Mitigation of Black hole attack formation in Wireless Sensor Network using secure method

Dr Asa Jyothi.G

Professor, ECE Dept., Nalla Malla Reddy Engineering College, Narapally, Hyderabad, 500035, Telangana State.

Email: ashajyothi.gudavalli@gmail.com

Abstract:

Wireless sensor networks are getting a lot of attention because they are easy to set up and don't cost much. Because of this, sensor networks are very important in many military and private uses. But because these networks aren't managed from one place, they can be attacked in a number of ways. One of the methods is called a "packet drop attack," in which a node that has been taken over drops packets on purpose. Several ways have been suggested to find the "packet drop attack" in wireless sensor networks, but none of them are practical enough to stop or separate future attacks. Recently, WSNs have started using reputation systems more and more. The reputation method calculates each node's reputation based on how it acts. These reputation systems make it possible to find the nodes that can be trusted to forward data. Monitoring the nodes in open mode has been shown to be an effective way to watch how the nodes forward data. In this paper, a new CONFIDENT SCORE-based NODE MONITORING AGENT (CFS-NMA) is presented to find the packet-dropping nodes and stop them from taking part in the process of sending data. Node monitoring bots (BFNMA) keep an eye on how the nodes forward information and give a CONFIDENT SCORE based on how well they do it. Also, this BFNMA looks at the flow of traffic to make sure that the wrong node (one that drops packets because it's too busy) isn't marked as malicious. The simulations show that compared to other security methods, the proposed mechanism is a huge step forward in network security.

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

I. INTRODUCTION

With the advancement and development of Wireless technology, WSNs are employed inseveral areas including health monitoring, battlefield observation and environment monitoring[1]. Because of dynamic, data-centric and self-organizing nature of WSNs,these are deployed in various fields of data observation in such a way that sensor nodescooperate for support as well as communication of several high-level applications.WSNs consist of spatially deployed sensors that can measure as well as monitor anychange in environmental conditions without actually relying on any specific infrastructuresupport. In the recent past, several research efforts have been made to efficientlydeploy WSNs for a wide range of applications. The needs of all applications cannot befulfilled by a single general-purpose WSN design [2]. Therefore, several network parameterslike sensing range, nodes density, communication or transmission range have to beconsidered at the network design phase on the basis of specific applications. Therefore,to achieve this, it becomes necessary to analyze the impact of various parameters on theperformance of these networks.

However, the wide use of WSNs is also accompanied by numerous security issues[3-6]. Due to distributed and open nature of the transmission medium, WSNs suffers fromseveral attacks including Denial of Service attacks, sinkhole attacks, selective forwardingattacks, blackhole attack, hello-flood attack, tampering attacks, and hijack attacks. Prevention-based technologies cannot solve all these security issues, therefore detection-basedsupplement needs to be employed [7-8]. Due to constrained battery resources, routing becomesmore challenging in WSNs when compared to ad hoc networks [9]. Moreover, nodesin WSNs have limited memory, bandwidth and processing capabilities, therefore routingtechnique employed needs to be efficient in terms of resource utilization [10–12].

A sensor network is a compound, of sensing, processing, communication ability to observe and react to events ina specified environment. WSN is usually composed of tens to thousands of nodes. Which collect process andtransmit cooperatively information to a central location [13].

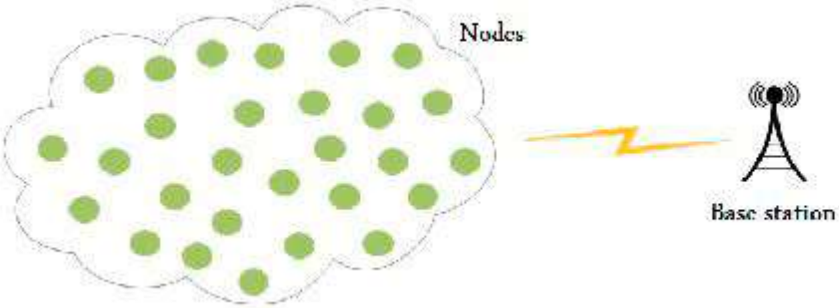


Fig.1.Wireless sensor network

WSN can be affected by several types of attacks damaging and making the network unreliable forcommunication and proper working. Various attacks on network layer such as wormhole, sinkhole, selectiveforwarding, hello flood, false routing attacks and acknowledgement flooding have recently attractedconsiderableattention [14-15]. The black hole attack is one of the most severe attacks on WSNs. In this work we present ourexperience to detect a Black Hole attack in WSNs using Hidden Markov Model technique [16].

PACKET DROPPING IN WIRELESS SENSOR NETWORKS

Like in any other network, packet loss is expected in sensor networks at least to an acceptable percentage [17]. Not all packets lost should be viewed as malicious. There are various reasons for a node to drop the packets. Those are:

Legitimate Packet Dropping: - Packet dropping can be experienced in wireless sensor networks where no compromised nodes are present [18]. This packet loss is mainly associated with the following events;

- **Network Congestion** Network congestion in wireless sensor networks is something unavoidable. These network channels are mostly occupied due to in and out movements of data traffic. As a result, congestion is more likely to happen which can lead to loss of packets.
- **Channel Conditions** In wireless networking the channel condition cannot be neglected since it changes drastically. Free path loss, interference, presence of noise on the channel and fading of the transmitted wireless signals are among the channel conditions that can lead to packet loss or bit errors in the transmitted signal. In the presence of these factors, some packets can get dropped.
- **Resource Constraints** Nodes in wireless sensor networks have limited energy resource. Intermediate nodes in these networks may behave selfishly and fail to forward the received packets in order to conserve their limited resources battery power. These packets in turn get dropped.

Malicious Packet Dropping: - Mostly, the first step in launching a packet dropping attack is for a malicious node to get involved during route formation. This is better done by exploiting the weakness of the routing protocols used in wireless sensor networks which are designed basing on the assumption of trustworthiness between nodes in a network. Once in the route, the malicious node can do anything including maliciously dropping packets [19]. This Packet dropping at a malicious intermediate node can lead to suspension of communication or generation of wrong information between the source and destination which is an undesirable situation.

Consider the route discovery process between source and destination. The source broadcasts a RREQ (Route Request) message with unique identifier to all its one hop neighbours [20]. Each receiver rebroadcasts this message to its one hop neighbours until it reaches the destination. The destination on receiving the message updates the sequence number of the source and sends a RREP (Route Reply) message back to its neighbour which relayed the RREQ. On the other hand, an intermediate node that has a route to the destination with destination sequence number equal to the one in RREQ can send back a RREP packet to the source node without relaying to the destination.

II. LITERATURE SURVEY

WSNs can be broadly categorized into two types on the basis of energy consumption:heterogeneous and homogeneous WSNs. In heterogeneous networks, different nodesare assigned different energy levels, whereas in homogeneous networks, all the nodes in network are given the same energy. On the basis of mode of operation, WSNs are oftwo types: Reactive and proactive. There is an immediate response in reactive networkswhereas nodes in proactive networks transmits data periodically. The general idea of clusteringin WSNs has been studied in several works [21].

Das et al. [22] proposed hexagonal sectoring method for deployment of nodes. Theproposed technique guarantees uniform load distribution over the CHs. This facilitatesnodes of one sector to integrate itself with other sector irrespective of which sector thenodes belong to.

Chan et al. [23] proposed LCM, a link aware clustering mechanism for WSNs in orderto establish a load balanced reliable path. The basis of CH selection is the condition of thelink and the status of the node. It uses predicted transmission count. Selection of CHs isdone based on the priority value and nodes having maximum priority value are chosen asCHs.

Zhang et al. [24] proposed E2HRC, a heterogeneous ring clustering algorithm thatemployed mechanism of CH rotation. It imposed a split ring structure, non-uniform innature, in order to balance the cluster heads energy consumption. E2HRC balances as wellas mitigates the energy consumption of the network. However, it does not focus enoughon the security aspect of the network. Also, the performance of E2HRC degrades withthe increase in number of nodes leading the need of new routing strategy to counter suchproblems.

Khan et al., [25] have developed the routing protocol RAEED (Robust formally Analyzed protocol for wireless sensor networks Deployment) which is able to address the problem of black hole attacks usingformal modeling and avoid such attacks.

A proposed detection Technique of Black Hole attack is gives in [26] to analysis and defines Black Hole attack nodes in the route discovery process by improving the AODV (Ad-hoc On-demand Distance Vector) routing protocol.

The authors of [27] proposed a trust model and define trustlevel of relationship between nodes in network. One node believes or disbelieves its trustee depending on trust level. With disbelief of thruster, black hole attacker are prevented and removed from route.

In Zougagh et al., [28] checks correct forwarding packets by intermediate nodes based on an authenticated end-to-end acknowledgment approach. Their proposed solution prevents the black hole launched in simple or cooperative manner.

Using a new acknowledge scheme withlow overhead, the authors of [29] are successfully eliminate Black Hole and False Data Injection attacks initiated by the compromised inside nodes and outside malicious nodes respectively.

(Bharat Bhushan, Gadadhar Sahoo) In this paper, Intelligence based secured fuzzy clustering algorithm (ISFC algorithm) is proposed that concentrates on Sub cluster-based routing using fuzzy S-means mechanism. This reduces the energy consumption and enhances the networks lifetime by introducing load balancing concept. If few sub cluster nodes are heavily loaded, there occurs increased energy consumption therefore for balancing the normal energy depletion; this balanced load sub-cluster head selection is initiated. Here in this paper, distance-based energy model is proposed for balanced load sub-cluster head selection. As the major criteria on which the energy consumption in sensor network depends is the distance between the communicating nodes or the transmission distance, the proposed BLS scheme mitigates the energy depletion of each node in the network. [30].

(Hanane Kalkha, Hassan Satori, Khalid Satori) This paper provides a Hidden Markov Model solution to identify malicious nodes in wireless sensor networks through prevention of black hole attack. Our proposed approach based on a new routing algorithm which analyses shortest path in order to avoid malicious node path. Our results demonstrate the success and the efficiency of our proposed routing algorithm. [31]

III. PROPOSED SYSTEM

The node monitoring technique has been the most well know node misbehaviour detection in wireless networks. In this technique, every node acts as a monitoring agent monitoring packet transmissions to neighbouring nodes in promiscuous mode. The monitoring agents save a copy of packets in their buffers before their transmission to the next node. This serves to monitor packet relay from a neighbouring node to the next node.

In our proposed BFNMA (Bayesian filter node monitoring agent)module, every monitoring agent node uses promiscuous mode to listen the channel within its radio range and get the behaviours of other sensor nodes, and classifies the actions. Each monitoring agent node configured with several modules. Each module carries out a specific function that can classify the collected data based on node behaviours. The monitoring agents' module is divided into the following phases,

1) Data collection phase: the monitoring agent nodes use a promiscuous mode to record behaviour of nodes within its radio range in a fixed time window function.

) 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.

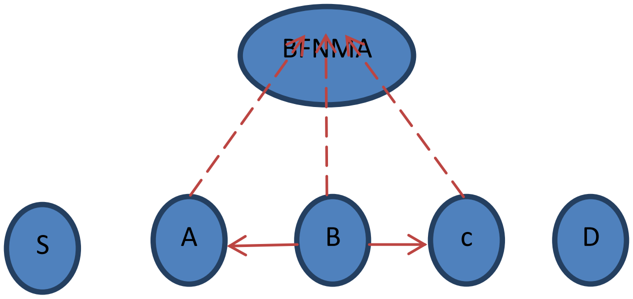


Fig.2.An example of BFNMA

The above figure 2 shows an example of BFNMA. S is the source node and D is the destination node. The other nodes are intermediate nodes in the route between S and D. Before A forwards a packet received from S, it saves the packet in its monitoring buffer. After forwarding the packet to B, BFNMA monitors whether the packet has been forwarded to C. This is because A is expected to receive a copy of the packet forwarded to C since it's within B's transmission range. BFNMA then compares the received packet with the one saved in its monitoring buffer. If BFNMA fails to receive a copy of the packet from B within certain duration, it reduces the confidence score of B. When this happens in recurring manner, the confidence score is set to zero and A decides that B is a malicious node and drop the route through B.

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)

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

$CFS_n^{current}$ 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].

In our proposed model, the agent node uses a fixed time window function to record the traffic data. The agent node has different CFS value in each time window. The CFS of a node can be calculated as follows in equation (2)

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

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

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

$FCFS_n$ 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 source node transmits the data to their neighbour nodes.

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.

IV. RESULT AND DISCUSSION

4.1 Experimental setup

This simulation is conducted to analyze the performance of the proposed technique by comparingit with two different schemes. In this work we have used NS2 (Network Simulator 2) which is an object oriented, discrete event driven network simulator targeted at networking research. It provides support of UDP, routing and multicast protocol simulation on all wireless networks. The network model used in this work is as follows: All the sensor nodes in the network are fixed, homogeneous (All sensor nodes have the same capabilities, the same radio-transmitter devices and constrained power resources), uniformly deployed, and they have the same initial energy. The base station is fixed and located far from the sensor node. Tests are conducted using plane coordinates and static nodes. Nodes are assumed to have limited energy supply and once the initial energy of the nodes are used up, they cease to receive or transmit data. The simulation parameters are given in the table below (Table 1).

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 m x1000 m
Malicious nodes	3
Transmission Protocol	UDP
Initial Energy	100j

Table1: Simulation table

4.2 Simulation result and analysis

In this section, the results obtained from simulation on various scenarios are presented and discussed in detail.We implemented our attack model under a network of 50 nodes in area of 1000 x1000 m.

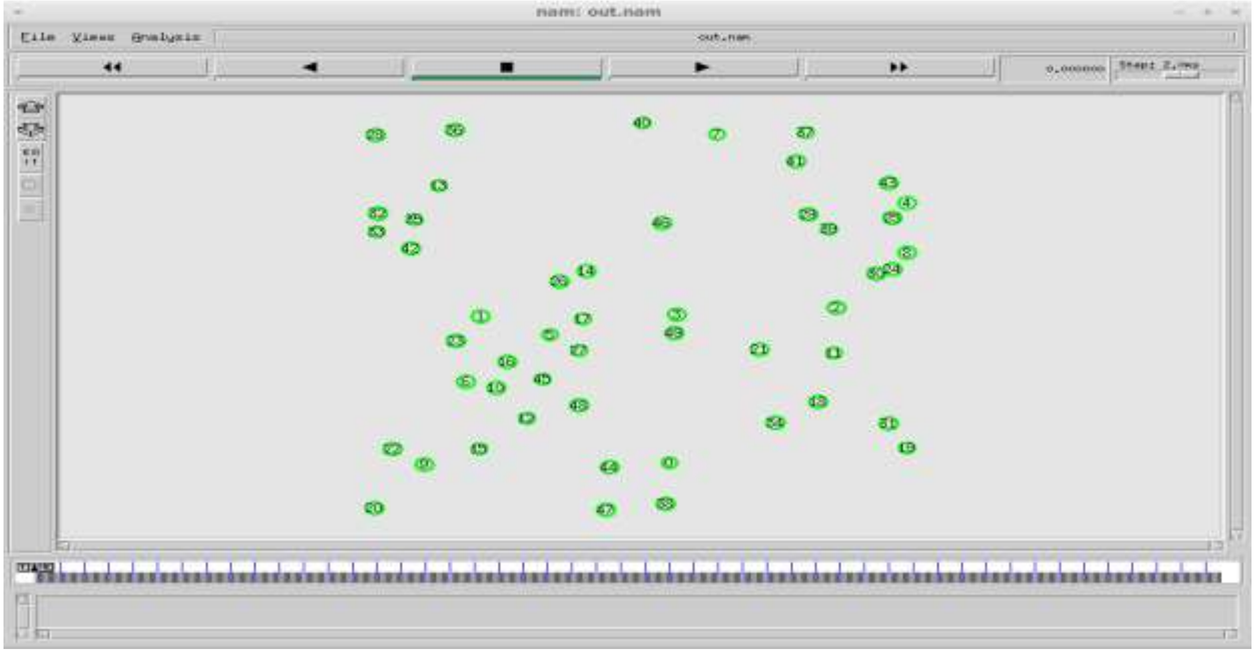


Fig.3. Network deployment

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.

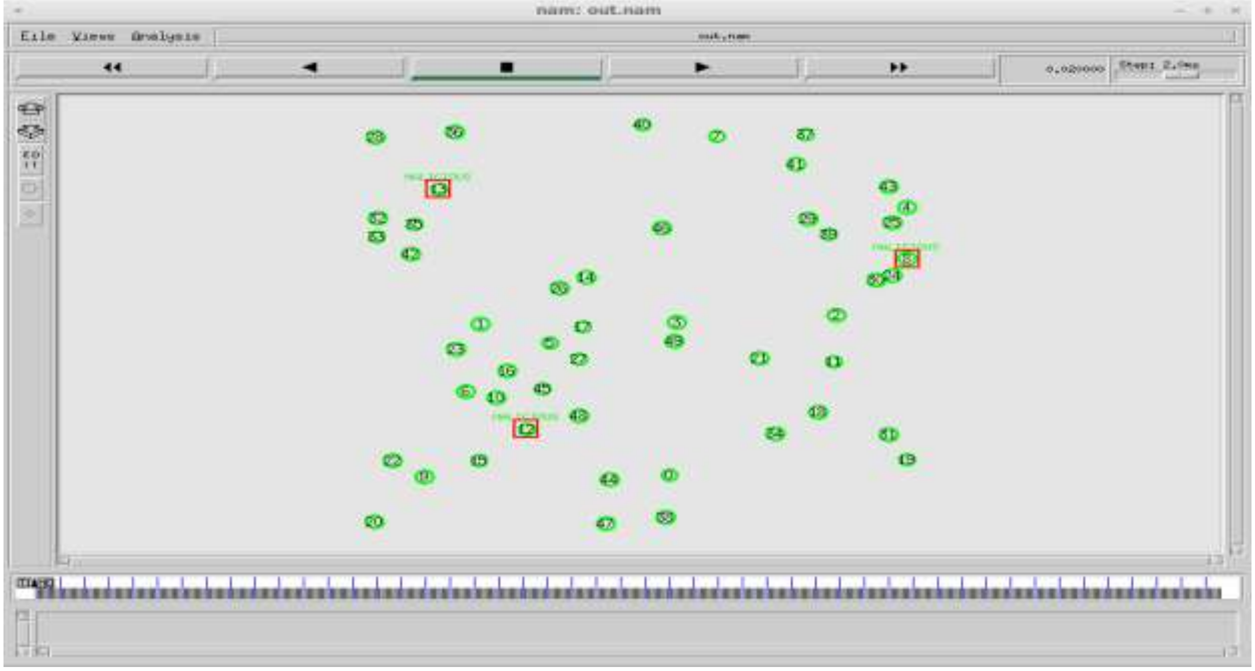
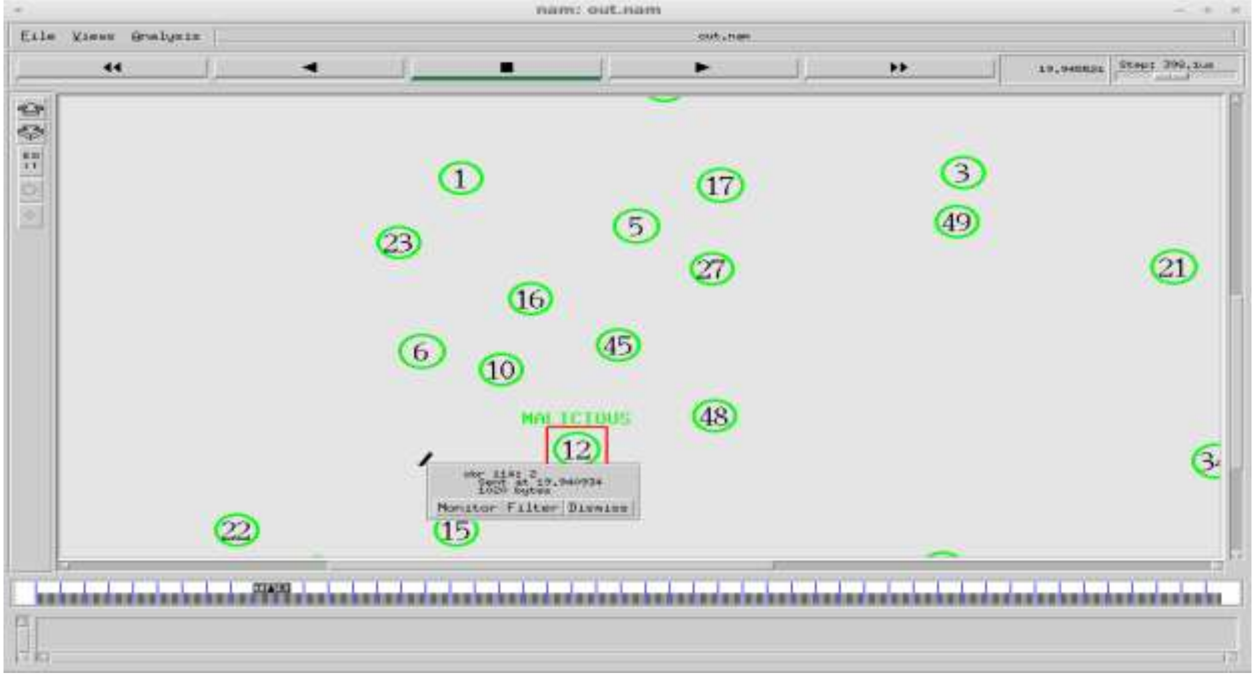


Fig.4. Malicious node displaying

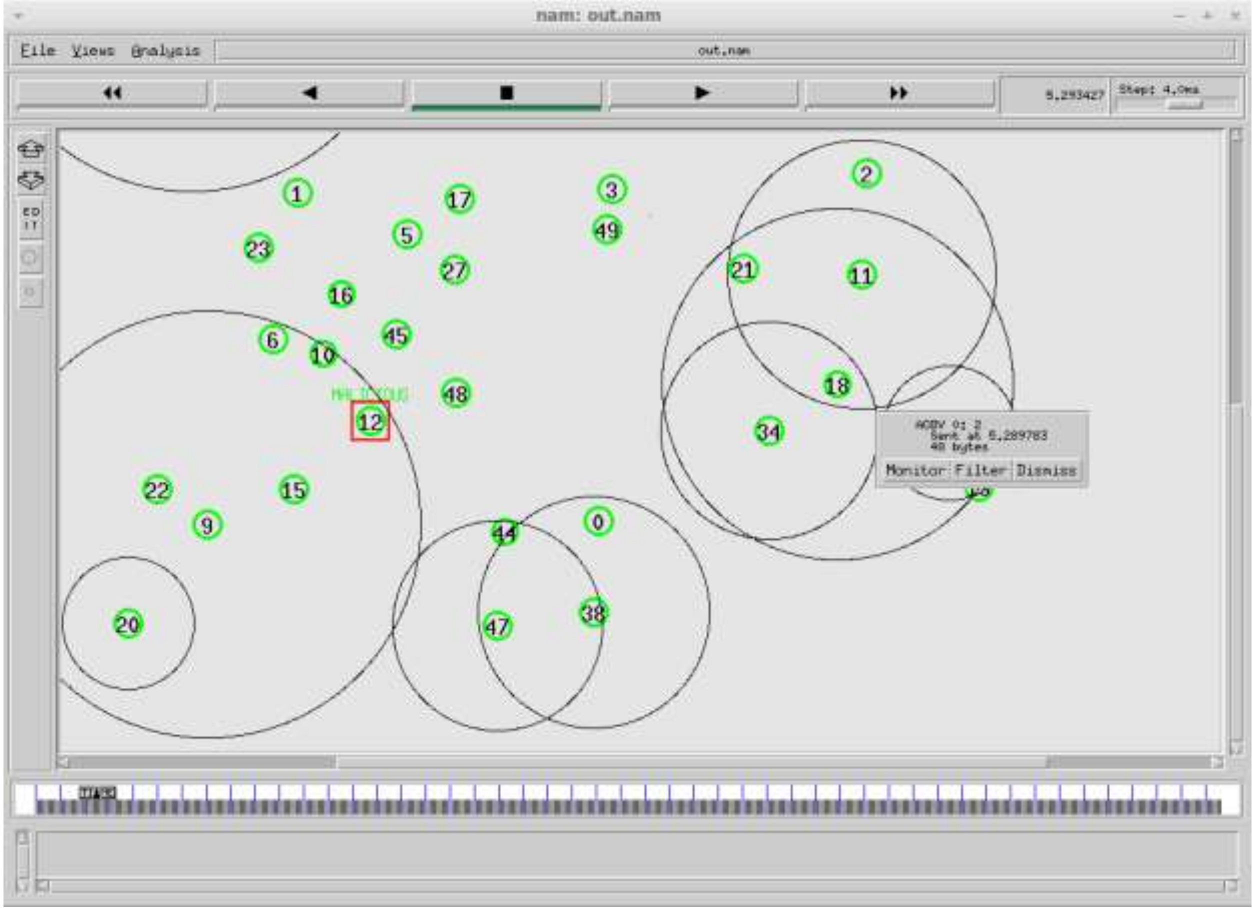
The presence of MALICIOUS nodes interrupts the data transmission. Random nodes are configured as Malicious and they can interfere in the ongoing communication in any means and drop the data packets not intended for them.



dsr 114: 2
Sent at 19.940934
1020 bytes

Fig.5. Data transfer process through traffic protocol

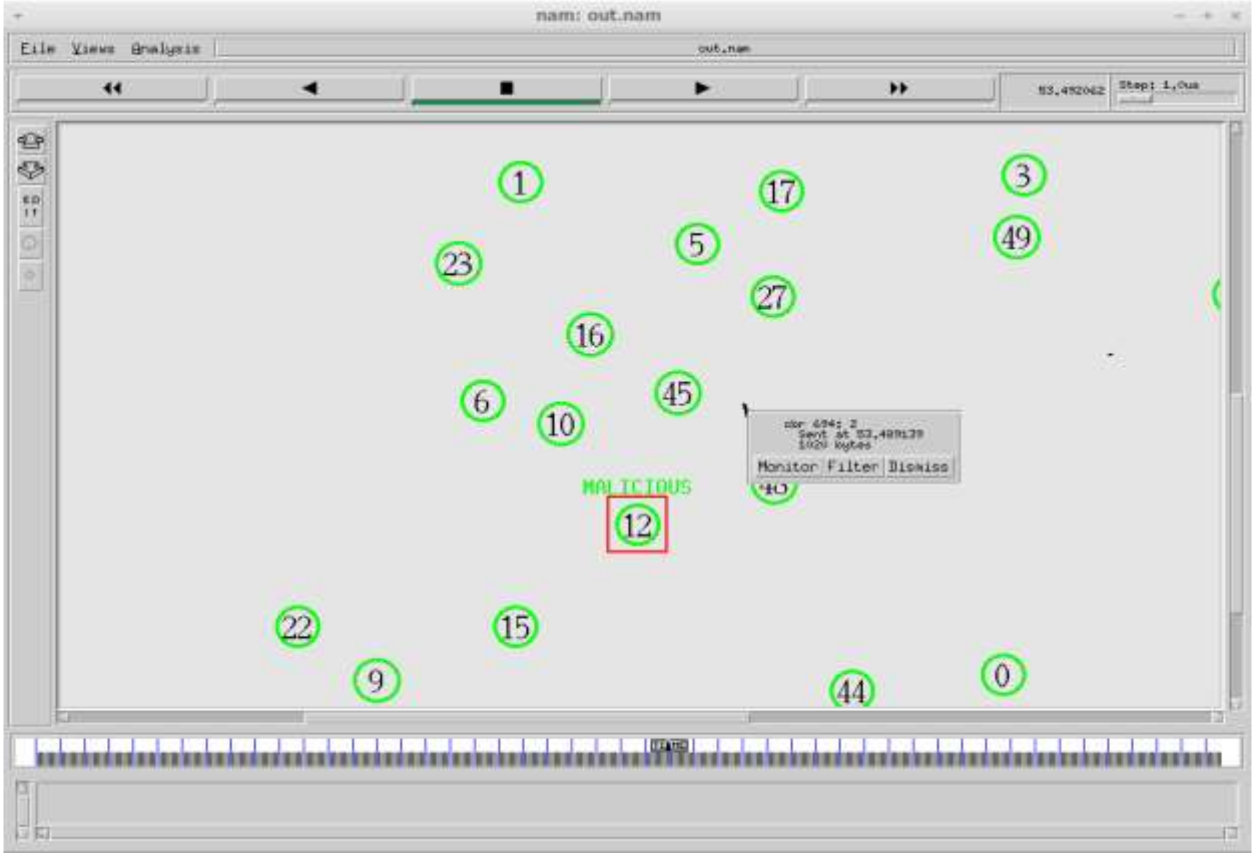
After exchanging control packets, the sensor nodes share the data with the target nodes. Initially, CFS of the nodes is set to 0. So the chances for the data packets being captured by the Malicious is HIGH.



```
AODV 0: 2
  Sent at 5.289783
  40 bytes
```

Fig.6. Broadcasting through routing protocol

Nodes exchange their CFS score and other details like routing information, residual energy using control packets to select the node with good CFS.



cbr 494: 2
Sent at 53.489139
1020 bytes

Fig.7. Data transfer through CFS system

Despite the presence of malicious in the network, the forwarder nodes managed to identify the nodes with good CFS for uninterrupted data transmission. A data packet of 1020 bytes is transferring between the nodes.

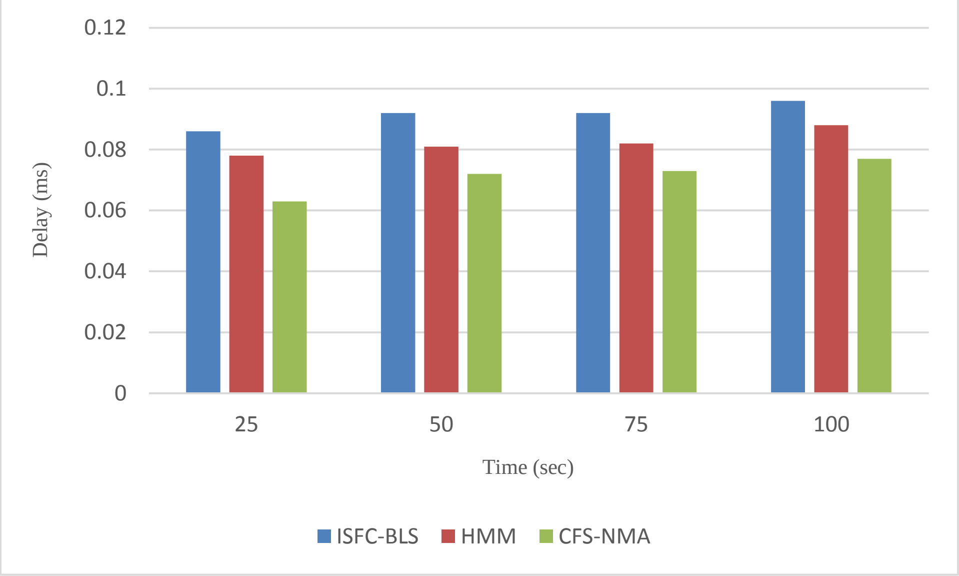


Fig.8. Performance on Delay

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.

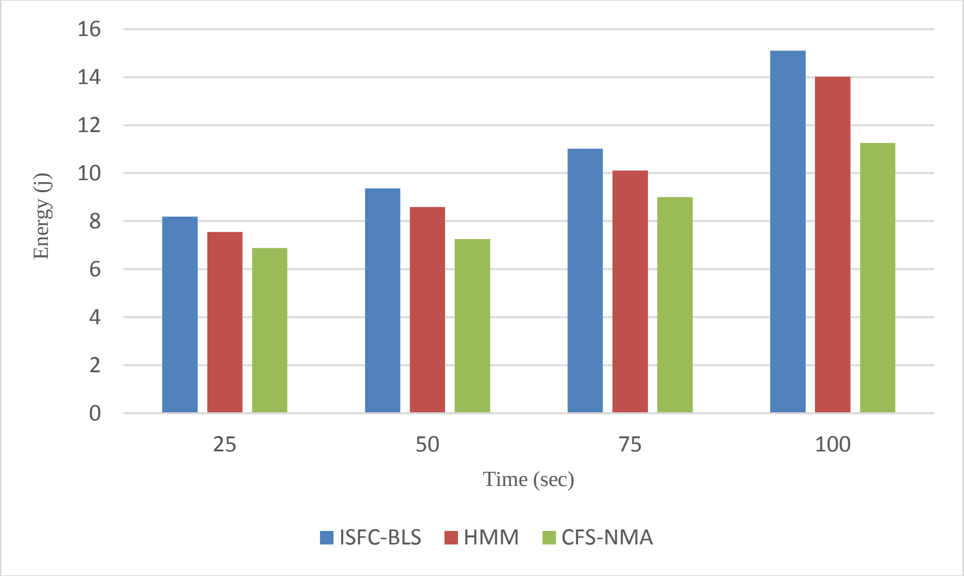


Fig.9. Energy Consumption

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 shows that the proposed approach improves energy consumption of the network and achieves increased lifetime over the other protocols.

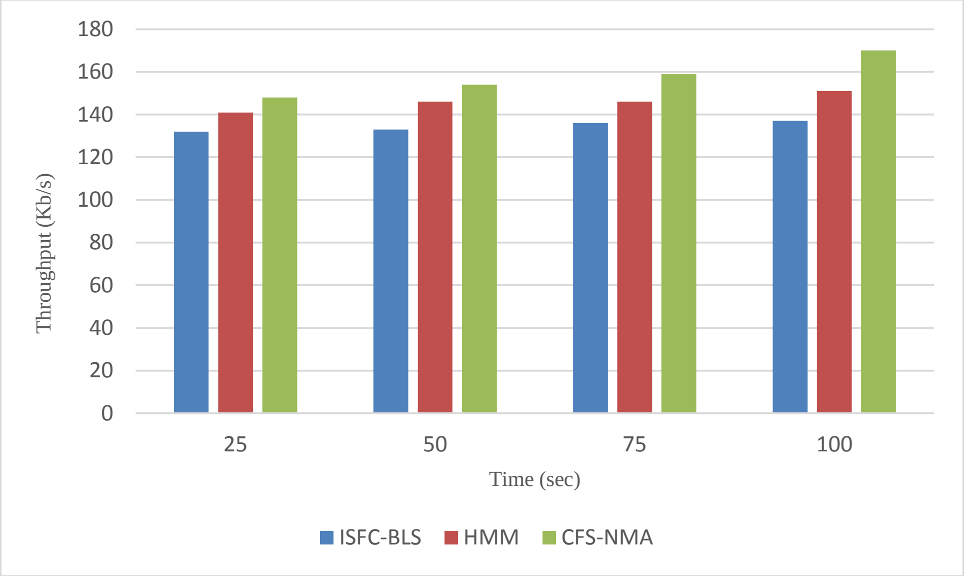


Fig.10. Network Performance

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 result shows that the proposed approach improves throughput than its competitors.

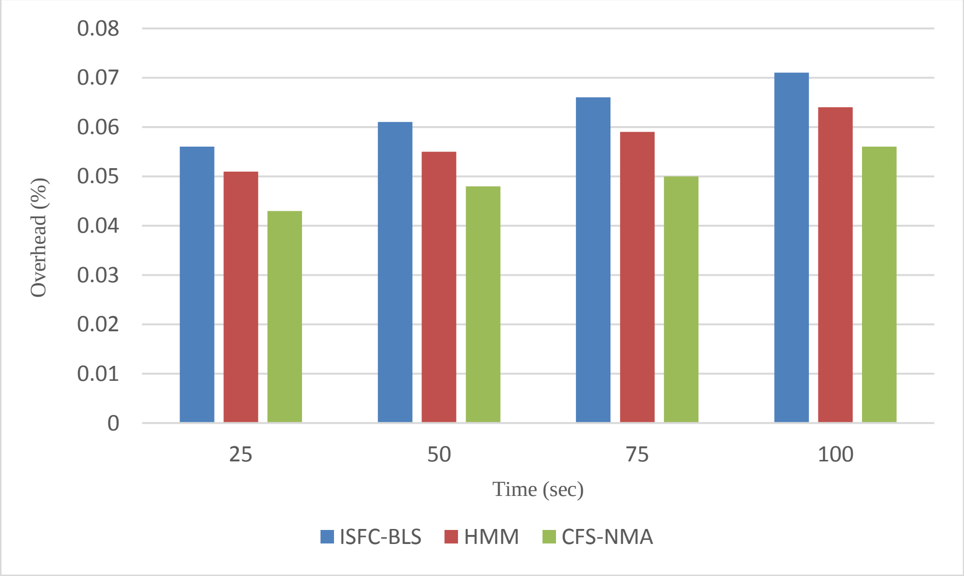


Fig.11. Routing Overhead

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. Hence the overhead of the proposed approach is lower than the previously used protocols.

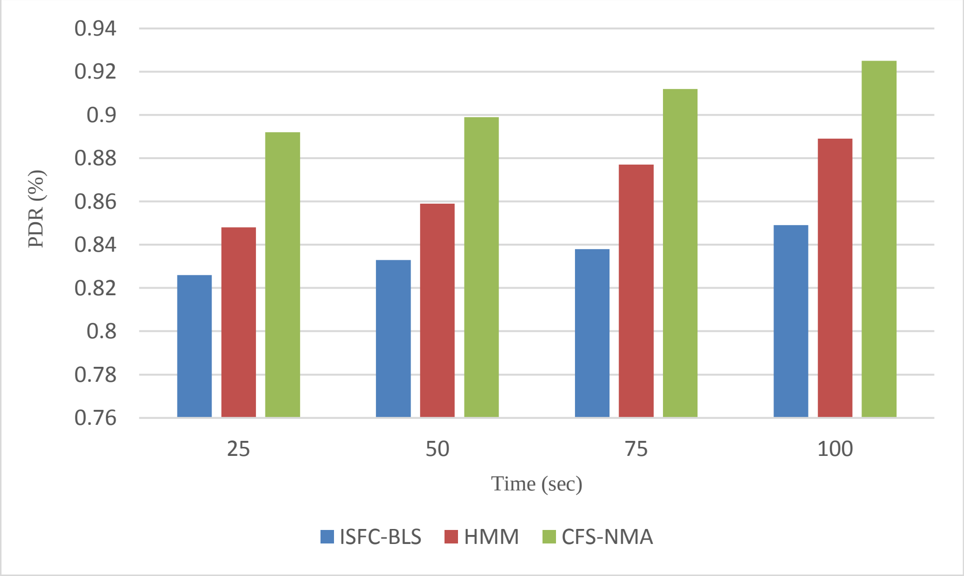


Fig.12. Packet Delivery Ratio

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. The result proves that the proposed approach performs well and achieves high PDR rate than the other protocols.

Conclusion:

In order to ensure the security of wireless sensor networks, we suggest in this paper a CONFIDENT SCORE based BAYESIAN FILTER NODE MONITORING AGENT (CFS-BFNMA) method. To determine the CFS, the monitoring nodes observe the actions of sensor nodes within their radio range. Since the system is entirely distributed, no sophisticated techniques are required to determine which nodes are trustworthy. It is applicable to massive wireless sensor networks. Compared to the other traditional security mechanisms of WSNs, this approach aids in providing a more accurate mechanism to detect the rogue node.

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]. Gaglio, Salvatore, Giuseppe Lo Re, Gloria Martorella, and Daniele Peri. "WSN Design and Verification Using On-Board Executable Specifications." *IEEE Transactions on Industrial Informatics* 15, no. 2 (2018): 710-718.

[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]. Mehetre, Deepak C., S. Emalda Roslin, and Sanjeev J. Wagh. "Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust." *Cluster Computing* 22, no. 1 (2019): 1313-1328.

[8]. Chen, Wei, Derui Ding, Hongli Dong, and Guoliang Wei. "Distributed resilient filtering for power systems subject to denial-of-service attacks." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 49, no. 8 (2019): 1688-1697.

[9]. Xie, Guangqian, and Feng Pan. "Cluster-based routing for the mobile sink in wireless sensor networks with obstacles." *IEEE Access* 4 (2016): 2019-2028.

[10]. Al-Turjman, Fadi, and Ayman Radwan. "Data delivery in wireless multimedia sensor networks: Challenging and defying in the IoT era." *IEEE Wireless Communications* 24, no. 5 (2017): 126-131.

[11]. Teng, Z., Xu, M., & Zhang, L. (2016). Nodes deployment in wireless sensor networks based in improved reliability virtual force algorithm. Journal of Northeast Dianli University, 36(2), 86–89.

[12]. Sun, Z., & Zhou, C. (2016). Adaptive cluster algorithm in WSN based on energy and distance. Journal of Northeast Dianli University, 36(1), 82–86.

[13]. Olofsson, Tomas, Anders Ahlen, and Mikael Gidlund. "Modeling of the fading statistics of wireless sensor network channels in industrial environments." *IEEE Transactions on Signal Processing* 64, no. 12 (2016): 3021-3034.

[14]. Abdollah, Kavous-Fard, Wencong Su, and Tao Jin. "A Machine Learning Based Cyber Attack Detection Model for Wireless Sensor Networks in Microgrids." *IEEE Transactions on Industrial Informatics* (2020).

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

[16]. Mehetre, Deepak C., S. Emalda Roslin, and Sanjeev J. Wagh. "Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust." *Cluster Computing* 22, no. 1 (2019): 1313-1328.

[17]. 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.

[18]. 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.

[19]. 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.

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

[21]. Santos, Andréa Cynthia, Christophe Duhamel, and Lorena Silva Belisário. "Heuristics for designing multi-sink clustered WSN topologies." *Engineering Applications of Artificial Intelligence* 50 (2016): 20-31.

[22]. Das, Tisan, Rakesh Ranjan Swain, Pabitra Mohan Khilar, and Biswa Ranjan Senapati. "Deterministic linear-hexagonal path traversal scheme for localization in wireless sensor networks." *Wireless Networks* (2020): 1-17.

[23]. Wang, S.-S., & Chen, Z.-P. (2013). LCM: A link-aware clustering mechanism for energy-efficient routing in wireless sensor networks. IEEE Sensors Journal, 13(2), 728–736.

[24]. Zhang, W., Li, L., Han, G., & Zhang, L. (2017). E2HRC: An energy-efficient heterogeneous ring clustering routing protocol for wireless sensor networks. Special Section On Future Networks: Architectures, Protocols, and Applications, IEEE Access, 5, 1702–1713.

[25]. Khan, Naveed Ahmed, Kashif Saghar, Rizwan Ahmad, and Andan K. Kiani. "RAEED-EA: A formally analysed energy efficient WSN routing protocol." In *2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, pp. 346-349. IEEE, 2016.

[26]. Singh, Sushama, Atish Mishra, and Upendra Singh. "Detecting and avoiding of collaborative black hole attack on MANET using trusted AODV routing algorithm." In *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*, pp. 1-6. IEEE, 2016.

[27]. Liu, B., Zhou, Q., Ding, R.X., Palomares, I. and Herrera, F., 2019. Large-scale group decision making model based on social network analysis: Trust relationship-based conflict detection and elimination. *European Journal of Operational Research*, *275*(2), pp.737-754.

[28]. Zougagh, Hicham, Noureddine Idboufker, Rida Zoubairi, and Rachid El Ayachi. "Prevention of Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems." *International Journal of Business Data Communications and Networking (IJBDCN)* 15, no. 2 (2019): 73-91.

[29]. Dorri, Ali. "An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET." *Wireless Networks* 23, no. 6 (2017): 1767-1778.

[30]. Bhushan, B., Sahoo, G. ISFC-BLS (Intelligent and Secured Fuzzy Clustering Algorithm Using Balanced Load Sub-Cluster Formation) in WSN Environment. *Wireless Pers Commun* **111,** 1667–1694 (2020). https://doi.org/10.1007/s11277-019-06948-0.

[31]. Hanane Kalkha, Hassan Satori, Khalid Satori, Preventing Black Hole Attack in Wireless Sensor Network Using HMM, Precedia Computer Science, Volume 148, 2019, Pages 552-561. https://doi.org/10.1016/j.procs.2019.01.028.