Incorporating Node Behavioral Analysis with On-Demand Secured Routing of Improving the Efficiency of Wireless Sensor Networks Applications

Y.P.Makimaa

Research Scholar, Department of ECE, School of Engineering, Avinashilingam Institute for Home Science and Higher Education for Women, Avinashilingam Nagar. Varapalayam, Thadagam Post, Coimbatore-641108
makimaa261994@gmail.com

Dr.R.Sudarmani

Associate Professor, Department of ECE, School of Engineering, Avinashilingam Institute for Home Science and Higher Education for Women, Avinashilingam Nagar. Varapalayam, Thadagam Post, Coimbatore-641108
sudarmaniece@avinuty.ac.in

Abstract

Wireless Sensor Network provides an unbelievable platform and resources for various recent real-time applications, can prove their potentiality in terms of Quality of Service. WSN applications need to improve in energy efficiency, throughput, and packet delivery ratio. Several earlier routing protocols have been proposed to improve the QoS in WSN, whereas they are application or environment-specific. Due to the Adhoc nature, most of the WSN applications are similar and require a common routing protocol suite highly. Thus, these papers motivated to design and implement a common routing protocol for WSN with two major objectives: On-demand and Node Behavior (ODNB) based routing. First, the routing process is carried out between any two nodes that the user prefers. Then data collection, aggregation, and transmission by the cluster head nodes in the clustered network. Second, the data routing is carried out on-demand, where the source and the destination nodes are selected according to the application requirement. The proposed ODNB is simulated in Network Simulator software, and the results are verified. The obtained results are compared with the existing routing protocols for evaluating its performance. From the comparison, it is identified that ODNB outperforms the existing routing protocols.

Keywords: **Routing Protocol; On-Demand Routing; Node Clustering; Node Behavioral Routing; WSN-Applications.**

1. Introduction

Wireless sensor networks are an advanced form of wireless technology because wireless technologies are controlled remotely. The number of sensors deployed in the network depends on the application of the network. Some applications require a limited number of sensor nodes while some require a countless number for the longer term. The main disadvantage of the sensor network is the limited power backup of sensors. A longer network lifetime requires an uninterrupted power supply. This is difficult in remote sensor networks. Therefore it is essential to preserve the energy of each sensor. Apart from energy conservations, several other physical problems are arising in sensor networks such as physical node defect, node failure, etc. Physical effects are because sensor networks are usually deployed in harsh environmental conditions. Malicious or internal attacks on sensor nodes also have a greater impact on the network. An attack in a single node will block the data from being transmitted and creates message overload. In such cases, the intermediate node will carry out the transmission. But end-to-end transmission consumes higher energy than usual. Routing protocols are good at energy conservation, especially in mobile wireless networks. Intrinsic intermediate nodes are the last resources in wireless networks. Without any routing protocol, communication to the base station from the sink is complex. Initially, flooding algorithms are used as a routing protocol for broadcasting the data packets continuously. The flooding algorithm is a simple routing protocol and it has its limitations such as node failure because of continuous transmission of data packets and it lacks data processing. This results in copies of the same data packets. These situations create the need for routing protocol to overcome the limitations of the nodes. Routing protocols manage and operate the nodes in different ways.

Routing protocols are generally classified into centralized, distributed, and locally-based routing protocols. In centralized algorithms, the nodes gather complete information of the network and transmit the messages to the base stations. Distributed routing algorithms communicate with the help of message passing. Local-based routing algorithms use complicated data and the algorithm is implemented on the main node. The efficiency of the routing protocol depends on node optimization. Routing protocols are not applied directly; some require conditions and scenarios for routing. The autonomy unit of the sensor must be manually controlled for preventing attacks from outside. Routing protocols are capable of improving the network lifetime and provide seamless communication between the nodes. In some cases, sensors do not have much energy for message transmission. Routing protocols are suitable for larger networks. Most applications of wireless networks depend on homogeneous sensor nodes. Routing protocols allow the homogenous sensor nodes for processing the collected information and then the information is transmitted to the neighbour node and the base station. In this paper, we focus on routing algorithms for increasing the network lifetime and maintaining connectivity between distant nodes. We mainly focus on incorporating two different security processes such as node-behaviour analysis and On-Demand secured data transmission, since detecting the node behavior is important in the network.

Detecting the node behaviour will help us to monitor the transmission pathways for continuous message passing. It will help to detect the malicious nodes that block the communication path. The main task is finding the malicious or selfish nodes which cause packet loss. Selfish nodes can cause an overall communication breakdown called congestion. Changes in node behavior will cause disruptions in the network. It is avoided by removing the malicious node from the network. This will create an overload in work by neighbour nodes. The isolated node results in network instability and poor performance. The behavioral prediction will bring trust to the network by detecting the malicious nodes in the network. The main advantage of this prediction method is to differentiate between the malicious nodes and selfish nodes and removes the nodes from the network which causes errors in transmissions. Behavioral prediction provides a generic model for identifying the behavior of individual nodes by routing process. The routing is done on node-level starting from the first node to the last node. The semi-Markov process is used in predicting the behavior of the sensor nodes. Estimating the behavioral probability will bring trust to the network. Reliable category nodes are formed for enabling trust between the distant nodes and provide support for detecting malicious nodes.

On monitoring the behavioral pattern, the stability of the network must be considered because network traffic will cause network stability issues. Traditional communication networks depend on efficient routing protocols for reliability and node resilience. Mobile ad hoc network (MANET) routing depends on the distant nodes for gaining trust in the network. Handling the forward node is essential for completing the routing process in this wireless sensor network. Detecting the behavioral pattern is done by a semi-Markov process in an Adhoc network. The main reason for choosing this method is that the ability to alter the node formation at the point. This method detects malicious attacks and gains trust between the distant nodes. Different behavioral changes occur in the network such as power loss, failure in node reconfiguration, etc. Power loss could affect the node and there is a chance of outside attacks. Whenever a malicious or selfish node is detected, the respected node must be reconfigured. If the node is not reconfigured, there occurs overconsumption of resources. A malicious node is considered a failure node, if the behavior of the malicious node is strange then it affects the complete network. Predicting the behavior of each node is complex. Therefore, the node requires complete routing. Early detection of the malicious node will bring the node to normal, but if the node is considered selfish, the respected node must be isolated.

Routing protocols are generally energy-efficient and provide better service to the networks. Another type of routing protocol is the on-demand routing protocol which does not consider any information about the sensor if there exists no communication between the neighbor nodes. The pathway is found by sending continuous data packets for entire networks. Different on-demand routing protocols are existed such as DSR, FSR, DYMO and AODV, etc. and they are used in wireless sensor networks. The main goal of this routing protocol is to find the route in the network for establishing a secured connection between the neighbour nodes. On-Demand Routing (ODR) protocols are mainly used and it is suitable for MANET applications.

The ODR protocol will monitor the node and analyses for any defects. They also maintain node cooperation till the task is completed. The ODR protocols are way better than table-driven routing protocols especially in maintaining node formation and node cooperation. Mobile ad-hoc networks are generally centralized in nature and the topology of the network is altered based on the geographical conditions. Table-driven routing protocol does monitor the selfish node or detects changes in the behavior. The ODR protocol monitors the behavior of the network and each sensor node. Gaining trust in the network is achieved by ODRprotocol and they are also called trusted routing protocols. For gaining trust between the sensor nodes, an agent-based trust source is used. The agent-based source is dynamic which will prevent message overload and time delay. A multi-agent system is installed for node monitoring. It consists of two types of agents called monitoring agents and routing agents. The routing mechanism in wireless networks is categorized into two categories called detecting selfish nodes and malicious nodes. These detection mechanisms operate in Discovery and route maintenance phases. Selfish nodes use resources from neighbour nodes but it does not use its nodes. Malicious nodes are responsible for manipulating the routing process by making a false hop count. In this paper, we will combine ODRprotocol and node behavior detection protocol for obtaining the best routing results. The contribution of the paper is given below:

- Constructing a network model in NS_2 simulation environment based on the Node behavior analysis.
- Implement a routing protocol based on ODRwith respect to the node behavior and verify the data transmission with QoS factors.
- Compare the simulation results and the performance evaluated.

2. Literature Review

Researches were done on identifying the behavioral pattern of a sensor node in wireless networks. They analyzed failure nodes and recorded multiple node failures which were occurred for multiple reasons. The authors researched the node path in which the information travels. They identified the malicious nodes which cause propagation failure in the network. They also used a trustworthy routing approach to recover the particular node. The main drawback of this method is gaining trust in this process is complex. The trust scheme will avoid false message detection [Marchang and Datta (2012)]. The trust restoration process is proposed for restoring the malicious nodes for avoiding further false messages. In this method, nodes with the least trust are removed from the network for enhancing the network capability. Low trust nodes are identified by analyzing the behavioral pattern. Only limited numbers of nodes are recovered in this method. Isolated nodes are directly removed from the network [Marti et.al (2000)]. The authors proposed a distribution scheme for managing the message duration in mobile ad-hoc networks. They proposed a trust management framework for establishing a relationship between the sensor nodes. This framework also prevents attacks from outside. The node's reliability is improved by this approach. The trust calculation will determine the level of attack [Movahedi et.al (2016)].

The authors calculated the past performance in identifying the node behavior. The past behavior of the node is observed and they are evaluated for maintaining the network stability. Past negative nodes and their behaviors are assessed and predicted for future failures. Malicious nodes are predicted for maintaining credibility and stability [Mao and McNair (2010)]. Many studies are conducted for establishing trust in wireless networks. Monitoring the behavior of the neighbour node in terms of the trust is evaluated by a technique called CORE. This method performs evaluation in sensor networks for finding out the trustworthy nodes [Michiardi and Molva (2002)]. The trust value is computed by the source node and they detect for future message modification which leads to the selfish node.

On-demand protocol concentrates on the information provided by the sensor nodes for data transmission. The authors proposed a distributed trust model for exchanging fault entities during the transmission phase. This system is also called a recommendation protocol and each entity in this protocol has its trust level. This model is decentralized in nature for faster computation. Mobile ad-hoc networks are well suited for implementing distributed trust model [Rahman and Hailes (1997)]. The authors proposed a secure routing protocol for suppressing the effects of malicious nodes. This model can operate all keys in the network nodes. The nodes are communicated in a secured manner with the help of this routing protocol [Papadimitratos and Haas (2002)]. The malicious nodes sometimes cause more damage to the network. Another security protocol called trusted AODV is proposed to gain trust among the sensor nodes. In this method, a novel trust model is used for monitoring the behavior of the sensor nodes. This mechanism also has an intrusion detection scheme for enabling trust among neighbours. In this method, subjective logic is used for representing trusted nodes. This protocol is designed to exchange trust-related information among neighbour nodes [Li et.al (2004)].

The authors proposed a protocol that has no third-party mechanism for gaining trust. Dependable DSR requires no third-party mechanism to monitor the malicious nodes. This method controls the data traffic in the network by propagating the message packets to the trusted nodes. The trusted routes are then retrieved from the cache memory and thereby reduce communication overhead [Pirzada et.al (2007)]. The authors proposed DSR protocol for efficient routing in WSN. It is a type of reactive routing protocol which requires source routing. The message packets are updated similarly to table-driven routing protocols. This protocol is highly implemented in multi-hop wireless sensor networks. This is a lightweight protocol [Johnson and Maltz (1996)].

Another dynamic protocol is proposed called Dynamic MANET on-demand routing protocol. This protocol is similar to the AODV protocol and the implementation is easier on comparing with other routing protocols. DYMO protocol is executed whenever the node requires it. Routing reply packets are used in message transmission. Discovering the route from the source node to the destination node is done by this protocol [Sarkar and Murugan (2016)]. Advanced DYMO routing protocol is proposed for eliminating the previous generation issues. This protocol uses sequence numbers for creating a loop for message transmission. This protocol creates a demand for multi-hop routing between the nodes especially in ad-hoc networks [Arya et.al (2013)].

The authors proposed a routing protocol for managing the paths in the network. This protocol is called as Intra-zone routing protocol. In this method, the neighbour nodes with minimum distance are preferred for message transmission. This will detect the nearby malicious nodes by analyzing the behavior of the neighbour node [Rameshkumar (2016)]. The main drawback of this method is it requires a limited zone radius. Advanced IARP protocol enhances the network path for creating a unique path in the network. The quality of the routes is improved within the network topology. The main disadvantage of this method is the occurrence of link failures [Ahuja et.al (2013)]. Another route discovery method is proposed by authors called AODV. In this method,a route request packet is obtained by the nodes for message broadcasting. But repeated messages are identified in the nodes while broadcasting the request packets and results in request overload [Govindasamy and Punniakody (2018)].

2.1 Limitation and Motivation

From the literature review, it is found that, the earlier research work has focused on analysing the nodes for malicious detection by Id verification alone. Some of the researchers identify the malicious nodes in terms of mis-behaviour. Some of them found malicious nodes by analyzing their performance. Some of the authors have focused only on routing-path analysis. So, the earlier works are focusing any one point of aspects to identify the malicious activities. But the malicious activity can be created at any time anywhere in the network process. Thus, this paper is motivated to design and implement a complete security model for WSN by analyzing the node and route of the network.

3. Network Model

Consider a simple mobile wireless sensor network (MWSN) with $\boldsymbol{k}$ nodes. Let $\boldsymbol{I} = \{\mathbf{1}, \mathbf{2} \dots \boldsymbol{n}\}$. The overall network is built in three tiers (fig-1), where the lowest tier consists of sensor nodes with an individual identity$\boldsymbol{i}(\boldsymbol{i} \in \boldsymbol{I})$. We all know that sensor nodes are provided with only a small amount of power backup. It has sense, compute and transmit the sensed messages with this limited power. In this approach,a stable network is used and the nodes are arranged in a stable position. The location of the sensor node is denoted by $\boldsymbol{n_i} where \boldsymbol{i} \in \boldsymbol{I}$.The sink node is present in the top tier of the network. The sink can initiate communication with the sensor node but the energy consumption is higher than usual while using the sink node communicates directly. Therefore, we avoid direct communication by allocating the messages to other nodes called covering nodes. Covering nodes are usually present in the middle tier in the three-layered network. The key reason for covering node is to create a cluster head. Relay nodes are implemented for gathering the current status from each sensor. Covering nodes will cover every node in the network and they ensure that no sensor nodes are left uncovered. We create $\boldsymbol{n}$ number of hops in between covering node and sensor for communicating with the sink node. The number of hops should not exceed more than 3.

Consider a Euclidean plane with two points $(\boldsymbol{x}, \boldsymbol{y})$. The line segment and the Euclidean distance between $\boldsymbol{x}, \boldsymbol{y}$are denoted as $[\boldsymbol{x}, \boldsymbol{y}]$and $|\boldsymbol{x}, \boldsymbol{y}|$ respectively. Assume two sensor nodes $\boldsymbol{n_i}$ *and* $\boldsymbol{n_j}$for the communication process and R is considered a range of communication. The condition must be $|\boldsymbol{n_i}, \boldsymbol{n_j}| < R$ in the sensor network for long-range communications. In this paper, routing is implemented for message transmission by carrying out end-end communication protocols with the intermediate covering nodes. This helps us in establishing a shorter route for message transmission. Selfish nodes and malicious nodes are taken into account, if anything appears in the path, there will be some disruptions.

3.1 Source-Destination Confirmed On-Demand Routing Algorithm

The major disadvantage is discovering the shortest path is the cost of constructing a path. Bigger networks are not stable networks, the topology of the wireless networks changes and link breakages are also occurred. This requires node update if the position of the nodes gets changed. This will consume time and energy. This problem is solved by the Thourup-Zwick approach for efficient routing.

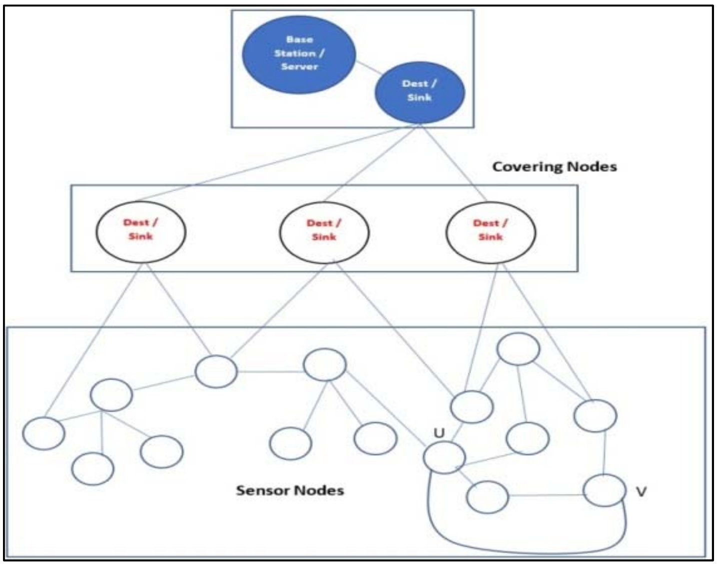

Fig 1. Architecture of the WSN.

3.2 Algorithm Overview

Algorithm-1 shows the source and the destination nodes are initialized and verified before routing using ODR protocol for establishing efficient routing in WSNs. Consider a network with a time $\boldsymbol{t}$. The mobile wireless sensor network is a weighted undirected graph and it is denoted by $\boldsymbol{G} = (\boldsymbol{S}, \boldsymbol{E})$. Consider $\boldsymbol{S}$ and $\boldsymbol{D}$ as sets of nodes and the status of their connection among the nodes. Before transmitting any data to the neighbour node, it verifies the local cache initially. If the nodes are not connected earlier, then the node $\boldsymbol{s}$ and node $\boldsymbol{d}$, then a request packet is sent to the sink for acknowledgment. The sink node is denoted as $(\boldsymbol{v})$. The structure of the data is required by the destination node for initiating communication and the structure of the data is obtained by preprocessing the graph $(\boldsymbol{G})$. The data structure contains the shortest path and the shortest is sent to the node for transmitting data packets. The on-demand algorithm is generally straightforward and provides the shortest path for message transmission.

Algorithm-1: On-Demand Routing Algorithm (S, V, E)

```
{
Path = checkCache(S)
If path == null
    r = ReqRoute(S, D)
    Path = QueryPath(S, V)
    Information(S, D, path)
Endif
dataPckt from S to V in path
r = r − 1
if V.dataPckt == success then
    r = 0
end if
return r
}
```

3.3 Status Allocation

The sink node will communicate directly to other nodes because of the effects of direct communication which is explained earlier. Sink nodes are responsibly initializing the source-initiated on-demand routing protocol by gathering basic information from the neighbour nodes. The information gathered by the sink node contains the connection status and location of the respected node. This process is illustrated in algorithm-2.

In this algorithm, the covering node receives a status report from its neighbour node individually. The status report from each node contains the parameters for message transmission and it is represented by$\boldsymbol{v_i} = \langle \boldsymbol{E_i}, \boldsymbol{PRR_i}, \boldsymbol{L_i}, \boldsymbol{C_i} \rangle$. The residual energy and the PRR (packet reception ratio) are denoted by $\boldsymbol{E_i}$ $\boldsymbol{and}$ $\boldsymbol{PRR_i}$. $\boldsymbol{L_i}$ $and\boldsymbol{C_i}$denotes the load status and connection status in the network.

For every window $\Delta\boldsymbol{w}$, $\boldsymbol{PRR_i}$ is computed and it is shown below;

$$\mathrm{PRR_i}(\Delta \mathrm{w}) = \frac{\mathrm{Num_{rp}}}{\mathrm{Num_{sp}}} \qquad (1)$$

From the above equation, $\boldsymbol{Num_{rp}}$ and $\boldsymbol{Num_{sp}}$ denotes the packets that are received and sent. Consider a time frame $\Delta\boldsymbol{t}$ with a load $\boldsymbol{L_i}$and it is calculated below;

$$L_i(\Delta t) = \frac{Num_{rdp}}{Num_{ldp}} \qquad (2)$$

Algorithm-2: Allocation Algorithm (S)

```
{
For $i = 1$ to path
        $S = S_i$
    get covered sensor nodes of $c$ as $U_i = \{u_1, u_2, \dots, u_q\}$
For $j = 1$ to $q$
        $S = S_j$
        $D = setStatusinfo(S)$
        $info = \langle j, D \rangle$
        $S = info(c)$
End for
forwardInfor(S, D)
end for
}
```

where $\boldsymbol{Num_{rdp}}$ and $\boldsymbol{Num_{ldp}}$ represents the relayed data packets and the generated local products. Once the information is collected, the information is forwarded by the sink node to the covering node.

In mobile wireless sensor networks, the status allocation has different cases. Consider the value of n as 3, then we have three different possibilities for status allocation, and this subnetwork is shown in fig-2. Consider 3 different scenarios, in the first scenario; if the sensor nodes ($n3$ and $n5$) are directly adjacent to the covering node, the nodes are only able to send the status vector. If the sensor nodes ($n2$, $n4$, and $n6$) are directly adjacent to the nodes mentioned in the first scenario, then they transmit the status vector to the covering node and two hops are required by the sensor nodes. In the last scenario, only one node ($n1$) will send the status vector to the covering node in three hops.

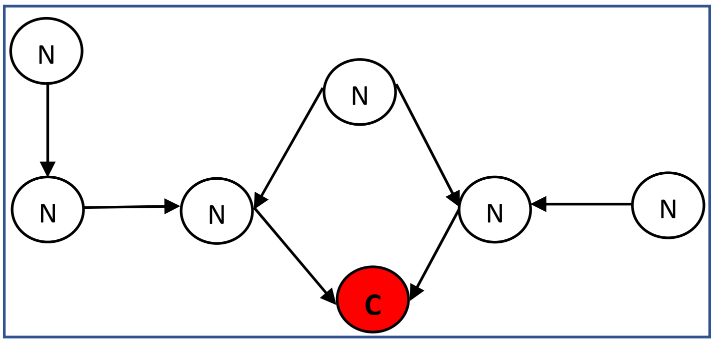

Fig. 2: Allocating the Node Status

3.4 Graph Construction

Once the status allocation is completed, the overall information is obtained by the sink node. The graph construction is done in the same weighted graph. Consider $|\boldsymbol{V}| = \boldsymbol{n}\ and\ |\boldsymbol{E}| = \boldsymbol{m}$, where V and E denote the sensor node and link between the nodes. The below equation is representing$\boldsymbol{e_{ij}} \in \boldsymbol{E}$;

$$e_{ij} = \begin{cases} w_{ij}.\left|n_i, n_j\right|, \left|n_i, n_j\right| < R \\ \infty, \qquad \left|n_i, n_j\right| \geq R \end{cases} \qquad (3)$$

The above equation represents the distance between the nodes in the graph. The distance is considered as infinity if distance among the nodes is greater than the range of communication. For avoiding such cases, fixed weight values are used and it is calculated below;

$$w_{ij} = \alpha.E_{ij} + \beta.Q_{ij} + \gamma.L_{ij} \qquad (4)$$

Different factors such as energy status etc are required for obtaining a constant weight value. The below equation shows the calculation of $\boldsymbol{E_{ij}}$;

$$E_{ij} = \frac{E_i - E_t}{E_i} \times \frac{E_j - E_t}{E_j} \qquad (5)$$

$\boldsymbol{E_i}$ and $\boldsymbol{E_j}$ represents the remaining energy of the node. The energy needed for transmission is denoted as $\boldsymbol{E_t}$ and the link quality is denoted as $\boldsymbol{Q_{ij}}$. In this approach, the link quality is evaluated by using software-based link quality estimator called ETX is implemented, (A. Woo and D. Culler (2003), D. Lal et al. (2003), R. Fonseca et al. (2007), A. Cerpa et al. (2005), M. Senel et al. (2007), D. S. J. de Couto et al. (2003). The below equation shows the calculation of $\boldsymbol{Q_{ij}}$;

$$Q_{ij} = \frac{1}{PRR_i \times PRR_j}, \qquad (6)$$

From the above equation $\boldsymbol{PRR_i}$ and $\boldsymbol{PRR_j}$ denotes the uplink and downlink quality. The load status is denoted by $\boldsymbol{L_{ij}}$ and it is shown below;

$$L_{ij} = \frac{1}{L_i \times L_j}, \qquad (7)$$

The coefficients of the weights are $\boldsymbol{\alpha}, \boldsymbol{\beta}\ and\ \boldsymbol{\gamma}$ and we obtained that the sum of all the coefficients is equal to **1**.

3.5 Graph Processing

The next part is processing the weighted graph, it is essential for transmitting the messages to other nodes more efficiently. Consider $|\boldsymbol{V}|$=$\boldsymbol{n}$ **and** $|\boldsymbol{E}|$=$\boldsymbol{m}$. The weighted graph is preprocessed by Thorup and Zwick technique proposed by M. Thorup and U. Zwick (2005). The preprocessing is done in $O(\boldsymbol{knm^{1/k}})$**.** This approach will preprocess the graph in a certain time and a data structure with a size of $\boldsymbol{O}(\boldsymbol{kn^{1+1/k}})$ is constructed. If any path responds to a query in $\boldsymbol{O}(\boldsymbol{k})$time, then the distance is ***2k-1***, where $\boldsymbol{k}$ belongs to an integ

er and k must be greater than or equal to 1. Once the status information is allocated, the network topology is completely obtained by the sink node and this is the result of preprocessing the weighted graph using the Thorup and Zwick approach and it is shown in algorithm-3.

Algorithm-3: GraphPreparation (S)

```
{
 Assume an integer $k \geq 1$
Time t, create topology of the network G = (S, E)
$prepara_{Thoyup-Zwick}(S, E, k)$
Store data in local DB of S
}
```

3.6 Path Query

Once the weighted graph is pre-processed, the sink node will be ready for sending a response based on the path query to the covering node. The path query algorithm is given in algorithm-4 and Thorp-Zwick approach is used to construct the structure of the database.

Algorithm-4: Query-Path-Algorithm ($\boldsymbol{S}, \boldsymbol{D}$)

```
{
Let k be an integer $k \geq 1$
    $\delta(S, D) = distance_{Thorup-zwick}(S, D, k)$
    Trace path from S to D
$Return\ E\ of\ path$
}
```

The above-said algorithms are incorporated together one by one to implement the proposed ODNB protocol.

3.7 Node Behaviour Analysis

The node behaviour is analyzed during route creation and data routing. For identifying and detecting malicious nodes, the behavior of the intermediate nodes including source and destination nodes. The applications of wireless sensor network communication and its performance is depending on the trustworthiness of the nodes. Each time of routing the efficiency of the forwarding node is verified for successful communication process, R. A. Shaikh et al. (2009). Based on the functionalities of the intermediate nodes the source and destination nodes perform well in the network. Each time, the ODNB determines the operations of the individual nodes to complete one single communication operation. According to the behavior of the nodes, they are classified as Reliable Nodes denoted as R, Un-Reliable Nodes denoted as U, Malicious Node denoted as M, and Selfish nodes denoted as S illustrated in Figure-3. According to the application environment and scenario of the WSN in real-time, they may be changed at any time for any reason, where it changes the behavior of the sensor nodes in the network. The reason may also be because of various malicious threats focusing on the links while data forwarding. The misbehaviour of the sensor node may be changed due to power loss, miscommunication, reconfiguring the node properties, changing the power sources, and irregular work assignments. In addition to that, for several reasons, the nodes' behavior may change and it makes data loss and leads to malicious activities that can be involved in the network. Thus, to identify and detect the node behavior $\boldsymbol{N}$ number of nodes is deployed in the defined network area. The nodes are classified into various categories such as $W = \{\mathrm{R}, \mathrm{U}, \mathrm{M}, \mathrm{S}\}$, are obtained based on various reasons and it is shown in Figure-3.

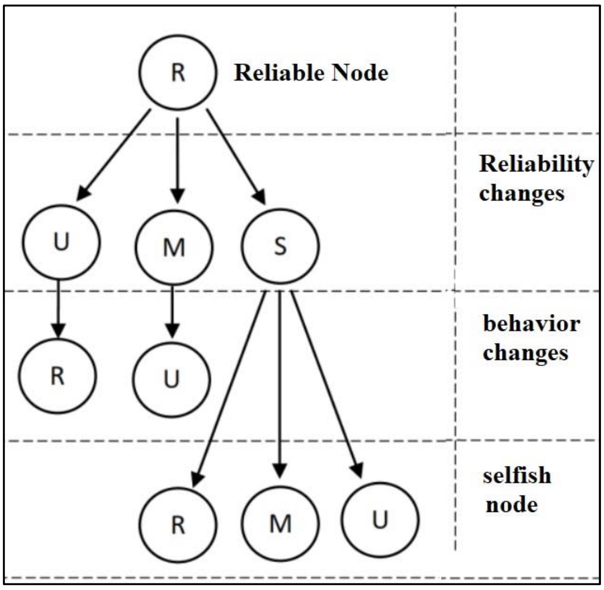

Fig. 3. Various Categories of Sensor Nodes

Within a time, interval **T**, the node behavior is analyzed. The changes of the nodes can be obtained arbitrarily and expressed as

$$W = \int_{n=0}^{N} T(probability(R, U, M, S)).$$

According to the behavior, the malicious nodes are predicted and eliminated from the data routing. Thus, the ODNB model uses node behavior analysis to improve the security in WSN applications. By incorporating the node behavior to on-demand routing the QoS factors of the WSN applications are improved. Some of the QoS factors calculated in the simulation are throughput, packet delivery ratio, delay, and data loss with respect to malicious nodes.

4. Experimental Results and Discussion

The ODNB protocol is simulated in Network Simulation-2 software and the network performance is verified in terms of Quality-of-Service factors. In order to do that, it is necessary to initialize the values of the network parameters in the software environment, and it is given in Table-1. The parameter values determine the output of the algorithm in the network scenario.

Parameters	**Values**
Network Area	1500m x 1500m
Execution Time	10s, 20s, …, 50s
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)
Malicious nodes	2%
Protocol	AODV/

Table-1. Simulation Settings

Based on the simulation parameters given in Table-1, various QoS factors are calculated and compared with the existing mechanisms such as RTA discussed by Kotari Sridevi and Mandapati Sridhar (2017), TMR discussed by Narula et al. (2008), FACE presented by S. K. Dhurandher et al. (2011), and TMS discussed by Abuhaiba and Hubboub (2013). The proposed ODNB model is also compared with the trust-based routing mechanisms, MRTS in N.Djedjig et al. (2017), MRHOF-RPL, and SecTrust in N.Djedjig et al. (2020) and the obtained results are given in the following figures.

For example, initially the packet delivery ratio (PDR) is calculated and the comparison is given in Figure-4. Packet delivery ratio is, the number of packets received successfully at the destination or sink compared to the number of nodes delivered at the source node. To evaluate the performance, the simulation is repeated five number of times with different number of nodes (10, 20, 30, 40, 50) used in the process and calculate the QoS values. For comparing the efficiency, the average value of the QoS factors obtained from the overall simulation is verified. The average packet delivery ratio obtained using the proposed ODNB model is 92.2%, which is higher than the existing methods TMS, MRHOF-RPL, and Sec-Trust obtained the PDR of 66%, 73.4%, and 79.4% respectively.

The number of packets dropped with respect to the malicious nodes is calculated from the simulation and the comparison result is shown in Figure-5.

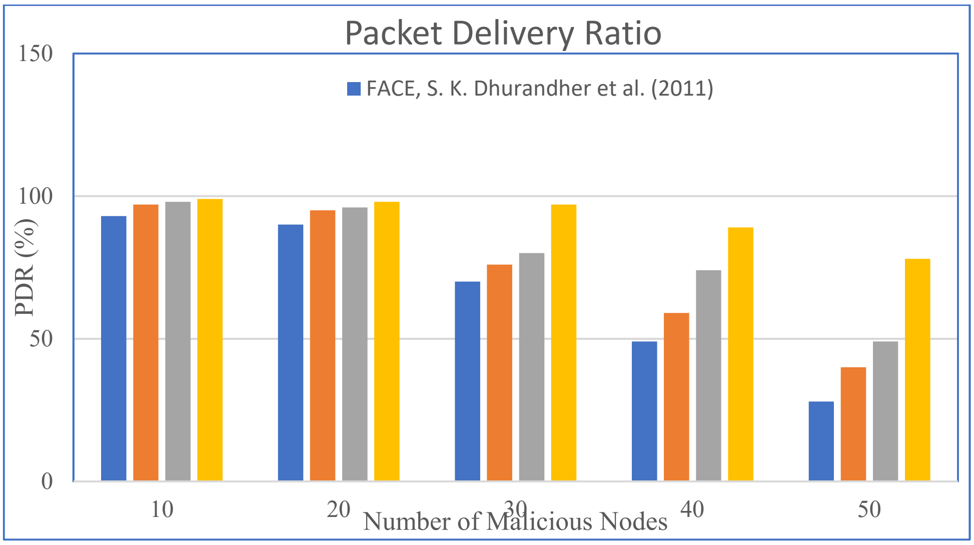

Fig. 4. Packet Delivery Ration with Respect to Malicious Nodes

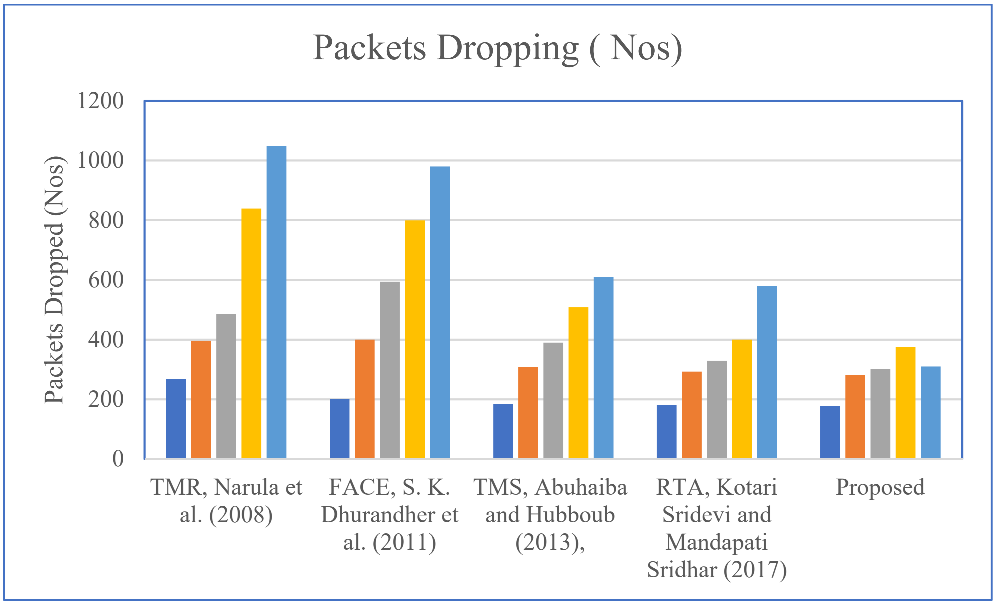

Fig.5 . Packet Dropping with Respect to Malicious Nodes

The number of packets dropped in the network is calculated by subtracting the number of packets received successfully at the destination node from the number of packets delivered by the source node. From the figure-5, it is noticed that the number of packets dropped by the proposed ONDB is very less than the other existing methods. Similar to that, the delay is calculated from the simulation and the comparison result is shown in Figure-6. The delay is the total amount of time taken for one round of data transmission, measured in milli seconds (ms). From the Figure-6, it is noticed that the proposed ODNB model obtained very less delay comparing with the other existing methods.

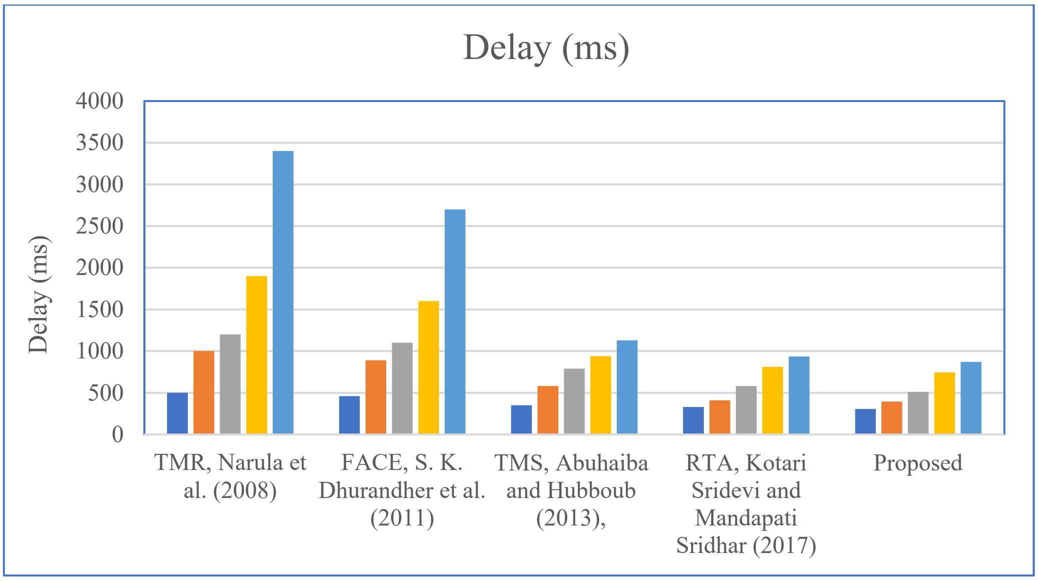

Fig.6. Delay with Respect to Malicious Nodes

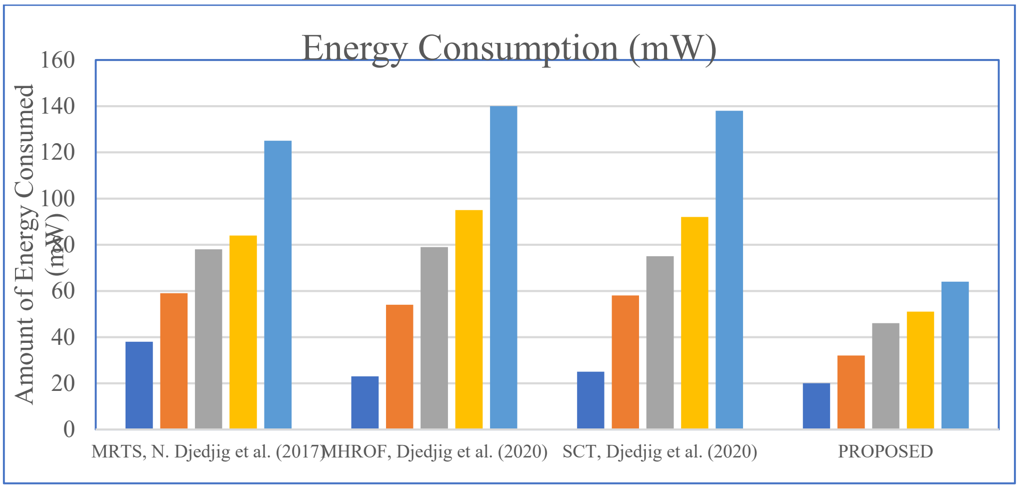

Fig.7. Energy Consumption with Respect to Malicious Nodes

Finally, the most important QoS factor, the energy consumption is calculated from the simulation and the comparison result is shown in Figure-7. The amount of energy spends to complete one round of operation is called as energy consumption and calculated for the proposed ODNB model and compared with the existing methods, MRTS N.Djedjig et al. (2017), MHROF-RPL N.Djedjig et al. (2020), and SCT N.Djedjig et al. (2020). From the Figure-7, it is noticed that the proposed ODNB consumed lesser amount of energy comparing with the other models.

From the overall simulation results, it is noticed that the proposed ODNB performs well than the other existing methods and proved.

5. Conclusion

The main objective of this paper is to design and implement a novel secured routing protocol for WSN applications. To do that, this paper integrated on-demand routing and node behavior analysis model. The node behavior analysis is applied from the beginning of the network construction, that is node deployment process to routing the data in the network. The on-demand routing model is used while do data routing. Both the models' functions are incorporated together for verifying the node, data, and routes for detecting and identifying the nodes as malicious nodes in the network. Finally, the proposed ODNB model proved its efficiency than the existing model in terms of PDR, packet dropping, delay, and energy consumption. From the simulation it is identified that the proposed ODNB model outperforms than the other existing methods. For example, the average packet delivery ratio obtained using the proposed ODNB model is 92.2%, 28.94% of packet dropping, 8.7% of delay, and 6.4% of energy consumption, is the better results. From the results, it is concluded that the proposed ODNB is better method for WSN in terms of security with the improved QoS factors.

6. Future Work

In future the proposed model is three level of security models such as user-level, data-level, and routing-level and the results are verified.

References

[1] N. Marchang and R. Datta, "Light-weight trustbased routing protocol for mobile ad hoc networks", IET Information Security, Vol. 6, No. 2, pp. 77 - 83, 2012.

[2] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad hoc Networks", In: Proc. of International Conf. on ACM Mobile Communication, pp. 255-265, 2000.

[3] Z. Movahedi, Z. Hosseini, F. Bayan, and G. Pujolle, "Trust-Distortion Resistant Trust Management Frameworks on Mobile Ad Hoc Networks: A Survey", IEEE Communications Surveys & Tutorials, Vol. 18, No. 2, pp. 1287- 1309, 2016.

[4] X. Mao and J. McNair, "Effect of on/off misbehavior on overhearing-based cooperation scheme for MANET", In: Proc. of International Conf. on Military Communication, pp. 1086- 109, 2010.

[5] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", In: Proc. of International Conf. on 6th Joint Working Communication, Multimedia Security, pp. 107-121, 2002.

[6] A. A. Rahman, and S. Hailes, “ A distributed trust model,” in Proceedings of the ACM New Security Paradigms Workshop, Cumbria, UK ,1997, pp. 48-60.

[7] P. Papadimitratos, and Z. J. Haas, “Secure routing for mobile ad hoc networks” in Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, 27-31, Jan 2002

[8] X. Li, M. R. Lyu, and J. Liu, “A trust model based routing protocol for secure ad hoc networks,” in Proceedings 2004 IEEE Aerospace Conference, Big Sky, Montana, U.S.A., March 6-13 2004.

[9] A. A. pirzada, C. McDonald, and A. Datta “Dependable dynamic source routing without a trusted third party,” Journal of Research and Practice in Information Technology, vol. 39, No. 1, pp71-85, Feb 2007.

[10] Johnson DB, Maltz DA. Dynamic source routing in ad hoc wireless networks. In Mob comput. 1996; pp 153-181.

[11] Sarkar A, Murugan TS. Routing protocols for wireless sensor networks: What the literature says?. Alexandria Engg J. 2016; 55(4): 3173-3183.

[12] Arya, Shobha, Nipur, Chandrakala Arya., "Performance Analysis of AODV, DSR and DYMO Protocols using Random Waypoint Mobility Model in MANET", Int J Computer Appl, 2013; 67: 13-17,

[13] Rameshkumar SG. Improving Quality of Service through enhanced node selection technique in Wireless Sensor Networks. Int J MC Square Sci Resear. 2016; 8: 133-142

[14] Ahuja R, Ahuja AB, Ahuja P. Performance evaluation and comparison of AODV and DSR routing protocols in MANETs under wormhole attack. In2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013). 2013; 699-702.

[15] Govindasamy J, Punniakody S. A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack. J Electrical Syst Inf Technol. 2018; 5(3): 735-744.

[16] M. Thorup and U. Zwick, “Approximate distance oracles,” Journal of the ACM, vol. 52, no. 1, pp. 1–24, 2005.

[17] A. Woo and D. Culler, “Evaluation of efficient link reliability estimators for low-power wireless networks,” Tech. Rep. UCB/CSD-03-1270, EECS Department, University of California, Berkeley, Calif, USA, 2003, http://www.eecs.berkeley .edu/Pubs/TechRpts/2003/6239.html.

[18] D. Lal, A. Manjeshwar, F. Herrmann, E. Uysal-Biyikoglu, and A. Keshavarzian, “Measurement and characterization of link quality metrics in energy constrained wireless sensor networks,” in Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM’03), pp. 446–452, December 2003.

[19] Fonseca, O. Gnawali, K. Jamieson, and P. Levis, “Four bit wireless link estimation,” in Proceedings of the 6th Workshop on Hot Topics in Networks, 2007.

[20] A. Cerpa, M. Potkonjak, J. L. Wong, and D. Estrin, “Temporal properties of low power wireless links: modeling and implications on multi-hop routing,” in Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC ’05), pp. 414–425, May 2005.

[21] M. Senel, K. Chintalapudi, D. Lal, A. Keshavarzian, and E. J. Coyle, “A Kalman Filter based link quality estimation scheme for wireless sensor networks,” in Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM ’07), pp. 875–880, Washington, DC, USA, November 2007.

[22] D. S. J. de Couto, D. Aguayo, J. Bicket, and R. Morris, “A high-throughput path metric for multi-hop wireless routing,” in Proceedings of the 9th Annual International Conference on Mobile Computing and Networking (MobiCom ’03), pp. 134–146, ACM, New York, NY, USA, September 2003.

[23] R. A. Shaikh, H. Jameel, B. J. d Auriol, H. Lee, S. Lee, and Y.-J. Song, "Group-based trust management scheme for clustered wireless sensor networks", IEEE Transaction Parallel Distributed System, Vol. 20, No. 11, pp. 1698- 1712, 2009.

[24] P. Narula, S. K. Dhurandher, S. Misra, and I. Woungang, "Security in mobile ad-hoc networks using soft encryption and trust-based multipath routing", International Journal of Computer Communication, Vol. 31, No.4, pp. 760-769, 2008.

[25] S. K. Dhurandher, M. S. Obaidat, K. Verma, P. Gupta, and P. Dhurandher, "FACES: FriendBased Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems", IEEE Systems Journal, Vol. 5, No. 2, pp. 176-188, 2011.

[26] I. S. Abuhaiba and H. B. Hubboub, "Reinforcement swap attack against directed diffusion in wireless sensor networks", International Journal of Computer Network Information Security, Vol. 5, pp. 13-24, 2013.

[27] Kotari Sridevi, Mandapati Sridhar, (2017), “A Reliable Trustworthy Approach Based on Node Behavior Prediction for Secure Routing in MANET”, International Journal of Intelligent Engineering and Systems, Vol.10, No.6, DOI: 10.22266/ijies2017.1231.25.

[28] N. Djedjig, D. Tandjaoui, F. Medjek and I. Romdhani, "New trust metric for the RPL routing protocol," 2017 8th International Conference on Information andCommunication Systems (ICICS), 2017, pp. 328-335, doi: 10.1109/IACS.2017.7921993.

[29] N. Djedjig, D. Tandjaoui and F. Medjek et al. (2020), "Trust-aware and cooperative routing protocol for IoT security", Journal of Information Security and Applications, Vol. 52, https: //doi.org/ 10.1016/ j.jisa. 2020.102467 2214-2126.

Author's Profile

Ms.Makimaa Y.P. received B.E degree in Electronics and Communication Engineering from Avinashilingam Institute for Home Science and Higher Education for Women in 2016 and M.E degree in VLSI design from PSNA College of Engineering and Technology in 2018. She is currently doing her Ph.D in Avinashilingam Institute for Home Science and Higher Education for Women. Her research area is Wireless Networks.

Mrs. Sudarmani R. has completed her Ph.D in 2014 from department of ECE, Anna University, Chennai. She is currently working as Associate Professor in department of ECE. She is currently guiding 5 Ph.D research Scholars in wireless networks domain. She has done more than 50 publications. Her area of interest is Wireless Communication