Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Confident-Based Intrusion Detection System to Avoid Packet Drop Attacks for Wireless Sensor Network

[1]D. V. Ashok,[2]V. Jaikumar. [3]S. Jafar Ali Ibrahim, [4]M. Sathya

[1,2]Department of Electronics and Communication Engineering, QIS College of Engineering and Technology, Ongole,Andhra Pradesh, India. E-Mail: ashokdevireddy2@gmail.com, vinayagam.jai@qiscet.edu.in

[3]Department of Internet of Things, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore – 632014, Tamilnadu, India, E-Mail: jafarali.s@vit.ac.in

[4]Department of Information Sciences, AMC Engineering College, Bangalore - 560083, Karnataka, India, E-Mail: msathya15@gmail.com

Article Info
Page Number: 9225 - 9238
Publication Issue:
Vol 71 No. 4 (2022)

Abstract

Wireless sensor networks have been played a key role in all digital applications owing to their low cost of deployment and easier to use. They have gained great importance in various applications like military and civilian fields. They become vulnerable for security attacks due to the lack of centralized management in the networks. The packet drop attack is one of the security attacks that creates the malicious compromised node packets dropping. In WSNs, various method have been proposed for detecting the packet drop attack. But, none of the methods can't be able to provide the feasibility for isolating or stopping the occurrence in the future. In recent times, the reputation systems' utilization has become an essential mechanism for WSNs. According to the behaviour of a node, the reputation has been calculated that assigns to each node using the reputation system. These systems create a way to detect the nodes that are trustworthy for data forwarding. The behaviour of data forwarding of a node is monitored effectively by the promiscuous mode when monitoring the nodes. A novel CONFIDENT SCORE based NODE MONITORING AGENT (CFS-NMA) technique introduces in this paper for detecting the packet drop nodes and preventing them in the process of data forwarding. The nodes' forwarding behaviour is monitored by node monitoring agents (BFNMA) consistently and the CONFIDENT SCORE is assigned by considering the successful forwards. The traffic pattern is analysed by BFNMA and the wrong node or malicious node is prevented. The network security enhances by the proposed mechanism based on simulation results compared to the other traditional security algorithms.

Article History
Article Received*: 15 September 2022*
Revised*: 25 October 2022*
Accepted*: 14 November 2022*
Publication*: 21 December 2022*

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

I. INTRODUCTION

The advancements and improvements of wireless technology make the WSNs to be deployed in various fields, like environment monitoring, battlefield observation, and health monitoring [1]. In different fields of data observation, WSNs are deployed in a way that the nodes are cooperated for communication and support for various high-level applications due to the data-centric, dynamic, and self-organization features of WSNs. The spatially deployed sensors include in the WSNs to measure and monitor the changes of environmental conditions without depending on the particular support of infrastructure. For deploying the WSNs, various research efforts have been performed for various applications. However, a single or general-purpose design of a WSN can't fulfill all these applications' needs [2]. At the phase of network design, the network parameters, like transmission or communication range, nodes' density, and sensing range have to be considered based on specific applications. It's required to assess the impact of different parameters on the networks' performance to achieve this.

Numerous security issues are accompanied in the explicit usage of WSNs [3-6]. WSNs are impacted by various attacks, such as hijack attacks, tampering attacks, hello-flood attacks, blackhole attacks, selective forwarding attacks, sinkhole attacks, and Denial of Service attacks because of the open and distributed characteristics of the transmission medium. All these security issues can't be resolved by prevention-based technologies. Therefore, it's require to implement the detection-based supplement needs [7-8]. By comparing ad-hoc networks, it becomes more challenging to implement the routing in WSNs because of the constrained resources [9]. In WSNs, the limited bandwidth, memory, and processing capabilities have included in nodes. It's required to incorporate the routing technique, which is an efficient method in terms of resource utilization [10-12].

The abilities of communication, sensing, and processing include in the sensor networks for observing and reacting to the events for a particular sensor environment. The WSNs contain the tens or thousands of nodes to collect the process and transmit the data to a central location cooperatively [13].

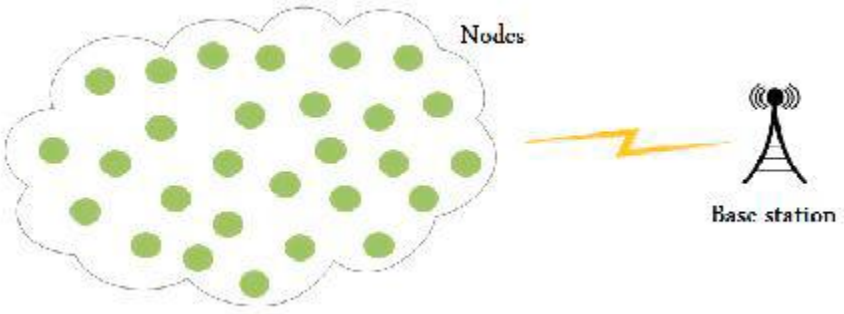

Fig.1.Wireless sensor network

WSNs can become unreliable and damaged with the several types of attacks for communication and proper working. Recently, the considerable attention has gained by various attacks on the network layer, such as acknowledgement flooding, false routing attacks, warmhole, hello flood, selective forwarding, and sinkhole [14-15]. One of the severe attacks is the black hole attack in WSNs. In this paper, the detection of a Black Hole attack is presented in WSNs based on Hidden Markov Model technique [16].

PACKET DROPPING IN WIRELESS SENSOR NETWORKS

In sensor networks, one should anticipate at least an acceptable proportion of packet loss, just as one would in any other kind of network [17]. It's important to remember that not every dropped packet contains hazardous code. There are many various reasons why packets might be lost from a node, including the following:

Legal Transmission of Data Packets: The dropping of packets has been observed in wireless sensor networks, but there has been no discovery of compromised nodes [18]. The following occurrences are connected to this packet loss:

- **Network Congestion**In WSNs, network congestion is not avoidable and occupied by these network channels because of data traffic in and out movements. The loss of packets can be resulted by the congestion.
- **Channel Conditions**As the channel conditions are changed drastically, they can't be neglected in wireless networking. In the transmitted signal, the bit errors or packet loss can be resulted due to the noise of a channel, inference, free path loss, and transmitted wireless signals' fading are presented in the transmitted wireless signals. Some packets can be dropped because of these factors.
- **Resource Constraints**The limited energy resources include in the nodes of wireless sensor networks. For conserving the limited battery power resources, the received packets may fail to forward by the intermediate nodes of a network. Thus, the packets could get dropped.

Malicious Packet Dropping: -During route formation, the packet dropping attack is to get involved for a malicious node in the first step. By assuming the trustworthiness between the nodes of a network, the routing protocols' weakness exploitation is used in WSNs. The malicious node can perform anything in the route, including the dropping packets maliciously [19]. The wrong information generation or communication suspension can be resulted with the packet dropping at an intermediate malicious node between the source and destination. Hence, this is an undesirable case.

The source and the destination are both taken into consideration throughout the route-finding process. A Route Request, or RREQ, message is sent out from the source with a unique identity to all of the nodes that are within one hop of it[20]. Until the receiver reaches to the destination, it has to rebroadcast the message for one-hop neighbours. The source's sequence number is updated by the destination upon the receiving the message and a RREP message is sent back to the neighbor that relays the RREQ. In

RREQ, an intermediate node with a route to the destination with sequence number is equivalent to the one that send back a RREP to the source node without relaying for the destination.

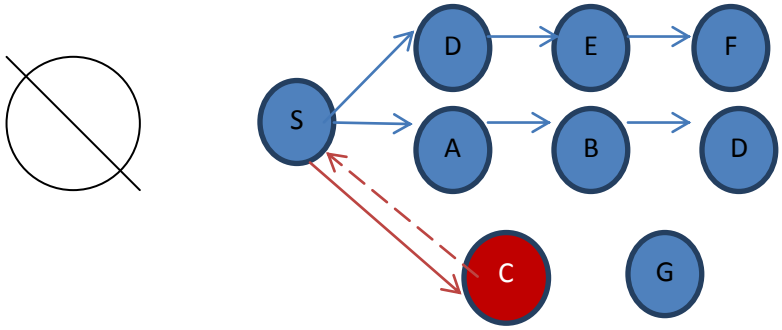

Fig.2. Routing process of packet drop attack by a malicious node C

In order for a node to carry out the packet dropping attack, it is necessary for the attack to be engaged in at least one of the network's routing pathways [21]. This is depicted in Figure C, which can be seen above; C is a hostile node that plans to drop the packets that are travelling from S to D. As part of the process of determining how to go from S to D, S will broadcast the RREQ packet to its neighbours. As was discussed before, the message is retransmitted by each of the neighbouring nodes until it reaches its final destination, which is denoted by the letter D. This rule is broken when the malevolent node C tells a falsehood to node S, which claims to have the shortest route to destination D, and then sends an RREP packet to node S. S assumes that the shortest path is from C to D and sends the data packets via C to D since this is the shortest route. As a consequence, this results in the loss of packets.

II. LITERATURE SURVEY

Based on the level of energy consumption, WSNs can be categorized into homogenous and heterogeneous WSNs. Different energy levels assign to different nodes in heterogeneous networks and the same energy levels are given to the sensor network nodes. Two different types of WSNs are included, such as proactive and reactive based on the operational model. In reactive networks, an immediate response is provided and the data transmitted by the nodes in proactive nodes periodically. In several works, the clustering concept has been investigated in WSNs [22].

Das et al., [23] proposes the method of hexagonal sectoring to deploy the nodes in a sensor network. The uniform load distribution is ensured over the CHs by the proposed technique. The nodes of one sector is facilitate the integration with other sector no matter the nodes belong to which sector.

Chan et al., [24] proposes LCM, a link aware clustering mechanism for establishing a load balanced and reliable path in WSNs. Based on the node’s status and link condition, the CH has been selected. The maximum priority values of nodes are selected as CHs.

Zhang et al., [25] has demonstrated the heterogeneous ring clustering algorithm, known as E2HRC, which employs the CH rotation mechanism. For balancing both energy consumption and the cluster heads, a split ring structure imposes and it is non-uniform in nature. The network's energy consumption is balanced by E2HRC, but it doesn't secure the network. Thus, the new routing strategy is required for encountering the problems of security and degraded performance of E2HRC due to the increased number of nodes.

Khan et al., [26] has improved a routing protocol, called as Robust formally analyzed protocol RAEED for deployment of wireless sensor network and addressing the black hole attacks' problem based on the formal modeling. In [27], a proposed detection method of Black Hole Attack is discussed that defines the nodes of Black Hole attack in the process of route discovery with the use of AODV routing protocol.

In [28], the authors have proposed a trust model and defined the trust level relationship among network nodes. Based on the trust level, the trustee is believed or disbelieved by one node. The black hole attacker prevents and removes from the route based on the thruster's disbelief.

Zougagh et al., [29] has validated the correct forwarding packets using the authenticated end-to-end acknowledgement method and intermediate nodes. The launching black hole is prevented by the proposed solution in a simple or cooperative way.

In [30], the authors has implemented a new acknowledge scheme using low overhead to remove the False Data Injection and Black Hole attacks that initiated by the outside malicious nodes and compromised inside nodes respectively.

Bharat Bhushan and Gadadhar Sahoo et al., [31] have proposed an intelligence based secured fuzzy clustering algorithm (ISFC) that focuses on the sub cluster-based routing based on fuzzy S-means mechanism. With the introduction of load balancing, the network lifetime improves and the energy consumption reduces. The increased energy consumption is occurred when few sub-cluster nodes are heavily loaded. Therefore, the balancing of load sub-cluster head selection and the normal energy depletion has initiated. For selection of balanced load sub-cluster head, the distance-based energy model proposes in this paper. Each node's energy depletion is mitigated by the proposed scheme of BLS by considering the major criteria, which includes the relying of sensor network's energy consumption is the distance between nodes or the transmission distance.

HananeKalkha et al., [32] has provided a Hidden Markov Model for detecting the WSNs' malicious nodes by preventing the black hole attack. For avoiding the malicious node path, the shortest path is analyzed by the proposed approach using a new routing algorithm. The proposed routing algorithm's efficiency is resulted.

III. The Confidential Score-based Node Monitoring Agent Method (CFS-NMA)

BFNMA: -

The node monitoring method is the most well-known method for detecting node misbehavior in wireless networks. This method includes the acting of the each node as a monitoring agent's packet transmissions to adjacent nodes in a promiscuous node. Promiscuous nodes can send packets to any other node in the network. A copy of the packets is saved by monitor agents in their buffers just before to the transfer of data towards next node. These agents are responsible for monitoring the packet relay that occurs between a neighbouring node and the next node.

For listening the channel within the radio range, the promiscuous mode is used by every monitoring agent node in the module of proposed BFNMA or Bayesian Filter Node Monitoring Agent and the other sensor nodes' behaviours are obtained while classifying the actions. Based on various modules, the configuration of each monitoring agent node has performed. The collected data is classified based on node behaviours by each module. The following phases are involved in the module of monitoring agents:

1) Data collection phase: A promiscuous node is used by the monitoring agent nodes for recording the nodes' behavior in a fixed time window function within the radio range.

2) Data classification phase: The nodes' behavior is classified by the monitoring and the score is assigned to the nodes based on the collected data of the previous data collection phase.

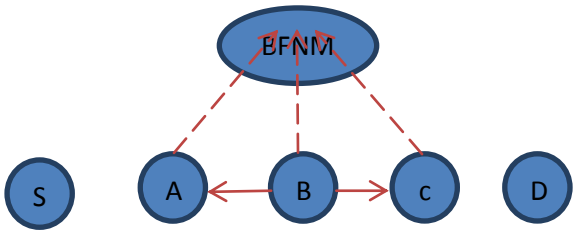

Fig.3. An example of BFNMA

The diagram that was just shown provides an illustration of BFNMA. In this illustration, S represents the source node, and D represents the destination node. The subsequent nodes are considered intermediate nodes since they are located along the path that leads from S to D. Before sending on the packet that was received from S by A, the packet is stored in the monitoring buffer for safekeeping. BFNMA is responsible for monitoring the process of forwarding a packet to C and determining whether or not the packet forwards to C after first being sent to B. Because the packet is located inside B's range of transmission, A is able to get a copy of the packet and then send it on to C. BFNMA will then do a comparison between the stored packet in the monitoring buffer and the received packet. When BFNMA is unable to obtain the packet copy from B within a particular amount of time, the confidence score of B is lowered as a result. If it continues to occur in the same pattern, the confidence score will be reset to

zero. Due to the fact that A has determined that B is a malicious node, the route will no longer pass via B.

CALCULATION OF CFS

In two different ways, the node's confidence score can be determined:

1. Monitoring agent CFS
2. Neighbour CFS

In the previous transmissions, the aggregation of the CFS is the neighbor CFS that assigns the neighbor node to the forwarder or source nodes. Based on the node behavior, the CFS records are also maintained by the monitoring agents for every node. The multi-CFS aggregation considers as the particular node's final CFS. In the current node, the node's CFS can be estimated based on the below equation (1):

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

Where, $CFS_n^{previous}$ refers to the previous CFS value of a node n and $CFS_n^{current}$ refers to the node n's CFS for the current node based on the NMA. Primarily, $CFS_n^{previous}$ sets to 0 and CFS_{thresh} indicates the threshold value of CFS for each communication between [0, 1].

For recording the data traffic, the fixed time window function is used by the agent node in the proposed model. In each time window, different CFS value includes in the agent node. The below equation (2) can be determined the node's CFS.

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

Where, $CFS_n^{current}$ indicates the calculated current CFS of a node n, CFSn refers to the node's CFS, and $CFS_n^{previous}$ refers to the previous values of CFS that estimated by the NMA. Here, the initial value of $CFS_n^{previous}$ sets to 0.

During the selection of a node, the nodes' CFS calculates based on the above equations and compared other nodes using the equation 3.

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

Where, CFS_n^{BFNMA} refers to the CFS value of a node n that estimated using the BFNMA, $CFS_n^{neighbor}$ refers to the calculated CFS for a node n in the neighbor nodes, and FCFSn is the node n's final CFS. The CFS's aggregation considers as the nodes' final CFS.

CFS-BFNMA includes the following procedure:

First step: The data transmits to the neighbor nodes from the source node.

Second step: As the source nodes' neighbor and the NMA agent are in the same wireless radio range, the copy of data is received by them.

Third step: The neighbor nodes and their forwarding is monitored by the NMA.

Fourth step: If data is successful or correct, the data is compared by NMA and CFS is assigned when it forwards to the neighbor data.

Fifth step: Based on the threshold value of CFS, the node's CFS is updated by NMA.

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

IV. RESULT AND DISCUSSION

4.1 Experimental setup

Based on the comparison of two different schemes, the proposed method's performance is analyzed using this simulation. Here, the NS2 simulation is used for simulation and it is a discrete-event driven and an object-oriented network simulator. The routing, UDP, and multicast protocol is provided to simulate it on all wireless networks. In this work, the network model is used: all network nodes' are fixed and homogeneous with uniform deployment and similar initial energy. The BS is located far away from the node and is fixed. Based on the static nodes and plane coordinates, the simulation tests are performed by assuming the nodes having limited energy supply. The data transmission or reception is terminated by the nodes when they used the initial energy. Table 1 shows the simulation parameters.

Table1: 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
Routing methods	ISFC-BLS, HMM, CFS-NMA

4.2 The results of the simulation and an analysis

The simulation results are obtained based on the different scenarios and discussed in detail. The attack model is implemented for a network of 50 nodes over the area size of 1000*1000 m2.

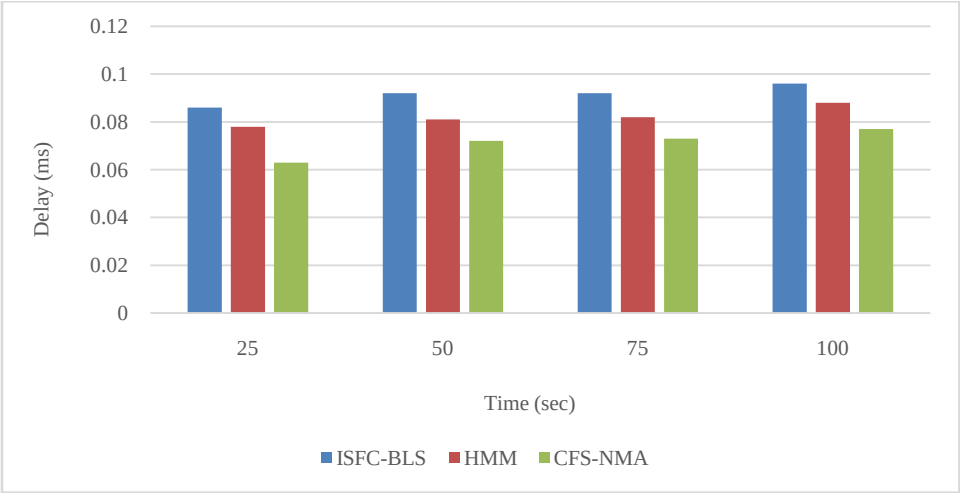

Fig.4. Performance on Delay

Fig 4 shows the results of nodes' end-to-end delay. The figure illustrates that the delayed data delivery will be higher when proper forwarder nodes are not chosen. The behavior of node forwarding is viewed by the node monitoring agent and the nodes are avoided if they have poor delivery rate. The network delay is effected and less end-to-end delay is provided compared to the other techniques.

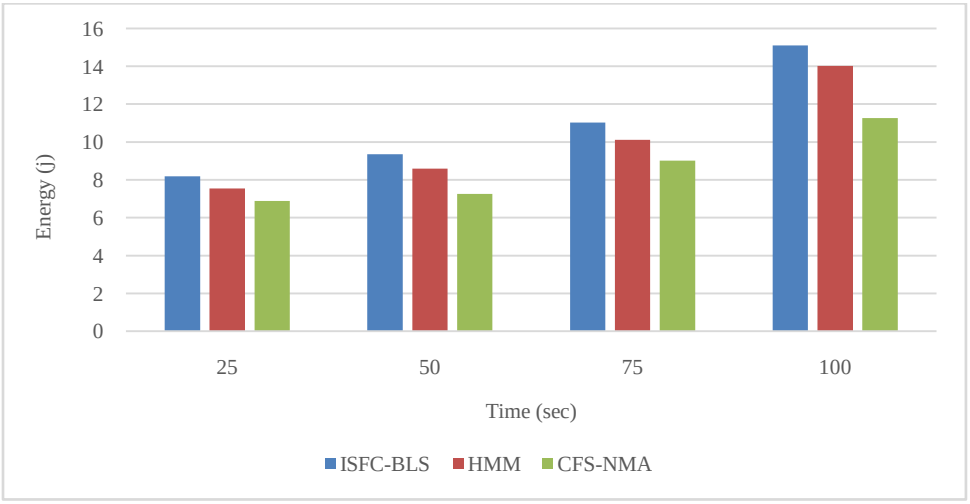

Fig.5. Energy Consumption

Fig 5 illustrates the energy consumption results. Due to the energy depletion, the network system's failure is occurred. The data forwarding is ensured by using the CFS and NMA based forwarder selection, which optimizes the energy usage. The network's energy consumption is improved by the proposed technique and increased network lifetime is achieved than the other protocols.

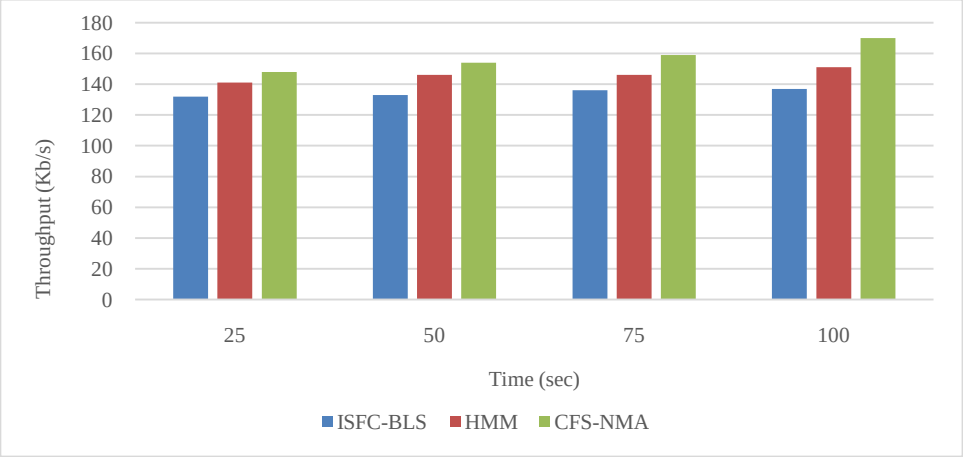

Fig.6. Network Performance

Fig 6 describes the network performance or throughput outputs. It describes how the network is successful in the reliable communication. The effective data delivery is ensured by the fair selection of the forwarder nodes that impacting the throughput. Thus, the results is showed that the throughput is improved by the proposed approach than the other earlier approaches, such as HMM and ISFC-BLS.

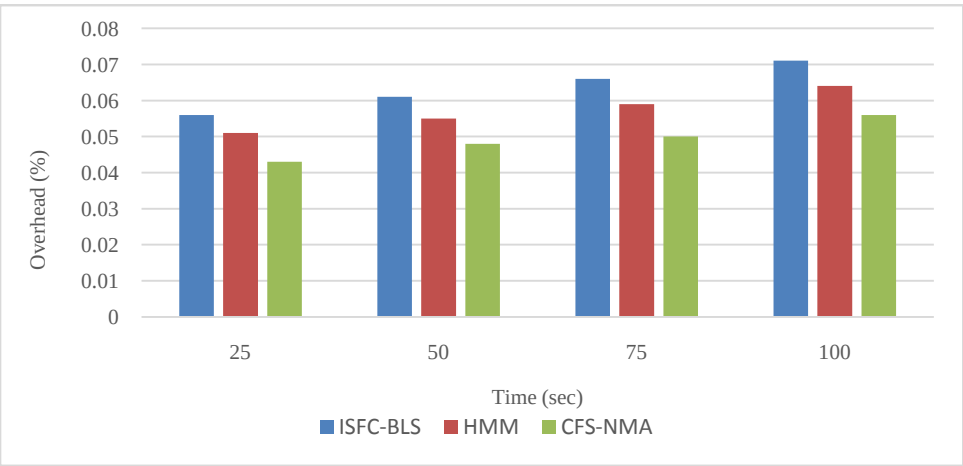

Fig.7. Routing Overhead

Fig 7 shows the simulation graphs of routing overhead for proposed technique CFS-NMA. The performance of a node is effective when good CFS results for the nodes. The continuous routing process is simplified by choosing these good CFS nodes that doesn't require fewer or additional control packets. Compared to the existing protocols like ISFC-BLS and HMM, the proposed approach's overhead is lower.

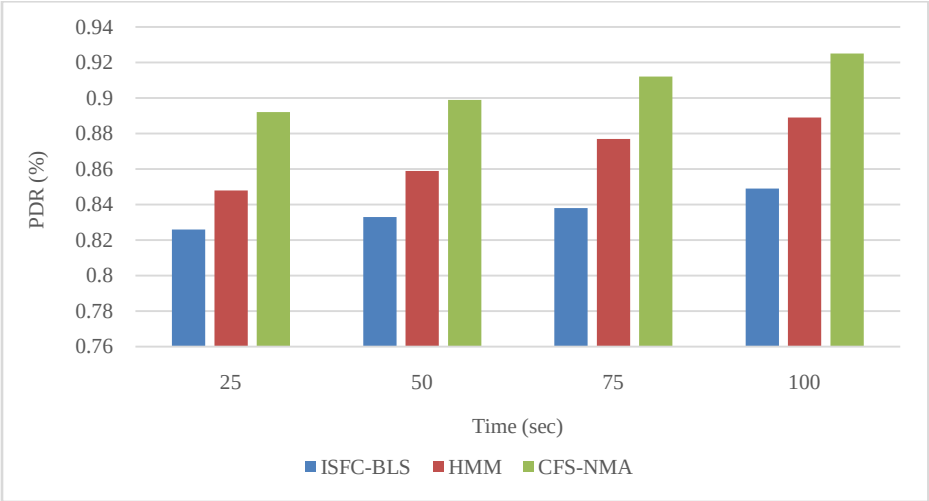

Fig.8. The percentage of delivered packets

Fig 8 describes the packet delivery ratio results for CFS-NMA and other previous protocols like ISCF-BLS and HMM. The seamless data delivery will improve within the estimated time and the data is delivered quickly as the proposed CFS performs well in the previous transmissions. The proposed method is outperformed in terms of PDR rate than the other methods.

Conclusion:

The mechanism of CONFIDENT SCORE based BAYESIAN FILTER NODE MONITORING AGENT (CFS-BFNMA) is proposed for enforcing the wireless sensor networks' security. Within the radio range, the sensor nodes' behavior is monitored by the nodes for estimating the CFS. To detect the nodes' trustworthiness, the system is distributed completely and it doesn't require to use any complex algorithms. In the large WSNs, it can be used. The mechanism considers as a more accurate algorithm for identifying the malicious node than the other traditional security mechanism of WSNs.

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, WencongSu, 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, YoucefBegriche, LyesKhoukhi, 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]. 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.

[22]. 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.

[23]. 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.

[24]. 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.

[25]. 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.

[26]. 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.

[27]. 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.

[28]. 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.

[29]. 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.

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

[31]. 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.

[32]. HananeKalkha, 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

[33]. .S. Jafar Ali Ibrahim et al., "Rough set based on least dissimilarity normalized index for handling uncertainty during E-learners learning pattern recognition", *International Journal of Intelligent Networks*, Volume 3, 2022, Pages 133-137, ISSN 2666-6030, https://doi.org/10.1016/j.ijin.2022.09.001. (https://www.sciencedirect.com/science/article/pii/S2666603022000148)

[34]. Jeyaselvi, M., M. Sathya, S. Suchitra, S. Jafar Ali Ibrahim, and N. S. Kalyan Chakravarthy. "SVM-Based Cloning and Jamming Attack Detection in IoT Sensor Networks."*Advances in Information Communication Technology and Computing, pp. 461-471. Springer, Singapore, 2022.https://link.springer.com/chapter/10.1007/978-981-19-0619-0_41*