International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 08, Issue: 06 (November -December, 2022)

Malicious Attack Detection and Prevention using Packet Filtering in Wireless Sensor Network

Pragati Nigam Dr. Vivek Sharma
CSE Department, TIT Bhopal (M P.)
priyanigam4795@gmail.com, Sharma.vivek95@yahoo.in

Abstract- A Wireless Sensor Network (WSN) is a network in which nodes form a temporary dynamic link without the help of a centralized administration and unstable infrastructure. Because of the absence of a central controller, it isn't easy to maintain reliable and secure communication between the sender and receiver. In WSN, a centralized unit is also helpful for data collection, but with stationary nodes, it performs better. The malicious nodes' activities are different in the network, and a strong security scheme can filter packets an attacker sends. Each node in the network has to work as a router to take part in route establishment and data delivery, so highly cooperative nodes must ensure that the initiated data transmission process does not fail. A malicious attack is a type of attack that works by continuously flooding useless packets and affecting the receiver or other node's processing capability. If the sender starts data transmission, then, in that case, the attacker will not forward packets to other nodes or take part in routing. In this research, we proposed detection and a prevention technique against malicious attacks (MDP) with AODV routing. We use a packet filtering method for detection and prevention to identify attacker node behaviour in the network. The packet filtering technique prevents attackers and, through our proposal, provides secure and reliable communication. It can also be simulated through network simulator-2 and analyze network behaviour in malicious, normal and prevention (MDP-AODV). It means a greater number of trusted nodes have to give the possibility of secure communication. After that, we measure the network's performance based on network parameters like throughput, packet delivery ratio, throughput and routing load.

Keywords: Malicious, packet filtering, Routing, flooding, WSN.

I. INTRODUCTION

Recent years have seen an increase in interest shown by researchers in wireless sensor networks (WSNs) due largely to the widespread use of Micro-Electro-Mechanical Systems (MEMS) technology, which has eased the creation of smart sensors. These sensors are less costly than conventional ones but are also smaller and have less processing and computational power. These sensor nodes can detect, measure, and collect data from their surroundings, and depending on a local decision-making process, and they may relay that data to the user. Low-power gadgets called "smart sensor nodes" are outfitted with one or more sensors, a radio, a power source, a processor, memory, and an actuator. [1] the sensor node can be equipped with a range of mechanical, thermal, biological, chemical, optical, or magnetic sensors to monitor environmental characteristics. A radio is installed for wireless communication to convey the data to a base station since the sensor nodes often deploy in difficult-to-access areas and have limited memory (e.g., a laptop, a personal handheld device, or an access point to a fixed infrastructure). A sensor node's primary power supply is a battery. Depending on the suitability of the location where the sensor will be placed, a supplementary power supply that gathers electricity from the environment, such as solar panels, may be added to the node. Actuators could be integrated into the sensors, depending on their intended function and method.

Typically, a WSN has very little or no infrastructure. It comprises many sensor nodes (from a few tens to thousands) cooperating to monitor an area and gather environmental data. WSNs come in two flavours: structured and unstructured. A dense cluster of sensor nodes constitutes an unstructured WSN. Sensor nodes may be set up in the field on a whim [2]. The network is deployed and then left unattended to carry out monitoring and reporting tasks. Because there are so many nodes in an unstructured WSN, it is challenging to manage the connection and identify faults. In a structured WSN, the placement of the sensor nodes follows a predetermined pattern. ([3] A structured network allows for the deployment of fewer nodes with cheaper network administration and maintenance expenses. Since nodes are now positioned at particular places to provide coverage, fewer nodes may be deployed, whereas ad hoc deployment could leave regions unattended. The article

consists of VII section, in section describe the introduction to WSN, section II elaborate on existing work on the security issue and their prevention, section III describe the proposed MDP-AODV technique, in section IV discuss the proposed MDP-AODV working architecture, section V describe the simulation environment in section VI, describe the simulation analysis result, and in section VII describe conclusion and future approach on WSN network.

II. RELATED WORK

In this section, we describe various existing WSN security techniques used to improve the WSN service, i.e. energy issues and security. Here those are working in the field of WSN service improvement. Dr.K.Sasi Kala Rani, *et.al.* [1] "Experimental Evaluations of Malicious Node Detection on Wireless Sensor Network Environment" utilizes the same logic of WSN in an enhanced way using adding some security metrics and associated communication strategies. A Modified Ad-hoc-On-Demand-Distance-Vector (mAODV) is introduced in this book to carry out the routing setups effectively. This suggested method of mAODV is derived from the logic of the conventional AODV model, but the metrics are improvised instead of employing the standard transmission and reception power ratio. Balakrishnan *et al.* [4] proposed a two-hop acknowledgement detection scheme (TWO PACK) based on the checkpoint node. The checkpoint node in the TWOACK technique is each node along the forwarding chain. An acknowledgement packet will be sent by node I, the receiving node, to node j, which is two hops distant. If node j does not receive the acknowledgement packet, it assumes that the link between nodes I and j is malicious and issues a warning to the source node. The TWOACK technique significantly increases the conflict and collision of network messages. Xiao et al. [5] presented a multi-hop acknowledgement-based detection technique to address this issue (CHEMAS). The CHEMAS system randomly chooses certain nodes along the route from the source node to the base station to serve as checkpoint nodes. The acknowledgement packet is sent to the upstream node by the checkpoint node when it receives a packet. Liu. *et al.* [6] Novel system, based on a multi-hop acknowledgement mechanism, was presented to address Per-Hop acknowledgement(PHACK). In the Per-Hop acknowledgement system, each node in the forwarding path must transmit an acknowledgement packet for every packet with forwards along with the regular packets to the originating node. However, these multi-hop acknowledgement-based techniques call for sending several confirmation packets, which will raise communication overhead and significantly shorten network life. To improve the effect of malicious node detection. Yang *et al.* [7] proposed a malicious node detection model based on reputation with enhanced low energy adaptive clustering hierarchy, MNDREL. The cluster head nodes are chosen based on the upgraded routing protocol, and other nodes create various clusters by selecting the appropriate cluster head. The network's malicious nodes can be successfully discovered by analyzing the reputation value for the parent node as evaluated by the child node. The MNDREL model beat other WSN malware detection models with a decreased false alarm rate. However, the MNDREL model's real-time performance has to be enhanced. A reputation model for sensor networks based on a Gaussian distribution was developed by Xiao et al. (GRFSN). In this paradigm, each node's trust value is determined by summing its direct and indirect reputations, and then that value is compared to the trust threshold. A malicious node has a trust value lower than the trust threshold. This approach needs to establish a trust threshold. However, since the trust threshold is static, it frequently misjudges legitimate nodes as malevolent. Zheng *et al.* [9] proposed a network security mechanism based on trust management to deal with the threats faced by WSNs (DNSMTM). This mechanism is designed to rapidly and effectively detect un-trusted nodes in the network and ensure the dependable functioning of the network (DNSMTM). This mechanism derives the comprehensive trust degree of nodes, which can reflect the trust degree of nodes based on the trusted access of nodes. It detects malicious nodes per the comprehensive trust degree of nodes. It first calculates the local trust degree of nodes based on the interaction behaviour of the currently used nodes. The technique has a greater detection rate for rogue nodes and can efficiently stop them from using as much energy. [10] Suggested a hybrid monitoring-forwarding game detection technique to identify targeted forwarding assaults (MSGSFS). This system builds a set of techniques by including elements like packet loss, data corruption, and forwarding delay. To play the monitoring-forwarding game and gather the routing trust value of the suspicious node, the data transmitting node and its one-hop neighbour nodes choose strategies from a set.

Zhou *et al.* [11] presented an enhanced trust evaluation model (ITEMBB). In this paradigm, the node's

direct trust value is computed first. If the direct trust value is deemed insufficiently dependable, the indirect trust value of the node is determined. A complete trust value is created by combining the direct and indirect trust values, and entropy is employed to give highly trusted nodes more weight. The methodology somewhat gets over the drawbacks of subjective weighting, but it still can't deal with the issue of enduring reputation value. A cluster-based selective forwarding attack detection system was proposed by Zhou et al. [12] by combining the neighbour node monitoring and watchdog mechanism (SMCSF). This scheme divides the cluster nodes into cluster head nodes, monitoring nodes, and cluster member nodes. By choosing the monitoring node in the cluster, the monitoring node performs the calculation and adjustment of the overall reputation of the cluster head nodes and cluster member nodes. And in this scheme, the monitoring nodes are in charge of not only determining and adjusting a node's reputation as well as judging and spotting malicious nodes in the cluster but also keeping an eye out for any malicious behaviours on the part of the cluster head node, such as data tampering or packet loss during the data forwarding process. Even though this method may rapidly and precisely identify rogue nodes, it is too difficult to maintain track of all the nodes.

Sheetal *et al*. [13] introduce a blockchain trust model (BTM) for malicious node detection in wireless sensor networks to address the issue that the fairness and traceability of the detection process cannot guarantee the current malicious node detection methods in wireless sensor networks. In BTM, it is realized through 3D space, blockchain intelligent contracts, and WSN quadrilateral measurement for the localization of the identification of rogue nodes. The consensus voting results are also recorded in the blockchain's distributed ledger. The model can successfully identify malicious nodes in WSNs and ensure that the discovery process can be tracked back. Although the model's consensus approach is the conventional POW workload-proof method, which demands a lot of energy and computer resources, it is not well suited for the operating environment of wireless sensor networks. Li *et al.* [14] suggested a distributed and randomized detection technique (IPAs). Each node in this system keeps a list of questionable nodes. All node i's neighbours are first put on a list of suspicious nodes; if the packets sent by its neighbours are invalid, the neighbour's nodes that transmit valid packets are subsequently removed from the list of suspicious nodes. The nodes in the group of suspicious nodes are bad neighbours after n detection rounds. The system can detect rogue nodes in the network, but it requires n rounds, making network communication considerably more difficult.

In conclusion, each type of current research strategy has unique characteristics. Comparing comparable tasks is examined by comparing each plan's benefits and drawbacks. High communication overhead will result from the multi-hop acknowledgement-based detection techniques [4–6] having to send many acknowledgement packets. The number of monitoring nodes required by the detection systems [7–12] based on trust evaluation substantially increases network overhead. Furthermore, the present methods for finding malicious nodes generally concentrate on finding them along a single path. In order to determine a node's trust value, no monitoring nodes or intricate assessment models are required for the HFDLMN technique described in this book. Malicious nodes can also be found and located in many other methods.

III. PROPOSED RESEARCH

Sensors are lightweight and low-capable devices, which increase the chance of unauthorized access at the time of communication. It's an emerging technology applicable for weather forecasting, tsunami detection, military service, agriculture monitoring and control. Sensors help implement internet of things (IoT)-based operations. A wireless sensor network is a collection of lightweight nodes that perform a specific task and have at least one central controller and wireless communication between sensors and the base station controller. Security issues are considered in the communication phase, such as routing, missing activity (black hole, grey hole), unwanted flooding, denial of service (DoS), packet injection, etc. Some of the author's proposed security mechanisms are based on misbehaviour symptoms. This dissertation proposes a security system that detects and protects against malicious activity in a wireless sensor network (MDP-AODV) using a packet filtering approach.
The proposed MDP-AODV is executed during the route establishment process up to the data transmission phase. While awaiting data transmission, the source sensor node executes the MDP-AODV routing protocol, which is broadcast throughout the network in order to locate the destination device, i.e., the base station (BS). While the source is not in direct range of BS, other movable sensors perform the task of routing because it's capable of routing

formations that can provide inter-sensor communication from one sensor to another and create multipoint-based communication. In the network field, while any node initiates unwanted message flooding to gain the network resource and disrupt the other node's communication, it's assumed to be an attacker. The attacker node's goal is to disrupt the entire communication by flooding the network with unwanted messages. The proposed MDP-AODV-based security system is always active, which aims to monitor, detect, and protect the network from attacker nodes and provide reliable communication to communicator nodes. Let's assume any attacker node belongs to the network and tries to inject the wanted message into the network; its motive is to disrupt the network. The attacker node identifies the network's vulnerability and gets the idle channel and movable sensor node for useless data transmission. It aims to consume the network resources. After some time, this useless data capture the major part of the network and disrupts normal communication, which is important to serve the network.

On the other hand, let's try to use the proposed security system name MDP-AODV, which is inbuilt into the network for security during communication from the sensor to the base station or from other sensors. MDP-AODV monitors every node's activity as packets arrive at the movable sensor (router) or base station because only those devices are driving the security system and providing communication to other sensor nodes; without those devices, communication to other sensor nodes is impossible. The time of the proposed security system when any attacker wants to spread an unwanted message, if a packet comes into the movable sensor (router) or base station, then the device will execute the security module before direct forwarding to the destination node. The network layer on the movable sensor or base station retrieves from incoming packets their source id field, packet type, packet length, and route expiration time. With the retrieved information, we identify which field value does not match the criteria of network protocol, including their packet type and route expiry time. While we get the packet type is unknown and their route expiry time is infinite, it means the packet is not legitimate and dropped. Finally, the detector node takes the source id from the packet. It blocks the source node, an unwanted message spreader, and broadcasts its information to all other routers or base stations so no more communication can occur from those nodes. The proposed MDP-AODV security system helps to detect and protect the system using the packet filtering method. It's a light-weighted security system because it's only executed during communication under the network layer.

IV. PROPOSED ARCHITECTURE

This section describes the proposed architecture of malicious detection and prevention techniques in the sensor network. The base station uses the MDP-AODV module to detect whether the packet is valid or not as well as route expiration time which is useful to the decision-making about malicious activity and blocking the node.

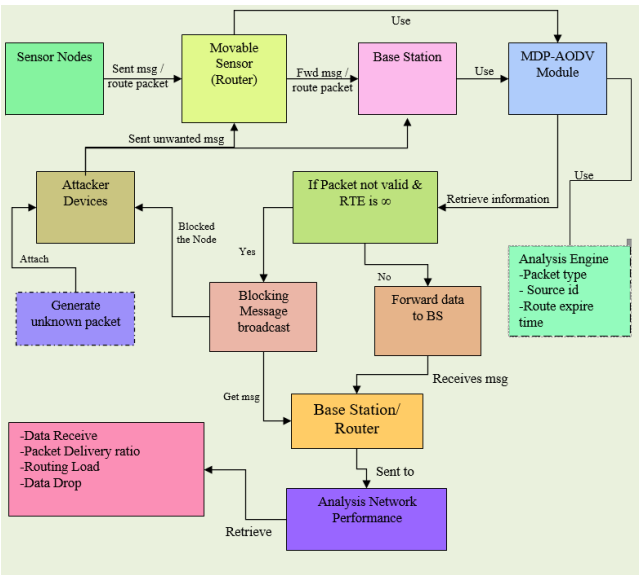

Figure 1: Proposed ECCO Working Architecture

V. SIMULATION ENVIRONMENT

The simulation of normal malicious attacks, MAODV, and MDP-AODV schemes is done based on the following simulation parameters shown in table 1. These simulation parameters are decided based on dynamic topology. In the case of normal routing, all 100 nodes are considered, but in the case of a malicious scenario, only some of the nodes are attackers, and the rest are normal nodes. In the case of MPD-AODV, apply the packet filtering technique on all nodes to detect and prevent the network from attackers. The rest of the information is available in table 1.

V. SIMULATION RESULT

A. Percentage of Data Receives (PDR) Analysis

This graph represents the Packet Delivery Ratio (PDR) analysis in the case of normal AODV routing, in the case of wormhole attack, and the case of the MDP-AODV

scheme. The previous MAODV routing is only considered to match the network performance after applying the protection scheme. Here we visualize the effect of malicious attacks on the network by only measuring about 71% of packet delivery. In an attacker's presence, the ratio of packets received to packets sent is lower than the security scheme. After applying the MDP-AODV scheme, the PDR performance of MAODV is 4% more or less. The PDR improves after applying a security scheme against attack.

Table 1: Simulation Parameter for Deployment of WSN

Parameters	Configuration Value
Simulation Tool	NS-2.31
Routing Protocol	MAODV, MDP-AODV
Simulation Area	1000m*1000m
Network Type	WSN
Number of Nodes	100
Number of Base Station	4
Physical Medium	Wireless, 802.11
Simulation Time (Sec)	550Sec
MAC Layer	802.11
Antenna Model	Omni Antenna
Traffic Type	CBR, FTP
Propagation radio model	Two ray ground
Energy (Initial)/J	Random

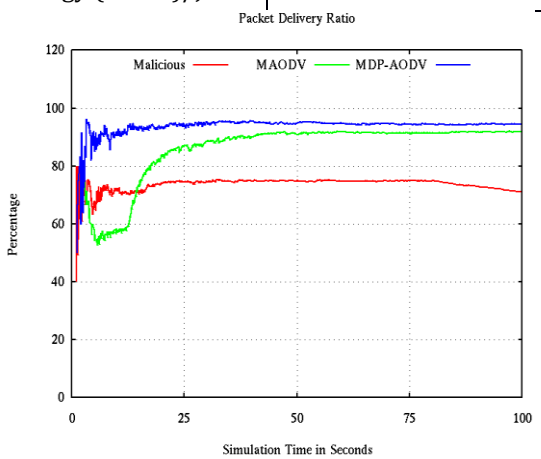

Figure 2: Percentage of Data Receives (PDR)

B. NRL Analysis

The routing load analysis is required to determine the number of routing packets delivered in the network to connect the sender and receiver. The routing packets contain information about the receiver that is important to know. In this graph, the routing load or the number of routing packets in the case of MDP-AODV is the lowest and most genuine. The presence of malicious attackers is shown on overhead 71 due to the presence of fake and useless packets. The important point of normal routing is that the minimum value of routing packets shows better performance in the network, and this performance is determined in the event of an attack. The important point is that in minimum routing packets, the actual data packets being delivered in the network are negligible compared to normal and MDP routing. In the case of MDP, the routing packets are less flooded and provide a more secure path for communication.

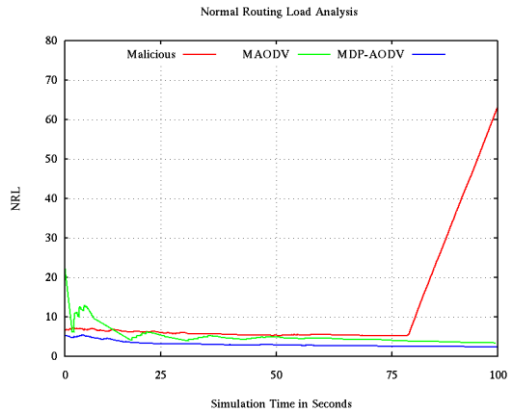

Figure 3: NRL Analyses

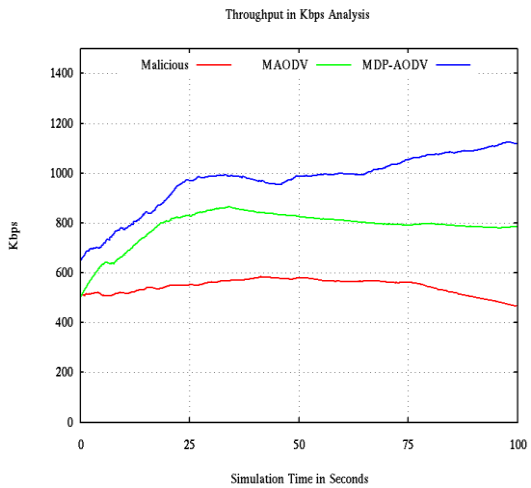

Figure 4: Throughput Analysis

C. Throughput Analysis

The throughput is measured by the number of data packets received at the destination per second. During the attack, throughput decreases due to heavy routing packet flooding in the network. This graph represented the throughput analysis of a malicious attack, previous MAODV and proposed MDP-AODV. The throughput is measured in Kbps, and MDP-AODV performance is better than the rest of the schemes. During the attack,

throughput decreases due to heavy routing packet flooding in the network. It is measurable up to the end of simulation time. But after applying the MDP-AODV scheme, the throughput is better than the previous scheme.

D. Packets Receiving Analysis

This graph represents packets receiving analysis of malicious attacks, MAODV and proposed MDP-AODV. The attacker's presence in the network directly affects packets received because of heavy flooding.

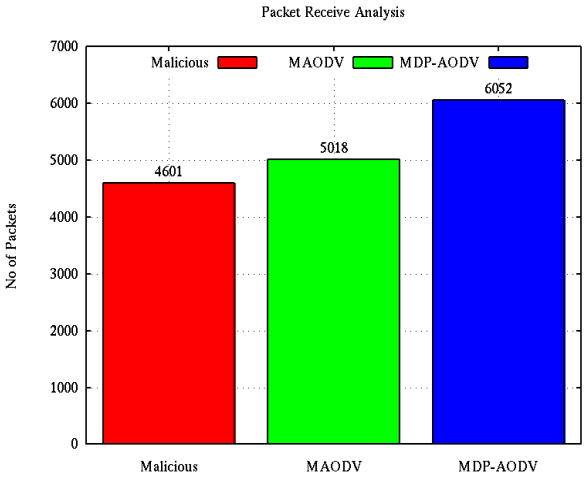

Figure 5: Packets Receiving Analysis

Here the packets are received less in the case of malicious attack and MDAODV, i.e., about 4600 and 5018, but in the case of proposed MDP-AODV, 6050 packets are received at the destination. The better performance of a network depends on good packet reception. The greater number of packets received shows an improvement in routing performance. The proposed scheme blocks the whole activity of a malicious attack and removes the infection from the network.

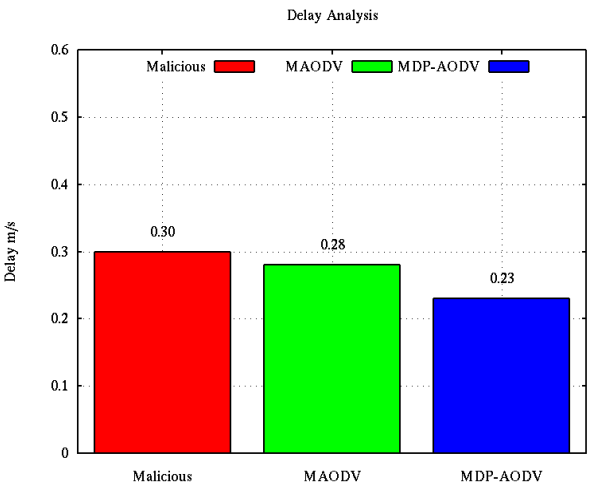

Figure 6: Delay Analysis

E. Delay Analysis

Senders send the number of packets to the destination, and some packets are dropped for some reason in the network. The number of packets received on time implies no data delay, but packets may arrive late at the destination due to an attacker or other factors. The number of senders sends data on time, but due to a delay in network data, the data arrives late at its destination. The delay in malicious nodes is the highest. The previous MAODV scheme reduces delay and provides security from malicious attackers. The performance of the proposed MDP-AODV is shown to have less delay because of packet filtering and better route selection in WSN. If the delay is high, there is some strong link establishment problem. The proposed scheme takes 0.5 milliseconds less time than the MAODV scheme.

F. Summarized Performance Analysis

The overall performance of the network is shown in table 3. This table represents the complete summary of performance metrics in exact figures, which means how many packets are sent, received, and lost in the network in case of attack, previous MAODV, and MDP-AODV. The protection scheme provides for normal behaviour in the presence of an attacker.

Table 2: Performance Analysis

	Malicious	M-AODV	MDP-AODV
Send	5174	5473	6409
Receive	4601	5018	6052
Drop	573	455	357
PDR	71.14	91.69	94.43
NRL	63.35	3.33	2.48
Delay [ms]	0.30	0.28	0.23

VI. CONCLUSION AND FUTURE WORK

WSNs can set up networks in harsh environments where it may not be possible to deploy a traditional network infrastructure in areas humans cannot reach. Whether WSN has vast potential, there are many challenges left to overcome. Security is an important feature for the deployment of WSNs. Security is such an important feature that it could determine the success and wide deployment of WSNs. Malicious nodes either drop valuable data packets or inject useless packets into the network. A malicious node attack is a type of attack that performs malicious activity by flooding unwanted or

useless packets into a network. The proposed Malicious Detection and Prevention scheme with AODV (MDP-AODV) is applied to detect malicious attackers by packet filtering in a network. MDP-AODV aims to detect malicious nodes by the packets they flood the network. The packets sent by the attacker are completely different because they contain no message misbehaving links to prevent them from communicating networks. This MDP-AODV protects against malicious node attacks and blocks the activities of attacker nodes. In the case of an attack, almost all the network performance is completely down, but the proposed scheme improves performance to nearly equal normal routing. The routeing overhead is less than one as compared to MAODV. The PDR improvement is 4% compared to the previous MAODV scheme, and the rest of the metrics also show performance improvement. This work explores a vigorous and very simple idea, which can be implemented and tested in the future for a greater number of attacks by increasing the number of nodes in the network. To this end, we have presented an approach to a network-layer security solution against attacks that protects routing and forwarding operations in the network. In the future, we will also examine the behaviour of other attacks like vampire attacks and remapping attacks and try to make protection schemes for them and try to enhance the performance of the routing protocols that have been considered in this dissertation to improve their routing capability.

Reference

[1] Dr K.Sasi Kala Rani, Ms R.Vijayalakshmi "Experimental Evaluations of Malicious Node Detection on Wireless Sensor Network Environment" IEEE Xplore (ICICCS 2021).

[2] Christian Miranda, Georges Kaddoum, Elias Bou-Harb, Sahil Garg and Kuljeet Kaur, "A Collaborative Security Framework for Software-Defined Wireless Sensor Networks", IEEE Transactions on Information Forensics and Security, 2020.

[3] Muhammad Nawaz Khan, Haseeb Ur Rahman, Mohammed Amin Almaiah, Muhammad Zahid Khan and Ajab Khan, "Improving Energy Efficiency With Content - Based Adaptive and Dynamic Scheduling in Wireless Sensor Networks", IEEE Access, 2020.

[4] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: preventing selfishness in mobile ad hoc networks," in Proceedings of the Wireless Communications & Networking Conference, pp. 2137–2142, IEEE, New Orleans, LA, USA, April 2005.

[5] B. Xiao, B. Yu, and C. Gao, "CHEMAS: i," Journal of Parallel and Distributed Computing, vol. 67, no. 11, pp. 1218–1230, 2007.

[6] A. Liu, M. Dong, K. Ota, and J. Long, "PHACK: an efficient scheme for selective forwarding attack detection in WSNs," Sensors, vol. 15, no. 12, pp. 30942–30963, 2015.

[7] H. Yang, X. Zhang, and F. Cheng, "A novel algorithm for improving malicious node detection effect in wireless sensor networks," Mobile Networks And Applications, vol. 2020, Article ID s11036-019-01492-4, 2020.

[8] D. Xiao, J. Feng, and Q. Zhou, "Gauss reputation framework for sensor networks," Journal on Communications, vol. 29, no. 3, pp. 47–53, 2008.

[9] G. Zheng, B. Gong, and Y. Zhang, "Dynamic network security mechanism based on trust management in wireless sensor networks," Wireless Communications and Mobile Computing, vol. 2021, Article ID 6667100, 10 pages, 2021.

[10] H. Liao and S. Ding, "Mixed and continuous strategy monitor-forward game based selective forwarding solution in WSN," International Journal of Distributed Sensor Networks, vol. 2015, no. 11, Article ID 359780, 13 pages, 2015.

[11] Z. Zhou and N. Shao, "An improved trust evaluation model based on Bayesian for WSNs," Chinese Journal of Sensors and Actuators, vol. 29, no. 6, pp. 927–933, 2016.

[12] H. Zhou, Y. Wu, L. Feng, and D. Liu, "A security mechanism for cluster-based WSN against selective forwarding," Sensors, vol. 16, no. 9, pp. 1537–1552, 2016.

[13] W. She, Q. Liu, Z. Tian, J.-S. Chen, B. Wang, and W. Liu, "Blockchain trust model for malicious node detection in wireless sensor networks," IEEE Access, vol. 7, pp. 38947–38956, 2019.

[14] Y. Li and J. C. S. Lui, "Identifying pollution attackers in network-coding enabled wireless mesh networks," in Proceedings of the 2011 20th International Conference on Computer Communications and Networks (ICCCN), pp. 1–6, Maui, HI, USA, August 2011.