International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/221900 Volume 10, Issue 3, May – June (2023)

RESEARCH ARTICLE

Robust Tristate Security Mechanism to Protect Against Selective Forwarding Attack and Black Hole Attack in Intra-Cluster Multi-Hop Communication

A. Anitha
Department of Computer Science, Kongunadu Arts and Science College, Coimbatore, Tamil Nadu, India.
anithaaruchamy91@gmail.com

S. Mythili
Department of Information Technology, Kongunadu Arts and Science College, Coimbatore, Tamil Nadu, India.
smythili78@gmail.com

Received: 21 April 2023 / Revised: 02 June 2023 / Accepted: 05 June 2023 / Published: 30 June 2023

Abstract – Security is the most vital issue to be addressed in Wireless Sensor Networks (WSNs). The WSN dominates since it has an effectiveness of applications in numerous fields. Though it has effectiveness towards its applications likewise it is susceptible to two different kinds of attacks (i.e.) external attacks and internal attacks existence of constrained reckoning resources, low memory, inadequate battery lifetime, handling control, and nonexistence of interfere resilient packet. Handle internal attacks such as selective forwarding attacks (SFAs) and black hole attacks (BHA) are considered to be the most common security extortions in wireless sensor networks. The attacker nodes will execute mischievous activities during data communication by creating traffic load, delaying packet delivery, dropping packets selectively or dropping all packets, energy consumption, and depleting all network resources. These attacks can be handled efficiently by implementing the proposed methodology for detecting, preventing, and recovering Cluster Heads (CHs), Cluster Members (CMs), and Transient Nodes (TNs) from SFAs and BHA in intra-cluster multi-hop. It is accomplished by proposing a robust strategy for overcoming internal attacks on cluster head, cluster member, and transient node. The Fuzzy C-Means clustering is used to discover the prominent cluster head. The uncertainty entropy model is used to detect internal attacks by removing the malicious node from the transition path. The intermediate node is been selected based on the degree and dimension. The experimental results of the proposed Robust Tristate Security Mechanism (RTSSM) against SFAs and BHA are evaluated with packet delivery ratio, throughput, and packet drop and the results prove the effectiveness of the proposed methodology and it also aids in the extension of the network lifetime.

Index Terms – Cluster Head, Cluster Member, Intra-Cluster, Multi-Hop, Clustering, Wireless Sensor Networks, Uncertainty, Robust, Fuzzy Membership, Entropy.

1. INTRODUCTION

Wireless sensor networks comprise a group of sensor nodes that are scattered over the network. It is a distinct practice of ad hoc networks. This network ensures a great sector of applications conversely which are defenseless from extortions. Current developments in sensors are largely fortified with data processing and communication competencies [1]. Likewise, wireless sensor networks have great data sensitivities, allowing attacker to access the data from the sensor nodes indiscernibly [2]. Wireless sensor networks are infrastructure-less and the connections are wireless since it is wide-open to several security attacks [3]. Many existing approaches are used for the detection and prevention of sensor nodes in WSNs and very few works are done for only recovering from SFAs and BHA. These are the internal attacks that are difficult to handle. It has various forms of dropping the data packets during data transmission. SFAs have more than three ways of attacking strategies. They are the attacker node that will drop the entire data packets before reaching the desired destination and this form is called the BHA [4]. It is highly vulnerable since no data can be received at the destination. The next form is the attacker node will selectively drop the forwarded data packets when the data transmission occurs between the source and destination which leads to data loss. And the third form is that it will selectively forward the data packets to the destination and cause infinite routing loops and traffic.

Clustered Wireless Sensor Network (CWSN) is formed by the process of clustering. It is a technique that can be defined as an assemblage of independent sensor nodes to form different clusters and there are two types of routing process or cluster communication is established [5]. They are intra-cluster

RESEARCH ARTICLE

communication and inter-cluster communication. The intra-cluster communication takes place within the cluster (between CH and CMs). The inter-cluster communication takes place between the CHs to BS (between one CH to another CH). Further, intra-cluster communication is classified into two types and it is depicted in Figure 1. They are intra-cluster single-hop communication and intra-cluster multi-hop communication. In [4] secure data transmission in intra-cluster single-hop communications is successfully implemented by detecting and preventing CH and CM from SFAs and BHA. This paper demonstrates secure data transmission by implementing RTSSM for intra-cluster multi-hop communication by detecting, preventing, and recovering from SFAs and BHA encounters during the three states of sensor nodes (CH, CM, and TN).

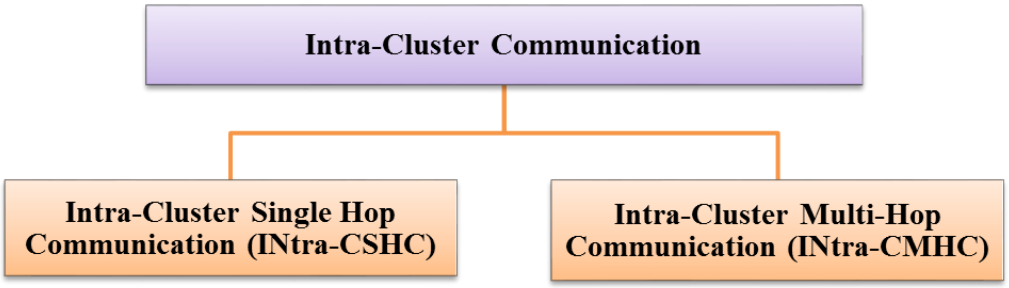

Figure 1 Types of Intra-Cluster Communication in CWSN

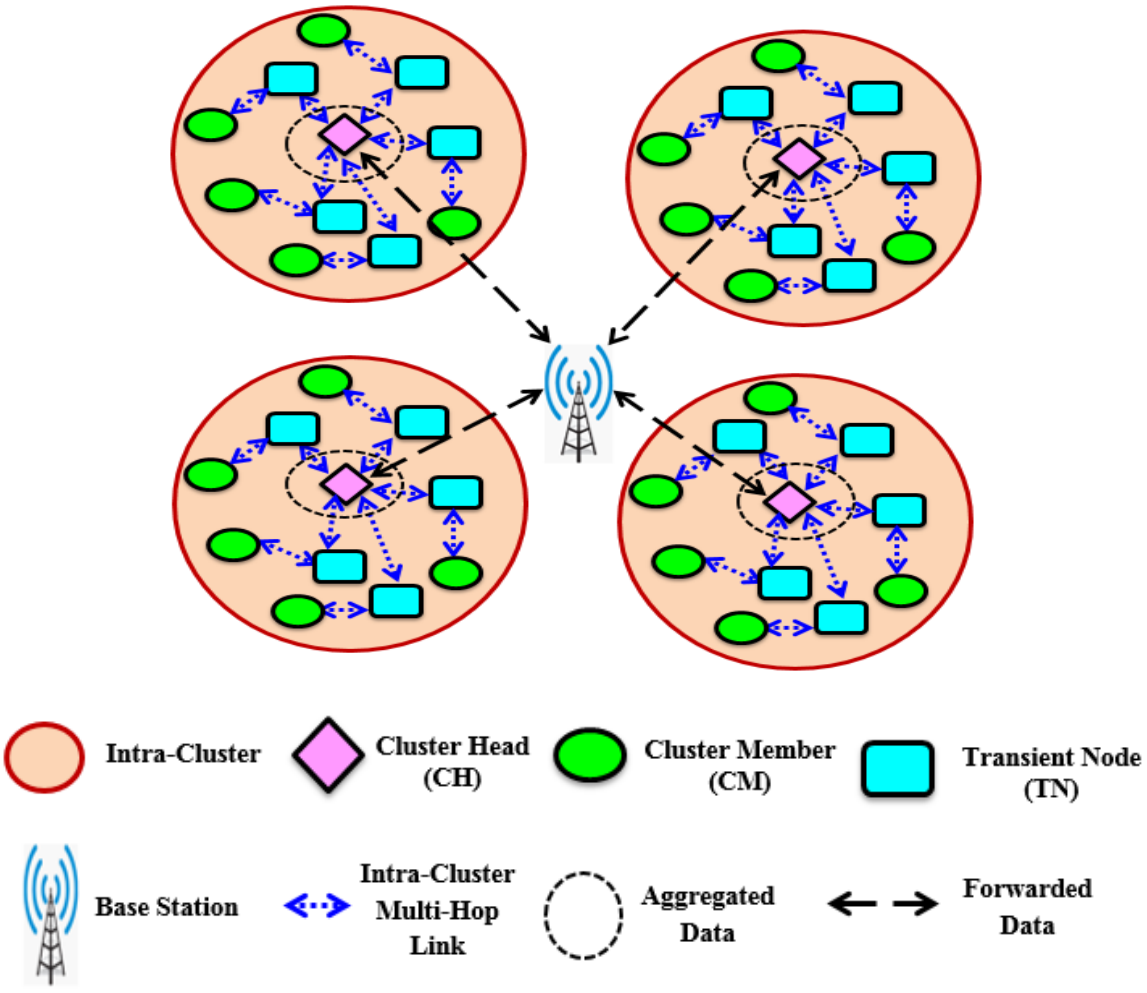

Figure 2 Framework of Intra-Cluster Multi-Hop Communication

RESEARCH ARTICLE

1.1. Problem Description

When the network size is large, the CH and CMs will be deployed in a wider range then direct communication or intra-cluster single-hop communication is not applicable as in [2]. Hence, the work has been extended by proposing a methodology for secure intra-cluster multi-hop communication from SFAs and BHA which leads a path to provide a well-established data link between CHs and CMs via TN. The unfair selection of CH among the sensor nodes will create chaos in network operation and drain all necessary network resources. And also persisting network lifetime in intra-cluster multi-hop communication becomes vital to minimize the energy consumption of each sensor node [10]. There are many existing approaches available in the detection, and prevention of SFAs and BHA of sensor nodes which have a limitation that it does not include the recovery mechanism. Similarly, those approaches have not enforced the detection and prevention approaches for all states of nodes in the intra-cluster. So, the problem of each state of nodes (CHs, CMs, and TNs) in intra-cluster multi-hop wants to be safeguarded separately to provide a secure data transmission; the proposed work develops energy-efficient Fuzzy C- means clustering with entropy-based trust computation to select potential cluster head (CH) of each cluster.

1.2. Objectives

The proposed methodology focuses on detecting, preventing, and recovering the CH, CM, and TN from SFAs and BHA in intra-cluster multi-hop communication. Major contributions of the proposed work are as follows:

- ✓ Introducing the algorithm for detecting, preventing, and recovering from SFAs and BHA.
- ✓ Selection of the most suitable sensor node with the highest enduring energy as the CH using Fuzzy C-Means Clustering
- ✓ Assistant CH is elected in advance to avoid network disruption when CH energy gets drained or turned into an attacker node.
- ✓ Each sensor node (CH, CM, and TN) of the intra-cluster multi-hop is protected separately by RTSSM.
- ✓ Providing secure data transmission in intra-cluster multi-hop communication
- ✓ To be responsible for maximizing the packet delivery ratio, and throughput and minimize the energy consumption and packet loss to enhance network performance.

1.3. Organization of the Paper

Section 2 gives an overview of the existing works and its drawbacks. Section 3 provides a detailed explanation of the proposed methodology RTSSM. Section 4 delivers the results obtained and also a comprehensive discussion about comparative analysis based on packet delivery ratio, throughput and packet drop, and energy consumption. And Section 5 determines the efficiency of the proposed methodology in association with the research objectives.

2. LITERATURE REVIEW

Turgut and IpekAbasıkeleş [11] proposed a multi-hop intra-cluster clustering architecture. It is been designed in a way that all sensor nodes will get into their sleeping mode in the initial stage by computing their time to wake up depending on two criteria (i.e.) degree and average distance to reach their neighbors. Sensor nodes that contain N number of neighbors and also with short average distance will wake up earlier to compete in the CH selection. Therefore, it involves more energy consumption of sensor nodes during the CH selection phase and also in balanced cluster formation. The time duration for clustering is high.

Mezghani [12] presented a distributed multi-hop intra-clustering approach based on Khalimsky topology. The sensor nodes deployed have formed into large dynamic clusters based on K-hop.CH selection made by an aspect of weight. The weight of all sensor nodes depends on their remaining energy, nodes degree, and probability of communication between neighbors. The sensor node which contains the highest weight will gets selected as CH. This approach results in the finest intra-cluster routing and reduces energy consumption. But the problem of uncertainty in the detection of outliers is still challenging.

Wu et al [13] suggested "Low-Energy Adaptive Clustering Hierarchy with Adaptive Balance Function (LEACH_ABF) strategy" is the combination of diversity and convergence functions together. It uses genetic operations to provide better solutions to help with finding the finest solution. The author also discussed the competitiveness of the algorithm. Incorporation of the extra three procedures will increase the intricacy of the algorithm. Meantime it is not suitable for multi-channel issues.

El Alami and Najid [14] proposed Enhanced Clustering Hierarchy (ECH) for maximizing in extending network lifetime, minimizing data redundancy and energy consumption. It has been done by lowering the rate of data redundancy via sleeping and waking nodes. The CH selection is executed randomly in the initial phase which leads to the wrong selection of CH with low energy causing the CH node to die soon.

Gohar Ali et al [15] presented a new intra-cluster scheduling scheme for real-time flow. Three scheduling algorithms are used for sending and receiving data based on the scheduled time slot. But this may need much time to complete the data transmission due to the scheduling process. The network

RESEARCH ARTICLE

resources may drain fast before participating in the communication.

Hasan et al [16] conducted the performance of ad hoc Internet of Things (IoT) networks utilizing the Ad-hoc On-Demand Distance Vector (AODV) routing protocol is forensically examined in this study under the black hole attack, a type of denial-of-service assault that is harmful to IoT networks. This study also analyses the protocol's vulnerability and looks at the network's and nodes' traffic patterns to assess the damage caused by the attack. It also reconstructs networks with various modes and parameters to confirm the study and offers recommendations for developing robust routing methods. The black hole attack with vague information about the nodes is not reliably handled in this work.

Malik et al [17] stated that by identifying BHA at an early stage of the route discovery process, a novel approach dubbed detection and prevention of a BHA is offered to safeguard and enhance the overall security and performance of the Vehicular Ad hoc Networks (VANETs). The suggested model is based on creating a forged route request (RREQ) packet and manipulating a dynamic threshold value. The static assumption of route discovery is not suitable in real-time ad hoc networks and the effectiveness in secure data transmission is ineffective without dealing with a dynamic environment.

The longer the distance between the nodes and sink, the larger the energy consumption that occurs during data transmission in WSNs, and this is advocated in [18] [19] and [20] by network clustering to tackle this problem. The fundamentals of WSN performance serve as a standard for WSN performance. For random CHs, a low-energy adaptive clustering hierarchy (LEACH) would partition the whole network into many clusters. Because LEACH does not take into account the remaining energy of the node, its implementation would result in an unequal distribution of CHs.

Ramesh et al [21] introduced an unsupervised algorithm that integrates the LEACH protocol and k Means clustering for cluster head selection. It aggregates the data within the cluster and transmitted it via the cluster head. The conventional Euclidean distance is used. The problem of selecting cluster head is done arbitrarily and only the measure of distance alone is considered for clustering. The computation complexity and time complexity in re-clustering and selection of cluster heads still exist.

Sangeeth and Sabari [22] designed a hybrid model which integrates k-means clustering to generate an algorithm to improve the inequality in clustering the mobile nodes. The genetic algorithm is deployed with a new fitness value evaluation. But still, the problem of local optima in the searching process is not treated in this work and it affects the detection of black hole attacks and selected forward attacks. This work consists of two centralized dynamic genetic algorithm-constructed algorithms for achieving the objective in MWSNs. The first algorithm is based on an improved Unequal Clustering-Genetic Algorithm, and the second algorithm is Hybrid K-means Clustering-Genetic Algorithm.

Zannou et al [23] suggested the “DP Clustering Algorithm” which permits the sensor nodes grouping based on their coordinate locations. It facilitates the sensor nodes to take up their own decisions based on the occurrence of the data flow in the network and also creates an automatic routing path that prolongs the network lifespan. The algorithm has focused on prolonging the network lifetime in multi-hop data transmission. It has the limitations of selecting the low-energy sensor node as the cluster head which fallouts into uneven circulation of the cluster head.

From the existing study, it is analysed that the performance of the secure data transmission affected due to uncertainty behaviour exhibited by the black hole and selective forwarding attacks, the conventional classical theories based security mechanism cannot able to handle the outliers, mischievous nodes accurately. To overcome the aforementioned issues, this proposed work, uses the uncertainty theory known as fuzzy C Means clustering, which handles the vague information about the outliers and anonymous data packet loss more precisely with the grade of membership and density defining with fuzzy Euclidean distance instead of conventional Euclidean distance to build a strong tristate security mechanism.

3. PROPOSED METHODOLOGY

The proposed methodology is a Robust Tristate State security mechanism (RTSSM) based on Detection, Prevention, and Recovery from Selective Forwarding and Black Hole Attacks of Cluster Head, Cluster Member, and Transient Node. RTSSM focuses on providing secure intra-cluster multi-hop communication. By coupling three mechanisms altogether and offering secure data communication on each state of intra-cluster sensor nodes CMs, CHs, and TNs from SFAs and BHA. Figure 3 represents the overall architecture of the proposed methodology. At the time of network model generation, the sensor nodes deployed in the specific deployment area are in a distributed way. Then the cluster formation and cluster head selection is executed using Fuzzy C-Means clustering. The nodes with the highest objective function will get selected as the potential CH. Elected CH will announce its election to its neighbour sensor nodes to become its CMs. Based on the distance of CH and sensor nodes the intra-cluster single-hop or multi-hop architecture is formed. The proposed methodology mainly concentrates on intra-cluster multi-hop. The distance is computed using Euclidean distance, and entropy-based trust value is used for forwarding the packets in the intra-cluster between the CH and

RESEARCH ARTICLE

intermediate sensor nodes as TN. The CMs will respond to the CH announcement status through their respective TNs. Intra-cluster multi-hop communication is established between CMs and TNs to reach its CH.

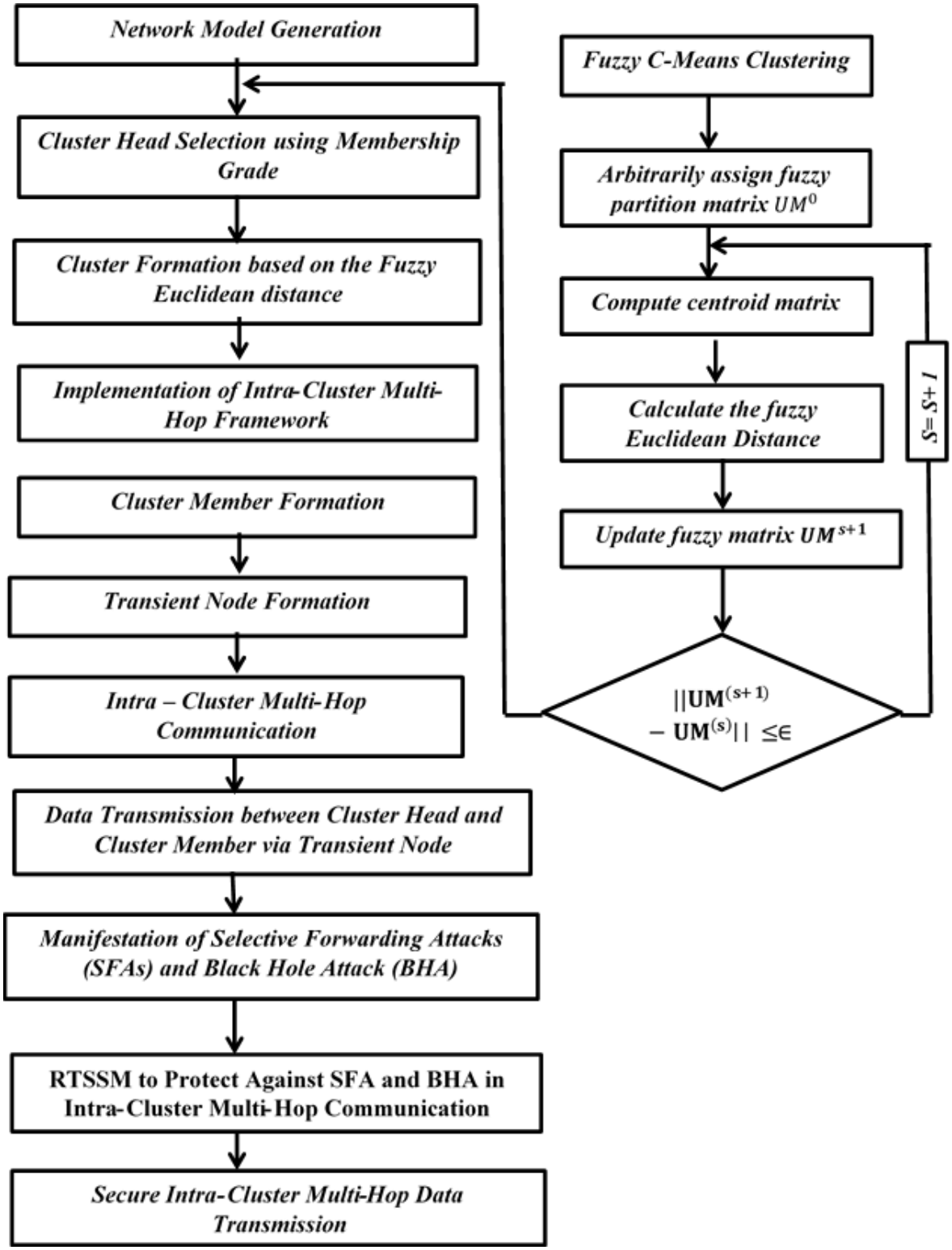

Figure 3 Overall Architecture of the Proposed Methodology

RESEARCH ARTICLE

Once the cluster formation is complete, next the data communication takes place between CHs and CMs through their TNs. During this data transmission process CH, CM, and TN may suffer from internal attacks such as SFAs and BHA which is challenging to identify, prevent and rectify. Hence, the proposed methodology is implemented to protect each sensor node presented in intra-cluster multi-hop.

3.1. Cluster Head (CH) Selection and Cluster Formation

During CH selection, each sensor node presented within the cluster will compete with one another to get elected as the CH to establish the cluster communication. All sensor nodes will share the control message with their neighbor sensor nodes within its cluster. The first time, one sensor node is elected randomly as CH, and then that node analysis will compare with the other sensor nodes. After the initial fuzzy membership partition, the cluster head is selected by performing Fuzzy C-Means clustering. Sensor nodes with the highest objective function or fitness value are selected as cluster heads instead of randomly selecting CH in traditional clustering. Then the selected CH announces its selection to its cluster sensor node by sending them JOIN_REQUEST_MSG and once those sensor nodes receive this message, it verifies the distance between CH and the sensor node. When the distance is not reachable, then it replies with the response that it will become its cluster members (CMs) and this occurs when the network size is small where the direct communication takes place within the intra-cluster. When the CH distance is not reachable then it seeks the help of the transient node (TN) acts as a communication bridge between CH and CM. The data communication is done via multi-hop. CMs communicate with their CH via the TNs and vice versa.

3.1.1. Fuzzy C-Means Algorithm Based Cluster Head Selection

In Fuzzy C-Means Clustering each instance can be a member of several clusters under the clustering paradigm, which depends on the membership value. The objective function is minimized for it to operate. A cluster's membership ratings define the extent to which instances are a part of each cluster. So, instances with lower degrees of membership at the cluster peripheral may be part of it to a lesser extent than the cluster head. Basic procedure involved while using Fuzzy C-means clustering [24]. The Algorithm 1 explains the selection of cluster head using Fuzzy C-Means clustering.

Step 1: Assign sensor nodes randomly to be the initial cluster heads.

Step2: Repeat until the stop criteria are satisfied:

a) Compute the membership matrix of each node in the network as formulated as shown in equation (1).

$$\mathrm{UM_g} = \frac{1}{\sum_{l-1}^{n} \left(\frac{\rho(\mathrm{CL_i},\mathrm{H_g})}{\rho(\mathrm{CL_i},\mathrm{H_l})}\right)^{2/(m-1)}} \quad (1)$$

b) The fuzzy Euclidean distance measure is represented in equation (2). Where represents the membership value of ith N node on gth cluster, CLi refers to cluster member, and H is the cluster head or centroid in equation (2).

$$\rho(CL_i, H_g) = \sqrt[2]{\sum_{i=1}^{n}(H_g - CL_i)} \quad (2)$$

c) Update fuzzy cluster center modeling back into the equation (3). In equation (3) r refers to the number of cluster heads in the network and refers to updated cluster heads using fuzzy clustering.

$$H_r = \frac{\sum_{i-1}^{L} \mathrm{UM_{gi}^m CL_i}}{\sum_{j-1}^{L} \mathrm{UM_{gj}^m}} \quad (3)$$

Step 3: Sort the nodes based on the membership value and the node with the highest membership value is declared as the cluster head in each cluster.

Step 4: List potential cluster heads in each cluster.

Step 5: End the process

Algorithm 1 Cluster Head Selection Using Fuzzy C – Means Clustering

For cluster head selection, in this proposed work the fuzzy c means clustering is adopted as given in algorithm 1. Each node in the WSN is converted into a fuzzy representation using fuzzy membership computation. Next, the initial cluster head is selected arbitrarily, and then based on its other nodes evaluated using a fuzzy objective function. The cluster centroids are rearranged based on the membership values. Then the finalized centroids are considered cluster heads. Further data transmission from a particular node to another node or destination node is done through the cluster head alone.

3.1.2. Determining the Entropy Based Trust Value of Transmission Nodes

Keeping track of Node X's general behavior depends on success (sc) and failure (fl) [25]. To keep track of the number of successes and failures for packets that ndx forwards from source node nd*i*, rendering to X's packet forwarding behavior to node ndi, ndm verifies source node evidence for each packet that X is promoting and updates a pair of discrete counters, sci, and fli, where I is the packets of the source node.

Data gathered in the first step, and Node Member (NM) evaluates Y's source-level trust values Ti[x] grounded on (sci,fli) in addition to its overall trust value Trstβ, i[Y] founded on sc and fl to determine how much NM trusts X in

RESEARCH ARTICLE

forwarding packets from source node ni. To specify X's source-level trust value for source node ni when the beta trust model is in use is formulated as in equation (4).

$$Trst_{\beta,i}[Y] = (sc_i + 1) / (sc_i + fl_i + 2) \quad (4)$$

The equation (5) is used for the calculating the computation of trust value based on entropy and it is given as follows:

$$Trst_{\beta,i}[Y] = \begin{cases} 1 - HY(PB_i), 0.5 \leq pb \leq 1 \\ HY(PB_i) \;\; 0 \leq pb \leq 0.5 \end{cases} \quad (5)$$

The transient nodes and the potential CH nodes entropy values are also considered for transmitting the data packets in a more optimized manner.

3.2. Robust Tristate Security Mechanism (RTSSM) to Protect Against Selective Forward and Black Hole Attack in Intra-Cluster Multi-Hop Communication

Algorithm 2 presents the methodology for protecting the cluster heads, cluster members, and transient nodes by detecting, preventing, and recovering those nodes from SFAs and BHA. The sensor nodes are deployed in a scattered manner in the specified area. Then Algorithm 2 implements the CH selection to initiate the communication. In algorithm 2, the Elected CH will broadcast its elected status with a JOIN_REQUEST_MSG to its neighbor sensor nodes to become its CMs. The neighbor sensor nodes will calculate the CH distance from its pre-defined distance when the distance of CH is higher subsequently to ensure the data transmission through multi-hop and the sensor nodes which need to become the CMs of that CH will seek the help of its intermediate member node or TN by sending JOIN_REPLY_MSG. The TNs will forward that message to its CH and this helps to create an intra-cluster data link between CMs and CH via its TNs. When the distance between the CH and CM is not far away automatically, it performs direct communication with CH to become its CMs by sending JOIN_REPLY_MSG. Actual data transmission within the intra-cluster takes place after the completion of this process. CH is monitored frequently to detect whether it suffers from SFAs and BHA. When the timestamp of elected CH is greater than the threshold value of SFA, then that elected CH is encountered with the attack. After the detection is made, the intimation about the malicious elected CH is removed from the routing table and also notification about the attacker node (elected CH) is sent to its CMs and TNs. Meantime, when the timestamp value of the elected CH is not greater than the threshold value of SFA, then the CMs of the cluster will forward the data packets to its elected CH through the TNs. The elected CH will perform the process of data aggregation of the received data packets from its CMs and TNs. Once the data aggregation gets over, all the accumulated data is dispatched to BS. The Assistant CH is an added advantage of our proposed methodology to provide effective working of the network. The energy of the CM and TN is compared with the energy of the elected CH then the CM and the TN which contains the highest energy will be assigned as the assistant CH. Again for detecting the BHA the sequence of data packets sent and received by the CH is verified along with the threshold value BHA to find whether it encounters with BHA or not. When there is a difference then elected CH acts as an attacker node. The information about the attacker CH node will be notified to its CMs and TNs then routing information about that node will be removed from the routing table. During the time of SFA and BHA in elected CH, the assistant CH will be assigned as the newly elected CH will announce itself as the CH to its CMs and TNs then it plays the role of the elected CH suffers with the SFA and BHA. This results in the easy prevention and recovery of the whole network data communication with any suspension.

Step 1: Initialization of Network Model Analysis (N_a) [2]

Step 2: CH Selection Algorithm

Step 3: For n=1 to K

Each CH announces JOIN_REQUEST_MSG packets to CMs

Elected $_{CH}$ receives JOIN_REPLY_MSG, routing information from its CMs

If CMs Distance > Pre-Defined Distance Then

CMs communicates via TNs

TNs help in data transmission between CH and CMs

End If

End For

Step 4:

If Timestamp (JOIN_REQUEST_MSG) by Elected $_{CH}$ < (threshold_SFA) Then

Elected $_{CH}$ = Attack

Confiscate Routing Info of Elected $_{CH}$ from CH routing table

Notify CMs and TNs that Elected $_{CH}$ is an attacker node

Else

CMs Sends Data Packets to Elected $_{CH}$ via TNs

Elected $_{CH}$ does data aggregation of its CMs and TNs

Accumulated data is dispatched to BS

If ((ECM > Elected $_{CH}$) || (ETN > Elected $_{CH}$)) Then

Higher Energy CM = Assistant $_{CH}$

Higher Energy TN = Assistant $_{CH}$

End If

End If

RESEARCH ARTICLE

: If Target_Node $_{CH\ sequence}$>final(Target_Node$_{CHsequence}$) || NodeCountLast (Target_Node $_{CH\ sequence}$) > threshold_BHA then

Elected $_{CH}$ = Attack

Confiscate Routing Info of Elected $_{CH}$ from CH routing table

Notify CMs and TNs that Elected $_{CH}$ is an attacker node

Else

CMs Sends Data Packets to Elected $_{CH}$ via TNs

Elected $_{CH}$ does data aggregation of its CMs and TNs

Accumulated data is dispatched to BS

Higher Energy CM or TN = Assistant $_{CH}$

End if

Step 6:If Elected $_{CH}$ == Attacker Node Then

Broadcast ADV_REQ for Assistant $_{CH}$

End if

: ADV_ REQ and the routing information are received and processed by the Assistant $_{CH}$

Assistant $_{CH}$ announces itself as the Newly Elected $_{CH}$ to its CMs and TNs

Step 8:If Newly Elected $_{CH}$ =! Attacker Node then

CMs Sends Data Packets to Elected $_{CH}$ via TNs

Newly Elected $_{CH}$ does data aggregation of its CMs through TNs

Accumulated data is dispatched to BS

End if

Step 9: End Process

Algorithm 2 Detection, Prevention and Recovery of CHs from SFAs and BHA

3.3. Detection, Prevention and Recovery of CMs and TNs from SFAs and BHA

The intra-cluster multi-hop communication is done based on transmitting and receiving the data packets through multiple hops (i.e.) the data communication established by the cluster members and its cluster head with the help of the intermediate cluster member nodes which are also called the transient nodes. The CH receives the data packets from its TNs. The TNs act as a bridge of communication between the CMs and their CH which are interconnected with each other. Once the first round gets completed the CMs and TNs will share the remaining energy of those nodes with their respective CH. So that this will help any of those CMs and TNs to take part and the node with the highest remaining energy next to the ECH is selected as the assistant cluster head (ACH). So the following algorithm 3 depicts the process of detecting, preventing, and recovering the CM and TN from SFAs and BHA. In algorithm 3 the CHs and the CMs will receive the information about the chosen TN via an announcement message. Once it is made the TNs will accept all the information concerning routing, and hop information about all of its CMs and CH to begin the data transmission. The total number of data packets transmitted between the CMs and TNs is verified to protect against SFAs and BHA. For this purpose, the CM q designates the total number of data packets dispatched to its TNs, and TN q represents the total number of data packets that are forwarded to its CH and CH receives data from each of its CMs after a time interval time round. After the completion of one round, all the CMs will send their residual energy information to their CH to become the assistant CH which leads that CM to become the next CH. CH of the current round and α is the threshold for the number of packets received at CH (α = 0 in the case of SFAs and BHA). Then the Flag q value gets incremented for each round of time. When the total number of data packets dispatched by the CM q is less than the average number of data packets received by the TN, then that CM is considered to suffer with the SFAs and BHA. Once the detection is made it is notified to the entire network by intimating about the CM attack to its CH, CMs, and TNs.

All the information concerning the attacker CM will be removed from the routing table. The data transmission process will get resumed. Likewise, when the total number of data packets forwarded to CH is less than the average number of data packets received by CH. Then that TN node will act as an attacker node. Hence, its neighboring CHs and CMs are intimated about the attack and immediately get detached from that attacker TN. The CMs of that TN will choose a new TN to establish the communication to its CH and the process of data transmission gets resumed. The information about the attacker TN and CM will be maintained in an attacker list for secure communication.

Step 1: Initialization of Network Model analysis (N_a) [2]

Step 2: CH selection using CH Selection Algorithm

Step 3: For n=1 to k

Each CH and CM receives ANNOUNCE_MSG_REQ from selected TN

TN accepts all routing information, hop information from its CM neighbors and CH

End for

Step 4: For q=1 to m

CM PACKETS_SENT (CM $_q$) = Number of data packets dispatched to TN

RESEARCH ARTICLE

TN ACCEPT_REQ_TIME (TN $_q$) = Number of data packets forwarded to CH

If (m =T $_{round}$) then

If (TN $_q$ <= α) and (CM $_q$<= α) then

Flag $_q$ = Flag $_q$ +1

End if

End if

If (T $_{round}$ ==T_{CH}) and (T $_{round}$ ==T_{CM})

If ((Flag $_q$ = = 0) and (CM $_q$< avg (TN $_{PC}$)) and (TN $_q$ < avg (CH $_{PC}$))

Attack A $_q$ = CM $_q$

Attack A $_q$ = TN $_q$

Attacker List = {Attack List} ∪ A $_q$

Else

Attack A $_q$ = 0

End if

End if

End for

Step 5: End Process

Algorithm 3 Detection, Prevention and Recovery of CMs and TNs from SFAs and BHA

4. RESULTS AND DISCUSSION

In this proposed work, MATLAB software is used for simulating the performance evaluation of the Fuzzy C-Means clustering-based Robust Tristate state security mechanism, it is developed to detect, prevent and recover against selective forward and black hole attack detection in WSN. The wireless sensor nodes are deployed in a 100 × 100 area. Table 1 indicates the simulation setup used for the proposed methodology. The newly developed RTSSM performance compared to the Genetic Algorithm [21] and E-LEACH [22] models.

Table 1 Simulation Setup

Parameter	Value	Description
TN	100	Total nodes in WSN
IE_0	0.5J	initial energy Node's
BS_{LC}	50,50	Base station location
ε_{fs}	10 pJ/bit/m2	amplifier energy spent at short distance during transmission
ε_{mp}	0.0013 pJ/bit/m4	amplifier energy spent at a longer distance during transmission
size(pkt)	500 bytes	Packet size of data
Msg	25 bytes	Hello/broadcast/CH join message

4.1. Packet Delivery Ratio (PDR)

PDR is defined as [2]

$$PDR = \left(\frac{ADPCH}{DPSCMVTN}\right) \times 100 \qquad (6)$$

Equation (6) is used for calculating the packet delivery ratio. In equation (6), ADPCH represents the total number of aggregated data packets received by the CH, and DPSCMVTN is the total number of data packets sent by the CMs through TNs to reach their respective CH.

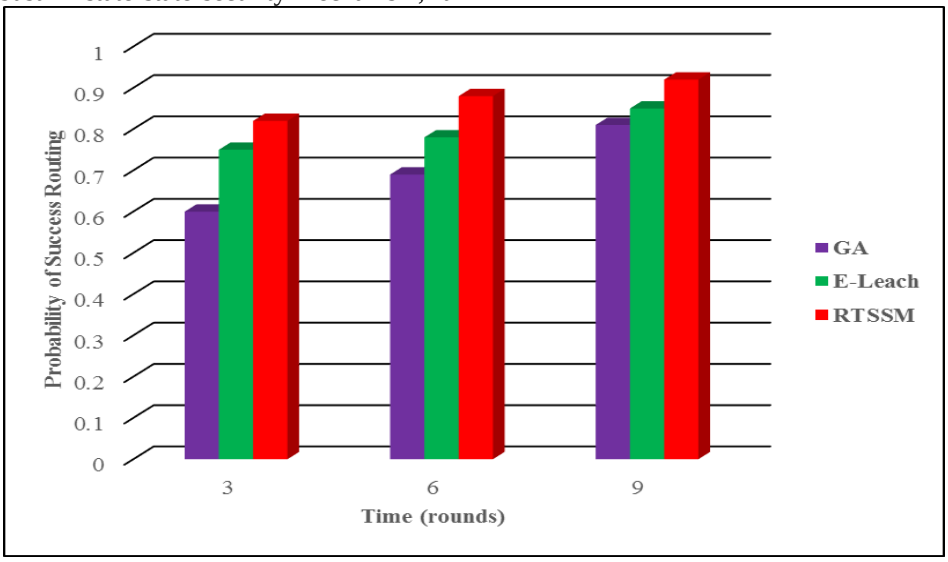

Figure 5 RTSSM Packet Delivery Ratio during Secure Intra-Cluster Multi-Hop Data Transmission

RESEARCH ARTICLE

Figure 5 illustrates that the probability of successful routing selection is accomplished by the proposed robust tristate security mechanism. In Figure 5, X-axis denotes the time (i.e.) the number of rounds and Y-axis denotes the probability of successful routing (i.e.) packet delivery ratio. The nodal propagation radius r rises, and the possibility of successful routing similarly grows, as can be observed. The cause is that the nodal density increases as r increases. The robust tristate security mechanism performs detection, prevention, and recovery of three levels of nodes namely cluster head, cluster member, and transient nodes. The black hole attack and the selective attacks are handled by determining the trust value of transmission nodes to avoid data transmission via malicious nodes. Hence, RTSSM produced a high probability of successful routing compared with existing E-LEACH and GA algorithms.

4.2. Throughput

Throughput is defined in [2]

$$\text{Throughput} = \frac{\text{TTDGRES}}{\text{TTDAREQ}} \quad (7)$$

Equation (7) is used for calculating the throughput. In equation (7), TTDGRES refers to the time taken for the data aggregation response, and TTDAREQ refers to the time taken for the data aggregation requests or the total number of data requests processed and response for the total number of requests received.

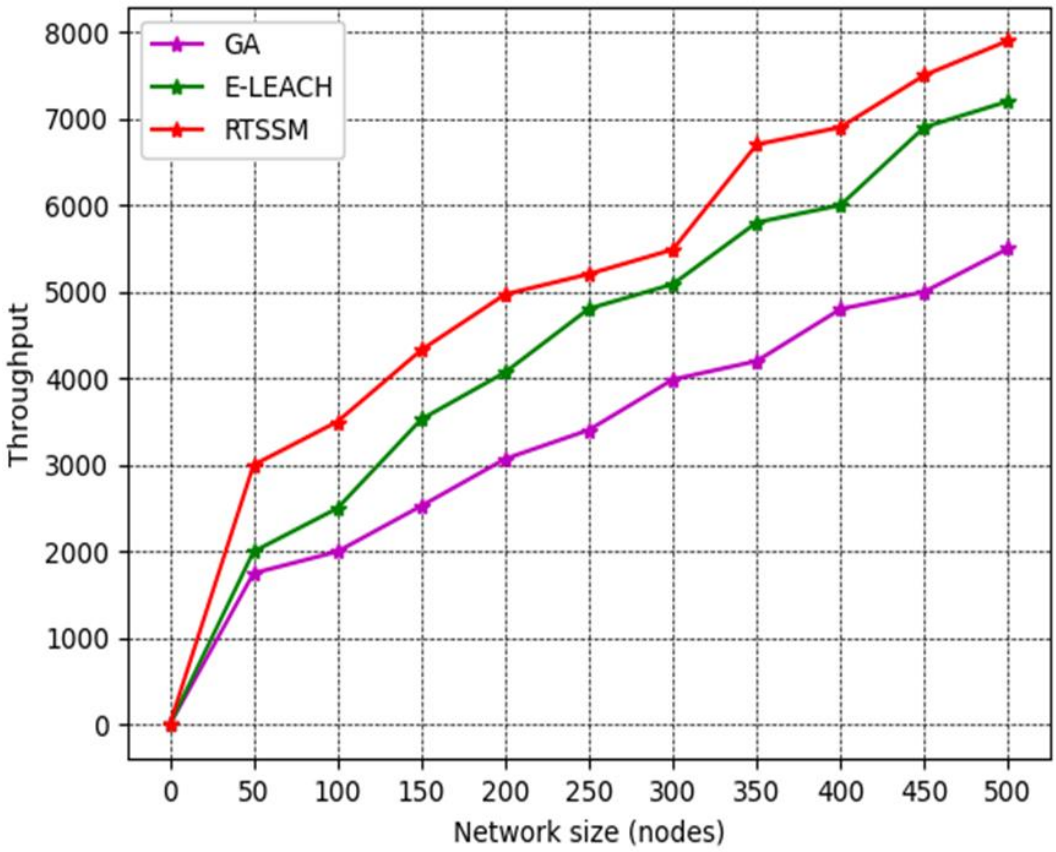

Figure 6 RTSSM Throughput during Secure Intra-Cluster Multi-Hop Transmission

The throughput of the proposed RTSSM is high compared with the GA and E-LEACH as depicted in Figure 6, wherein the X-axis represents the network size and the Y-axis represents the throughput of GA, E-LEACH, and the proposed methodology RTSSM. This provides the maximum throughput while comparing with the GA and E-LEACH. The selective forward attack and black hole attack are handled effectively by the proposed RTSSM by checking the trust value of each CHs, CMs, and TNs involved in the process of data transmission. The intra-cluster multi-hop communication is done based on transmitting and receiving the data packets through multiple hops.

4.3. Packet Drop

Packet Drop is defined [2]

$$\text{Packet Drop} = \frac{\text{TNDPT}-\text{TNDPR}}{\text{TNDPT}} \quad (8)$$

RESEARCH ARTICLE

Equation (8) is used for calculating the packet drop. In equation (8), TNDPT indicates the total number of data packets transmitted, and TNDPR indicates the total number of data packets received. Figure 7 represents the occurrence of packet drop during data communication concerning our proposed methodology.

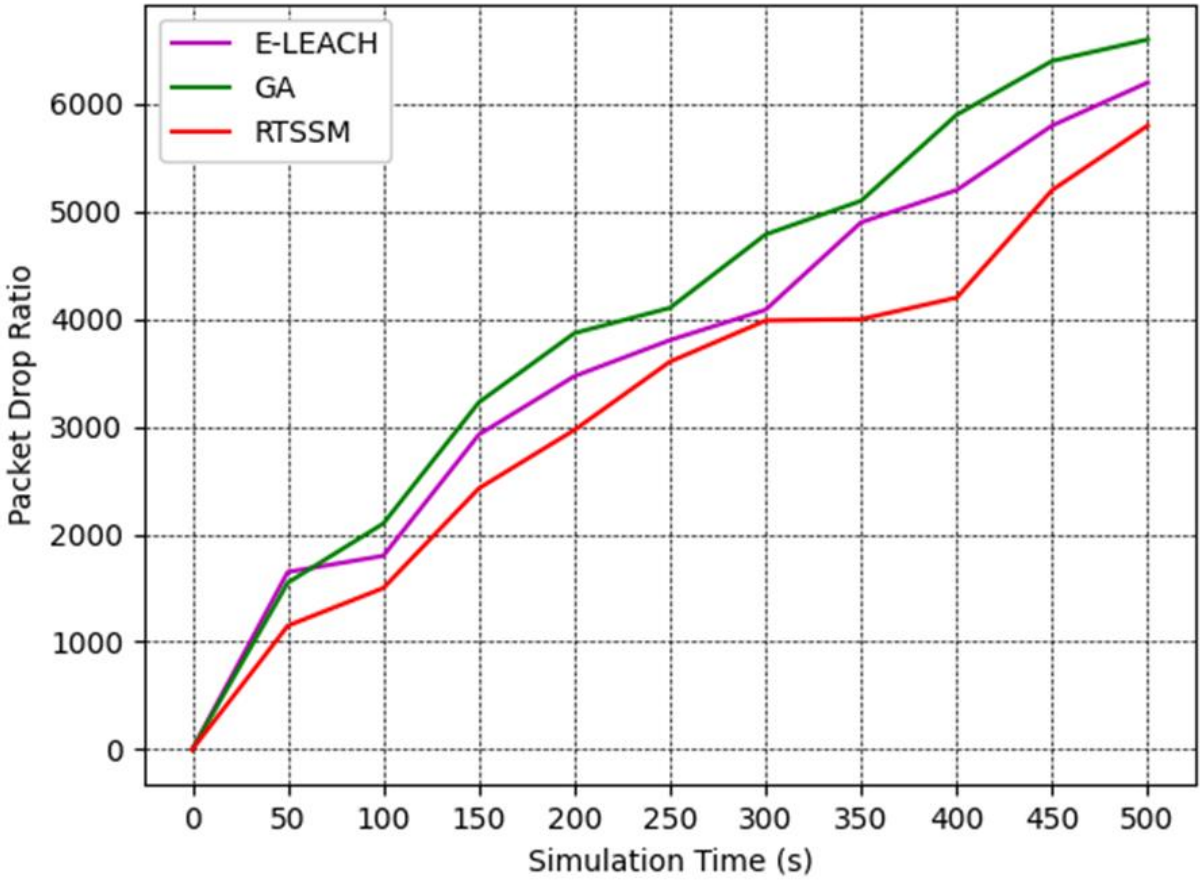

Figure 7 RTSSM Packet Drop Ratio during Secure Intra-Cluster Multi-Hop Transmission

Figure 7 shows the display of performance comparison of three different routing algorithms based on the throughput in WSN during data transmission from the source to the BS, where the X-axis represents the simulation time and Y-axis represents the packet drop ratio during the data transmission. It has observed that the proposed scheme RTSSM works correctly and prevents both the black hole and selective forward attacks more effectively, resulting in reduced packet drop. The cluster head selection is done based on the membership value obtained using a fuzzy objective function, and during each data packet transmission, the trust values of the intermediate nodes are checked continuously.

4.4. Energy Consumption

Energy Consumption is essential in extending the lifetime of the network, hence the energy of the nodes which perform the sensing operation needs to be minimized. To govern the network lifetime, all sensor nodes must function effectively with sustainable energy. Equation (9) is used for calculating the energy consumption. In equation (9), ET represents the energy consumption that occurs during data distribution, PS refers to the size of the data packet, D is the distance, EL is the energy loss that occurs during data transmission, AE is the amplifier energy, DSD is the distance that takes place between the source and destination nodes.

$$E_T(PS, D) = [(E_L) \quad X \quad (PS)] \quad + [(A_E) \; X \; (D_{SD})] \qquad (9)$$

The energy required for secured data transmission is calculated during the detection, prevention, and recovery process. In Figure 8, X-axis denotes the node density and Y-axis represents the energy consumption during the process of data communication. It also explores the comparative results for different algorithms involved in security mechanisms during data transfer. When compared to Genetic Algorithm (GA), E-LEACH, and the proposed RTSSM, it is obvious that the proposed RTSSM utilizes significantly less energy. With its fuzzy domain knowledge and route selection based on the trustworthiness of nodes involved in data transmission.

RESEARCH ARTICLE

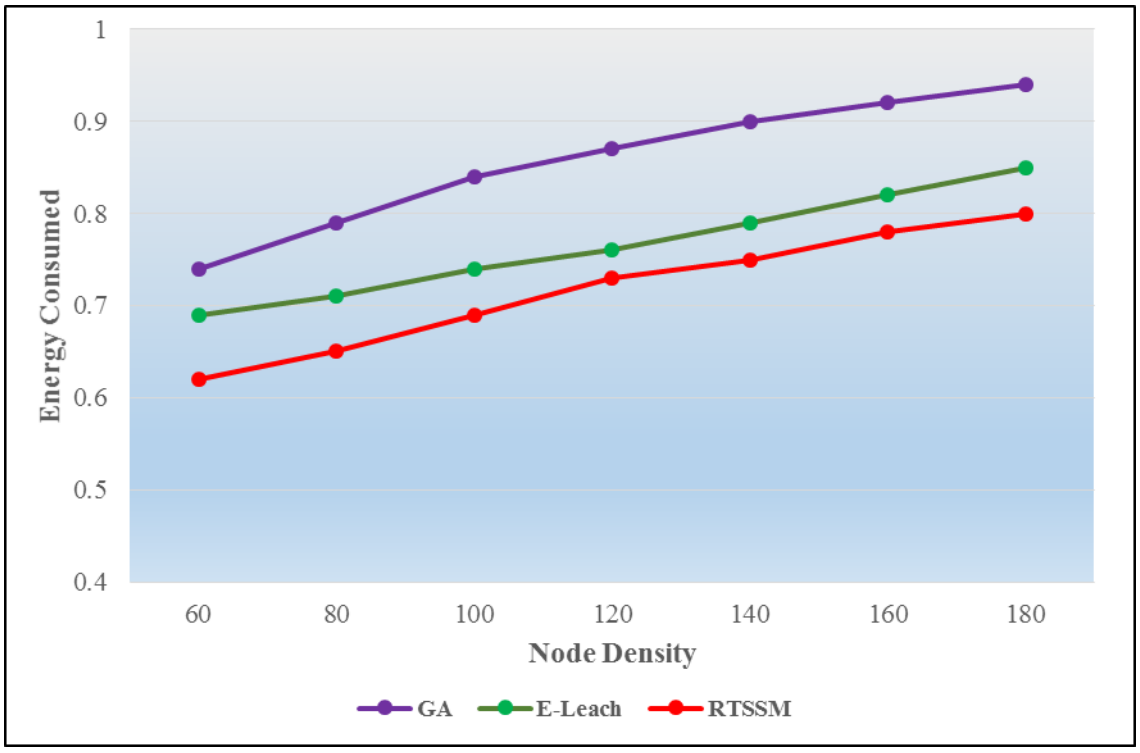

Figure 8 RTSSM Energy Consumption during Secure Intra-Cluster Multi-Hop Transmission

5. CONCLUSION

This research work focused on the methodology for detecting, preventing, and recovering (DPR) the CHs, CMs, and TNs from SFAs and BHA in intra-cluster multi-hop communication. The proposed work improves the process of DRP by determining the membership value of each node based on the cluster heads. The fuzzy membership value greatly helps in determining the trust value of transient nodes and the cluster head during each transmission process. This proposed work also includes the selection of assistant CH which is used to extend the network lifetime and make the communication also undisrupted. The proposed RTSSM for effective multi-hop communication results in minimal packet drop and maximum packet delivery provided with a good range of throughput. The results spectacle this methodology is operative in terms of the packet drop, higher rate PDR, maximum throughput, and also the energy consumption which takes place in the intra-cluster multi-hop communication in CWSN.

REFERENCES

[1] Jayachandran J, Vimala Devi K, "A Survey on Clustering Algorithms and Proposed Architectural Framework for Border Surveillance System in Wireless Sensor Networks", International Journal of Computer Networks and Applications (IJCNA), 9(6), PP: 785-805, 2022, DOI: 10.22247/ijcna/2022/217710.

[2] Iqbal, U., & Mir, A. H. (2022). Secure and practical access control mechanism for WSN with node privacy. Journal of King Saud University-Computer and Information Sciences, 34(6), 3630-3646.

[3] Feng H, Fu W. Study of recent development about privacy and security of the internet of things. In: 2010 international conference on web information systems and mining, Sanya, China, 23 October 2010. IEEE, pp. 91–95.

[4] Anitha, S.Mythili, "An Approach for Detection and Prevention of Cluster Head and Cluster Member from Selective Forwarding Attacks and Black Hole Attack in Intra-Cluster Multi-Hop Communication," Design Engineering, Vol. 2021, Issue.06, pp. 1032-1060.

[5] Bouarourou, Soukaina & Zannou, Abderrahim & Boulaalam, Abdelhak & Nfaoui, El Habib. (2022). Sensors Deployment in IoT Environment. 10.1007/978-3-031-01942-5_27.

[6] Munir, A.; Gordon-Ross, A.; Ranka, S. Multi-core Embedded Wireless Sensor Networks: Architecture and Applications. In IEEE Transactions on Parallel and Distributed Systems (TPDS); IEEE: Piscataway, NJ, USA, 2014; Volume 25, pp. 1553–1562

[7] Faris M, Mahmud MN, Salleh MFM, Alnoor A. Wireless sensor network security: A recent review based on state-of-the-art works. International Journal of Engineering Business Management. 2023;15.

[8] Tam, Nguyen & Dat, Vi & Lan, Phan & Binh, Huynh & Vinh, Le & Swami, Ananthram. (2021). Multifactorial evolutionary optimization to maximize lifetime of wireless sensor network. Information Sciences. 576. 10.1016/j.ins.2021.06.056.

[9] Maivizhi, Radhakrishnan & Yogesh, Palanichamy. (2021). Q-learning based routing for in-network aggregation in wireless sensor networks. Wireless Networks. 27. 1-20. 10.1007/s11276-021-02564-8.

[10] Lalitha, K., Thangaraja, R., Siba, K. U., Poongodi, C., & Prasad, S. A. (2017). GCCR: An efficient grid based clustering and combinational routing in wireless sensor networks. Wireless Personal Communications.

RESEARCH ARTICLE

[11] Turgut, "Analysing Multi-hop Intra-Cluster Communication in Cluster-Based Wireless Sensor Networks", Natural and Engineering Sciences (2019).
[12] Mezghani, M, "An Efficient Multi-Hops Clustering and Data Routing for WSNs based on Khalimsky IpekAbasıkeleş Shortest Paths," Journal of Ambient and Intelligence and Humanized Computing, Vol. 10, 1275-1288, 2019.
[13] D.Wu, S. Gene, X. Cai, G. Zhang and F.Xue, " A Many-Objective Optimization WSN Energy Balance Model," KSSII Transactions on Internet and Informatiom Systems, Vol.14, No. 2, pp. 514-537, 2020.
[14] H. El Alami and A. Najid, "ECH: An Enhanced Clustering Hierarchy Approach To Maximize Lifetime of Wireless Sensor Networks," IEEE Access, Vol. 7,pp. 107145-107153,2019.
[15] Gohar Ali, Fernando Moreira, Omar Alfandi, Babar Shah and Mohammed Ilyas, "A New Intra-Cluster Scheduling Scheme for Real-Time Flows in Wireless Sensor Networks," Electronics 9, No.4, 2020.
[16] Hasan A, Khan MA, Shabir B, Munir A, Malik AW, Anwar Z, Ahmad J. Forensic Analysis of Blackhole Attack in Wireless Sensor Networks/Internet of Things. Applied Sciences. 2022; 12(22):11442.
[17] Malik A, Khan MZ, Faisal M, Khan F, Seo J-T. An Efficient Dynamic Solution for the Detection and Prevention of Black Hole Attack in VANETs. Sensors. 2022; 22(5):189
[18] Ali, Haider & Tariq, Umair & Hussain, Mubashir & Lu, Liu & Panneerselvam, John & Zhai, Xiaojun. (2020). ARSH-FATI a Novel Metaheuristic for Cluster Head Selection in Wireless Sensor Networks. IEEE Systems Journal. PP. 1-12. 10.1109/JSYST.2020.2986811.
[19] Amutha, J. & Sharma, Sandeep & Sharma, Sanjay. (2021). Strategies based on various aspects of clustering in wireless sensor networks using classical, optimization and machine learning techniques: Review, taxonomy, research findings, challenges and future directions. Computer Science Review. 40. 100376. 10.1016/j.cosrev.2021.100376.
[20] Rawat, Piyush & Chauhan, Siddhartha. (2021). Clustering protocols in wireless sensor network: A survey, classification, issues, and future directions. Computer Science Review. 40. 100396. 10.1016/j.cosrev.2021.100396.
[21] S. Ramesh, R. Rajalakshmi, Jaiprakash Narain Dwivedi , S. Selvakanmani,
Bhaskar Pant, N. Bharath Kumar , Zelalem Fissiha Demssie, Optimization of Leach Protocol in Wireless Sensor Network Using Machine Learning, Computational Intelligence and Neuroscience Volume 2022, Article ID 53932, 8 pages.
[22] M. Sangeetha, and A. Sabari, "Genetic optimization of hybrid clustering algorithm in mobile wireless sensor networks," Sensor Review, vol. 38, no. 4, pp. 526-533, 2018.
[23] Zannou, A., Boulaalam, A., & Nfaoui, E. H. (2022). Data Flow Optimization in the Internet of Things. Statistics, Optimization & Information Computing, 10(1), 93-106. https://doi.org/10.19139/soic-2310-5070-1166.
[24] Firas Ali Al-Juboori & Ismail, E. S. F. (2014). A modified fuzzy C-means cluster-based approach for wireless sensor network. The Mediterranean Journal of Electronics and Communications, 10(2).
[25] D. Hongjun, J. Zhiping and D. Xiaona, "An Entropy-based Trust Modeling and Evaluation for Wireless Sensor Networks," 2008 International Conference on Embedded Software and Systems, Chengdu, China, 2008, pp. 27-34.

Authors

A. Anitha received her Bachelor's degree in Information Technology, Master's degree in Computer Technology and M.Phil in Computer Science from Kongunadu Arts and Science College, Coimbatore, Tamil Nadu, India in 2011, 2013 and 2017 respectively. She is currently pursuing her Ph.D in field of Computer Networks with Dr.S.Mythili at Kongunadu Arts and Science College, Coimbatore, Tamil Nadu, India. She has published 4 research papers in International Journals and 1 book chapter in Lecture Notes in Networks and Systems. She has presented papers in National and International Conferences and also participated in Webinars. She completed Introduction to Cybersecurity course from CISCO Networking Academy. Her research interests include Wireless Sensor Networks, Wireless Ad hoc Networks, Network Routing and Security.

Dr. S. Mythili working as Dean, School of Computer Science, Associate Professor and Head, Department of Information Technology, Kongunadu Arts and Science College, has about 20 Years of experience in academic and research. She has completed her Under graduate degree from Avinashiligam Institute for Home Science and Higher Education for Women and thereafter completed her Master of Computer Applications (MCA) and M.Phil from Kongunadu Arts and Science College. She has completed her Ph.D from Bharathiar University and has qualified UGC - National Level Eligibility Test (NET) and State Level Eligibility Test (SET). She is a Life Member of Indian Science Congress Association. Her research area is Detection of Clones in Programming Language Paradigms and Model Driven Architectures. She has published 20 research papers in reputed International Journals and in 7 Conferences out of which 8 Publications are in Scopus and 1 publication in Science Citation Index. To her credit she has published 3 National Patent and one International Patent. She has organized various National/ International Conferences Seminars and workshops. She has been a member in Board of studies in other colleges and universities and has also served as resource person in various colleges. Her current area of interest is Software Engineering and Data Mining. She has guided 6 Research Scholars for M.Phil and currently guiding 4 Ph.D Research scholars.

How to cite this article:

A. Anitha, S. Mythili, "Robust Tristate Security Mechanism to Protect Against Selective Forwarding Attack and Black Hole Attack in Intra-Cluster Multi-Hop Communication", International Journal of Computer Networks and Applications (IJCNA), 10(3), PP: 443-455, 2023, DOI: 10.22247/ijcna/2023/221900.