CHAPTER 4

ROUTING

4.1 INTRODUCTION

Routing is an important technique that involves finding a path from a sensor node to CH and from CH to the base station. The network lifetime of WSN can be increased by selecting the shortest path. Routers, router outlets, and router link directives form the major components of routing. Routing concepts apply to all types of networks, including public transport and telephones. In packet switching networks, such as the Internet, routing determines the route that packets travel from their source to their destination. Routers select the best route to route data across the internet.

The frequent restructuring and implementations of Wireless Sensor Networks (WSNs) in the harsh environment and their limited-resource sensor devices have resulted in a growing need for routing protocols that are both safe and energy-efficient. Routing and data aggregation are the focus of significant studies due to their frequent occurrence in network operations. Therefore, for the secured data aggregation protocol to be highly efficient, it is essential to have a secure underlying routing protocol as its basis. The security considerations in routing protocols have been insufficiently addressed, as the majority of routing protocols in WSNs have not been specifically built to meet security needs, primarily due to limitations in energy resources. In sensitive situations, it is crucial to protect data from unwanted activities while also ensuring the network remains available and reliable. Securing the routing process is crucial to guarantee the smooth execution of routing operations.

Attackers can readily compromise sensor nodes in WSNs, transforming them into hostile nodes that carry out a range of assaults, including selective forwarding, wormhole, sinkhole, hello flooding, and Sybil attacks. If the routing protocol is not resistant to assaults, malicious nodes can drop certain or all packets, resulting in the sink node not receiving vital data. Furthermore, there is a possibility that the network could experience partial or total failure. The conventional routing algorithms were specifically developed for the transport of data and are therefore not suitable for

WSNs when there are malicious nodes present. In addition, the routing in WSNs is limited by the energy and computing capabilities of the sensor nodes. WSNs' routing security has gained significant attention in recent years as a prominent area of research.

The main goals of the routing algorithm are:

- **Correctness:** Routing must be done in such a way that the information reaches the proper destination.
- **Simplicity:** Routing overhead must be as low as possible.
- **Optimality:** It must be capable of computing the best route.
- **Robustness**: It must be stable and perform correctly in any unusual **circumstances.**
- **Rapid convergence:** The response must be fast in case of a change in the network.
- **Flexibility:** It needs to be capable of adapting to different networks.

4.1.1 Challenges in Developing a Routing Protocol

While developing a routing protocol, the following challenges must be addressed:

- Node deployment
- Energy
- Node heterogeneity
- Data delivery delay
- Fault tolerance
- Scalability
- Network lifetime
- Connectivity
- Coverage
- Transmission media
- Data aggregation
- Quality of service

4.2 ROUTING METRICS

Routing metrics are used by routing algorithms to choose or reject routing paths for data transfer. Depending on the routing algorithm used, metrics are assigned to each route and calculated differently. The following parameters are used to calculate routing metrics:

- Hop count
- Reliability of path
- Path speed
- Load
- Bandwidth
- Latency
- Maximum transmission unit

4.3 CLASSIFICATION OF ROUTING PROTOCOL

Routing protocols are classified as

Proactive: This method evaluates the route within the network. It means this protocol maintains the routing information continuously so that the data can be forwarded immediately as the path is already known.

Advantage:

- Delay is negligible in determining the route.

Disadvantage:

- Huge amounts of data are required to maintain the routing information.
- Less reaction in case of re-structuring of the network and failure of nodes.

Reactive protocols: This protocol does not maintain routes but it builds routes only on demand. A global search is initiated when the route is required.

Advantages:

- There is no overhead for maintaining the routing information.
- Respond quickly in cases of network restructuring and node failure.

Disadvantage:

- High latency time.
- Excessive flooding.

Hybrid protocols: Hybrid protocols take advantage of both proactive and reactive methods. They initiate the route discovery on demand but at a limited cost.

4.4 ROUTER AND ITS WORKING

A router is a networking device that links two or more networks. The primary function of a router is to manage traffic and allow multiple nodes to use the same path. The router directs the data packets to its destination without any loss or disruption and it uses an internal routing table to deliver the data packets effectively to the proper destination. A router analyses the data header to identify the destination, locates the most optimal route to reach the destination, and subsequently transmits the data to the subsequent node in the route.

4.5 PROPOSED WORK

An uninterrupted power supply is needed for a longer network lifetime. However this is difficult in the case of remote sensor networks. So, energy preservation of all nodes of a network is necessary. Along with energy preservation, different issues such as physical node defects, node failure, etc. also arise due to harsh environmental conditions. Malicious attacks have a more significant influence on the network. An attack on a single node prevents data from being transferred and causes message overload; in such a scenario, the intermediate node will carry transmission, resulting in high end-to-end transmission energy.

So, end-to-end communication becomes complex in the absence of a routing protocol. Routing protocols need scenarios and conditions to be applied; they are not applied immediately.

Routing protocols establish perfect communication between nodes and extend the life of networks. Since node behaviour detection is crucial, the primary goals of

this study are to keep the nodes connected and extend the network lifetime by implementing node behaviour analysis and on-demand secured data transmission.

By identifying the behaviour of the nodes, it will be possible to identify malicious nodes that obstruct the path by continuously monitoring the transmission path for message transmission. Congestion occurs when selfish nodes interfere with overall communication. Nodal behavior changes create network disruptions. Predicting node behavior detects malicious nodes in the network. Distinguishing between malicious nodes and selfish nodes is crucial for anticipating node behaviour and preventing errors that could lead to the removal of nodes from the network. The semi-Markov process can forecast node behaviour in a network, enhancing trust by identifying and handling malicious nodes while fostering trust among nodes.

As the traffic causes stability issues, network stability has to be considered when monitoring node behavior. Differential behavioral changes are due to power loss, failure in node configuration, etc. If a malicious or selfish node is identified, the respective node needs to be adjusted to prevent resource overconsumption. Unusual behaviour from a rogue node might impact the entire network and be classified as a failed node. Node necessitates comprehensive data to accurately forecast its behaviour. A selfish node must be isolated.

The On-Demand Routing (ODR) protocol will monitor the nodes, analyze their defects, and maintain their cooperation until the task is completed. It also gains trust in the network and is named a trusted routing protocol. For gaining trust, an agent-based trust source is used, which is dynamic and also prevents time delays and message overload. Detecting selfish and malicious nodes operates in the discovery and route maintenance phases.

4.5.1 Network Model

Consider a basic Mobile Wireless Sensor Network (MWSN) consisting of k nodes. Let I be the set of integers from 1 to n. The network is structured in three layers, with the lowest tier comprising nodes with identity i (where $i \in I$). Each node

will detect, process, and send the sensed message using a certain amount of power. Here, the nodes are positioned steadily. Each node's location is represented by ni, where i belongs to the set I. The sink is positioned at the top and establishes communication with the node; however, it requires more energy than normal when engaging in direct communication between the nodes. Covering nodes are utilised to prevent direct communication, which occurs within the middle layer. The primary purpose of the covering node is to establish a Connected Hull to guarantee that no node remains uncovered. There are 'n' hops between the covering node and the sensor for communication with the sink node.

Let us take the 2 points (x, y) in Euclidian plane. The distance between two nodes is denoted by$|x, y|$. Assume two nodes n_i and n_j for the process of communication and R is named as the range of communication. For long range communication, the condition is $|ni, nj|$<R.

The following steps are followed once the source and destination have been identified.

1. On-Demand Routing (ODR)
2. Status allocation.
3. Construction of graph.
4. Processing of the graph.
5. Preparation of graph.
6. Path query.
7. Node behavioral analysis.

4.5.1.1 On Demand Routing (ODR)

The cost of path construction is one of the disadvantages of discovering the shortest path. Large networks are unstable; network topology changes and breakage also occur. If the node position is changed, the change in the position of the node has to be updated, which in turn consumes more energy and time. This issue is rectified by the approach named as Thourup-Zwick.

Consider a network at time *t.* The MSWN is a graph that is both weighted and undirected. It is represented as$G = (S, D)$. Before transmitting the data to a neighbor, it initially verifies the local cache. If the nodes $S$and $D$are were previously interconnected; the request packet is transmitted to the sink to get acknowledgment. The sink node is represented by the symbol (v). Graph preparation (G)yields a data structure that the destination node needs to start the conversation. The data packets are transmitted using the shortest path.

4.5.1.2 Status Allocation

The sink node establishes direct communication with the other nodes, which are responsible for the source-initiated ODR protocol, by collecting essential information from its neighbouring nodes. The data includes the present condition and the position of the node.

In this approach, the covering node obtains the status information from its neighbouring node. The status report from each node includes the parameters for message transmission. E_i and $PRRi$ indicate the remaining energy and packet reception ratio. $E_i$and C_i denote the current state of the load and the state of the connection, respectively.

$PRRi$ is computed for every window and is represented as in equation 4.1.

$$PRRi(\Delta w) = \frac{Num\,(rp)}{Num(sp)} \tag{4.1}$$

where packets received and sent are represented as $Num\,(rp)$ and $Num\,(sp)$ respectively. The load Liat time frame Δt is calculated using equation 4.2.

$$Li(\Delta t) = \frac{Num\,(rdp)}{Num(ldp)} \tag{4.2}$$

The relayed data packets and the generated local packets are represented by $Num(rdp)$and $Num(ldp)$. The collected information is forwarded to the covering node by the sink.

Within the context of MSWN, the process of assigning status involves several scenarios. Let's assume the value of n is 3. Figure 4.1 depicts many potential allocations of status. If nodes n3 and n5 are in direct proximity to the covering node, they can only transmit the status vector. If nodes n2, n4, and n6 are adjacent to the covering nodes, they will broadcast the status vector to the covering node in two hops. When node n1 transmits the status vector to the covering node, it necessitates three hops.

4.5.1.3 Graph Construction

Once the status allocation is done, the sink node receives the entire information. Graph construction is done by the weighted graph. Consider $|V| = n$and$|E| = m$, where the node and the distance between the nodes are represented by Vand E. $eij \in E$is represented in equation 4.3;

$$eij = \begin{cases} Wij|ni, nj|, & |ni, nj| < R \\ \infty, & |ni, nj \geq R| \end{cases} \quad (4.3)$$

When the distance between the nodes exceeds the communication range, the transmission distance becomes infinite. Fixed weights are used to avoid the infinity range.

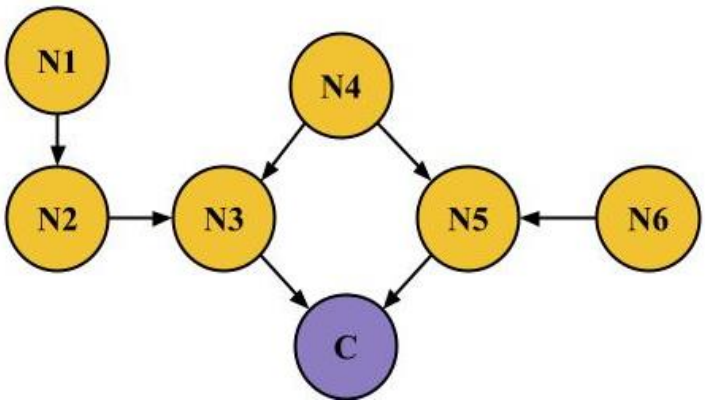

Figure 4.1 STATUS ALLOCATION WHEN n=3

Fixed weights are calculated using equation 4.4,

$$wij = \alpha.Eij + \beta.Qij + \gamma.Lij \quad (4.4)$$

Energy status (Eij), quality of link(Qij) and load status(Lij) are required for obtaining constant weight value and is calculated using the equation 4.5, 4.6, 4.7.

$$Eij = \frac{Ei-Et}{Ei} * \frac{Ej-Et}{Ej} \quad (4.5)$$

The residual energy of the nodes is represented by Ei and Ej and the energy needed for transmission is denoted by Et.

$$Qij = \frac{1}{PRRi * PRRj} \quad (4.6)$$

where $PRRi$ and $PRRj$ denote uplink and downlink quality respectively.

$$Lij = \frac{1}{Li * Lj} \quad (4.7)$$

α, β, γ represent coefficients of weight and the value for the sum of coefficients is 1.

4.5.1.4 Graph Processing

Graph pre-processing is crucial for efficient message transmission to neighbouring nodes. Let's assume that the cardinality of the set V is denoted as n, and the cardinality of the set E is denoted as m. The graph with assigned weights is analyzed using the Thorup and Zwick method. The pre-processing is performed via the formula O(knm1/k). The graph undergoes pre-processing at a specific moment, resulting in a data structure of size O(kn1+1/k). If a path has a query response time of O(k), then the distance is equal to 2k-1, where k is an integer higher than or equal to 1. After the allocation of status information, the sink node acquires the network topology.

4.5.1.5 Path Query

After the weighted graph has been analyzed, the sink will prepare to respond to the covering node, depending on the path query.

4.5.1.6 Node Behavioral Analysis

Node behaviour is assessed during the process of data routing and the development of routes. It is necessary to observe and identify the actions of

intermediary nodes, which include the source node and destination node, to detect and identify nodes that are acting maliciously. The performance of a WSN relies on the trustworthiness of its nodes. The functioning of intermediary nodes influences the performance of source and destination nodes in the network. ODNB controls the behaviour of individual nodes to carry out a specific communication operation. Nodes are categorized as Reliable (R), Un-Reliable (U), Malicious (M), and Selfish (S) based on their nodal behaviour. Figure 4.2 depicts the process of node classification. Node behaviour can be altered by power loss, miscommunication, reconfiguration of node attributes, changes in power sources, and abnormalities in job allocations. This leads to data loss and triggers hostile activity within the network. To identify and detect the activity of the nodes, a certain number of nodes, denoted as N, are distributed within the network. The nodes are categorized into different classes, denoted by the set W={R, U, M, S}.

- **A reliable node (R)**: This node is responsible for delivering control information and data packets, as well as determining the most efficient way for routing.
- **Unreliable node (U):** This sort of node is characterized by instability in the network due to factors such as being out of communication range, experiencing excessive congestion, and frequent link failure.
- **Malicious node (M):** This node engages in suspicious behaviors that disrupt routing by occasionally spreading denial of service attacks, causing delays in packet forwarding, manipulating routes, and so on.
- **Selfish node (S):** In the context of routing, a selfish node is a node that intentionally does not reply to control messages to conserve its resources, even though these resources may be unreliable.

Consider a network region with N nodes as W that consists of different node categories. It can be represented as $W = \{\mathrm{R}, U, M, S\}$. The node behavior changes over a particular time *T*in *W* is represented in equation (4.8).

$$W = \int_{n=0}^{N} T(prob[R, U, M, S]) \tag{4.8}$$

Based on different node behavioral changes, a probability matrix is presented in Table 4.1.

	R	**U**	**M**	**S**
R	**1**	1	1	1
U	1	**1**	0	0
M	0	1	**1**	0
S	0	1	1	**1**

Table 4.1 Probability of behavior changes matrix

If a node remains unaffected while distributing its behaviour while new behaviour is detected, one can evaluate the chance of change as zero, assuming that changes occur one at a time. Figure 4.2 displays this information.

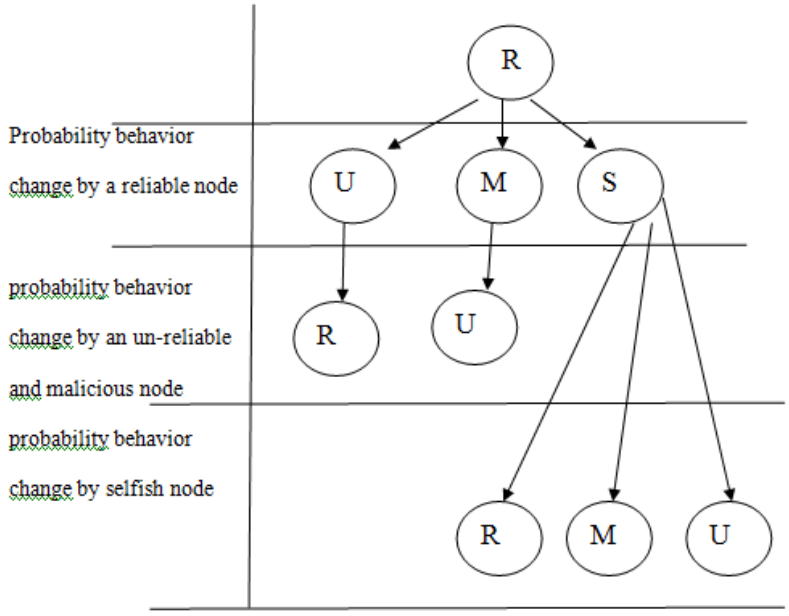

Figure 4.2 Probability of behavioral changes

4.6 RESULTS AND DISCUSSION

The ODNB protocol is emulated using the Network Simulator-2 and its performance is assessed in terms of Quality-of-service. Table 4.2 provides a detailed description of the network parameters within the software environment.

Table 4.2 Simulation Parameters

PARAMETERS	VALUES
Network area	(100 *100)m^2
Execution time	10s,20s,….,50s
Mobility	Yes
Number of nodes	100
Packet size	256 bytes

Packet Delivery Ratio (PDR)

PDR refers to the count of packets that have been received without any issues at the intended destination. The performance is assessed by simulating varying quantities of malicious nodes and computing QoS values. The proposed approach achieves an average packet delivery ratio that is 92.2% greater than that of other current methods.

From Figure 4.3 and Table 4.3, it is evident that the ONDB protocol performs better than the Trust Management System (TMS) and Reliable Trustworthy Approach (RTA).

Table 4.3 Packet Delivery Ratio w.r.to malicious nodes

Number of malicious nodes	Packets Delivery Ratio (PDR) (%)		
	TMS	RTA	PROPOSED (ODNB)
10	92	93	99
20	85	90	98
30	62	75	95
40	55	70	90
50	30	49	75

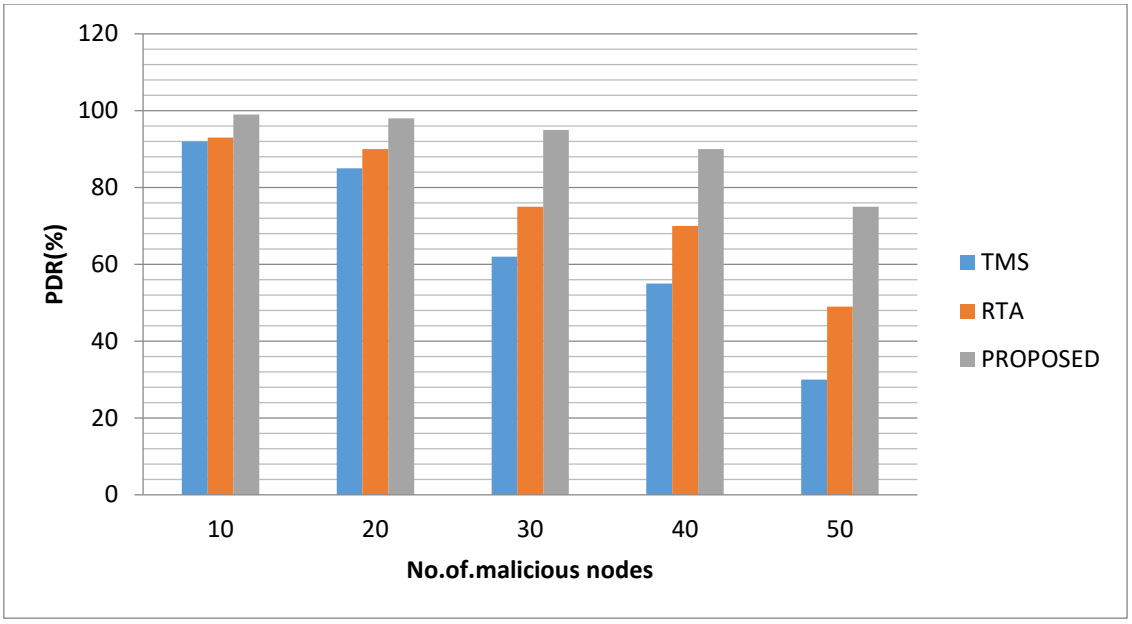

Figure 4.3 Packet Delivery Ratio w.r.to malicious nodes

Packets dropping

The number of dropped packets is determined by subtracting the count of successfully received packets at the sink from the number of packets transmitted from the source node. 1000 data packets are transmitted initially. As the quantity of malicious nodes grows, the quantity of packets dropping also increases.

When the number of malicious nodes is 10, only 17.5% of packets are dropped and when 50 malicious nodes are considered, 39% of packets are dropped which very much less than the other two existing methods. From figure 4.4 and Table 4.4, The proposed method exhibits much lower packet drop rates compared to alternative methods.

Table 4.4Packets Dropping w.r.to malicious nodes

Number of malicious nodes	Number of packets dropped		
	TMS	**RTA**	**PROPOSED(ODNB)**
10	198	180	175
20	300	275	250
30	399	300	275
40	500	400	300
50	600	590	390

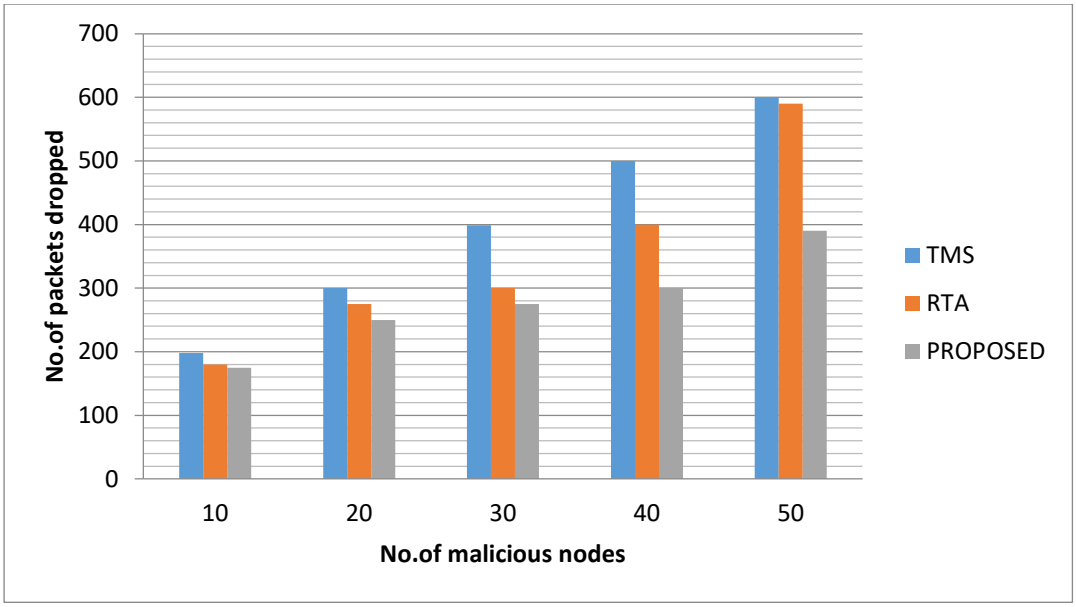

Figure 4.4Packets Dropping w.r.to malicious nodes

Delay

From Figure 4.5 and Table 4.5, it is noticed that the delay in the proposed model is much less than that of the other methods. The initial period is 1500ms. When 50 malicious nodes are considered, the delay is almost 47% which is less than the other two existing methods.

Table 4.5 Delay w.r.to malicious nodes

Number of malicious nodes	DELAY(ms)		
	TMS	RTA	PROPOSED
10	400	400	200
20	510	490	300
30	600	550	500
40	900	800	600
50	1050	950	700

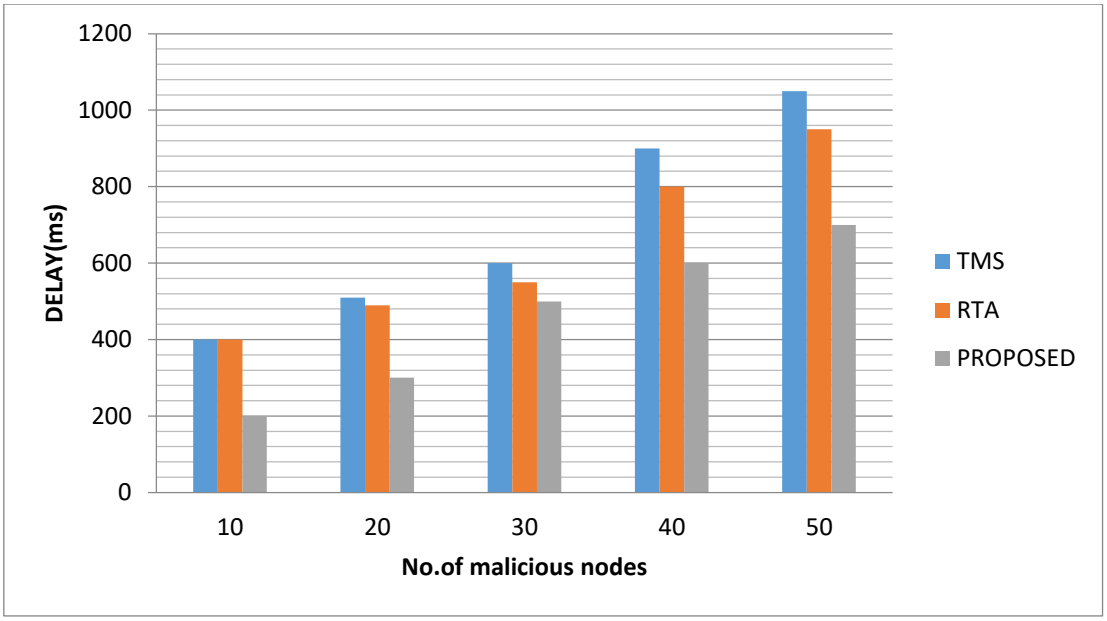

Figure 4.5 Delay w.r.to malicious nodes

Energy

According to Figure 4.6 and Table 4.6, the proposed method consumes less energy than other existing methods. The initial energy is 200mW. When the number of malicious nodes is 50, 31% of energy is consumed which is less than the other two existing methods.

Table 4.6 Energy consumption w.r.to malicious nodes

Number of malicious nodes	ENERGY CONSUMPTION(mW)		
	TMS	RTA	PROPOSED
10	38	21	20
20	60	56	30
30	79	79	42
40	81	90	46
50	120	140	62

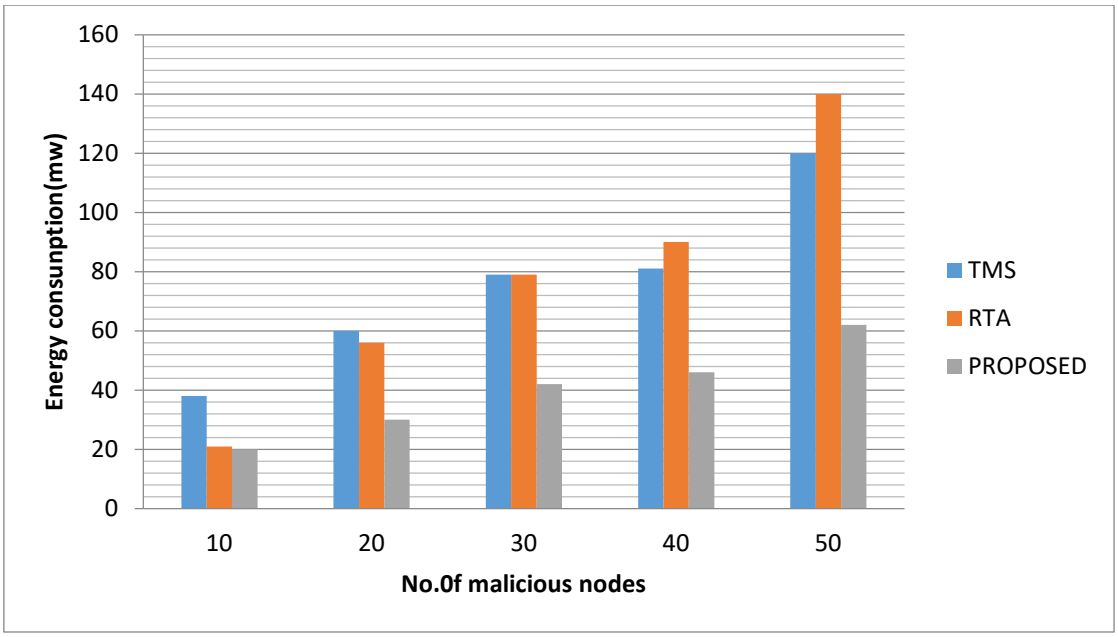

Figure 4.6 Energy consumption w.r.to malicious nodes

4.7 CONCLUSION

The proposed work is carried out using the node behaviour of the sensor nodes based on demand and finds the secured routing path. The different network parameters are compared with existing methods such as TMS and RTA. It is concluded from the results that the proposed work outperforms the other two methods.