I. J. Computer Network and Information Security, 2021, 6, 41-56
Published Online December 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2021.06.04

A Node Confident based IDS to Avoid Packet Drop Attacks for Wireless Sensor Network

Kareti Madhava Rao[1] and S Ramakrishna[2]
[1]Research Scholar, Department of Computer Science, Sri Venkateswara University, Tirupati-517501, Andhra Pradesh, India
[2]Professor, Department of Computer Science, Sri Venkateswara University, Tirupati-57501, Andhra Pradesh, India
Corresponding author email address: amsmadhava@gmail.com

Received: 02 November 2020; Revised: 17 January 2021; Accepted: 25 February 2021; Published: 08 December 2021

Abstract: Because of the great characteristics of Wireless Sensor Networks like easier to use and less cost of deployment, they have attracted the researchers to conduct the investigations and received the importance in various civilian and military applications. A number of security attacks have been involved due to the lack of centralized management in these networks. The packet drop attack is one of the attacks and it has a compromised node which drops the malicious packets. In WSNs, different techniques have been implemented to identify the packet drop attack but none of them provides the feasibility to stop or isolate their occurrence in the future. In recent times, the reputation systems provide the way to identify the trustworthy nodes for data forwarding. But the lack of data classification in the reputation systems affects the false positive rate. In this paper, a novel CONFIDENT SCORE based BAYESIAN FILTER NODE MONITORING AGENT (CFS-BFNMA) mechanism is introduced to identify & avoid the packet drop nodes and also to monitor the node behaviours to improve the false positive rate. The final CFS of a node is estimated based on the node past and threshold CFS values. The node monitoring agents (BFNMA) constantly monitors the forwarding behaviour of the nodes and assigns CFS based on the successful forwards. The NMA saves the copy of the data packets in their buffers before forwarding to the neighbour nodes to compare them. Also, this BFNMA analyses the traffic pattern of every round of transmission to improve the false positive rate. By comparing with other conventional security algorithms, the proposed mechanism has been improved the network security & false positive rate drastically based on the simulation results.

Index Terms: Energy Efficient, Wireless Sensor Networks, Packet Drop Nodes, Bayesian Filter, Malicious, Shortest Path, Confident Score, CFS-BFNMA.

1. Introduction

The applications of WSNs have included different kinds of fields such as battlefield observation, environment monitoring [1], and health monitoring due to the advanced features and improvements in the wireless technology. Because of the characteristics of dynamic, data-centric, and self-organization, the deployment of Wireless Sensor Networks is made [2]. The sensor nodes limit by the resources such as power, memory size, processor speed, and radio range. So, it's required to design the application-specific systems that leads to the particular communication patterns in WSNs. The traffic in WSNs is unlike to the ad-hoc networks which includes the random nature.

The nature of WSNs is mostly non-guarded and the broadcasting nature of wireless medium is involved inherently. The vulnerability of WSNs is made to various security issues [3-6]. Different types of attacks like hijack attacks, tampering attacks, hello-flood attack, blackhole attack, selective forwarding attacks, sinkhole attacks, and Denial of Service attacks are involved in the WSNs owing to the transmission medium and distributed characteristics. The operation of WSNs can disrupt by these attacks and the deployment can even defeat. Some attacks can initiate by an adversary without using cracking keys for cryptography-based solutions.

To determine the best routing path based on trust-based systems like intrusion detection system and detect the malicious nodes from the network, the traditional methods have been proposed [7]. To obtain the trusted node in a network, some contradictory issues are faced such as complicatedness, security, and energy-efficiency although some benefits have provided by using these techniques [8-9]. Most of the existing models of trust or reputation could have different requirements for different trust value rank and were application-driven.

Therefore, the main purpose of this paper is to improve a robust and scalable reputation model to identify and avoid the malicious nodes in the communication phase. In this paper, a confident score calculation mechanism is introduced to calculate the trustworthiness of the forwarder nodes based on the transmission behavior. Also, a

BAYESIAN FILTER NODE MONITORING AGENT is employed to reduce the false identification of the nodes as malicious by constantly monitor and classifying the traffic patterns received from the sensor nodes.

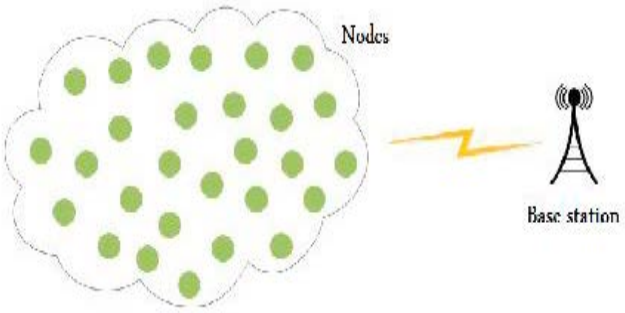

Fig.1. The basic architecture of a Wireless sensor network

For providing secure and trustable data forwarding, the paper has included the main contributions as follows:

- Calculation of CONFIDENT score CFS to evaluate the trustworthiness of a node. The score can be calculated based on nodes past behavior.
- The BFNMA constantly monitor the node forwarding behavior and analyze the received traffic pattern in order to classify the nodes based on the traffic pattern.

Based in these contributions, the BFNMA monitors the neighbor nodes and their forwarding behavior. Finally, it assigns the score to the nodes and data forwarding is carried out by the trustworthy nodes selected based on the CFS score.

1.1. Packet dropping in wireless sensor networks

In sensor networks, packet loss is expected for at least to an acceptable percentage [10] similar to any other network. All of the lost packets shouldn't be seen as malicious. There are various reasons for a node to drop the packets. Those are:

Legitimate Packet Dropping: - Generally, wireless sensor networks can experience the packet dropping and they don't have compromised nodes [11]. The following events are associated with this packet loss mainly;

- **Network Congestion:** In WSNs, network congestion is not avoidable. Owing to the in and out movements of data traffic, these channels of a network are occupied mostly. It will lead to the network congestion that results in packets loss.
- **Channel Conditions:** As drastic changes are involved in wireless networking; the channel condition can be considered. Different channel conditions are included such as noise presence on a channel, interference, free path loss, and transmitted wireless signals fading which can lead to bit errors or packet loss in the transmitted signal. Some of the packets can be dropped due to the presence of these factors.
- **Resource Constraints** Limited energy resource has included in the nodes of WSNs. To consume the battery power of limited resources, intermediate nodes are failed to forward the received packets and behave selfishly. As a result, these packets can be dropped.

Malicious Packet Dropping: -In a packet dropping attack launching, the primary step is mostly to get involved during the formation of a route for a malicious node. This could be achieved in a better way through the exploitation of routing protocols' weakness used in WSNs that are designed by assuming the trustworthiness between nodes in a network. The malicious node has a capability of doing anything like maliciously dropping packets [12] in the route. At a malicious intermediate node, this packet dropping can be resulted in the communication suspension or wrong information generation between the source and destination which is not a desirable situation.

Consider the route discovery process between source and destination. A RREQ or Route Request message is broadcasted by the source with unique identifier to all its one hop neighbors [13]. Each receiver rebroadcasts this message to its one hop neighbours until it reaches the destination. Upon receiving the message updates about source's sequence number, the designation sends a RREP or Route Reply message back to its neighbor which is depend on the RREQ. Without relying on the destination, a route with sequence number of a destination has included an intermediate node which equivalents to the one in RREQ which can send back a RREP packet to the source node.

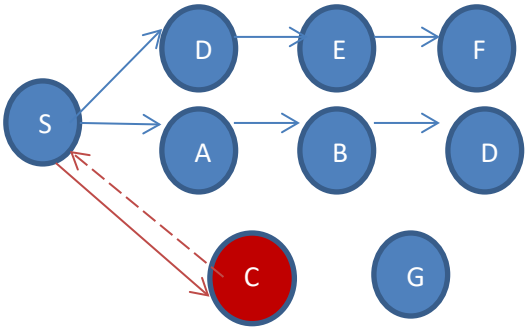

Fig.2. Routing process of packet drop attack by a malicious node C

At least one routing path should be included in the network [14] to launch a packet dropping attack for a node. In the above figure, this is demonstrated; C is a malicious node that intends to drop packets from S to D. Primarily, RREQ packet is broadcasted by S to its neighbors for discovering a path from S to D. As described earlier, each neighboring node is continued for message rebroadcasting until reaches to D. The breaching of this rule is done by a malicious node C and lies to S as it claims that the shortest path to D and a RREP packet sends to S. S initiates for sending data packets to D and the shortest route to D through C that leads to get dropped. The process of route level represents in Figure 2.

2. Literature Survey

Based on the reputation or trust model, the conventional methods are enlisted for WSN routing as follows:

Karthick et al., [15] was improved a novel protocol known as trust-distrust protocol (TDP) for data routing among the nodes in WSNs. By using the devised protocol, the routing process was categorized into four stages. With the implementation of k-means algorithm, the management of network topology was processed in the first stage. The node quality determines using the Link Quality Appraisal (LQA) in the second stage. Based on the value of LQA and a grade point, grading includes in the third stage. For routing data in WSNs, the secure path determines in the last stage. High security with less consumption of energy provides using the proposed technique. To improve the performance of routing in WSNs, the agent-based system is used which fails in the proposed method.

Selvi M et al., [16] has designed an algorithm of a secure routing called as energy-aware trust-based secure routing algorithm for the WSN routing. For evaluating the suspicious users in WSNs, the trust score was evaluated. To select the optimal route, the decision tree algorithm implements with the spatio-temporal constraints. Based on the security and packet delivery ratio, improved performance generates by using the algorithm. For handling incomplete knowledge, fuzzy constraints didn't consider in the method.

Udhayavani and Chandrasekaran et al., [17] has improved a trust-aware routing framework using an energy-efficient network protocol in order to provide trust-based routing. An energy-efficient route provides in the method with the increased network lifetime. The selective forwarding attacks and DOS couldn't address by this technique.

Asha and Santhosh et al., [18] has designed a protocol known as trust-based self-organized hierarchical energy balance routing protocol for addressing the issues of WSNs which concerns the storage and security. Based on the maintenance of sensor nodes energy level in the wireless networks, the protocol assists in improving the network lifetime. By using this protocol, the packet delivery rate enhances without considering the delay and jitter.

Gilbert et al., [19] has developed a time-series trust model (TSTM) based on a process of trust-based auto-regressive (TAR) and Toeplitz matrix for data transmission securely in WSNs. In determination of attacks, the proposed technique was effective but it wasn't implemented in heterogeneous large-scale networks.

Desai and Nene et al., [20] has designed a trust evaluation algorithm called as Self-Attestation and Self-Scrutiny in which the node-level trust evaluates using the resource of an internal node. The technique was considered as a mediating method which was sovereign with network topology and other data. The computation provides by the model for the trust evaluation itself and the providing of secure communication by its peer nodes. The enhancement of nodes' energy was improved by the technique but the communication was only processed when the node trusts itself.

3. Proposed System

Confident score based bayesian filter node monitoring agent (cfs-bfnma) method:

Methodology:

The node confident score-based Bayesian filter node monitoring agent method is proposed and the process of score calculation and node monitoring & classification is given in detail. The goal of the proposed method is to identify the trustworthy forwarder nodes & identify the malicious nodes based on received traffic pattern.

For providing data transmission securely, two phases include in the proposed model such as node monitoring and score calculation. Primarily, the deployment of sensor nodes is made and the environment is sensed by the node. The

periodical data transmission to the sink is required at the sensor nodes. The transmission interval is application-specific. To initiate the routing process, the nodes with high CFS should be selected for secure data transmission. The CFS can be calculated based on the past transmission behavior of the sensor nodes. All the sensor nodes configured to monitor the node behavior during every round of communication. Within the communication range, each sensor node monitors the other located sensor nodes. The initial routing is done as per the routing protocol since the initial CFS of the nodes is 0. The monitoring node and the neighbor of the source nodes receives the copy of the data since they are in the same wireless radio range. The monitoring agent keep an eye on the current forwarder node and monitor the forwarding pattern. If the data is successfully forwarded by the forwarder node, then the monitoring agent compare the pattern and increase the CFS of the current forwarder node.

3.1. BFNMA

In wireless networks, the most popular node misbehavior detection is the node monitoring technique in which each node can act like a monitoring agent and transmission of monitoring packet to neighboring nodes is made in promiscuous mode. In prior to the transmission of packets to the next node, the monitoring agents save a copy of packets in their buffers. To monitor packet relay from a neighboring node to the next node, this has been served.

To listen the channel within its radio range and get the other sensor nodes behaviors, and classify the actions, each monitoring agent node is used promiscuous node in the proposed BFNMA module. Several modules are configured in each monitoring agent. A specific function is performed by each module in such a way that it can classify the collected data according to the node behaviors. The following phases are categorized by the module of monitoring agents.

1) Data collection phase: To record the nodes behavior within its radio range in a function of fixed time window, a promiscuous node is used by the monitoring agent nodes.

2) Data classification phase: Based on the collected data in the previous Data collection phase, the monitoring node classifies the behaviour of the nodes and assigns the score to the nodes.

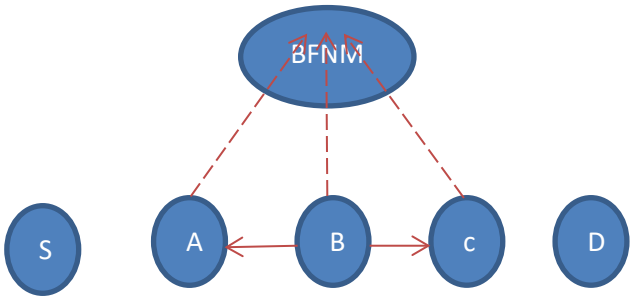

Fig.3. An example of BFNMA

An example of BFNMA is shown in the above figure 3 where S is denoted the source node and D is indicated the destination node. In the route between S and D, the other nodes are intermediate nodes. The packet is saved in the monitoring buffer before A is forwarded a packet received from S. BFNMA is monitored whether the packet has been forwarded to C after forwarding the packet to B. As A is within the transmission range of B, it is expected to receive a copy of packet that is forwarded to C. The received packet is compared with the one which is saved in the monitoring buffer in the BFNMA. The confidence score of B is reduced if in case it has failed to receive a copy of packet from B within certain duration. The confidence score is set to zero if this happens in recurring way and A is taken a decision that B is a malicious node and the route through B is dropped.

3.2. Calculation of CFS

The confidence score of a node can be calculated in two ways.

1. Neighbour CFS
2. Monitoring agent CFS

The neighbour CFS is an aggregation of the CFS values the neighbour node assigned to the source or the forwarder nodes in the previous transmissions. Likewise, the monitoring agents also maintain their own CFS records for every node based on the behaviour. The aggregation of these multi CFS is taken as the final CFS of a particular node. The CFS of a node in the current node can be calculated using the below equation (1).

$$CFS_n^{current} = CFS_n^{previous} + CFS_{thresh} \quad (1)$$

$CFS_n^{current}$ is the CFS of node n for the current round, $CFS_n^{previous}$ is the node n's previous CFS value calculated by the NMA. Initially, $CFS_n^{previous}$ is set to 0. CFS_{thresh} is the threshold CFS value set for each communication

between [0,1].

A fixed time window function is used by the agent node for recording the traffic data in the proposed model. The agent node has different CFS value in each time window. The CFS of a node can be calculated as follows in equation (2).

$$CFS_n = CFS_n^{current} + CFS_n^{previous} \quad (2)$$

CFS_n Is CFS of node n, $CFS_n^{current}$ is the current calculated CFS of the node n and $CFS_n^{previous}$ is the node n's previous CFS value calculated by the NMA. Initially, $CFS_n^{previous}$ is set to 0.

So, from the above equations, the CFS of the nodes during node selection is calculated and compared with other nodes using the following equation 3.

$$FCFS_n = CFS_n^{neighbor} + CFS_n^{BFNMA} \quad (3)$$

$FCFS_n$ is the finalCFS of node n, $CFS_n^{neighbor}$ is the calculated CFS for the node n in their neighbour nodes and CFS_n^{BFNMA} is the node n's CFS value calculated by the BFNMA. The aggregation of these CFSs' are considered as the final CFS of the nodes n.

The procedure of CFS-BFNMA is as following.

First step: The information is transmitted to their neighbor nodes by the source node.

Second step: The NMA agent and the neighbour of the source nodes receives the copy of the data since they are in the same wireless radio range.

Third step: The NMA monitors the neighbour nodes and their forwarding.

Fourth step: If neighbour node forwards the data, NMA compares the data and assign CFS if data is correct and successful.

Fifth step: NMA updates the CFS of the node based on CFS threshold value.

Algorithm- CFS calculation

CFS_n = CFS of the node n; CFS_{thresh} = CFS threshold value; $CFS_{current}$= Current CFS of node n;
##
For each node n
Set $CFS_{current}$ = 0
    Data forwarding
        If ($CFS_{current}$ == 0)
            If node n forwards the data
    $CFS_n = CFS_{current} + CFS_{thresh}$
            End if
Else
$CFS_n = CFS_{prev} + CFS_{thresh}$
End if
End for

Algorithm- Node selection based on CFS

For each node n
    If $CFS_n > CFS_{n+1}$
        NH = CFS_n
    Else
        NH = CFS_{n+1}
            If node NH forwards the data
                $CFS_{nh} = CFS_{current} + CFS_{thresh}$
            End if
    End if
End for

4. Result and Discussion

4.1. Experimental setup

To assess the proposed method's performance, the simulation is conducted by comparing with two different schemes. NS2 or network simulator 2 has been used in this project and it is an object oriented and discrete event driven network simulator that targets at the research of networking. The support of routing, UDP, and multicast protocol

simulation is provided on all wireless networks. In this work, the network model is used in which fixed sensor nodes in a network are existed with homogeneous types with same radio-transmitter devices, same capabilities, and constrained power resources, having same initial energy, and uniform deployment. The BS is fixed and located away from the sensor node. Based on the static nodes and plane coordinates, the simulation tests are conducted. Limited energy nodes are assumed and the transmission or reception of information can be restricted after the nodes initial energy is used up. In the below table (Table 1), the simulation parameters are considered.

Table 1. Simulation table

PARAMETER	VALUE
Application traffic	CBR
Transmission rate	1024 bytes/ 0.5ms
Radio range	250m
Packet length	1024 bytes
Routing Protocol	AODV
Simulation time	100s
Number of nodes	50
Area	1000 x1000
Malicious nodes	3
Transmission Protocol	UDP
Initial Energy	100j

An attacker not involves in the network deployment which assumes initially. The node attacks by attacker after sometime and its behavior is changed. The ranging value of CFS is from 0 to 1. The misbehavior or good neighbor nodes has decided by the CFS threshold value. The detection rates are low and high when the threshold values are high and low respectively. The value of threshold set to 0.05. To restrict the false positive rate, the value considers as between 0 to 1. The ratio of incorrectly nodes is indicate by false positive rate in presence of malicious nodes in a network.

4.2. Simulation result and analysis

The presentation of obtained results from simulation on different scenarios is discussed in this section. In the area of 1000 x1000 m and a network of 50 nodes, the attack model is implemented.

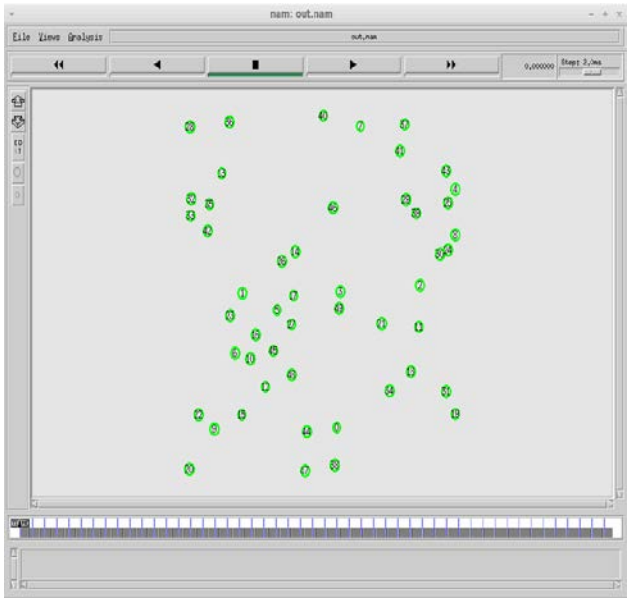

Fig.4. The sensor nodes are deployed in the random locations within 1000 x 1000 network area.

The sensor nodes are deployed in 1000 x 1000 wide network area depends on the network size. The nodes are scattered in the network instead of fixed positions. The nodes are equipped with wireless medium to communicate with the neighbor nodes. Every node is configured with IEEE 802.11 standards. The nodes are fed with 100 joules of initial energy. Figure 4 represent the network deployment.

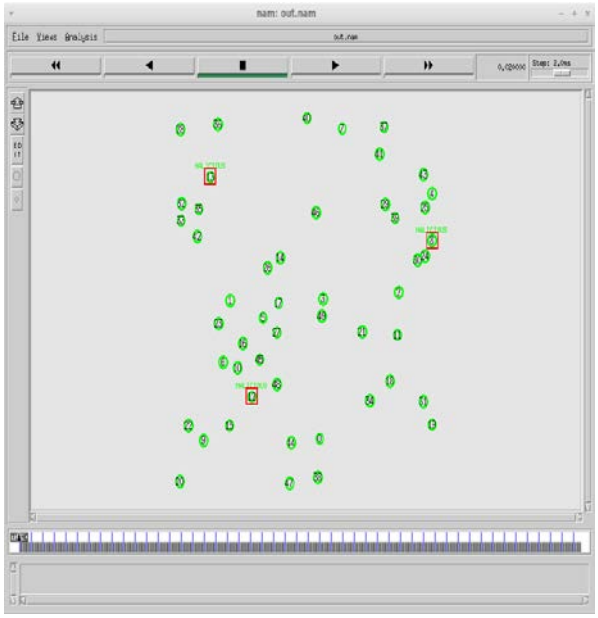

Fig.5. Some random sensor nodes are configured as malicious to inject the packet drop attacks

The presence of MALICIOUS nodes interrupts the data transmission and it shows in figure 5. Random nodes are configured as Malicious and they can interfere in the ongoing communication in any means and drop the data packets not intended for them. The malicious nodes uses RREQ and RREP control packets to interrupt the data transmission path, which are used during route discovery phase. Once the malicious node compromise themselves with the routing path, then they start receiving the data packets with an intention to drop them.

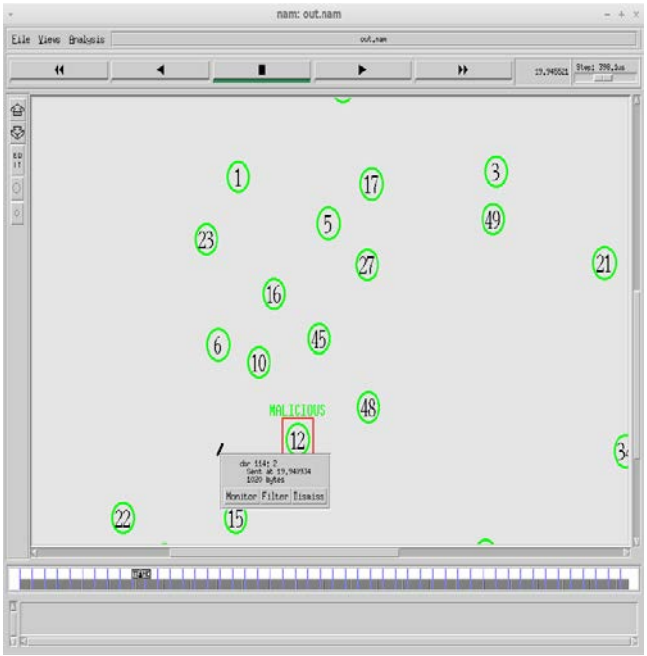

Fig.6. A data packet of 1020 bytes is being transferred from a sensor node to SINK, despite the presence of malicious nodes

After exchanging control packets, the sensor nodes share the data with the target nodes. A data unit of 1020bytes are transmitted among the nodes. CBR is used as traffic agent which introduce the constant traffic at fixed intervals. Initially, CFS of the nodes is set to 0. So the chances for the data packets being captured by the Malicious is HIGH. Our mechanism monitors each and every node transmission and the pattern for monitoring. Here figure 6 represent the CBR information.

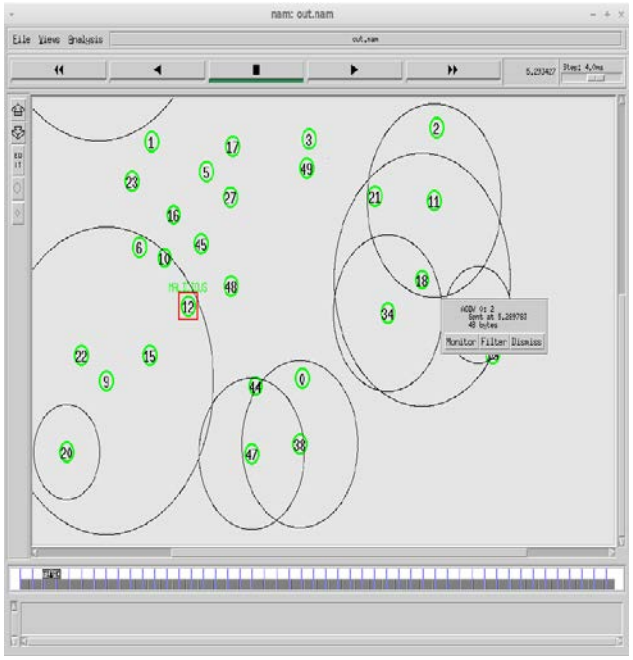

Fig.7. Nodes share their CFS score and other vital information needed for secure communication in the form of control packets

Nodes exchange their CFS score and other details like routing information, residual energy using control packets to select the node with good CFS. The control packet available in the routing protocol is used for this purpose. In our case, since we are using AODV routing protocol, the existing HELLO packets are used to exchange the information among the sensor nodes. Each hello packets size is 48 bytes only and it will cause only less overhead in the network.

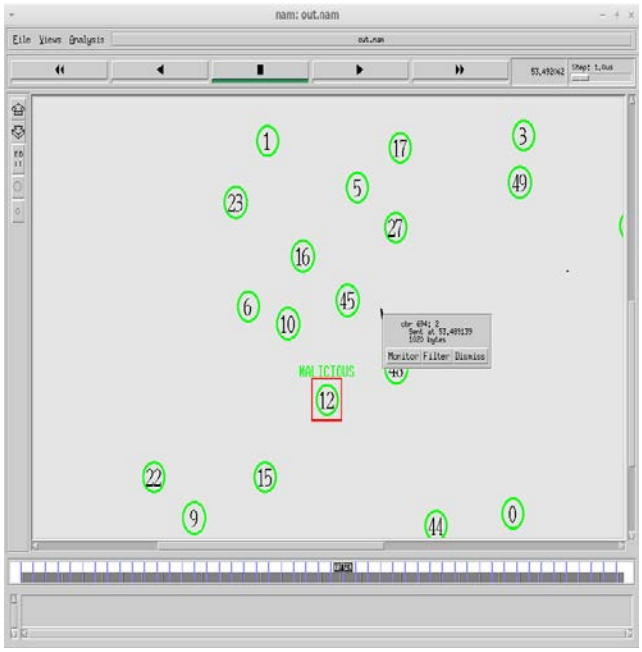

Fig.8. Data transmission without uninterrupted communication over the presence of the malicious nodes

Despite the presence of malicious in the network, the forwarder nodes managed to identify the nodes with good CFS for uninterrupted data transmission. After the deployment and the initial rounds of communication, the routing table of each and every node is updated based on the CFS of the nodes. High CFS nodes have high chances of being selected as forwarders. Routing table is updated after every round of communication based on the node successful forwards. A data packet of 1020 bytes is transferring between the nodes and it shows in figure 8.

```
CFS value of node 1 is 0.139869
CFS value of node 2 is 0.425263
CFS value of node 3 is 0.425061
CFS value of node 4 is 0.140169
CFS value of node 5 is 0.711342
CFS value of node 6 is 0.722060
CFS value of node 7 is 0.140384
CFS value of node 8 is 0.140039
CFS value of node 9 is 0.723903
CFS value of node 10 is 0.541820
CFS value of node 11 is 0.695750
CFS value of node 12 is 0.139729
CFS value of node 13 is 0.140400
CFS value of node 14 is 0.151116
CFS value of node 15 is 0.716579
```

Fig.9. The CFS score of each sensor node is updated during every round of communication

CFS values of first 15 nodes after 'n' rounds of communication. The node which forwards high data have the high CFS and having the chance of selected as next forwarder. Figure 9 shows the CFS file.

```
index :10  dest :2 source :1 nexthop :14 prevhop :1
index :45  dest :2 source :1 nexthop :14 prevhop :1
index :27  dest :2 source :1 nexthop :14 prevhop :1
index :42  dest :2 source :1 nexthop :14 prevhop :1
index :14  dest :2 source :1 nexthop :14 prevhop :1
index :26  dest :2 source :1 nexthop :46 prevhop :14
index :17  dest :2 source :1 nexthop :46 prevhop :14
index :5  dest :2 source :1 nexthop :46 prevhop :14
index :46  dest :2 source :1 nexthop :46 prevhop :14
index :3  dest :2 source :1 nexthop :46 prevhop :14
index :27  dest :2 source :1 nexthop :46 prevhop :14
index :49  dest :2 source :1 nexthop :46 prevhop :14
index :1  dest :2 source :1 nexthop :46 prevhop :14
index :14  dest :2 source :1 nexthop :7 prevhop :46
index :3  dest :2 source :1 nexthop :7 prevhop :46
index :26  dest :2 source :1 nexthop :7 prevhop :46
index :7  dest :2 source :1 nexthop :7 prevhop :46
index :23  dest :2 source :1 nexthop :14 prevhop :1
index :16  dest :2 source :1 nexthop :14 prevhop :1
index :5  dest :2 source :1 nexthop :14 prevhop :1
index :6  dest :2 source :1 nexthop :14 prevhop :1
index :26  dest :2 source :1 nexthop :14 prevhop :1
index :17  dest :2 source :1 nexthop :14 prevhop :1
index :10  dest :2 source :1 nexthop :14 prevhop :1
index :45  dest :2 source :1 nexthop :14 prevhop :1
index :27  dest :2 source :1 nexthop :14 prevhop :1
index :42  dest :2 source :1 nexthop :14 prevhop :1
```

Fig.10. The routing table is updated as **per** the node CFS score and the next hop nodes are assigned based on the final score of the nodes.

Routing table information of various nodes captured during data transmission and shows in figure 10.

If proper forwarder nodes are not selected, the chances of delayed delivery of data will be high. The node monitoring agent watches node forwarding behavior and avoids the nodes with poor delivery rate. It impacts the delay of the network and provides less end-end-delay than other methods. In the results, the maximum time delay experienced in the 50 node network is 0.07 under proposed scenario where as the end to end delay touched almost 0.1 ms in the existing algorithms. Figure 11 represent the End-to-End delay.

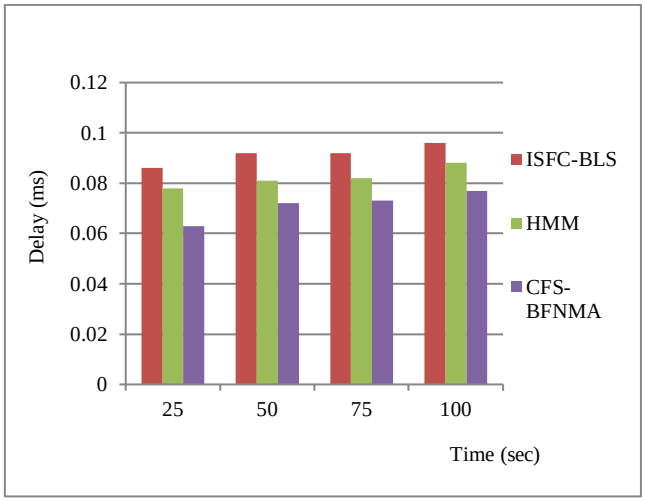

Fig.11. Comparison of end-to-end delay over time

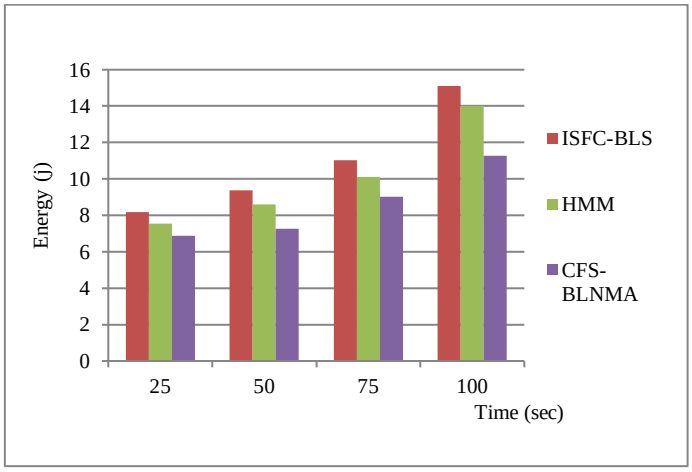

Fig.12. Energy Consumption of the sensor nodes during data communication

Energy is the limited resource for wireless networks. Energy depletion is a major reason for network failure. The use of NMA and CFS based forwarder selection ensures that data are forwarded in the nodes where energy usage is optimized. The result is showed that the proposed method reduces the network's energy conservation and achieves increased lifetime over the other protocols. The energy consumption is shows in figure 12. The proposed mechanism consumes the energy at the range of 8-10 joules in the deployed 50 nodes network. The total simulation time is 100 s. The energy consumption went up to 12 joules in the previous algorithms and prove that our mechanism energy efficient.

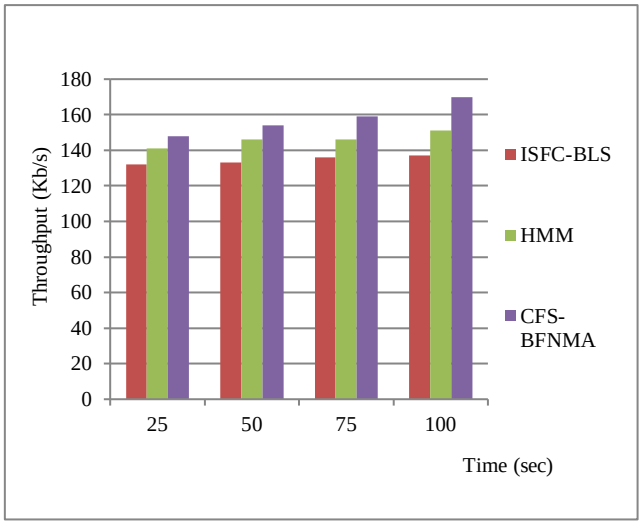

Fig.13. Throughput comparison of the proposed method

Throughput describes how successful the network is for reliable communication. The fair selection of the forwarder nodes based the past activity ensures effective data delivery, which highly impacts the throughput. The maximum throughput achieved in the network under the proposed scenario was almost 165kpbs whereas the lowest throughput achieved 135kbps in ISFC-BLS method. The result shows that the proposed approach improves throughput than its competitors. Figure 13 represent the throughput of network.

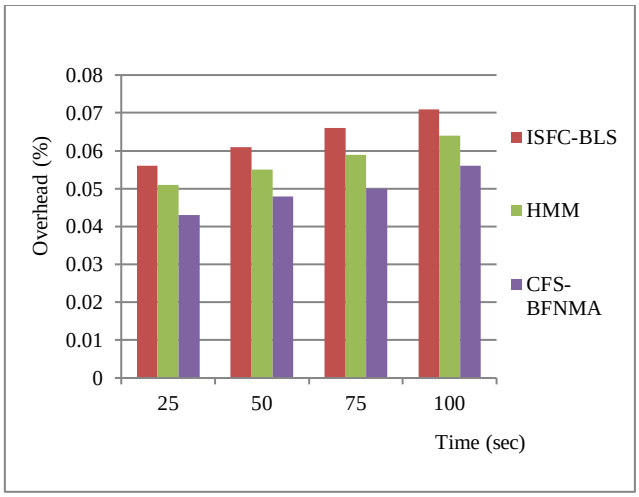

Fig.14. Routing Overhead comparison

Overhead is a parameter that describes the complexity of the proposed algorithm. The good CFS of the nodes means that the node's performance was good in the past. Selecting these good CFS nodes simplifies the routing process without any interruption, which requires no additional / fewer control packets. The total overhead incurred to the network under proposed scenario is as low as 0.04 whereas the network experienced overhead almost 0.07 in the existing scenarios. The reason was the intelligent selection of the forwarding nodes based on their forwarding behaviors. Hence, the lower overhead is achieved with the proposed approach when compared to the previously used protocols. The routing overhead is showed in figure 14.

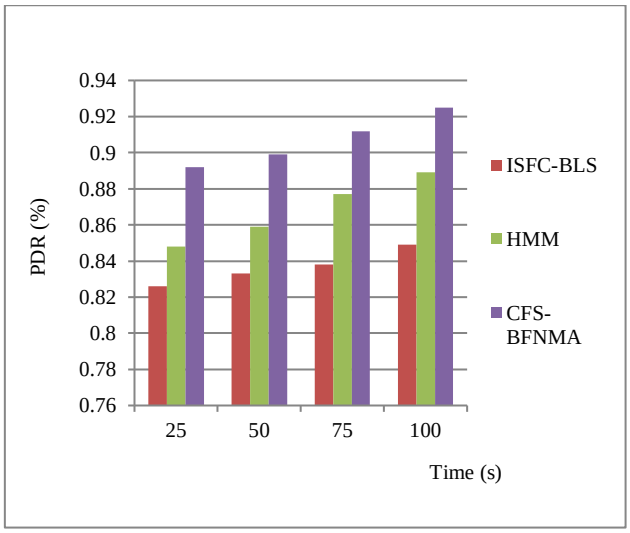

Fig.15. Packet Delivery Ratio comparison of the proposed method

The proposed CFS based method ensures that the nodes which were performed well in the previous transactions get the chance for further transmissions. This will improve the seamless data delivery within the estimated time and deliver the data quickly. In the execution, the proposed algorithm yields PDR almost 0.93 which is considered among the best pdr rate. As a worst case, the ISFC-BLS achieved only 0.84 as the maximum pdr which should be improved for a better data delivery rate. The result proves that the proposed approach performs well and achieves high PDR rate than the other protocols. Figure 5 represent the packet delivery ratio.

4.3. Experimenta process

In order to analyze the stability of the proposed algorithm, the algorithm was tested under various network

conditions by varying the network size from 100 to 500 in the 1000x1000 network area and by varying the total number of malicious nodes from 3 to 7. The random nodes were picked and configured as malicious which were present in the different locations of the network area. The CBR traffic agent was used in the entire experiment to enable the data traffic at the constant bit rate. Multiple nodes were randomly picked and communication was enabled between them. Each data packet size was 1020bytes. The experimental simulation time was 100 s in all the scenarios.

A. Number of nodes Vs Parameters

The proposed algorithm is tested by varying the network size from 100 to 500 nodes with the presence 5 malicious nodes in the network. The primary parameters like end-to-end delay, energy consumption & throughput is analyzed and illustrated from Figure 16-18. The results prove that despite the presence of the malicious nodes, the proposed protocol achieves better results in all means compared with the existing protocols.

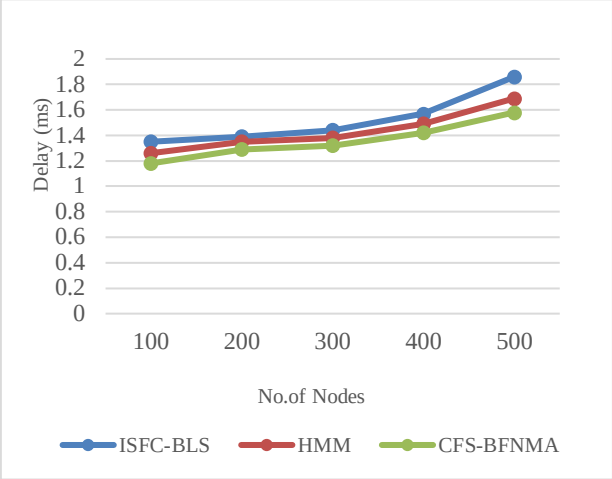

Fig.16. Analysis of delay vs No.of Nodes

When the number of nodes increases, the amount hop count increases in the transmission path. The more hop count cause more delay. In our experiments also the end to end delay increases when the number of node increases. In our executions, the proposed mechanism provides the delay from 1.2 to 1.6 ms with the presence of 5 malicious nodes. But the end to end delay touched almost 2.0 ms in the existing algorithms that affected the data transmission.

Fig.17. Analysis of Energy vs No. of Nodes

The energy is one of the most affected parameter under any malicious circumstances. The network size also plays a vital role in total energy consumption rate. In our experiment, the proposed algorithm spent only 65-70 j of energy despite the presence of 5 malicious nodes.

In a network with malicious presence, the data transmission gets affected prominently. The throughput rate decreases when large number of malicious present in a network. In our experiments, the throughput was not affected by the malicious nodes due to the CFS based node selection and the highest throughput recorded was 0.7 in the proposed algorithm.

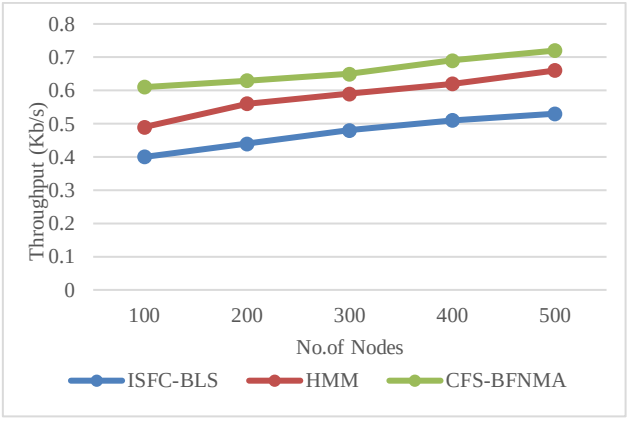

Fig.18. Analysis of Throughput vs No.of Nodes

B. Varying malicious nodes: time Vs Parameters

To analyze the false-positive rate, stability & the attack prevention rate of the proposed algorithm, the number of malicious nodes were increased from 3 to 7 in the 100-node network. The parameters like end-to-end delay, PDR, throughput, energy consumption & overhead are measured and shows in Figure 19-23. The network performance is not much affected even the number of malicious nodes is high in the network. Particularly the parameters like energy consumption, overhead are less affected in the high malicious node scenario. The evaluation results proves that the proposed protocol is reliable and having good stability in multiple malicious scenarios,

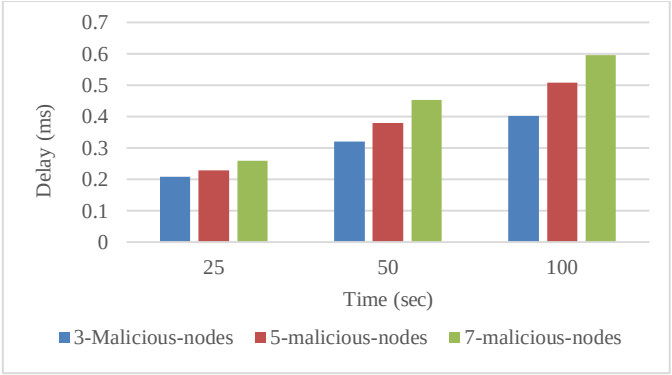

Fig.19. Delay by varying malicious nodes

The malicious nodes may increase the delay by interrupting the data transmission. With the presence of 5-7 malicious nodes in our experiments, the total time delay increases slightly up to 0.6ms in the network under proposed algorithm.

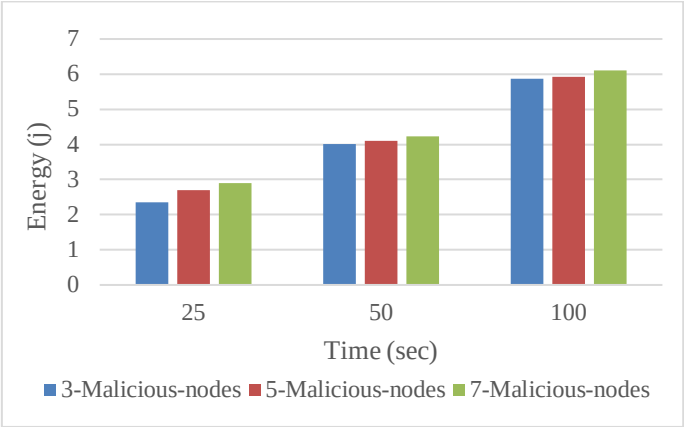

Fig.20. Energy by varying malicious nodes

The total energy consumption of the network is not much affected as like other algorithms in our experiment with proposed algorithm. The energy consumption is almost same and not affected badly when the number of malicious is increased to 7 in the experiment.

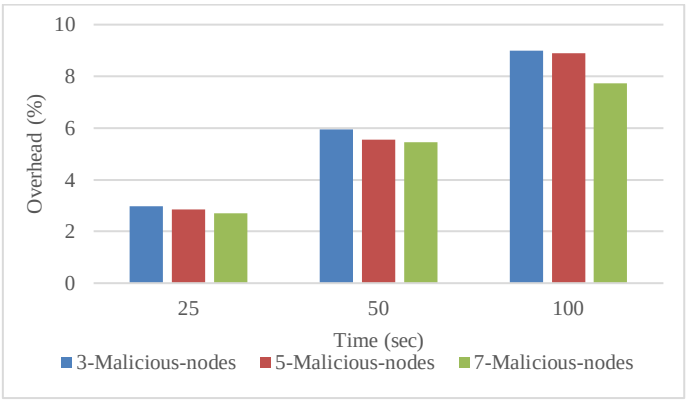

Fig.21. Overhead by varying malicious nodes

The overhead increases when more control packets are used by the nodes. In our experiment, the overhead is affected but not in a maximum range due to the monitoring of the traffic pattern and the less false positive rate.

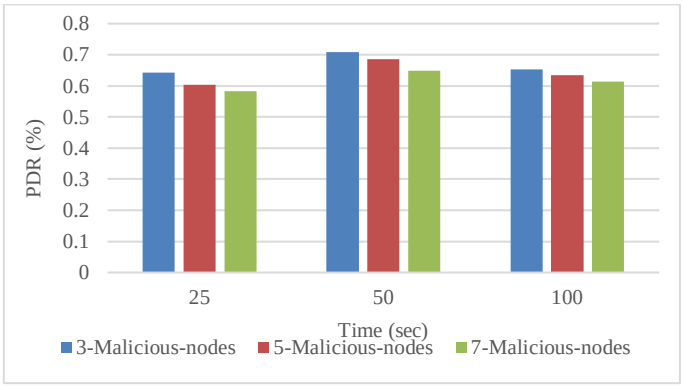

Fig.22. PDR by varying malicious nodes

The PDR rate is not much affected when the number of malicious nodes increase from 5 to 7 in the network. Our experimental findings shows that the PDR is maintained almost 0.65 consistently despite the presence of high number of malicious nodes.

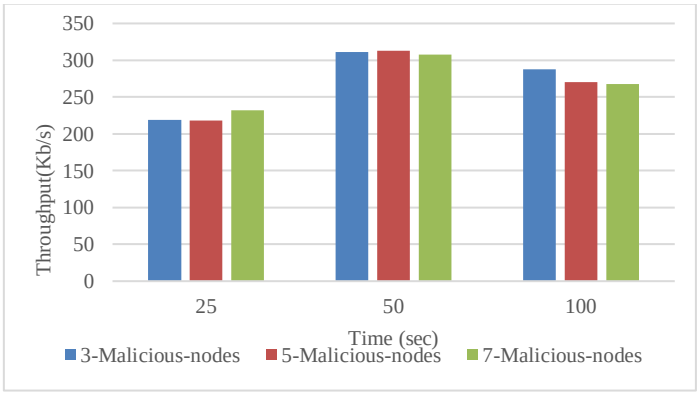

Fig.23. Throughput by varying malicious nodes

The throughput defines the successful data delivery. But in the network with packet drop attackers, the throughput is the worst affected parameter. In our experiments, the proposed algorithm helped the network to maintain the throughput rate high by selecting the high confident nodes.

5. Conclusion

By proposing a score-based trustworthiness calculation & traffic classification, a platform provides for secure data communication in WSN with the integration of CFS calculation and Bayesian filter based on the algorithm of node monitoring agent. According to the previous data transmission behavior of a node, the sensor nodes' scores are computed. By selecting the high CFS nodes, the communication initiates by the sensor nodes using the CFS calculation. Before processing the data communication, the sensor nodes are monitored and their traffic pattern in evaluated and classified. Every sensor node in the network is configured as monitoring agents. They can monitor their neighbor sensor nodes and evaluate the CFS based on the data transmission behavior. By using 50 sensor nodes, the methods are assessed in the simulation environment and the proposed method's efficiency shows in the comparative analysis based on different parameters like minimal delay, throughput, and maximal PDR. The simulation results of proposed technique produce such as less delay, improved network lifetime, high throughput, and increased packet delivery rate. To evaluate the trustworthiness and fitness of nodes, additional parameters consider like link quality, coverage, and several other related parameters for designing the fuzzy logic further so as to achieve high network performance despite the presence of multiple malicious nodes.

References

[1] Rajeswari, Kasilingam, and Subbu Neduncheliyan. "Genetic algorithm-based fault tolerant clustering in wireless sensor network." *Iet Communications* 11, no. 12 (2017): 1927-1932.

[2] Jasvir Kaur, Sukhchandan Randhawa, Sushma Jain,"A novel Energy Efficient Cluster Head Selection Method for Wireless Sensor Networks", International Journal of Wireless and Microwave Technologies, Vol.8, No.2, pp. 37-51, 2018.

[3] Tomić, Ivana, and Julie A. McCann. "A survey of potential security issues in existing wireless sensor network protocols." *IEEE Internet of Things Journal* 4, no. 6 (2017): 1910-1923.

[4] Zhao, Nan, F. Richard Yu, Ming Li, Qiao Yan, and Victor CM Leung. "Physical layer security issues in interference-alignment-based wireless networks." *IEEE Communications Magazine* 54, no. 8 (2016): 162-168.

[5] Ding, X., Sun, X. J., Huang, C., & Wu, X. B. (2016). Cluster-level based link redundancy with network coding in duty cycled relay wireless sensor networks. Computer Networks, 99(C), 15–36.

[6] Akram, Vahid Khalilpour, and Orhan Dagdeviren. "Deck: A distributed, asynchronous and exact k-connectivity detection algorithm for wireless sensor networks." *Computer Communications* 116 (2018): 9-20.

[7] Mahaboob Sharief Shaik, Fahad Mira, "A Comprehensive Mechanism of MANET Network Layer Based Security Attack Prevention", International Journal of Wireless and Microwave Technologies, Vol.10, No.1, pp. 38-47, 2020.

[8] Ch Rambabu, V.V.K.D.V.Prasad, K.Satya Prasad, "Multipath Cluster-based Hybrid MAC Protocol for Wireless Sensor Networks", International Journal of Wireless and Microwave Technologies, Vol.10, No.1, pp. 1-16, 2020.

[9] Amin Rezaeipanah, Hamed Nazari, MohammadJavad Abdollahi, "Reducing Energy Consumption in Wireless Sensor Networks Using a Routing Protocol Based on Multi-level Clustering and Genetic Algorithm", International Journal of Wireless and Microwave Technologies, Vol.10, No.3, pp. 1-16, 2020.

[10] Kavitha, M., B. Ramakrishnan, and Resul Das. "A novel routing scheme to avoid link error and packet dropping in wireless sensor networks." *International Journal of Computer Networks and Applications (IJCNA)* 3, no. 4 (2016): 86-94.

[11] Rmayti, Mohammad, Rida Khatoun, Youcef Begriche, Lyes Khoukhi, and Dominique Gaiti. "A stochastic approach for packet dropping attacks detection in mobile Ad hoc networks." *Computer Networks* 121 (2017): 53-64.

[12] Vanitha, K., and AMJ Zubair Rahaman. "Preventing malicious packet dropping nodes in MANET using IFHM based SAODV routing protocol." *Cluster Computing* 22, no. 6 (2019): 13453-13461.

[13] Gurung, Shashi, and Siddhartha Chauhan. "A novel approach for mitigating route request flooding attack in MANET." *Wireless Networks* 24, no. 8 (2018): 2899-2914.

[14] Jamali, Mohammad Ali Jabraeil. "A multipath QoS multicast routing protocol based on link stability and route reliability in mobile ad-hoc networks." *Journal of Ambient Intelligence and Humanized Computing* 10, no. 1 (2019): 107-123.

[15] Karthick, S. (2018). TDP: A novel secure and energy aware routing protocol for wireless sensor networks. International Journal of Intelligent Engineering and Systems, 11(2), 76–84.

[16] Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Nehemiah, H. K., & Kannan, A. (2019). An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. Wireless Personal Communications, 105(4), 1475–1490.

[17] Udhayavani, M., & Chandrasekaran, M. (2018). Design of TAREEN (trust aware routing with energy efficient network) and enactment of TARF: A trust-aware routing framework for wireless sensor networks. Cluster Computing, 22, 11919–11927.

[18] Asha, G., & Santhosh, R. (2019). Soft computing and trust-based self-organized hierarchical energy balance routing protocol (TSHEB) in wireless sensor networks. Soft Computing, 23(8), 2537–2543.

[19] Gilbert, E. P. K., Kaliaperumal, B., Rajsingh, E. B., & Lydia, M. (2018). Trust based data prediction, aggregation and reconstruction using compressed sensing for clustered wireless sensor networks. Computers & Electrical Engineering, 72, 894–909.

[20] Desai, S. S., & Nene, M. J. (2019). Node-level trust evaluation in wireless sensor networks. IEEE Transactions on Information Forensics and Security, 14(8), 2139–2152.

Authors' Profiles

Kareti Madhava Rao Received MCA from Sri Venkateswara University, Tirupati and pursuing Ph.D. in Computer Science from S.V. University, Tirupati 2015. His areas of interest are Computer networks.

Dr. S. Rama Krishna is a Professor, Department of Computer Science and Applications in Sri Venkateswara University. He has guided about 23 Ph.D. students and 22 M.Phil. Students so far. His areas of interests are Fluid Dynamics, Computer Networks and Data Mining.

How to cite this paper: Kareti Madhava Rao, S Ramakrishna, "A Node Confident based IDS to Avoid Packet Drop Attacks for Wireless Sensor Network", International Journal of Computer Network and Information Security(IJCNIS), Vol.13, No.6, pp.41-56, 2021. DOI: 10.5815/ijcnis.2021.06.04