Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7752048

ENHANCED SECURITY AGAINST INTRUDER BASED ON BAFFLEMENT TECHNIQUE FOR WIRELESS SENSOR NETWORK USING TRACKING NODE WITH SCRUTINY ALGORITHM

S Sowndeswari
Research Scholar,Dept. of Electronics & Telecommunication Engg., Sir M VIT, Bangalore.
Asst.Prof.,Dept. of ECE, Sambhram Institute of Technology, Bangalore.

E.Kavitha
Prof. & Head, Dept. of Electronics & Telecommunication Engg., Sir M VIT, Bangalore.

Abstract—Wireless Sensor Networks (WSN) provides extra vulnerabilities to overflow observer intruders because of the revealed pattern of authority overloading via the leader node. Studying packet overflow for an attack requires skill.
Aim/objective: The main challenge is to find a correlation between the cost of energy used, packet forwarding reliability, and the sensor network's level of protection. In this collective, previous methods focused mostly on cryptographic algorithms to achieve better packet security; however, this only shows a detachment of the safeguard matter of fact based on a mixture of operational network security and an energy-aware messaging platform that gives the same level of security. Still, it uses more energy during the route discovery process.
Methodology: This research demonstrates how a method called "Enhanced Security Against Intruder Based on Bafflement" (ESAIB) can use to make rank-based route changes safer. It depends on how the routes overlap, how much energy they use, how much the links cost, and how safe the nodes are. After which, the k-anonymity model says that monitoring nodes with the scrutiny algorithm can choose several intruder receiver nodes that look exactly like real target nodes. Ultimately, the best routes and selected items are chosen, and a higher risk level is reached without sacrificing energy efficiency.
Findings: The simulation results show that this method can effectively stop traffic monitoring attacks and hide the network topology for software-defined WSNs. Also, the proposed approaches can make attacks less likely to work while using less energy and making the network last longer. It needs to use the least energy and time from beginning to end. It makes it easier to find things, lasts longer, delivers more packets, and makes the network safer.
Keywords— Wireless Sensor Networks, energy-aware communication, Enhanced Security against intruders based on the Bafflement technique, scrutiny algorithm, k-anonymity model, security management intrusion detection.

I. INTRODUCTION

As seen in Figure 1, a WSN is a wirelessly connected network consisting of devices that are set up separately and use sensors that monitor their surroundings [1]. WSNs are used for many things, including video surveillance, tracking the surroundings, monitoring targets, military defence, detecting intrusions, etc. The primary reason why protection in WSNs is still evolving is that there need to be more effective security schemes; rather, the primary reason is that the

majority of the already available schemes are inadequate due to the distinctiveness of WSNs [2]. That is, nodes in WSNs are limited in how much they can compute and how much energy they can use. In WSNs, sensor networks can talk to each other, but their main purpose is to sense, collect, and process data. All such data is transmitted to a sink that might use them or send them to other networks through some hops. For WSNs to communicate well, they need routing algorithms that work well [3]. They make it easier for devices in WSNs to talk to each other by finding the best way to send data and keeping track of those routes. Because the nodes in WSNs are distinctive, network protocols had to be made for each WSN. For example, there is a network protocol that is only used by MWSNs and procedures that are only used by SWSNs [4].

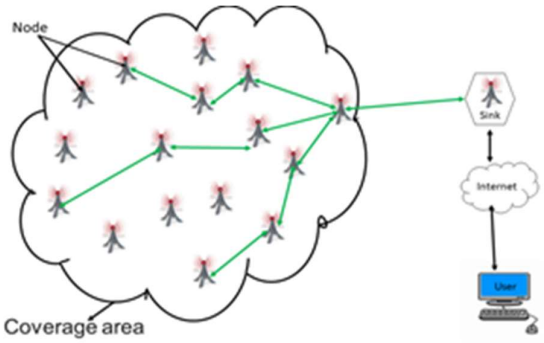

Fig. 1. A typical architecture of wireless sensor networks (WSN) [1].

In a WSN, there are two kinds of communication: single-hop and multi-hop. In a single-hop data transfer, the source node sends its data packets directly to the destination inside a single hop. In WSNs, the sensor networks may need to rely on each other to send packets to faraway places, named "multi-hop" communication. Multi hop is a type of routing in which data is sent from the source node to the destination node with the help of intermediate nodes [5]. It enhances the efficiency of WSNs by letting a node with low energy send data to the destination node through its neighbours on the routing path. Multi-hop routing comes with some safety and privacy problems. These problems, such as eavesdropping, wormhole, malicious attacks, Sybil, clone, black hole, impersonation attacks, etc., affect the WSNs' data security, accessibility, and truthfulness.

The sensors can use a multi-hop route discovery in various sensor network models to send data to the access point or sink. In summary, the WSN routing algorithm determines the best way to send the data from the source node to the base station (the destination node) [6]. Most of the WSN's performance depends on routing, which affects how long the network will last. Routing protocols are a big part of making networks last longer and more reliable. They do this by considering that sensor nodes have limited resources, such as a small amount of energy and a slow processor [7]. Reducing the amount of communication needed to send the data and figure out the best route is a difficult issue that needs to be kept in mind. The clustering method is the most widely recognized and often used for routing protocols [8].

As the need for real-time information has grown, WSNs that use a multi-hop transmission scheme to get around their limitations have become more useful. The main problem with multi-hop transmission is that the nodes' source data and affiliations can be attacked while hopping [9]. For a WSN with limited resources where the source node sends data to the destination nodes through several intermediate nodes, an attacker can break in, find out who the source

node is, glean information from the source data, or change the source data. Often, WSNs work in dangerous locations and can be attacked through side channels like differential power analysis. In such attacks, the attacker keeps an eye on the system, does the same thing repeatedly, and carefully measures the amount of energy used from cycle to cycle to either find the secret key or change it [10].

Several security solutions for WSNs have been thought of, but some don't work because sensors need more resources. Some WSNs, in contrast to other connections, are made up of mobile nodes that modify the network's structure from time to time, which means that these mobile networks can't use protocols made for networks with static nodes [11]. Furthermore, WSNs transfer a lot of data, adding to the traffic on their wireless telecommunications infrastructure. These things show that security and confidentiality solutions for WSN must not only be light in computation power, information exchange, and resource overheads, but they must also endorse accumulation and multi-hop to cut down on traffic and make the networks last longer. In the meantime, most security mechanisms already out there don't meet these performance standards.

Encryption technology, which uses a key to protect the original data, is a technique often discussed in the literature to secure these kinds of networks and can use the same key to encrypt and decrypt data or different keys for both encryption and decryption. The keys used in cryptography take up a lot of storage and energy space, which are in short supply in WSNs [12]. Access control is also hard because it must be sent to all network nodes, even those trying to harm. For security and decryption, cryptanalysis needs keys. Each node that joins a network is given its unique key. So, for complex systems, making a key is more difficult, takes up more space, and needs more hardware, increasing the amount of power used. For security, hybrid cryptographic techniques like elliptic cryptography, message authentication, and a mix of both symmetric and asymmetric cryptographic algorithms are also used. But these methods might not work well in WSNs because a large network makes things more complicated [13].

This work proposes a new ESAIB based on four important criteria: route overlap, energy usage, link costs, and node trustworthiness. This new ESAIB is designed to maximize the costs of an attack while being efficient and easy to use. Then, a tracking node with a scrutiny algorithm is made by choosing several intruder sink nodes that look exactly like real sink nodes by the k-anonymity model. Lastly, many simulations show that the proposed methods can effectively stop traffic analysis attacks and hide the topology of software-defined WSNs' networks. Also, the proposed approaches can lower the number of successful attacks while using less energy and making the network last longer.

Here's how the rest of the paper is put together. In Section II, we talk about work that is related. Section III shows the network and threat models and gives an overview of the ESAIB framework. In Section IV, an evaluation of ESAIB's work is given. Section V wraps up the paper and discusses what needs to be done in the future.

II. RELATED WORK

As was said above, the difficulty of detecting intrusions in WSNs can be modelled as the issue of finding the best way to encompass the intruder continuously and well. The Intrusion Detection Mechanism for Empowered Intruders in WSN (IDEI) that Wang et al. [14] proposed is made up of an intended pursuit algorithm for mobile sensing automobiles and a sleep-scheduling approach for node density. Remote sensing and geographical information

automobiles will accompany the armed intruder and fill in the gaps in media attention. At the same time, static nodes will consider a sleep schedule and be woken up by proximity identification nodes when the intruder is found. Simulation experiments are done to compare the proposal to established techniques of how well they detect intrusions, how much energy they use, and how far sensor nodes can move. Simulations are also used to study how sensitive IDEI is to parameter changes. The results of the conceptual model and the simulations show that the proposal can improve availability and reliability.

Basan et al. [15] came up with a way to find malicious nodes when physical features are broken. The suggested method is based on probabilistic functions, determining the coefficient of determination, and determining how likely the identified parameters will be outside the error range. The method is new because this part estimates the likelihood that an observation will fit into the error range and doesn't compare it to the statistical distribution. Most intrusion detection systems (Id cards) look at network traffic, but the proposed method looks at the physical characteristics of a malicious node. The idea's benefit is backed up by the fact that there could be attacks against workouts (e.g., node movement disorders, communication noises, etc.). Because an intruder can physically attack a sensor node, the Private Key Management strategy is useful for many WSN problems.

Kamble and Jog [16] suggested that the flexibility of the nodes is used to make key management in WSN less efficient for communication security using protocol certificates. Even if a new node joins a cluster, a GEO makes it easy to update the keys and keeps the keys secret. By removing a vulnerable node, the protocol limits the damage a malicious node can do to protect active communication links. An authentication process of this method showed that it worked well in a fight against a mobile wireless sensor network with many nodes. Network protection is the most difficult part of stopping deleterious types of attacks, and it's also a security issue in WSN and data security application fields.

The sensors in a WSN are set up so that their detection method can process data and talk to other sensors wirelessly. One of the best and most efficient ways to find and stop an intruder is to use traffic analysis to look for unusual patterns. In many WSN applications, one of the most important things to do is to safeguard the network of sensing devices from bad actors and attacks. Here, Kalnoor and Agarkhed [17] talk about some sophisticated preventative measures, security measures and intrusion prevention systems that help find and stop security problems in WSN.

Nabizadeh and Abbaspour [18] came up with IFRP, an Intrusion/Fault-tolerant Routing Protocol that uses both single and multi-path to enhance stability and resilience while also taking energy efficiency into account. In response to malicious behaviour by the local warden method, packet switching has been transitioning from a single route to a multi-path. IFRP also utilizes a local warden method and centralized decision-making to find and isolate nodes that have been hacked or aren't working properly. The experiments revealed that IFRP could make the network more reliable and productive against endpoints that drop packets without using too much energy.

Rajkumar and Vayanaperumal [19] suggested a Leader Based Intrusion Detection System [LBIDS] to find and stop DOS and other attacks like Sybil and Sinkholes in networks by putting them in base stations in the network systems. The proposed method uses three main security problems: authorization, providing positive incentives, and stopping DOS. In addition, it will

do message and IP validation to increase the accuracy of finding and stopping threats in networks that differ from each other.

Fan et al. [20] came up with a user authentication process for two-tiered WSNs that works well and is vulnerable to DoS attacks. The proposed method minimizes the work on the computer because it only does simple things like exclusive OR and one-way hashing. This feature is better for sensor nodes and portable devices that don't have a lot of resources. And expert nodes don't need to send login access requests to the access point or keep a long list of users. Also, a pseudonym identity is added to protect the privacy of users. The suggested methodology can stop smart card breaches by being well thought out. Lastly, protection and needs improvement demonstrates that the scheme works well and is strong.

Raja and Beno [21] showed a new security mechanism and method for wireless sensor networks and an example of how this algorithm could be used. Multifactor authentication against Denial-of-Service attacks is the plan's goal (DOS). Network simulator2 is used to test the plan (NS2). Then, this plan is looked at in terms of how often network packets are delivered, and discovered that throughput has increased.

Ovasapyan and Ivanov [22] used the trust model to consider security in wireless sensor networks. The design parameters of sensor networks are looked at, and a list of the different ways to route data is made. Attacks on Wireless Sensor Networks (WSNs) that have already happened are looked at and analyzed. The trust model is used to develop a way to protect against compromised nodes. A WSN simulation model is used to model how the technique works so that it can be tested to see how well it works.

Das [23] suggested a way for WSNs to increase security with three factors. This scheme also has a higher level of security and better security features than other schemes. This part also uses the widely used AVISPA (Automated Validation of Internet Security Protocols and Applications) tool to replicate the scheme for the formal security analysis. The outcomes of the simulation clearly show that the strategy is also safe.

Umarani and Kannan [24] proposed Hybrid Anomaly Detection Systems (HADS), also called Artificial Immune Systems in WSNs. In this schema, a new intrusion detection algorithm is made using the Hybrid Tissue Growing Algorithm (HTGA) to find networks acting strangely and an interaction tissue structure that works well to send data packets. This algorithm is used in the Networked Tissue Growing (NTG) model and the Swarm Tissue Growing (STG) algorithm. Both are self-sufficient because they can warn when they see something out of the ordinary on the route. The numbers of entries in the neighborhood table and route maintenance are the main things that affect the interconnectivity computation. If the surface predicts that a network will die in a week, it will immediately get rid of that network to keep it from becoming an intruder. The network-based computation retains the network in a clustering state that changes over time. This article aims to create a pertinently aware IDS by combining the concept of tissues. It will give stronger, more flexible, and more accurate protection against attacks in the sensor network from outsiders.

Das et al. [25] showed secure smart card-based biometrics-based user authentication system for WMSNs. This part shows that the strategy is safe from known attacks by conducting a thorough formal and informal security analysis. Also, this segment simulates the system using the Automated Verification of Cyber security Procedures and Implementations tool, which is

broadly used and acknowledged, and the results show that the system is safe. Compared to similar schemes, this one is also good at computing and communicating.

Das [26] devised a new way to authenticate users with three factors that work well for distributed WSNs. The plan is simple because it only needs an efficient hash function for cryptography and symmetric cryptographic decryption and encryption operational processes. Also, this plan is safe from known attacks, proven by a thorough informal and formal security analysis. This part also uses the Automated Verification of Internet Security Applications and Protocols tool to simulate the formal security authentication scheme. The simulation results clearly show that the scheme is safe from passive and active attackers.

Kumar and Sivagami [27] discussed a fuzzy logic system for finding malicious nodes. Using this fuzzy system, each sensor node of the network gets a trust score. The identification of malicious nodes is dependent on the trust score that has been generated. The Improved Elliptic Curve Cryptography (IECC) algorithm sends data securely. Oppositional Particle Swarm Optimization (OPSO) is part of ECC. The simulation results indicate that this suggested technique is better than the existing ones in terms of how much energy it uses, how long it lasts, and how long it takes to do something.

Orea-Flores et al. [28] came up with two ways to reduce the packets' size to send visual information for outdoor monitoring. Such techniques use a hashing algorithm of the descriptive statistics of image data in various formats to send small packets with necessary information about the surroundings being watched. Also, this part suggests an ON/OFF scheme cut down on energy use even more. The effectiveness of such solutions in various contexts is assessed using a telegraphic study. Increasing system longevity and high identification probability often compete for efficiency goals, but the resulting statistical model makes it possible to fine-tune the system characteristics to meet both.

Ngai et al. [29] showed a new way to find the intruder in an attacker node using an automated system. First, the algorithm checks for reliability in the data to discover a list of suspicious nodes. Afterwards, it analyses the dynamic network information to find the intruder on the ranking. The method is also strong enough to handle multiple bad nodes working together to conceal the actual intruder. This part used numerical models and experiments to test how well the proposed algorithm worked. These tests showed that the algorithm worked well and was accurate. The results also show that wireless sensor networks' computational and communication costs are not too high. Table 1 shows the research gap's details and its pros and cons.

TABLE I. THE RESEARCH GAP OF EACH METHOD WITH ITS ADVANTAGES AND DISADVANTAGES

Method	Advantages	Disadvantages
IDEI [14]	The proposed plan has a good detection system against intruders with more power and a lower cost of energy.	But a very large number of sensors are needed to build a complete barrier.
Security Key management technique [15]	In intrusion detection, this technique meets the need for reduced latency service.	The initial placement of the sensor nodes has a big effect on the quality of the coverage.
GEO [16]	This method has a high coverage rate, and the detection nodes use less energy.	But the way the test was performed in the scheme was pretty stable, so it couldn't accurately describe how intruders and nodes moved.
Preventive security mechanisms [17]	These methods provide better levels of security.	But sensor nodes only have a limited amount of processing power and memory, so the old ways of doing things can't just transfer to WSNs.

IFRP [18]	This method reduces the energy used and makes the network last longer.	But it is still hard to figure out how to choose the best edge nodes in the system.
LBIDS [19]	It offers protection for all the connections, individually or dispersed.	There is a desire for a multi-sensing platform that combines various technologies to identify human intrusion with enhanced system precision in flat disputed areas.
DoS-resistant user authentication scheme [20]	High data transmission and lifetime of the network.	But they are open to security attacks because they are hardto deploy and have few resources.
DoS security mechanism [21]	High data transmission, long network life, and the least amount of energy used.	But this technique is restricted in many ways, such as its limited intelligence to compute, its limited energy resources, and its susceptibility to put more emphasis, making it a specific security challenge that needs significant improvement.
Trust model [22]	This method makes the WSN as safe as possible.	But in its applications, WSN still faces problems with limited resources like devices, information processing, and energy, as well as other problems that have to do with availability, reliability, and security.
AVISPA [23]	The longest network life and the least amount of energy used.	It does not safeguard against sheltered insider attacks.
HADS [24]	Minimal transmitter hubs that can move into the target area to collect interesting information.	But secure transmission of data packets is the most important issue in this network because WSNs are vulnerable to attacks like black holes and warm holes.
Secure biometrics-based user authentication scheme [25]	Better efficiency and longer network life.	This approach needs to be in the registration stage for the sensor network.
a novel three-factor user authentication scheme [26]	High efficiency with the least amount of energy used.	This system can still be attacked by a privileged insider or a sensor node, and it doesn't protect user anonymity.
Fuzzy logic system [27]	High performance and network connectivity.	During the credential update phase, it doesn't update the user's new password correctly.
Hash function [28]	The system uses less energy because of this method.	It doesn't allow for interactive sensor node extension after the network's nodes have been set up.
SET [29]	This identification technique is quite effective at tracking intruders by analyzing their path.	This method has a lot of extra work and needs all of the nodes to coordinate with each other in terms of time.

Summary: The results of recent study evaluations are shown to give an idea of how security works. Recent analytic presentations will make it easier for people to get to work and connect in a safe and reliable way. Future work on this problem will include third-party authorization for each sensor network or new arrivals to the network, along with better key scheduling to make it harder for people from elsewhere in the network to get in easily. It will additionally show that approved sensor nodes in a wireless connection can act as third-party verification servers for each other and help the access point find intruders.

III. PROPOSED METHODOLOGY

This work suggests a way to make the network more secure against attacks from internet traffic intruders. The suggested solution strikes a balance between the need for protection and the limits on resources and trust. A ranking-based route mutation mechanism is proposed, in which the Bafflement Technique (Algorithm 1) is used to choose paths for flows' routes in the network. These routes are chosen based on various factors that ensure a high standard of base station security in the network by overlapping routes and considering WSN necessities like energy use and link cost. Also, numerous pathways that have been changed can be made to trick the enemy and provide scrutiny algorithms (Algorithm 2) for fully-centered WSNs. Numerous intruder sink nodes are chosen to trick an attacker trying to find the sink node, where a fitting parameter is used to take into account the residual energy of the neighbours of the

chosen intruder sink nodes due to the expected extra communication cost in their region. Also, the suggested solution is not too expensive and can be used for large sensor networks.

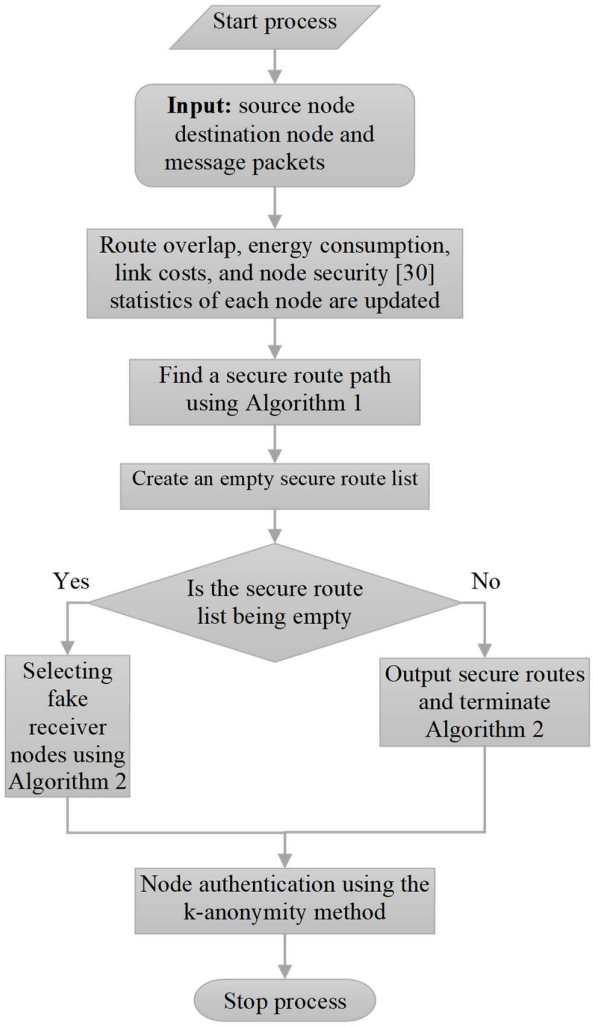

Fig. 2. Flow chart for the mechanism of proposed secure routing paths against an intruder in WSN.

A. Threat Model Assumption

In this research, this part assumes an outsider adversary, which is an unauthorized user who does not have permission to control the sensor network. The adversary wants to attack the network availability; however, s/he cannot attack the controller directly. To launch an effective attack, the adversary must learn the network topology and identify the high-profile nodes that play significant roles in network communication, including sink nodes, intermediate nodes, and shared nodes of both control and data traffic. Most messages are transmitted alongpaths with high-profile nodes and produce pronounced traffic patterns that reveal traffic path information, direction, and thus the location of these nodes. The adversary must first launch a traffic analysis attack, a remote software-based attack, or a physical attack on the network. This adversary can hijack (capture) sensor nodes; consequently, s/he can obtain its flow table, eavesdropping communications within the node's range (passive monitoring), and reveal some statistics about

the neighbourhood. The adversary can gather information about the network without detection, as the sensor node will continue to act normally with no malicious actions. The adversary can compromise only a small number of nodes at any reasonable cost (time). In this research, without loss of generality, this part considers that the adversary can only compromise one node during a control period Δt

In this work, imagine an intruder, which is an unauthorized client who does not possess authorization to govern the sensor system. The enemy desires to target the availability of the system. Nevertheless, they can't directly attack the controller. For an attack to work, the attacker needs to know how the network is set up and find the high-profile nodes that play important roles in communication networks, such as sink nodes, intermediate nodes, and nodes that control data traffic share. Often these messages are sent along pathways with nodes with a lot of traffic that make clear traffic patterns that show traffic path information [31], the traffic orientation, and where these nodes are. The enemy must launch a traffic monitoring attack, a faraway software-based intrusion, or a violent assault on the network. This enemy can take over sensor nodes, so they can get the node's forwarding table, listen in on conversations within the node's range, and share some information about the neighbourhood. The adversary can learn about the system without being noticed because the sensor node will keep doing normal things and not do anything bad. At any reasonable cost, the enemy can only take over a simple number of nodes. The cost of a route is the sum of all the links in that path .

$$\cos t(p) = \sum_{\forall E_{uv} \in p} \cos t(E_{uv}) \qquad (1)$$

Where E is the edge of the network structure and 'energy' is the residual energy consumed by each node, and it is an important factor in choosing a convinced node in the pathway and computing the energy level's weightiness of a node as follows:

$$E_{uv} = \frac{energy_u}{dist_{uv}} \qquad (2)$$

Here energy consumption model of packet transmission is a role of distance dist between two nodes of u and v. As a result, the distance is considered to determine the edge energy cost for edge .

B. Enhanced security against intruders based on the Bafflement technique

The proposed method employs an ESAIB to monitor wireless networks with more than one hop. The source node (S), the destination node (D), and the intermediate node ( ) make up a sensor network [32]. The sensor node has enough coverage to keep a constant eye on the information exchange. The other nodes are called non- nodes. It uses up the node's energy by being idle. 'In' does observe within its range of transmission. The idea behind ESAIB is to find the nodes that are supposed to be somewhere other than there in a large-scale scalable network. The 's job is to keep an eye on the new entry node, collect information about the node's settings, and decide whether or not to add the new entry node to a scalable network. The suggested method finds the intruder in the terrain and gives them a safe way to talk. Due to its ability to sense, WSN has limited energy, 'In' node is to watch the transmission of the two nodes, such as the source address and the neighbour node, within its range and regularly update the information about the neighbour node till it reaches its destination node.

ESAIB is used to choose the right set of nodes needed to monitor certain network connectivity from the node mobility. The sensor nodes know where they are being put. The algorithm in

utilizes the most energy as the parameter to monitor communication within that range. While it's doing this, it drains some energy and chooses a new node from what's left. The sensing power is divided by the time it takes for the network to communicate, and the 'In' node keeps an eye on this. The In changes based on how much energy is left.

Bafflement Technique: Figure 3 shows that the In-based monitoring mechanism comprises a sensor node in the network. 'In' has the most energy to find the external nodes and verify them. In a multi-hop wireless network, a malicious node can interfere with connectivity. This problem can be solved by the 'In', which verifies only trusted nodes and ensures that communication is secure within the transmission range. It sits at the edge of the network's transmission range and finds the bad node in a network with multiple hops. When an intruder node interacts with another node in the network, there is poor communication, which leads to more network congestion. It can be stopped by the authentication of the In, which finds the intruder node and blocks communication with it. Table 1 shows the step-by-step process of ESAIB, and Fig. 2 shows a flowchart of the process.

TABLE II. ALGORITHM FOR ENHANCED SECURITY AGAINST INTRUDER BASED ON BAFFLEMENT TECHNIQUE (ALGORITHM 1)

S- Source node
D- Destination node
$Pack$-packet
Step 1: sender --> (pack)
Step 2: for each node, find the best node
Step 3: $if\ (node == similar)$
Step 4: S->Pack.
Step 5: sender select that common node for data transmission.
Step 6: destination organize the information
Step 7: Pack->D
Step 8: $elseif\ (node == dissimilar)$
Step 9: sender node eliminate that common node for data transmission.
Step 10: node discover another node for communication
Step 11: End if.
Step 12: $discard < -\ (node)$
Step 13: discover$< -(\ node)$
Step 14: end for

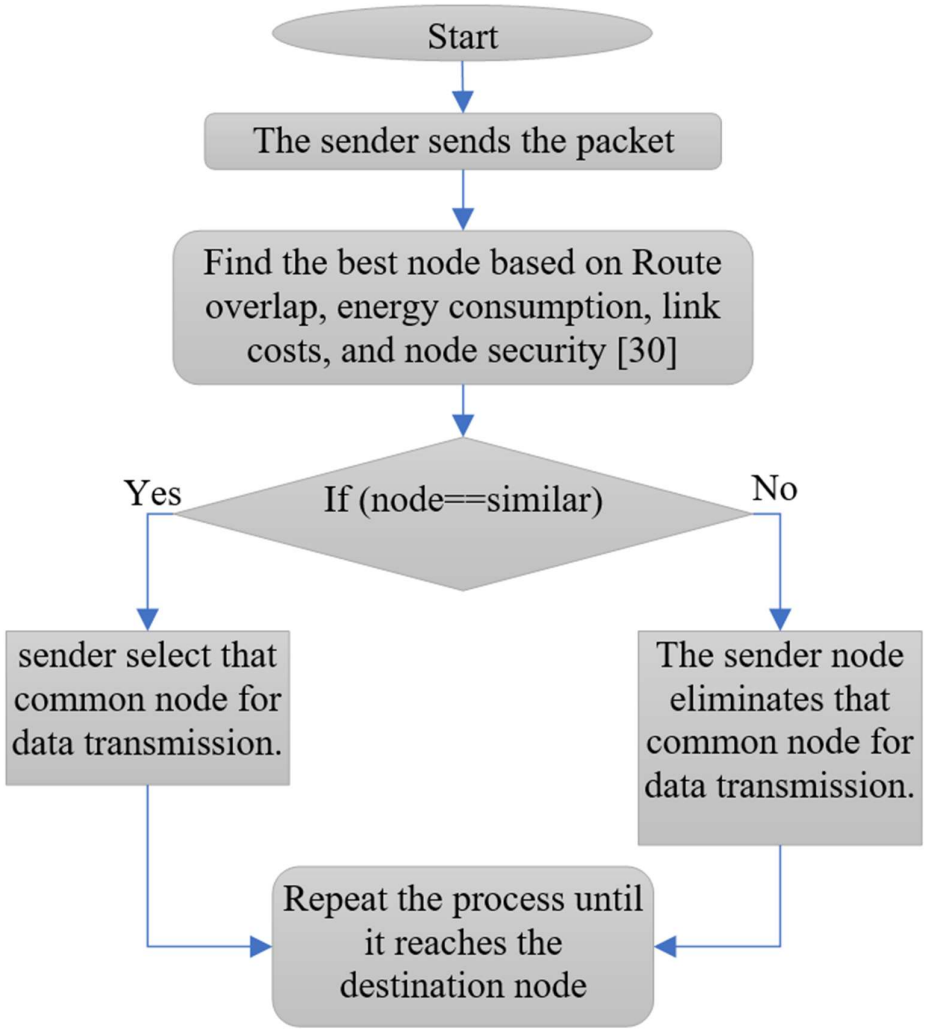

Fig. 3. Flowchart of ESAIB Model

C. Selection of Intruder Nodes using the scrutiny Method

This method separates the network into K networks that don't overlap, keeping the traffic load as low as possible. Then, one of the k intruders sinks nodes is chosen from each network to create local maxima, where deceptive traffic is made between the members of a network and the selected intruder sink node depending on the number of nodes, their distances, and how much traffic is projected. To find the intruder sink node in a network, the controller sorts all the nodes in the network by an energy-based fit score. Then, the top access points in each network are used to make the Sset. As all the nodes start with the same amount of energy, Sset is chosen randomly under the protection constraint. But after one round, the energy left over will be different. When the residual energy of the network's intruder sink node falls below one threshold thenergy, which is calculated depending on the energy level of all nodes in the network, the controller reselects the network's intruder sink node and updates the flow rules so that the cost of choosing the intruder to sink for each network is minimized as long as the selected node's residue left energy is higher than thenergy:

$$\max \sum_{\forall s \in s_{set}} ESAIB(s) \,\&\, \min \sum_{\forall s \in s_{set}} \cos t(s)$$

$$s.\text{t.energy } y_{it} > th_{energy}, \forall_s \in s_{set}$$

When a node in the S set is chosen, both its energy level and the tiers of the nodes around it is important. All the network nodes send false information to this intruder sink node. The leader nodes are sorted by a fit score (Fitenergy) to reduce the energy used by fake traffic inside the network. The fit score considers the node's energy level and the energy levels of its m nearest neighbours in the network. If the neighbour node has some less hop interconnection to the leader node, then its fit score has a bigger effect. Due to fake traffic delivery, the nodes nearest to the intruder sink node will use more transmission energy.

For instance, if node v is a leader node, node u is v's neighbour and is only one hop away, while node w is three hops away and takes three connections to reach v. When figuring out the fit score of node v, the energy levels of neighbouring nodes u and v are taken into account. But because node u is closer, its energy level must have more of an effect than that of node w. The challenge is to create it and take the enemy as many steps as possible to find the sink nodes. So, the higher steps mean that the level of obfuscation is higher. Use the cost of travel (TC) of a k-anonymity of the genuine and intruder sink nodes to figure out how many steps an adversary must take to move from a maximum local trap to the next closest trap. Table 2 and Fig.4 show the algorithm procedure of tracking nodes to find intruders with the scrutiny method and flowchart, respectively.

TABLE III. TRACKING NODES FOR INTRUDER DETECTION WITH SCRUTINY METHOD (ALGORITHM 2)

Step 1: for each node, observe its neighbour member node
Step 2: $if(node == intruder)$
Step 3: discover another optimal next-neighbour node
Step 4: data transmission proceeds for the next neighbour node
Step 5: else
Step 6:$if\ (node! = intruder)$
Step 7: Select the optimal threshold level node
Step 8: data transmission is performed for this neighbour node
Step 9: end if
Step 10: minimize energy consumption, end to end delay, and improve security
Step 11: End for

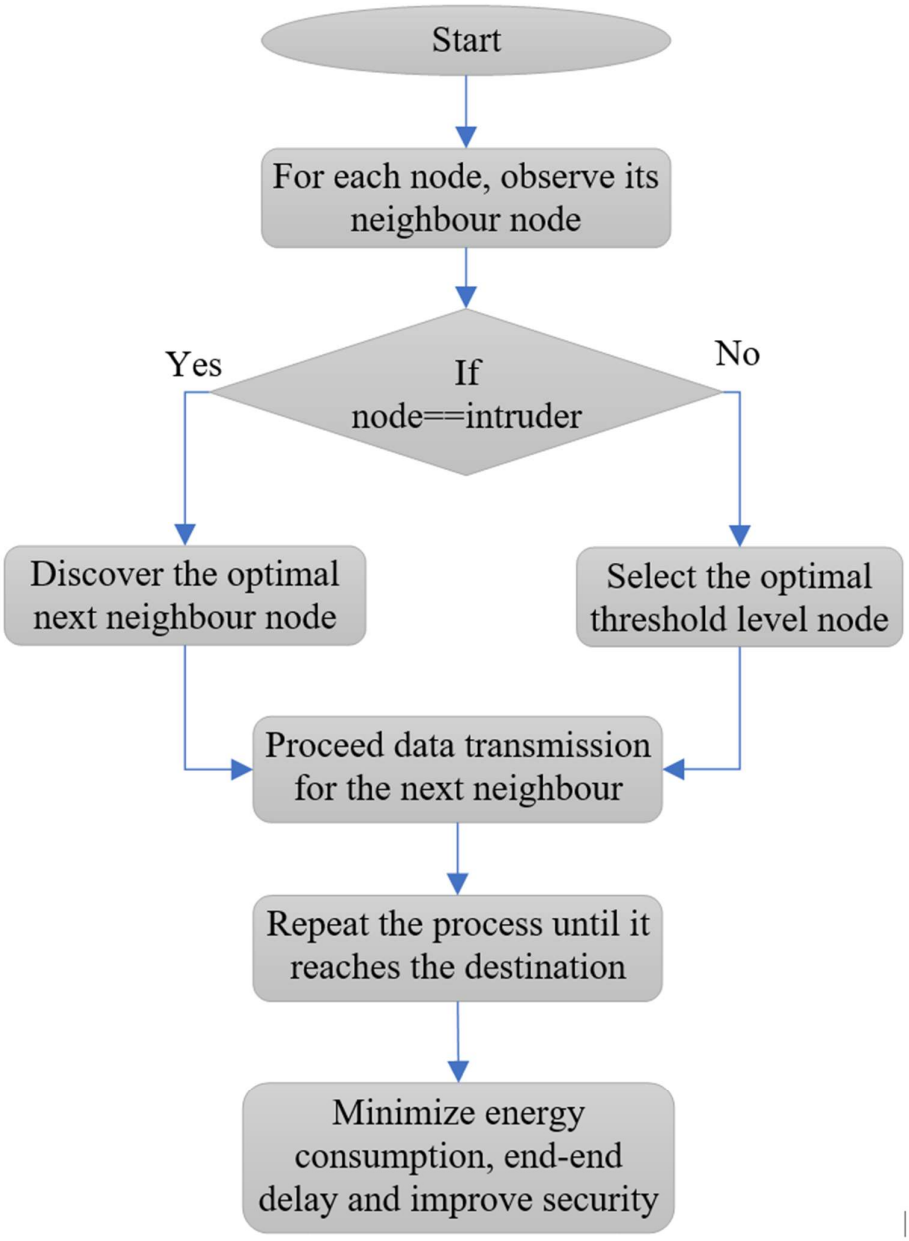

Fig. 4. The flowchart of tracking nodes for intruder detection with scrutiny method

IV. EXPERIMENTAL RESULTS AND DISCUSSION

This part looks at how the proposed plan would work out. This section looks at how useful the proposed method and mechanism are and how much it will cost to implement. Also, the presented scheme ESAIB is judged by comparing its performance with existing schemes like GEO [33] and SET [34], which is done by simulating the results using the well-known tool NS-2 and looking at metrics like energy consumption, security, End-to-End Delay, Detection Efficiency, Network Lifetime, and Packet Delivery Ratio (PDR).

Energy consumption.Fig.5 shows how the energy consumption of the current system and the proposed systems' energy consumption compare in a heterogeneous setting. The proposed system cuts down on communication costs because it eliminates intruders before routing data. When the network size is 100, the percentage of the system still alive for existing methods like GEO and SET is 213 and 180, respectively, but it is only 157 for the proposed system. Lastly, the proposed secure routing scheme keeps intruders out by keeping the energy consumption ratio as low as possible. The experimental observations are that in ESAIB, the average energy consumption is low for the first-time data is sent. The energy consumption in the first round of the ESAIB protocol with a single data transmission phase is higher because the initial setup cost is a little higher, and the energy used in the first phases is considered energy consumption when the k-anonymity and scrutiny method is used.

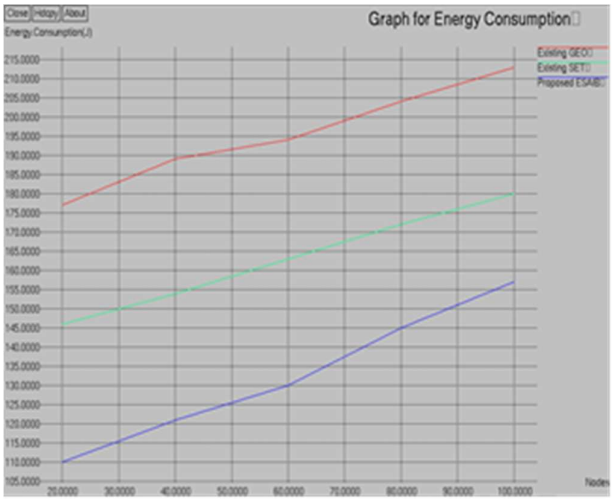

Fig. 5. Energy Consumption Comparison Results Between Proposed Method and Existing Method

TABLE IV. NUMERICAL RESULTS OF ENERGY CONSUMPTION COMPARISON RESULTS BETWEEN PROPOSED METHOD AND EXISTING METHOD

No of nodes	Energy consumption		
	Existing GEO	***Existing SET***	***Proposed ESAIB***
20	176	146	110
40	188	154	121
60	194	164	130
80	204	173	145
100	213	180	157

Security.Fig.6 shows how the existing and proposed systems compare in terms of security in a WSN environment. The proposed system reduces the time it takes to send a message because it eliminates both black hole attacks before the actual data routing. When the size of the network is 100, the percentage of the system that is still alive with existing methods like GEO and SET is 41 and 50 percent, but it is 87 percent with the proposed system. Lastly, the proposed secure routing scheme keeps intruders from getting in, which is done by making the ratio of connections as high as possible. The observations show that the average level of security in ESAIB during the first data transmission periods is high. In the ESAIB protocol with security measures, the reason for more trust scores in the first round is that the initial setup cost is a

little bit higher, and trust score in the first phases is considered to be wasted energy when a security model with trust is used.

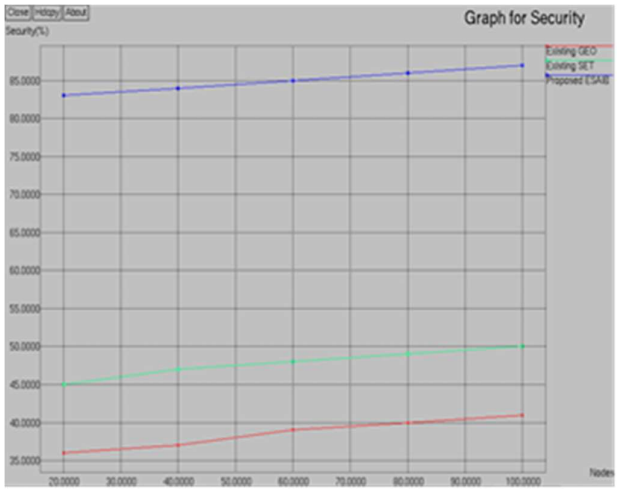

Fig. 6. SecurityComparison Results Between Proposed Method and Existing Method

TABLE V. NUMERICAL RESULTS OF SECURITYCOMPARISON RESULTS BETWEEN PROPOSED METHOD AND EXISTING METHOD

No of nodes	Security(%)		
	Existing GEO	***Existing SET***	***Proposed ESAIB***
20	36	45	83
40	37	47	84
60	39	48	85
80	40	49	86
100	41	50	87

End-to-End Delay.Table 6 shows that the time it takes to send a packet from the source node to the destination node is used to evaluate the end-to-end delay. Information about each node is kept in the routing table. Especially in comparison to GEO and SET, the proposed ESAIB scheme has less delay from beginning to end.

$$End\ to\ end\ delay = End\ time - Start\ time \quad (3)$$

Fig.7 shows an analysis of the end-to-end delay of the current system and the proposed system in a uniform environment. For a homogeneous network, the proposed system has a lot of energy. For example, when the size of the network is 100, the time the system stays alive with the existing approaches, GEO and SET, is 18.2s and 21.3s, respectively, but it only stays alive for 10.9s with the proposed system. The observations show that the average end-to-end time for ESAIB with the first data transmission times is low.

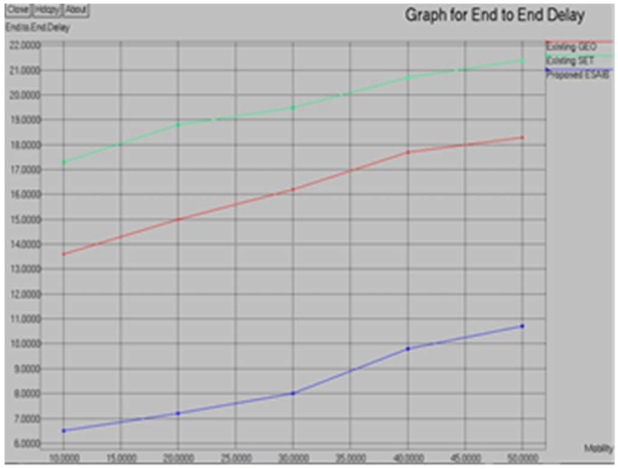

Fig. 7. End-to-End Delay Comparison Results Between Proposed Method and Existing Method

TABLE VI. NUMERICAL RESULTS OF END-TO-END DELAY COMPARISON RESULTS BETWEEN PROPOSED METHOD AND EXISTING METHOD

No of nodes	End-to-End Delay(sec)		
	Existing GEO	***Existing SET***	***Proposed ESAIB***
20	13.5	17.2	6.7
40	15	18.8	7.2
60	16.2	19.4	8
80	17.8	20.8	9.9
100	18.2	21.3	10.95

Detection efficiency. When comparing detection efficiency based on how much energy is used per packet, Table 7 shows that ESAIB has high detection efficiency with less energy. The observations show that the average amount of energy used in ESAIB during the first data transmission periods is higher. On the other hand, when GEO and SET are compared with more rounds of data transfer, SET is better than GEO. In ESAIB with a single data transmission phase, the average amount of energy used in the first round is higher because the initial setup cost is higher and the energy used in the first phases is considered to be overhead energy. But GEO and SET use less energy per packet than ESAIB after the whole round.

Fig.8 compares how well the existing and proposed systems can find intruder in a mixed environment called detection efficiency. The proposed system makes it easier to find intruders because it gets rid of them before actual data routing. When the network size is 100, GEO and SET have a 48 and 63 percent chance of keeping the system alive, but the proposed system has an 80 percent chance.

Fig. 8. Detection Efficiency Comparison Results Between Proposed Method and Existing Method

TABLE VII. NUMERICAL RESULTS OF DETECTION EFFICIENCY COMPARISON RESULTS BETWEEN PROPOSED METHOD AND EXISTING METHOD

No of nodes	Detection Efficiency(%)		
	Existing GEO	***Existing SET***	***Proposed ESAIB***
20	43	58	74
40	44	59	75
60	46	61	77
80	47	62	79
100	48	63	80

Network Lifetime.It is measured as the amount of time until the message loss rate goes above a certain level. The numbers are shown in Table 8. "Time to network partition" is a better way to describe how long a network will last. When there is a break in the network, this is called a "Slashed." It will be launched as a new metric that uses the difference in energy:

$$Network\ \text{lifetime} = \text{E-}\left(\frac{\sum U_i}{N} + \left(\frac{\left(\frac{U_i - \sum U_i}{N}\right)^2}{N}\right)\right) \qquad (4)$$

E is the total initial energy at each node (full battery charge), Ui is the average used energy, and N is the total number of nodes in the network.

Fig.9 compares the current system's network lifetimes and the proposed system in a mixed environment. Because it gets rid of both black holes before actual data routing, the proposed system makes the network last longer. Existing methods, like GEO and SET, keep the system alive for 38 and 66 minutes when the network size is 100, but the proposed system keeps it alive for 82 minutes. The observations show that the network lifetime used in ESAIB during the first data transmission periods is higher. On the other hand, when GEO and SET are compared with more rounds of data transfer, GEO is better than SET. In ESAIB with a single data transmission phase, the network lifetime used in the first round is higher because the initial setup cost is higher. The energy used in the first phases is considered overhead network lifetime. But ESAIB does better than GEO and SET regarding how much life it uses on average per packet after its whole round with cost score.

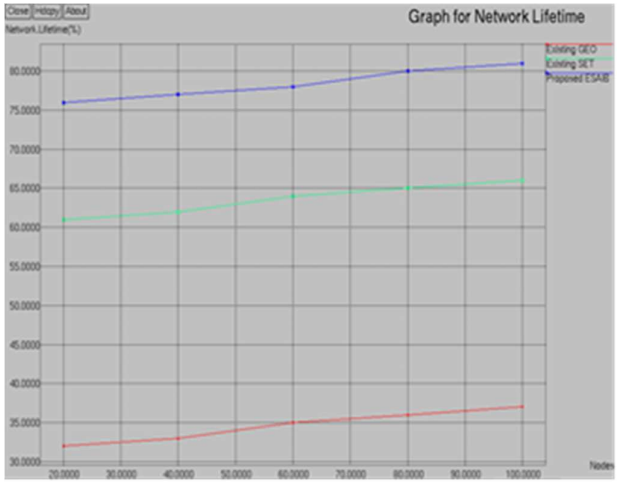

Fig. 9. Network Lifetime Comparison Results Between Proposed Method and Existing Method

TABLE VIII. NUMERICAL RESULTS OF NETWORK LIFETIME COMPARISON RESULTS BETWEEN PROPOSED METHOD AND EXISTING METHOD

No of nodes	Network Lifetime(%)		
	Existing GEO	***Existing SET***	***Proposed ESAIB***
20	32	61	76
40	34	62	77
60	35	64	78
80	36	65	80
100	38	66	82

Packet Delivery Ratio (PDR).Table 9 shows that the number of packets received is proportional to the number of packets sent at a certain speed. Node speed is sometimes different; simulation mobility is always 100. (bps). Compared to the existing methods, GEO and SET, the ESAIB scheme increases the number of delivered packets.

$$PDR = \frac{Number \text{ of packet received}}{sent} * speed \quad (5)$$

In a heterogeneous environment, Fig. 10 shows how the existing and proposed systems compare in terms of PDR. Because it gets rid of an intruder before actual data routing, the proposed system makes the network last longer. Existing methods, such as GEO and SET, keep the system alive for 54 and 41 minutes when the network size is 100, but the proposed system keeps it alive for 84 minutes. The observations show that more packets are delivered during the first data transmission periods in ESAIB. On the other hand, when more rounds of data transfer are used to compare GEO and SET, SET is found to be more efficient than GEO. In ESAIB with a single data transmission phase, the average energy used in the first round is higher because the initial setup cost is higher. The energy used in the first stages is considered overhead PDR. But GEO and SET use less energy per packet than ESAIB after the whole round.

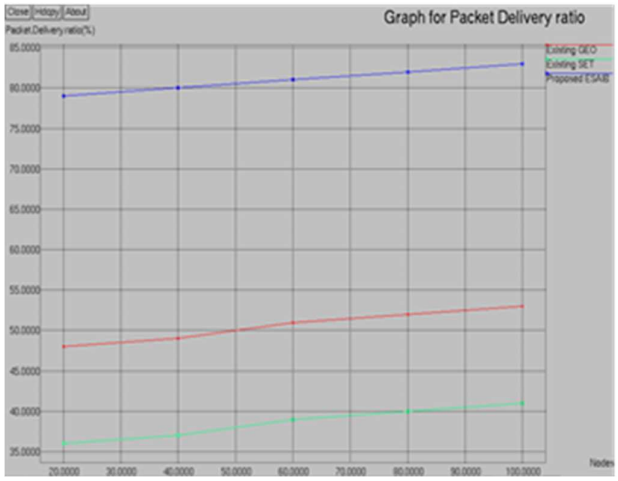

Fig. 10. Packet delivery ratio Comparison Results Between Proposed Method and Existing Method

TABLE IX. NUMERICAL RESULTS OF PACKET DELIVERY RATIO COMPARISON RESULTS BETWEEN PROPOSED METHOD AND EXISTING METHOD

No of nodes	Packet delivery ratio(%)		
	Existing GEO	***Existing SET***	***Proposed ESAIB***
20	47	36	78
40	48	37	80
60	52	39	82
80	53	40	83
100	54	41	84

V. CONCLUSION AND FUTURE WORK

This part of the presentation talked about an ESAIB framework that makes wireless sensor networks safer. There are two ways to look at it. On the one hand, the Bafflement technique describes a set of custom methods for hiding information that works safely. On the other hand, use k-anonymity and the scrutiny method to protect sensitive data stored in WSN nodes from being shared. The simulation results show that the proposed solution works: while the confusion factor went up, protection went up, and the overhead caused by the intruder changes was minimal in terms of energy use, network lifetime, delay, and how well it could find intruders. The ESAIB's methods make it hard to translate instructions and share sensitive information. Compared to other detection models, it makes it much easier to find an intruder in WSN. At the same time, the model's k-anonymity does not slow down the rate of detection, which means that the model can be found in real-time. In future research, this work will concentrate on figuring out how accurate intruder detection is in the case of an unbalanced intruder and how to tell normal system data from intruder data. At the same time, this will also concentrate on solving the problem of how much energy the system uses and how to make the algorithm work better in future research.

ACKNOWLEDGMENT

REFERENCES

[1] Alkhatib, A. A. A., & Baicher, G. S. (2012, April). Wireless sensor network architecture. In 2012 International conference on computer networks and communication systems (CNCS 2012). Singapore: IACSIT Press.

[2] Alcaraz, C., Lopez, J., Roman, R., & Chen, H. H. (2012). Selecting key management schemes for WSN applications. Computers & Security, 31(8), 956-966.

[3] Pantazis, N. A., Nikolidakis, S. A., & Vergados, D. D. (2012). Energy-efficient routing protocols in wireless sensor networks: A survey. IEEE Communications surveys & tutorials, 15(2), 551-591.

[4] Olakanmi, O. O., & Dada, A. (2020). Wireless sensor networks (WSNs): Security and privacy issues and solutions. Wireless mesh networks-security, architectures and protocols, 13.

[5] Akila, I. S., & Venkatesan, R. (2019). An energy balanced geo-cluster head set based multi-hop routing for wireless sensor networks. Cluster Computing, 22(4), 9865-9874.

[6] Zin, S. M., Anuar, N. B., Kiah, M. L. M., & Pathan, A. S. K. (2014). Routing protocol design for secure WSN: Review and open research issues. Journal of Network and Computer Applications, 41, 517-530.

[7] Akgül, F., & Frangopol, D. M. (2004). Computational platform for predicting lifetime system reliability profiles for different structure types in a network. Journal of Computing in Civil Engineering, 18(2), 92-104.

[8] Misra, S., & Kumar, R. (2016, November). A literature survey on various clustering approaches in wireless sensor network. In 2016 2nd international conference on communication control and intelligent systems (CCIS) (pp. 18-22). IEEE.

[9] Wei, X., Wang, Q., Wang, T., & Fan, J. (2016). Jammer localization in multi-hop wireless network: A comprehensive survey. IEEE Communications Surveys &Tutorials, 19(2), 765-799.

[10] Olakanmi, O. O., & Dada, A. (2021). An efficient point-to-point security solution for multi-hop routing in wireless sensor networks. Security and privacy, 4(5), e58.

[11] Jain, A., Kant, K., & Tripathy, M. R. (2012, January). Security solutions for wireless sensor networks. In 2012 Second International Conference on Advanced Computing & Communication Technologies (pp. 430-433). IEEE.

[12] Trad, A., Bahattab, A. A., & Othman, S. B. (2014, January). Performance trade-offs of encryption algorithms for wireless sensor networks. In 2014 World Congress on Computer Applications and Information Systems (WCCAIS) (pp. 1-6). IEEE.

[13] Gandara, R. B., Wang, G., & Utama, D. N. (2018, September). Hybrid cryptography on wireless sensor network: a systematic literature review. In 2018 International Conference on Information Management and Technology (ICIMTech) (pp. 241-245). IEEE.

[14] Wang, W., Huang, H., Li, Q., He, F., & Sha, C. (2020). Generalized intrusion detection mechanism for empowered intruders in wireless sensor networks. IEEE Access, 8, 25170-25183.

[15] Basan, A., Basan, E., & Makarevich, O. (2017, October). A trust evaluation method for active attack counteraction in wireless sensor networks. In 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) (pp. 369-372). IEEE.

[16] Kamble, S. B., & Jog, V. V. (2017, May). Efficient key management for dynamic wireless sensor network. In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information& Communication Technology (RTEICT) (pp. 583-586). IEEE.

[17] Kalnoor, G., & Agarkhed, J. (2016, March). Preventing attacks and detecting intruder for secured Wireless Sensor Networks. In 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) (pp. 1062-1067). IEEE.

[18] Nabizadeh, H., & Abbaspour, M. (2013). IFRP: an intrusion/fault tolerant routing protocol for increasing resiliency and reliability in wireless sensor networks. International Journal of Ad Hoc and Ubiquitous Computing, 14(1), 52-69.

[19] Rajkumar, D. U. S., & Vayanaperumal, R. (2015, September). A leader based intrusion detection system for preventing intruder in heterogeneous wireless sensor network. In 2015 IEEE Bombay Section Symposium (IBSS) (pp. 1-6). IEEE.

[20] Fan, R., He, D. J., Pan, X. Z., & Ping, L. D. (2011). An efficient and DoS-resistant user authentication scheme for two-tiered wireless sensor networks. Journal of Zhejiang University SCIENCE C, 12(7), 550-560.

[21] Raja, K. N., & Beno, M. M. (2014). On securing Wireless Sensor Network-Novel authentication scheme against DOS attacks. Journal of medical systems, 38(10), 1-5.

[22] Ovasapyan, T. D., & Ivanov, D. V. (2018). Security provision in wireless sensor networks on the basis of the trust model. Automatic Control and Computer Sciences, 52(8), 1042-1048.

[23] Das, A. K. (2016). A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks. Peer-to-peer Networking and Applications, 9(1), 223-244.

[24] Umarani, C., & Kannan, S. (2020). Intrusion detection system using hybrid tissue growing algorithm for wireless sensor network. Peer-to-Peer Networking and Applications, 13(3), 752-761.

[25] Das, A. K., Sutrala, A. K., Odelu, V., & Goswami, A. (2017). A secure smartcard-based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks. Wireless Personal Communications, 94(3), 1899-1933.

[26] Das, A. K. (2015). A secure and efficient user anonymity-preserving three-factor authentication protocol for large-scale distributed wireless sensor networks. Wireless Personal Communications, 82(3), 1377-1404.

[27] Kumar, A. R., & Sivagami, A. (2020). Fuzzy based malicious node detection and security-aware multi-path routing for wireless multimedia sensor network. Multimedia Tools and Applications, 79(19), 14031-14051.

[28] Orea-Flores, I. Y., Rivero-Angeles, M. E., Onofre-Soto, A. L., Azpeitia-Rebollar, E. G., Torres-Cruz, N., Villordo-Jiménez, I., ... &Menchaca-Mendez, R. (2022). Teletraffic analysis of energy-efficient intruder detection using hash function techniques in images for remote monitoring in Wireless Sensor Networks. Computers and Electrical Engineering, 103, 108373.

[29] Ngai, E. C., Liu, J., & Lyu, M. R. (2007). An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. Computer Communications, 30(11-12), 2353-2364.

[30] Bin-Yahya, M., & Shen, X. (2022). Secure and energy-efficient network topology obfuscation for software-defined WSNs. IEEE Internet of Things Journal.

[31] Deng, J., Han, R., & Mishra, S. (2005, September). Countermeasures against traffic analysis attacks in wireless sensor networks. In First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05) (pp. 113-126). IEEE.

[32] Spachos, P., Toumpakaris, D., & Hatzinakos, D. (2014, May). Angle-based dynamic routing scheme for source location privacy in wireless sensor networks. In 2014 IEEE 79th Vehicular Technology Conference (VTC Spring) (pp. 1-5). IEEE.

[33] Vinayagam, S. S., & Parthasarathy, V. (2018). A Energy Balanced Geo Cluster Head Set Based Multi-Hop Routing for Wireless Sensor Network. Adhoc & Sensor Wireless Networks, 42.

[34] Lu, H., Li, J., & Guizani, M. (2013). Secure and efficient data transmission for cluster-based wireless sensor networks. IEEE transactions on parallel and distributed systems, 25(3), 750-761.