronous localization algorithm with mobility prediction for underwater wireless sensor networks. Chaos, Solitons & Fractals, 143, p.110588.
10. KS Ananda Kumar, R Balakrishna, AY Prasad "Implementation of ITREE-MAC Protocol for Effective Power Management and Time Synchronization in Wireless Sensor Networks", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-12, October 2019.
11. Xia, H., Zhang, S.S., Li, Y., Pan, Z.K., Peng, X. and Cheng, X.Z., 2019. An attack-resistant trust inference model for securing routing in vehicular ad hoc networks. IEEE Transactions on Vehicular Technology, 68(7), pp.7108-7120.
12. Xia, H., Li, Z., Zheng, Y., Liu, A., Choi, Y.J. and Sekiya, H., 2018. A novel light-weight subjective trust inference framework in MANETs. IEEE Transactions on Sustainable Computing, 5(2), pp.236-248.
13. Chen, H.C., 2015. TCABRP: a trust-based cooperation authentication bit-map routing protocol against insider security threats in wireless ad hoc networks. IEEE Systems Journal, 11(2), pp.449-459.
14. Kavita K. Patil, Senthil Kumaran, T., Prasad, A.Y. (2022). Improved Congestion Control in Wireless Sensor Networks Using Meta-Heuristic Approach. Advances in Computational Intelligence and Communication Technology. Lecture Notes in Networks and Systems, vol 399.
15. Gaber, T., Abdelwahab, S., Elhoseny, M. and Hassanien, A.E., 2018. Trust-based secure clustering in WSN-based intelligent transportation systems. Computer Networks, 146, pp.151-158.
16. Sun, Z., Wei, M., Zhang, Z. and Qu, G., 2019. Secure routing protocol based on multi-objective ant-colony-optimization for wireless sensor networks. Applied Soft Computing, 77, pp.366-375.
17. Mehetre, D.C., Roslin, S.E. and Wagh, S.J., 2019. Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust. Cluster Computing, 22, pp.1313-1328.
18. Ahmed, A., Bakar, K.A., Channa, M.I., Khan, A.W. and Haseeb, K., 2017. Energy-aware and secure routing with trust for disaster response wireless sensor network. Peer-to-Peer Networking and Applications, 10, pp.216-237.
19. AlFarraj, O., AlZubi, A. and Tolba, A., 2018. Trust-based neighbor selection using activation function for secure routing in wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, pp.1-11.

20. Periyanayagi, S. and Sumathy, V., 2018. Swarm-based defense technique for tampering and cheating attack in WSN using CPHS. Personal and Ubiquitous Computing, 22(5-6), pp.1165-1179.
21. Kalidoss, T., Rajasekaran, L., Kanagasabai, K., Sannasi, G. and Kannan, A., 2020. QoS aware trust based routing algorithm for wireless sensor networks. Wireless Personal Communications, 110, pp.1637-1658.
22. Alqahtani, A.S., 2020. Security threats and countermeasures in software defined network using efficient and secure trusted routing mechanism. Computer Communications, 153, pp.336-341.
23. Shende, D.K. and Sonavane, S.S., 2020. CrowWhale-ETR: CrowWhale optimization algorithm for energy and trust aware multicast routing in WSN for IoT applications. Wireless Networks, 26, pp.4011-4029.
24. Revanesh, M., Sridhar, V. and Acken, J.M., 2020. Secure coronas based zone clustering and routing model for distributed wireless sensor networks. Wireless Personal Communications, 112(3), pp.1829-1857.
25. Sakthidasan, K., Gao, X.Z., Devabalaji, K.R. and Roopa, Y.M., 2021. Energy based random repeat trust computation approach and Reliable Fuzzy and Heuristic Ant Colony mechanism for improving QoS in WSN. Energy Reports, 7, pp.7967-7976.
26. Goyat, R., Kumar, G., Alazab, M., Saha, R., Thomas, R. and Rai, M.K., 2021. A secure localization scheme based on trust assessment for WSNs using blockchain technology. Future Generation Computer Systems, 125, pp.221-231.
27. Ramkumar, K., Ananthi, N., Brabin, D.D., Goswami, P., Baskar, M., Bhatia, K.K. and Kumar, H., 2021. Efficient routing mechanism for neighbour selection using fuzzy logic in wireless sensor network. Computers & Electrical Engineering, 94, p.107365.
28. Hajiee, M., Fartash, M. and OsatiEraghi, N., 2021. An energy-aware trust and opportunity based routing algorithm in wireless sensor networks using multipath routes technique. Neural Processing Letters, 53(4), pp.2829-2852.
29. Feroz Khan, A.B. and Anandharaj, G., 2021. A cognitive energy efficient and trusted routing model for the security of wireless sensor networks: CEMT. Wireless Personal Communications, 119(4), pp.3149-3159.
30. Rajasoundaran, S., Kumar, S.S., Selvi, M., Ganapathy, S., Rakesh, R. and Kannan, A., 2021. Machine learning based volatile block chain construction for secure routing in decentralized military sensor networks. Wireless Networks, 27(7), pp.4513-4534.\
31. Fang, W., Zhang, W., Yang, W., Li, Z., Gao, W. and Yang, Y., 2021. Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks. Digital Communications and Networks, 7(4), pp.470-478.