ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 17, Issue 2, 2023

Mitigating Packet drop attack using Confident Score based NMA Routing method for Wireless Sensor Networks

S Praveen Kumar, Assistant Professor of ECE, JNTUH College of Engineering Jagtial,
praveenkumar_00019@yahoo.com

Abstract:

Due to their ease of use and low deployment costs wireless sensor network has gained much popularity. In various military and civil applications, this has rendered sensor networks of great importance. However, the lack of centralized network control leaves them vulnerable to a range of security threats. One of the attacks is a packet drop attack, in which a compromised node maliciously drops packets. Various techniques were proposed to detect a packet drop attack on networks of wireless sensors, but none of them would enable them to avoid or isolate their event in the future. A major phase in WSNs has recently been the use of reputation systems. Each node is assigned a reputation based on node behavior in the reputation system. These renowned systems are the means of identifying the reliable data transmission nodes. The monitoring of nodes in the promiscuous mode is proved and tracks the data transmission behavior of node effectively. In this paper a new mechanism is implemented for identifying and preventing packet drop nodes in the process of data forwarding by CONFIDENT SCORE based on the NODE MONITORING AGENT system (CFS-NMA). Node monitoring agents (BFNMA) track the transmission behavior of nodes constantly and allocate CONFIDENT SCORE on the basis of efficient forwarding's. Furthermore, this BFNMA analyzes the traffic pattern and prevents a malicious mark of the incorrect node (node loses packets due to congestion). The results of the simulation show that the proposed mechanism significantly improves network security relative to other conventional security algorithms.

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

I. INTRODUCTION

WSNs are working in many areas with the introduction and advancement of wireless technology, including health surveillance, field monitoring and environmental surveillance [1]. Due to the complex, data-centered, and self-organizing nature of WSNs, they are used to support sensor nodes and communication of many top-level applications in a range of fields of data observation. Without special support for the infrastructure WSNs consist of spatially dispersed sensors which can measure and track changes in environmental conditions. Research on WSNs efficiently deployed for a range of applications has been carried out in recent years. Unable to meet the requirements of all applications may be the single general WSN design.[2] Consequently, in the design phase of a network on the basis of particular use, many network parameters such as sensor range, node density, touch or transfer range should be considered. To do so, the effect of different parameters on the efficiency of these networks must also be analyzed.

Numerous security concerns are also involved in the widespread use of WSNs [3-6]. Due to the dispersed and transparent existence of the transmission media, WSNs can be subjected to many aggressions including a denial of service attack, sinkhole attack, a target attack on forwarding media, blackhole attack, hello-flood and hijack attack. Prevention technology cannot resolve all these safety issues and must therefore also be implemented on the basis of detection [7-8]. The routing is more difficult in WSNs compared to ad hoc networks because of limited battery resources [9]. In addition, WSN nodes have restricted memory, bandwidth and process capacity, which means that routing techniques used must be resource efficient [10–12].
An overview of events in a certain location, sensor, operation, and communication is an integral compound of the sensor network. Tens to thousands of nodes are normally composed of WSN. It collects and communicates information collectively to a central location [13].

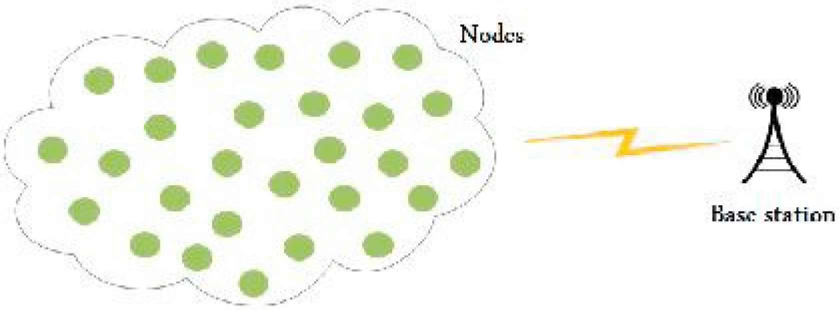

Fig.1. Wireless network sensor basic design

Many types of attacks which harm and make the network stable and functional can affect the WSN. Various network layer attacks, such as wormhole, sinkhole, selective transportation, hello float, fake routing and flood recognition [14-15] recently attracted considerable attention. The Black Hole Angriff is one of the most serious WSN attacks. In this paper, we demonstrate our experience using the Hidden Markov model [16] to detect a strike of a black hole in WSNs.

PACKET DROPPING IN WIRELESS SENSOR NETWORKS

Like every other network, the loss of packet is at least supposed to be a reasonable percentage in sensor networks [17]. Not all missing packages should be considered malicious. There are different explanations for dropping a node. Those are the following:

***Legitimate Packet Dropping*: -** In wireless sensor networks, packet falling is observed where there are no compromised nodes [18]. This loss of packets is primarily linked to the events below;

- **Network Congestion** of the network in networks of wireless sensors is inevitable. The majority of these network channels are dominated by data traffic movements. As a consequence, there is a greater risk of congestion leading to packet loss.
- **Channel Conditions** The state of the channel cannot be ignored in wireless networking as it changes dramatically. The channel conditions that may result in a packets or bit errors of a signal are, for example, free path loss, interference and the noisy presence on the channel and the decline in transmitted wireless signals. Any packets can be dropped in the presence of these factors.
- **Resource Constraints** The energy resources of wireless sensor networks are small. Intermediate nodes in these networks will act selfishly and fail to transmit the packets received, so as to maintain battery power with limited resources. The packets are lowered in turn.

Malicious Packet Dropping**: -** Most of the time, the first stage of launching a drop-off attack is to include a malicious node. This can be achieved best by taking advantage of the faults of the routing protocols in wireless sensor networks, built on the basis of the reliance on confidence in a network node. If the malicious node has been on the path, it can do everything, including drop packets maliciously [19]. Suspending communication or generating incorrect information between the source and destination may be caused by the drops in a malicious intermediate node. The result is an unwanted circumstance.

Consider the method of finding routes from source to destination. The source broadcasts a message from the RREQ (Route Request) to all its neighbors [20]. Each recipient transmits this message to its neighbors in one hop until the destination is reached. On receipt of the packet, the destination updates the sequence of the source to the neighbor who transmitted the RREQ with an RREP (Routing Repair) message. An REP packet to the source node can be returned without a transfer to the destination by an intermediate node that has a destination sequential number equal to RREQ.

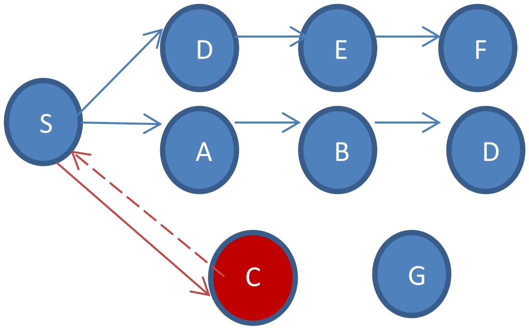

Fig. 2. Routing process of packet drop attack by a malicious node C

For a packet dropping attack node to launch, it needs to participate in at least one network routing path [21]. The figure above shows this: C is a malicious node for dropping S to D packets. First, the RREQ packet is distributed to its neighbors to discover a route from S to D. This message continues to be forwarded to every adjacent node until it is D. The malicious C node violates legislation and is found in S, which asserts the shortest route to D and sends an RREP to S. Thus, S assumes that C is the shortest path to D and sends the recycled data packets to D through C.

II. LITERATURE SURVEY

Based on the energy intake, WSNs can be generally classified into two types: heterogeneous and consistent WSNs. Different energy levels are allocated to various nodes in heterogeneous networks, while all nodes are given identical energy in homogenous networks. The WSNs are reactive and constructive, depending on the operating mode. Reactive networks provide instant responses, while proactive network nodes regularly transmit data. Several works have investigated the general concept of clustering in WSNs [22].

Das et al. [23] suggested hexagonal node deployment sectoring process. The technique proposed would ensure a consistent distribution of load across the CHs. This encourages the integration of nodes in one sector with other sectors, whatever the area of nodes.

Zhang et al.[24] proposed E2HRC, a heterogeneous clustering mechanism of CH. In order to align the cluster heads, it implemented a divised ring structure which was uniform in design. E2HRC balances and mitigates the network's energy usage. However, the safety element of the network is not sufficiently focused. In addition, with the increasing number of nodes, the efficiency of E2HRC degrades, which leads to the need for a new strategy for routing these problems.

The authors of [25] proposed a model of the trust and defined the degree of trust between network nodes. Depending on trust level, one node trusts or disbelieves his trustee. Increased thrustering prevents and removes black hole attacker from the path.

In Zougagh, etc.[26], the authenticated end-to-end recognition method controls accurate transmission of packets through intermediate nodes. The solution suggested prevents an easy or cooperative launch of the black hole.

The authors of [27] successfully remove Black Hole and False Data Injection attacks that have been launched using the new overhead recognition scheme by compromise internal nodes and malicious external nodes.

(Gadaadhar Sahoo, Bharat Bhushan) have proposed to focus on the protected clustering fused algorithm based on intelligence (ISFC algorithm) using fuszy S-means. This decreases energy consumption by implementing a load-balancing principle, improving network life. Therefore, if few subcluster nodes are heavily filled, the increase in energy use for the balance of normal energy depletion is achieved; a balanced head selection is initiated. In this paper, a distance energy model is proposed with regard to the selection of a balanced load subcluster head. Since the main parameters depend on the consumption of energy in a sensor network, the distance between communicating Nodes or transmission distance, the BLS device proposed mitigates the energy depletion from each grid node. [28]

(Hanane Kalkha, Hassan Satori, Khalid Satori) This article provides a Hidden Markov solution to identify and avoid black-hole attacks by wireless sensor networks of malicious nodes. Our system is based on a modern routing algorithm that analyzes the shortest way of avoiding malicious routing of nodes. Our findings show our proposed routing algorithm's success and performance. [29]

III. PROPOSED SYSTEM

CONFIDENT SCORE based MONITORING AGENT SYSTEM for Mitigating packet drop attack (CFS-MAS) METHOD:

***BFNMA*: -**

The technique of node surveillance was the most well-known identification of fraud in wireless networking. Each node acts as a monitoring agent in this techniques that monitors packet transmissions in promiscuous mode to nearby nodes. Before transmitting to the next node, the monitoring officers save a copy of packets in their buffers. This monitors packet transmission from a neighboring node to the next node.

Each monitoring agent node uses promiscuous mode in our proposed BFNMA module to listen to the channel within its radio range and gain information on other sensor nodes and classify behavior. Every node of the monitoring agent has several modules configured. The basic purpose of each module is to identify data collected based on node behaviour. The module for monitoring agents is divided into the next steps,

1) Data collection phase: The monitoring agent nodes in their fixed time window feature use a promiscuous module to record node behaviour.

2) Data classification phase: The monitoring node classifies the node behavior and assigns the resulting score to the nodes on the basis of the data collected in the previous data collection period.

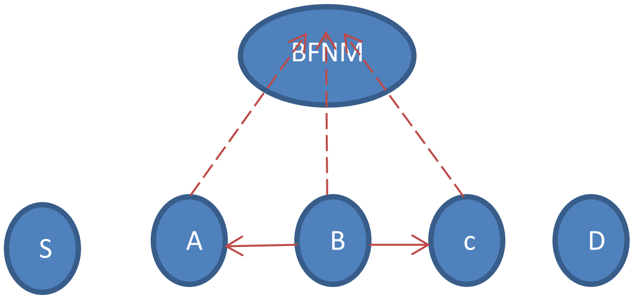

Figure3: An example of BFNMA

An example of BFNMA is given in the figure above. S shall be the source node, D shall be the destination node. The other nodes on the path between S and D are intermediate nodes. It saves the packet in its monitoring buffer until A transmits a packet received from S. BFNMA can monitor whether the packet has been transferred to C after transferring the packet to B. A should be sent a copy of the packet to C because it is inside the transmission range of B. A is supposed to receive. The recipient packet would then be compared to the packet saved in its control buffer. If the BFNMA does not obtain a copy of the packet from B for a certain period, the trust score of B is reduced. If that occurs repeatedly, the trust is set to zero and A determines that B is a malicious node and passes through B.

CALCULATION OF CFS

There is two ways to measure the confidence score of the node.

1. Neighbour CFS
2. Monitoring agent CFS

The nearby CFS is an aggregation of CFS values that the neighboring node allocated in previous transmissions to the source or the prefixing nodes. Also, for any node based on behavior, the monitoring agents maintain their own CFS records. The addition of these multi-CFS are considered to be the final CFS of a given node. The node CFS can be computed using the following equation in the current node

$$\boldsymbol{CFS_n^{current} = CFS_n^{previous} + CFS_{thresh}}$$

$CFS_n^{current}$ 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].

Agent node is used to store traffic information in our proposal model with a fixed time window. In each time window, the agent node contains various CFS values. The node CFS can be determined as follows

$$\boldsymbol{CFS_n = CFS_n^{current} + CFS_n^{previous}}$$

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.

Thus, the CFS of the nodes during node selection is determined using the following equation compared with other nodes.

$$\boldsymbol{FCFS_n = CFS_n^{neighbor} + CFS_n^{BFNMA}}$$

$FCFS_n$ 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. These CFS' aggregations are considered the ultimate CFS of n nodes.

The CFS-BFNMA procedure is as follows.

First step: The information is sent by the Source Node to its nearby nodes.

Second step: A copy of the data is sent to NMA agent and to the source node's neighbor as they are within the same radio range.

Third step: The NMA monitors and transfers the neighbor nodes.

Fourth step: NMA can compare the data and attribute CFS, where the data is right and efficient, to the neighboring node.

Fifth step: NMA changes the node's CFS according to the threshold value of the CFS.

IV. RESULT AND DISCUSSION

Experimental setup

This simulation is conducted to evaluate the performance of the technology by contrasting the technology with two different systems. This work uses a network simulator geared towards objects and discreet events, known as NS2 (Simulator 2 for network research). It provides support in any wireless network for UDP, routing and multi-cast protocol simulation. In this study, the network model used is the following: All network sensor nodes have the same fixed and standardized initial capability and are mounted uniformly (all sensor nodes have the same capacities, radio transmitters and restricted power resources). The base station is attached and located away from the sensor node. Testing is done with planes and static nodes coordinates. Nodes are supposed to have a small amount of energy and once the initial nodes' energy has been used, they stop receiving or transmitting data. The parameters of simulation are given in the following table (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 x1000
Malicious nodes	3
Transmission Protocol	UDP
Initial Energy	100j

Table1: Simulation table

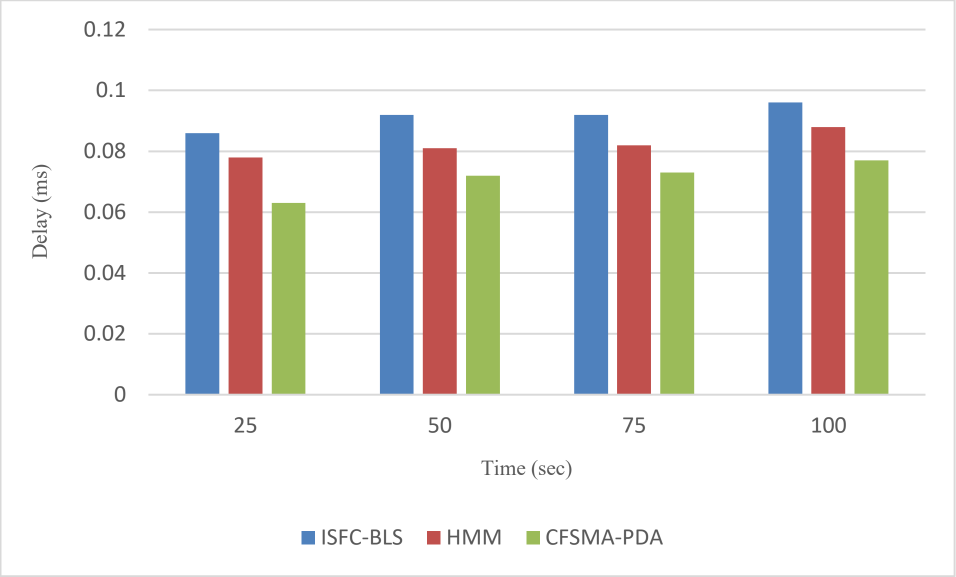

Fig4: Performance on Delay

The chances of delayed data transmission are strong if the correct forwarder nodes are not chosen. The node controller monitors node transmission activity and prevents weak distribution nodes. It affects the network's delay and gives less delay than other approaches.

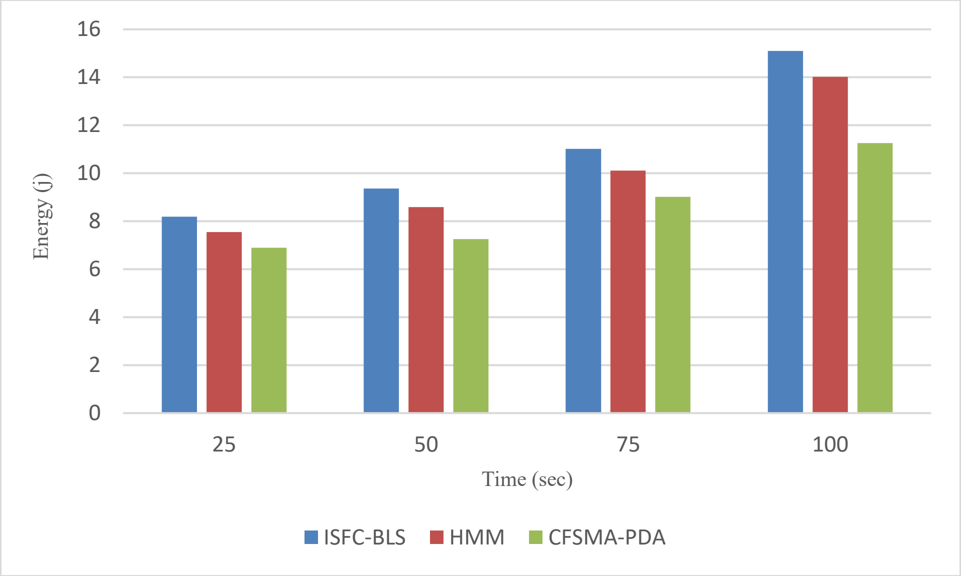

Fig5: Energy Consumption

Wireless networking's energy resource is small. Network failure is caused by an energy depletion. Using NMA and CFS-based transmitter collection, the data is transferred to nodes with optimal energy use. The result shows that the solution proposed boosts the network's energy efficiency and increases the life of the other protocols.

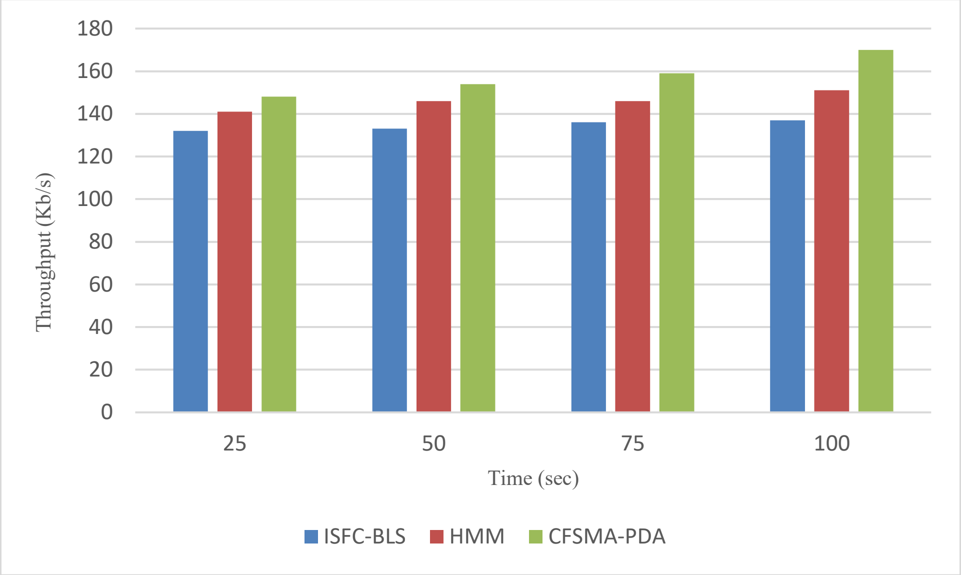

Fig6: Network Performance

The performance explains how secure contact is across the network. The equal selection of the sponsor nodes based on past activity ensures efficient data transmission, which greatly impacts efficiency. The result indicates that the solution suggested increases the performance of its rivals.

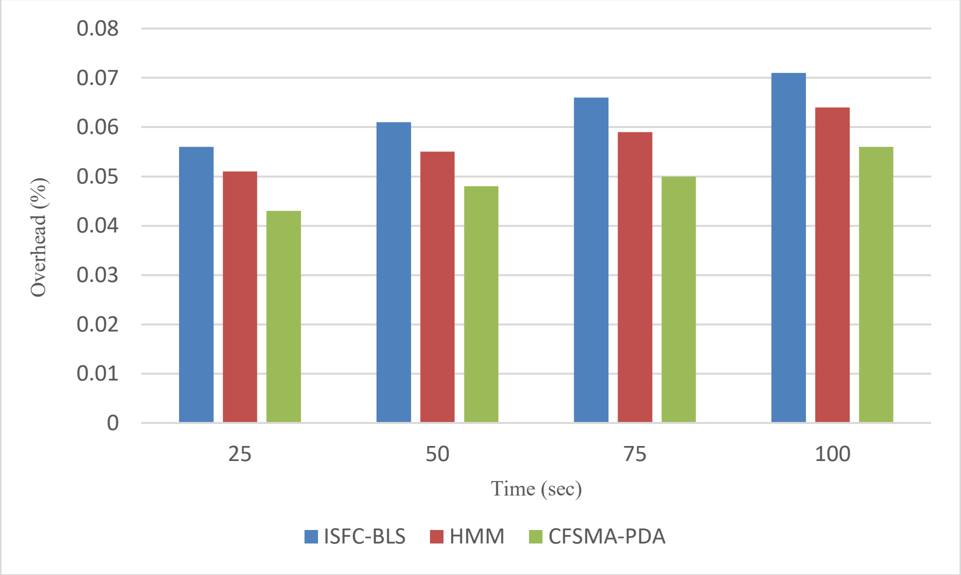

Fig7: Routing Overhead

Overhead explains the difficulty of the algorithm suggested. The strong CFS of the nodes means the output of the node has in the past been good. Choosing these good CFS nodes simplifies the routing process, which does not require more / lower control packets. The overhead of the solution proposed is therefore less than that of the protocols previously used.

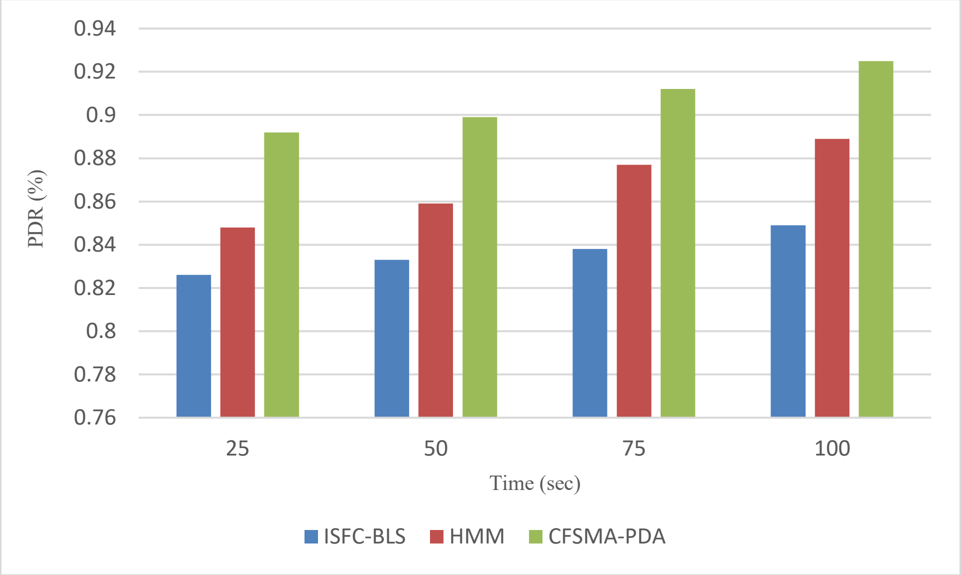

Fig8: Packet Delivery Ratio

The proposed CFS approach ensures the possibility of further transmissions for nodes that were successfully carried out during previous transactions. This improves the smooth data transmission and easily transmits the data within the expected time. This results in a good performance and a high PDR rate compared to the other protocols.

Conclusion:

In this article, we propose a framework for implementing the protection of Wireless Sensor Networks based on the BAYESIAN FILTER NODE MONITORING AGENT (CFS-BFNMA). In the CFS measurement range the monitoring nodes track the activity of sensor nodes. The system is fully distributed and the trustworthiness of the nodes is not recognized by complex algorithms. It can be used in large-scale wireless sensor networks. This mechanism helps to identify a malicious node more accurately than the other conventional WSN security mechanism.

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]. 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]. 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]. 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.

[26]. 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.

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

[28]. 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.

[29]. 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.