CHAPTER 5

SECURITY

5.1 INTRODUCTION

Many security solutions have been proposed for WSNs; however, due to the resource constraints of sensors, some of these solutions are not suitable for WSNs.WSN security approaches are heavily influenced by these constraints. This section describes someof the security issues and their solutions.

5.1.1 Security Goals and Challenges

The security of network attacks depends on understanding the various security goals of the network and the data traversing through it. A network security strategy includes Confidentiality, Integrity, Availability, and Authenticity, also known as CIAA.

- **Confidentiality:** Sensitive data is only accessed and viewed by authorized personnel. The confidentiality of data ensures that only those authorized to access it can do so. Data confidentiality is not assured when a node replication attack is launched because the clone nodes behave like the original nodes. The data stored in these nodes contains trade secrets for commercial businesses; secret government information, medical records, or financial records, so mishandling this data could harm networks and organizations.
- **Integrity:** It ensures that data is preserved and remains unharmed during transmission. It also assures that the message sent is received. When a node replication attack occurs, the attacker injects false data to corrupt sensitive data and overthrow the data aggregation.
- **Availability:** The goal is to ensure the survivability of network services rather than allowing them to be attacked. During a node replication attack, the attacker will launch a Denial of Service (DoS) attack, which can negatively impact the network's ability to process messages.

- **Authenticity:** Node authentication is a security objective that allows nodes to verify the identity of the nodes with which they communicate. In a node replication attack, the attacker produces a duplicate node that closely resembles the original node, possessing all the confidential information of the original node. Consequently, distinguishing between the cloned node and the original node becomes challenging. Authentication mechanisms are unable to identify the cloned node because it possesses the genuine key.

5.2 SECURITY ATTACKS ON WSN

WSN attacks can be classified as active and passive.

5.2.1 Active Attacks

A physical attack involves physical access to the data medium or the communication medium itself, or both. Without the owner's awareness, the attacker listens in and changes the channel.

These attacks are listed below:

- Routing attacks
- Denial of Service Attacks
- Node Subversion
- Node Malfunction
- Node Outage
- Physical Attacks
- Message Corruption
- False Node
- Node Replication Attacks
- Passive Information Gathering

Routing Attacks: This attack acts on network layer. Some attacks that happen during routing are listed below:

- Spoofed, altered, and replayed routing information.
- Selective forwarding.

- Sinkhole attack.

Denial of Service Attacks: Denial of Service (DoS) is a malicious, targeted attack that floods a network with false requests to disrupt its operation. DoS attacks prevent users from performing routine and necessary tasks.

Node Subversion: Node capture may reveal information that includes cryptographic key disclosure and compromises the full network. During an attack, a particular sensor is captured and its data may be obtained by the attacker.

Node Malfunction: Whenever the CH node or sink node is affected, inaccurate data is generated, exposing the network integrity.

Node Outage: This situation occurs when the node stops performing its function. To mitigate the effects of a CH failure, the network protocol must be robust enough to offer an alternate route if the CH stops working.

Physical Attacks: The sensor nodes may be susceptible to physical attacks because they operate in hostile outdoor environments. Unlike many attacks, physical attacks will destroy the sensors permanently, so the losses are irreversible. The attackers can extract the cryptographic secrets, damage the circuitry, modify the sensor programming, or replace it with malicious nodes under their control.

Message Corruption: An attacker modifying the message content will compromise its integrity.

False Node: The attacker adds an extra node and injects the malicious data. An intruder adds a node that feeds false data which prevents the passage of true data. Injecting a malicious node is the most dangerous attack as it may spread to all nodes potentially destroying the whole network.

Node Replication Attacks: This is a straightforward technique where the attacker copies the ID of an existing node to create a new node to an already existing sensor network. The performance of the network will be seriously harmed by this replicated node. The packets are misrouted, which causes misleading sensor readings, network disconnections, etc. The nodes are

replicated by replicating the cryptographic keys if the attacker acquires physical access to the entire network. Through the strategic placement of replicated nodes, an attacker can effortlessly influence a particular segment, ultimately causing the network to disconnect.

Passive Information: The attacker can use an intercepted message to locate and destroy sensor nodes based on their physical location.Besides the node location, attackers will observe message IDs, time stamps, and other fields. Strong encryption techniques are needed to reduce the gathering of passive information.,

5.2.2 PASSIVE ATTACK

An unauthorized attacker can compromise data privacy by listening to communication channels without physically altering the data being traversed. This type of attack is known as a passive attack.

These attacks are described as follows:

- **Monitoring and Eavesdropping:** This is a common privacy attack. The attackers can easily discover the communication content. As the traffic conveys control information about the network that contains more detailed information that can be accessed through the location server, eavesdropping can create a serious problem for privacy protection.
- **Traffic Analysis:** Even though the message is encrypted during transmission, it leaves some communication patterns. Sensor activities will reveal information that enables the attacker to harm the network.
- **Camouflage Adversaries:** One can hide the node in a sensor network. These nodes can act as normal nodes to attack the packets and mis-route them.

5.3 PROPOSED WORK

An energy-efficient and security-preserving routing protocol has been developed called Multi Criteria Based Secured Routing Protocol (MSRP). In this, every node can interact with the server and other nodes. Every time, the control layer

is responsible for performing additional processing and stops all network processes if malicious node behavior is suspected.

Several methods have been put forward to increase security and energy efficiency. By the current system, if malicious nodes are engaged in the network, it consumes more energy and produces more unwanted data, thus increasing computational time and complexity.

This research is carried out to reduce unwanted communication and data loss using the MSRP model to separate malicious nodes from the network once they are identified.

5.3.1 Network Model

This proposed system consists of a static sensor network with a sink node and N number of sensor nodes. The WSN is represented as a graph $G = (V, E)$, where V indicates the set of vertices and E indicates the set of edges. V includes all the sensor nodes. $E = (e_{ij})$ where, e_{ij}represents the link between v_i and v_j. These v_i and v_j denotes the sensor node. Here $v_i,\ v_j \in V$. The links among the sensor nodes are supposed to be symmetric. The neighbors are detected within the sensor node by using equation 5.1.

$$Nbr(v_i) = \{v_j | dist(v_i, v_j) \leq R_{comm} \forall j, 1 \leq j \leq N\} \quad (5.1)$$

$$Nbr(v_i) \subseteq V$$

$Rcomm$ denotes the communication range of nodes, $dist(vi, vj)$ is the distance between the nodes$vi$and vj The neighbor state is represented in equation 5.2.

$$Si = Uvj \in NiSj \quad (5.2)$$

where Sj is the state of node vj. The closest neighbor node Ni is represented by equation 5.3.

$$Ni = \{vi\} \cup \{Nbr(vi)\} \quad (5.3)$$

where $Nbr(vi)$ is the neighbor of sensor node vi.

5.3.1.1 Energy consumption:

The energy consumed for ƙ bits of data for transmission (E_{Tx}) is represented by equation 5.4.

$$E_{Tx} = E_{elec} \times ƙ + \varepsilon_{fs} \times ƙ \times d^2 \text{ , if d} \leq d_0 \quad (5.4)$$

$$E_{Tx} = E_{elec} \times ƙ + \varepsilon_{amp} \times ƙ \times d^4 \text{, if d} > d_0$$

$$\text{where } d_0 = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{amp}}}$$

Where, $d_0$is the threshold distance that is used for calculating the power loss model, ε_{fs} and ε_{amp} represent the energy required for amplifying transmission, and E_{elec} is the energy required for operating the transmitter circuit.

The energy consumed for receivingƙ bits of data (E_{Rx}) is represented by the following equation 5.5,

$$E_{Rx} = E_{elec} \times ƙ \quad (5.5)$$

where $Eelec$is the energy required for operating the receiver circuit.

The residual energy for t^{th} round is defined as from equations 5.6 to5.8

$$RE_i(t) = RE_i(t-1) - \left[E_{Tx}^i(t) + E_{Rx}^i(t)\right] \quad (5.6)$$

Where,$E_{Tx}^i(t) = rg_i(t) \times \left[E_{elec} + \varepsilon_{fs} \times d^{\gamma}\right]$ (5.7)

$$E_{Rx}^i(t) = r_i(t) \times E_{elec} \quad (5.8)$$

Where$rg_i(t)$ is the total traffic load in t^{th}round, $r_i(t)$ is the traffic load received by v_i.

The source node (v_s)is chosen based on the equation 5.9

$$v_s = argmin\{(dist(v_k, sink)RE_ƙ) \times DTF_ƙ\} \quad (5.9)$$

Where, $ƙ \in IR(H_i)$,$DTF_{ƙ}$ is the dynamic trust factor of node v_k.

$$DTF_{ƙ} = 1, \forall\, ƙ, 1 \leq ƙ \leq N$$

5.3.1.2 Problem formulation

Routing problems are dealt with event driven applications. Events are randomly generated using the sensing field. The influence region of the event is represented in equation 5.10.

$$IR(Hi) = \{vi|dist(Hi, vj) \leq Rsense \forall j, 1 \leq j \leq N\} \quad (5.10)$$

$$IR(Hi) \subseteq V$$

It helps the nodes to transfer their data to the sink. The source node must be appropriately selected to improve energy consumption and enhance QoS and security. The formula determines a routing path RP as in equation 5.11.

$$RP = (v1, v2, \dots\dots, vn) \quad (5.11)$$

Where v_1 represents the source node and v_n is the sink node.

$$v_{i+1} \in FN(v_i), \forall i, 1 < i < n,$$

Where FN indicates the set of forwarding neighbors as given in equation (5.12).

$$FN(v_i) = \{v_j |\, v_j \in Nbr(v_i) \&\& dist(v_j, Sink) \leq dist(v_i, Sink)\} \quad (5.12)$$

The following are the objectives of the routing path:

Minimization of Total Energy Cost (TEC): The cost of energy for transferring the data is represented by equation 5.13,

$$EC_{ij} = \frac{Energyneededfromnodev_itov}{remainingenergyatnodev_i} = \frac{e_{ij}}{RE_i} \quad (5.13)$$

The sender node finds the best node to provide direct communication with the sink. It is important to determine the total energy for reaching the destination via intermediate nodes.

The TEC_{ij} for a neighboring node is represented by equation 5.14

$$TEC_{ij} = EC_{ij} + EC_{jSink} \tag{5.14}$$

If $TEC_{ij} < EC_{iSink}$, v_i sends the data via v_j. Else, it forwards the data to the sink.

Minimization of Delay: A delay in a routing path can be determined using the number of hops and delay. If a path consists of fewer hops, then it reduces the end-to-end delay and the resource requirements. Delay depends on factors like queue length and forwarding delay. It is important to consider the path delay and the incurred delay. The node close to the base station will have fewer paths. The delay factor is represented in equation 5.15

$$DFij = \frac{dist(vj,sink)}{dist(vi,vj)} * dj \tag{5.15}$$

where$dj$is the incurred delay and is assigned to zero at the initial stage of the algorithm.

Maximization of trusted nodes: In WSN, node capture causes an attack. It is difficult to differentiate the nodes because of compromised node behavior, therefore it is essential to differentiate between the normal node and the compromised node. The trusted node delivers the data through the routing path. A trusted node is found using the trust factor that avoids the attacks. The formation of holes consumes energy when a node transmits more packets, which reduces the lifetime of the network. The trustworthiness of a node is determined using equation 5.16.

$$DTF = \omega_1 * \left(\frac{\rho_r+\rho_g-\rho_t}{\rho_r+\rho_g}\right) + \omega_2 * \left(\frac{\rho_g}{\rho_{max}*r}\right) \tag{5.16}$$

In Equation 5.16$\omega_1$and ω_2 indicate the weights, r represents the number of rounds in the network, ρ_r represents the number of packets that are received by a node, $\rho_g$is the number of packets that are transmitted by a node. ρ_{max} in equation 5.17denotes the maximum number of packets, which a node can transmit with the available energy at the initial stage.

$$\rho max = \frac{E(initial)}{P(size)*(1.5*E(elec)+\in fs*d0^2)} \quad (5.17)$$

The Selectivity Value of the Node (SVN) aims to reduce the total energy cost and delay and increase the trustworthiness of the node. This helps to determine the sender's neighbor node and find the best forwarding path. The selectivity value is represented in the equation 5.18.

$$SVN_{ij} = \omega_e * TEC_{ij} + \omega_q * PNDF_{ij} + \omega_s * DTF_j \quad (5.18)$$

Where ω_e indicates the weight that is associated with the energy parameter, ω_q indicates the weight of the QoS parameter, ω_s represents the weight of the security parameter. Here $0 \leq 0 \leq \omega_e, \omega_q, \omega_s \leq 1$ and $\omega_e + \omega_q + \omega_s = 1$. The weights of ω_e, ω_q and ω_s may lead to be adjusted based on the application requirements.

Multi Criteria based Decision Making Model: The functionalities of the multicriteriabased decisionmaking model is depicted in figure 5.1.

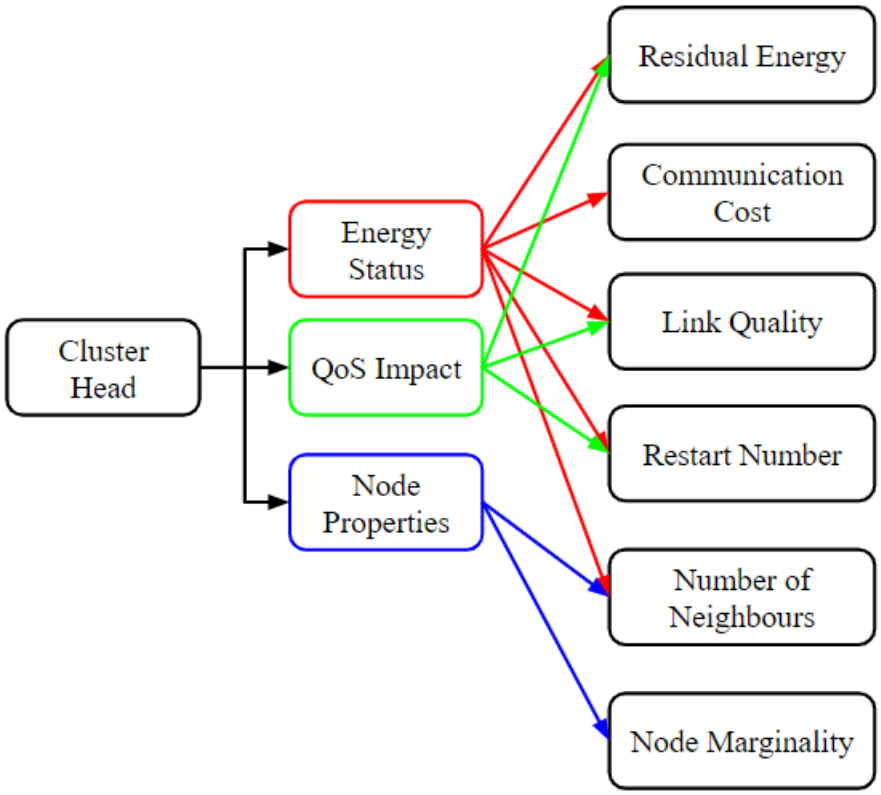

Figure 5.1 Multi-criteria-based Decision making for selecting the CH

The following steps elaborate on the various conditions used in the proposed model to select the CH for decision making.

Condition 1: Check whether the available nodes in the current round are clustered as in Figure 5.2. If the nodes are clustered then it moves to condition 2. Else, it verifies the location of the nodes in the cluster and clusters the available nodes.Then the weight ($Weight_i$)of the node is evaluated by updating the neighboring node and the weight of each node is shared with each neighboring node in the same cluster. Next, the loop moved to condition 2.

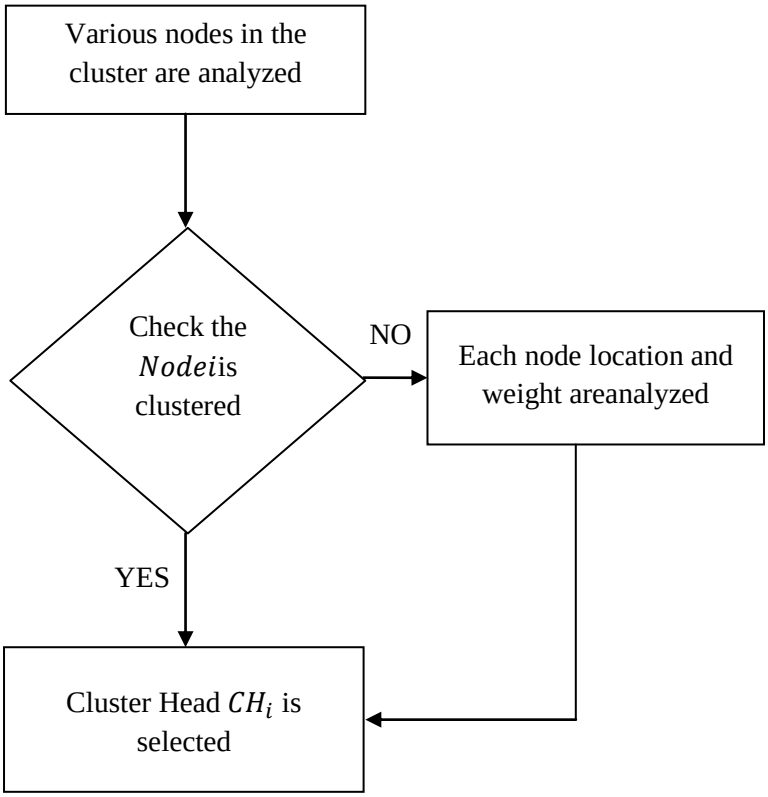

Figure 5.2 Condition 1for selecting CH

Condition 2: Check that, the weight of node i is greater than the other nodes in the cluster as in Figure 5.3. If $Weight_i > t\ (n)$, then the condition is satisfied and the message is sent to the selected node, then switched to condition 3. Otherwise, the

system waits to geta message from the CH_iwhich is obtained based on the location and weight of the current$node_i$.Condition 3 takes place, after identifying these parameters.

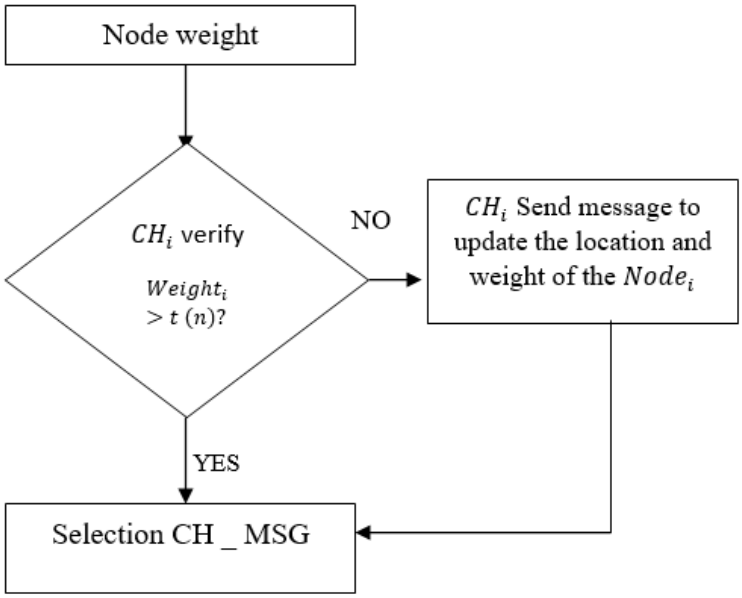

Figure 5.3 Condition 2for selecting CH

Condition 3: If $\boldsymbol{T > T_{round}}$, then the CH receives the message from each member node, and data aggregation is done for selecting the next CH. If condition 3 is not true**,** then T is reset and once again processed from condition2. This process ends if the optimal CH is selected as in Figure 5.4.

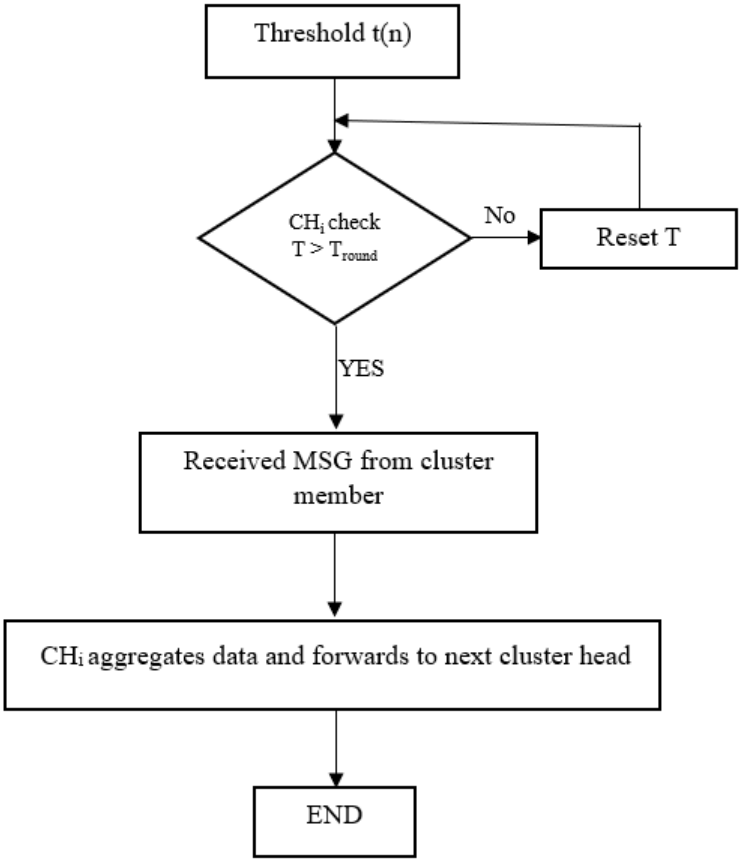

Figure 5.4 Condition 3for selecting CH

During route creation, the proposed multicriteria model is used. From the source to destination, all the possible nodes are considered and the best route is chosenfor data transmission. This routing protocol is simulated, and the results are verified.

5.4 RESULTS AND DISCUSSION

Network Simulator-2 is used to simulate the MSRP to verify the performance of the network in terms of Quality-of-Service. Table 1 describes the parameters of the network used for simulation.

Table 5.1 Simulation Parameters

Parameters	Values
Network Area	1500m x 1500m
Antenna	Omni Antenna
Propagation Model	Two-ray ground Model
Mobility	Yes
Number of Nodes	100, 200, 300, 400, 500
Packet Size	256 bytes, 512 bytes
Transmission Model	CBR (12 packets / s)
Protocol	AODV/ MLSRP

5.4.1Network Lifetime:

The Ad-hoc On-Demand Distance Vector Routing (AODV) Protocol, Trust-aware Secure Routing Framework (TSRF), and Energy-efficient and Secure Mobile node Re-authentication scheme (ESMR) are compared with the proposed MSRP to evaluate the network lifespan (figure 5.5 and table 5.2). The initial period is 1000s. The life duration is around 980 seconds when there are 10 malicious nodes. The lifetime is over 910 seconds when there are 10 malicious nodes, which is significantly longer than the other two techniques. The suggested model has a longer lifespan than the other protocols. Out of all the route lines, the MSRP chooses the one that is the most dependable and energy-efficient.

Table 5.2 Network lifetime w.r.to malicious nodes

Number of malicious nodes	NETWORK LIFETIME (sec)			
	(Proposed Work) MSRP	ESMR	AODV	TSRF
10	980	970	890	855
20	950	940	885	850
30	930	920	880	845
40	920	900	870	840
50	910	890	850	830

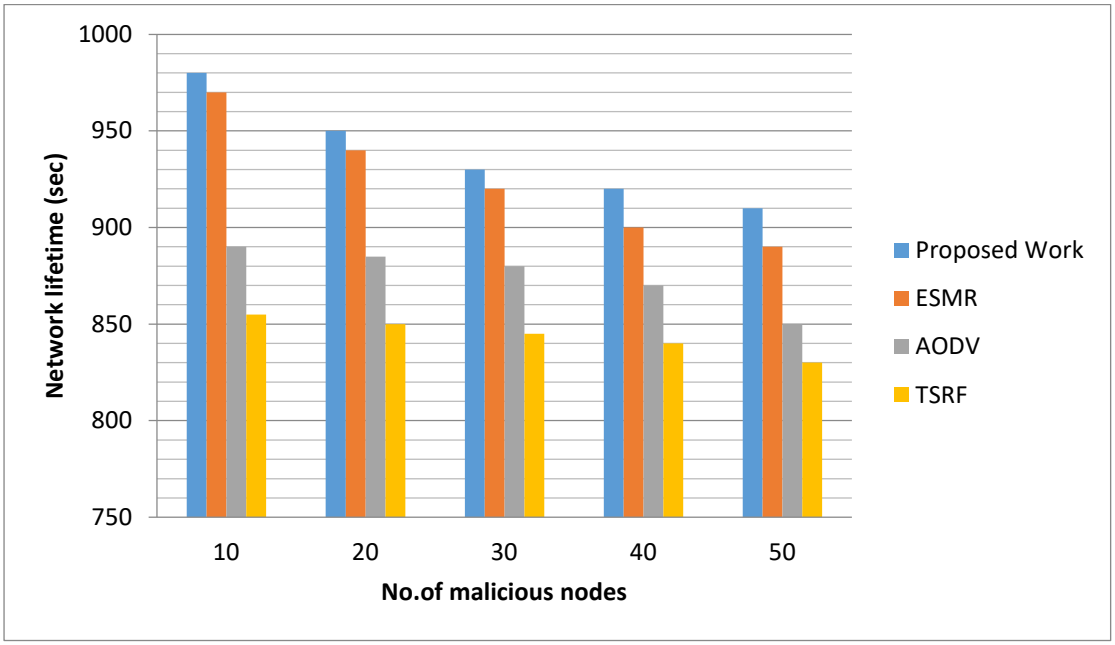

Figure 5.5 Network lifetime w.r.to malicious nodes

5.4.2 Network throughput

To assess the network throughput with different malicious nodes, the proposed MSRP protocol is compared with other existing protocols and is shown in Figure 5.6and Table 5.3. From the results, it is evident that the proposed MSRP outperforms other protocols in the literature in terms of network throughput. TSRF and AODV protocols forward data packets and harmful threats. The proposed model increases

network performance by 36% when compared with other protocols. It is ideal for handling energy-efficient systems.

Table 5.3 Network throughput w.r.to malicious nodes

Number of malicious nodes	NETWORK throughput (kbps)			
	Proposed Work (MSRP)	ESMR	AODV	TSRF
10	140	130	120	117
20	140	131	123	119
30	140	132	125	120
40	140	134	126	121
50	140	135	127	122

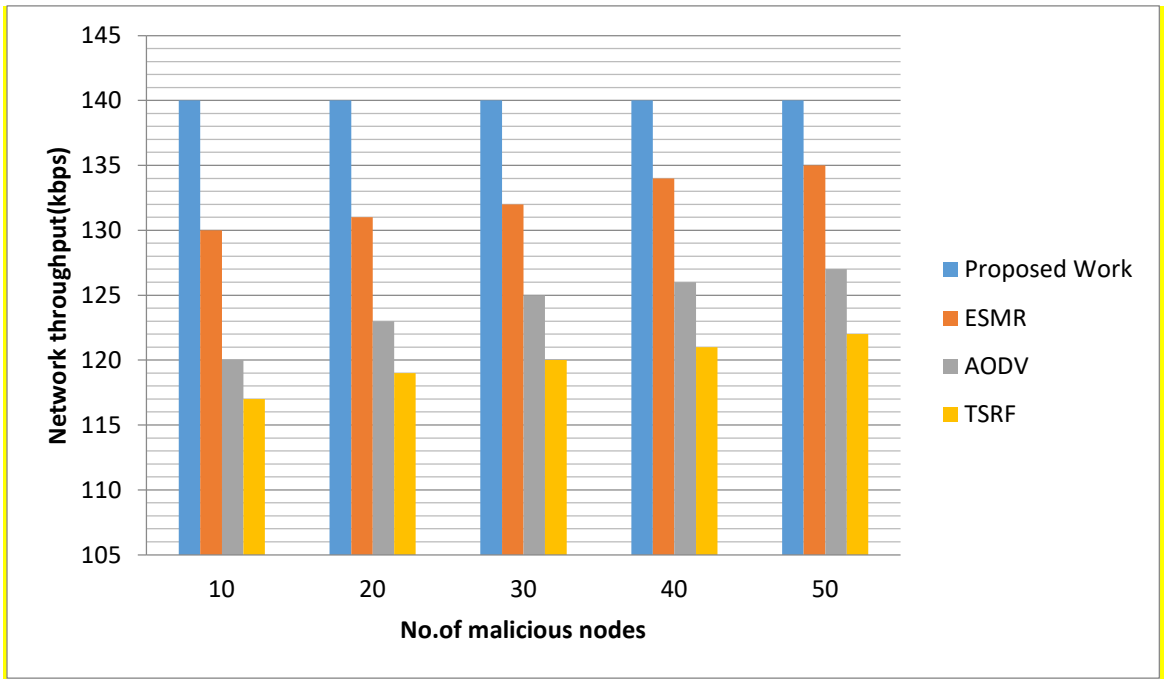

Figure 5.6 Network throughput w.r.to malicious nodes

5.4.3 Energy consumption

The initial energy is considered as 2J. Figure 5.7 and Table 5.4 compare the proposed work with the existing procedures in terms of energy usage. The proposed method enhances its performance by 34% when compared to the other methods. More energy is utilized in the existing procedures because of significant route breakage and because it also sends data along with the malicious nodes. When integrating with energy efficient and dependable nodes, MSRPmodel reduces the rate of re-transmission and efficiently uses energy.

Table 5.4 Energy consumption w.r.to malicious nodes

Number of malicious nodes	ENERGY CONSUMPTION (J)			
	Proposed Work (MSRP)	AODV	ESMR	TSRF
10	1	1.3	1.1	1.5
20	0.9	1.2	1	1.4
30	0.7	1.1	0.8	1.2
40	0.5	0.9	0.6	1.1
50	0.3	0.7	0.5	0.9

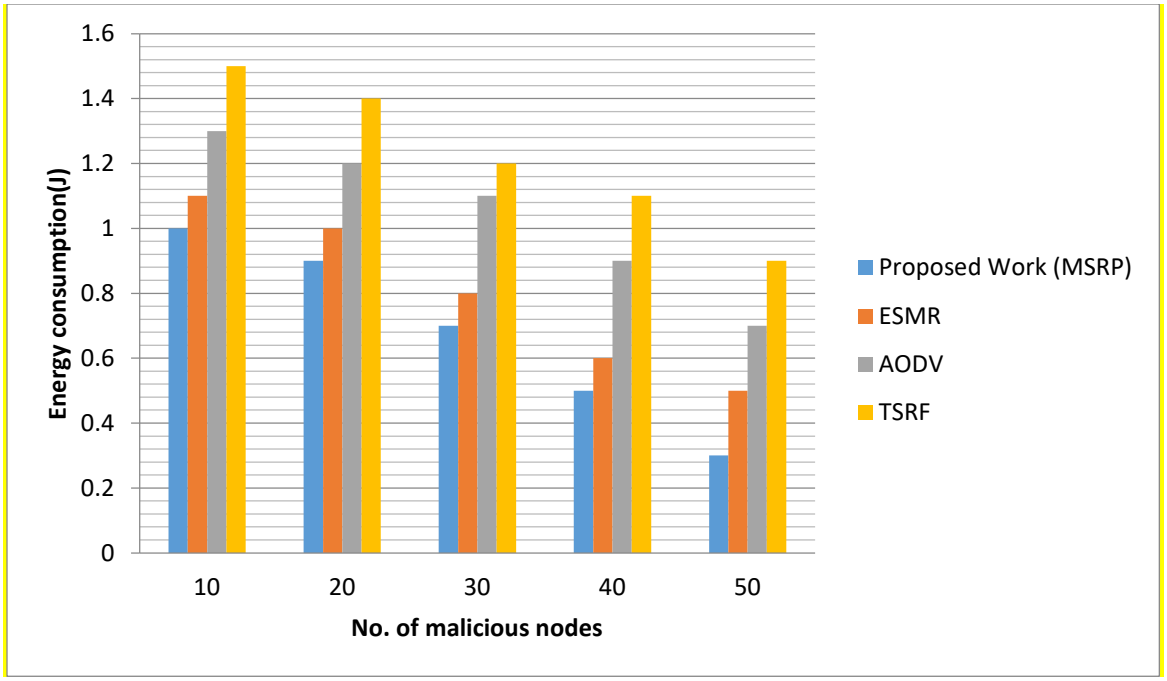

Figure 5.7 Energy consumption w.r.to malicious nodes

5.4.4 End-to-end delay

Figure 5.8 and Table 5.5 demonstrate the reduced delay in the proposed work when compared to the existing protocols in the presence of different malicious nodes. The proposed work performs almost 29% better than other protocols and theylack the ability to find the shortest routing pathway. The longest pathway results in many re-transmissions and end-to-end delays and causes many problematic connections. But the proposed model successfully selects the shortest routing path.

Table 5.5 Delay w.r.to malicious nodes

Number of malicious nodes	DELAY (sec)			
	Proposed Work (MSRP)	ESMR	AODV	TSRF
10	500	600	700	750
20	400	400	550	650
30	300	300	450	450
40	200	200	300	300
50	100	100	200	200

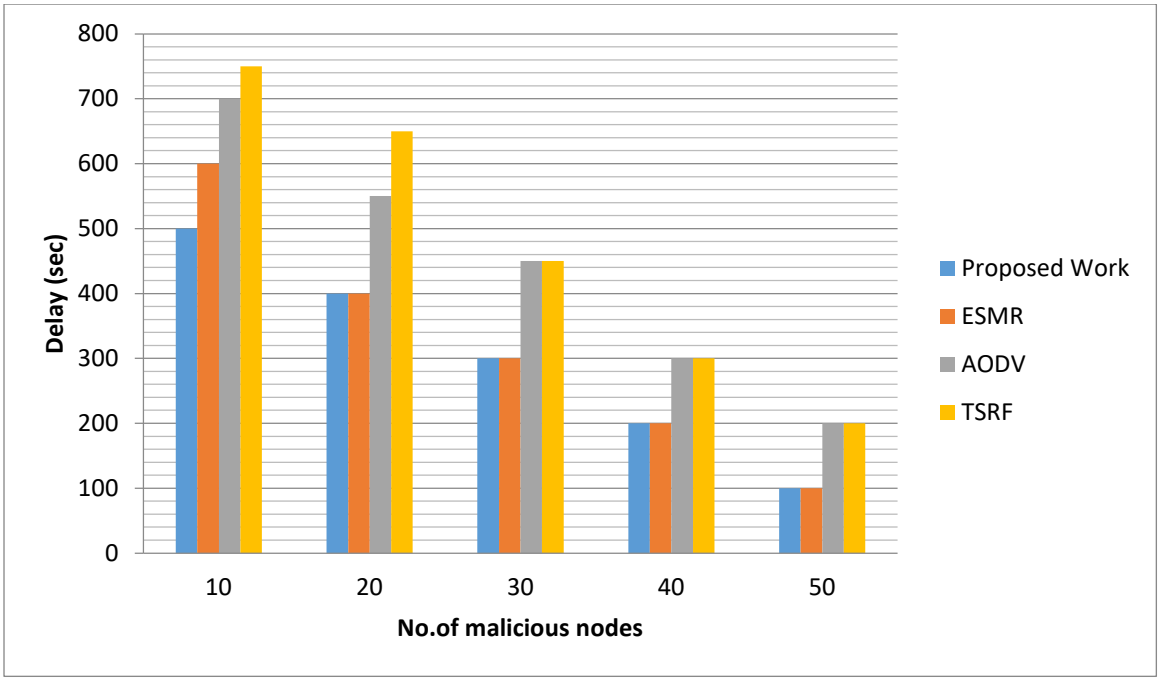

Figure 5.8 Delay w.r.to malicious nodes

5.5 Conclusion

The proposed Multi Criteria based Secured Routing Protocol performance parameters are compared with the ESMR, AODV, and TSRF techniques. From the results, it is observed that the proposed MSRP model is the suitable one for WSN compared to other existing methodologies in terms of security.