

## **Novel Methodology For Detection of Malicious Nodes In Wireless Sensor Networks**

**InzimamUl Hassan**

Dept. of computer science and engineering  
Lovely Professional University  
inzimamulhassan@gmail.com

**Amandeep Kaur**

Dept. of computer science and engineering  
Lovely Professional University  
amandeep3.kaur@lpu.co.in

**Abstract:**Wireless sensor network has emerged numerous applications in various fields with huge classification. Wireless sensor network is collection of self configure sensor nodes, in which nodes can join and leave the network as per access points. Nature of wireless sensor networks is decentralized; various malicious nodes might enter into the network at any time. An attack in which the radio signals are transferred is interfered by radio frequencies which have been utilized by the sensor network. With the technology advancement, security is the main concern. In case of DDoS attack, the raw packets are flooded to the victim nodes and it is type of active attack. When number of raw packets is flooded in the network, it increases energy consumption of the network and minimize the lifetime of the network. A novel approach is to be proposed in this work to detect the malicious nodes from the network which cause the DDoS attack. All the work has been done using the NS 2.35 simulator. After the simulation has done the proposed method give the feasible result against the DDoS attack. By this the attainment of the network is increased in various parameters.

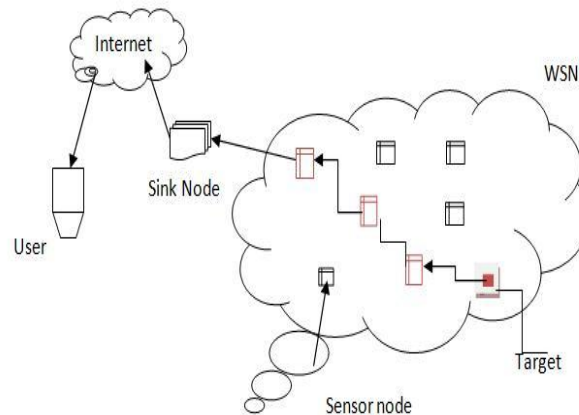
**Keywords:**

WSN, Threshold, Delay, DoS, DDoS.

### **I. Introduction**

Wireless sensor Network (WSN) is used in these days for many applications. WSNs are used for realization of ubiquitous computing. It can be deployed in indoor and outdoor. These sensor networks can establish ad-hoc network automatically, and sensing data as per request and event driven. Sensors node perform for routing services and creates a multi-hop network environment that transmit data sampling to external destinations. Sensor node deals with information sinks, receiving dynamic information from external nodes. WSN can be described as networks of sensor nodes which are spatially distributed and collect information after monitoring fields through wireless links communication. The data gathered by different nodes after aggregation is send to a base station which can be use by local users and remote users. Base station is consisting of storage capacity and data processing capabilities; it is very helpful in network [1]. The major task of the base station is to receive the information which is transmitted by the sensor nodes. The sensor nodes are deployed within the area of base station, which can form groups as per the requirement of the application. Due to the smaller sizes of the sensor nodes, the sizes of their batteries are also

small. The batteries of the sensors deplete very easily and cannot be recharged easily as they are deployed once in very large areas. Thus, the lifetime of the network reduces which is a major concern. In order to perform numerous operations within the wireless sensor networks, the basic requirement is power [5]. This information can be accessed by the different end users and can be utilized as per its requirement as shown in Fig. 1.



**Fig. 1:** Traditional structure of Wireless Sensor Network

Within numerous activities such as gathering or data, its processing and communication require energy. Even when the nodes are not performing any tasks, there is a need of huge amount of energy in the components of nodes when some dedicated operations are to be performed. Once, the energy of the nodes is consumed completely, the batteries of these nodes need to be changed or recharged. However, as the nodes are deployed in large areas where it's not possible for the humans to go, the replacement of these batteries is almost impossible. Thus, within the design and development of wireless sensor networks, this issue is very major. The energy efficient hardware and software protocols are proposed which are applied within these networks. Another challenging issue within the designing of WSN is the maintenance of security of these networks. Not only within the military applications but also in the huge buildings in order to provide alarms and monitor the surroundings, the WSNs are deployed [2]. There are number of attacks in WSN. Wormhole is a type of attack in which there is a formation of a tunnel by the malicious nodes and it is kept hidden from other legitimate nodes. This tunnel is used to send data packets from one malicious node to other. A malicious node in one area attracts the packets from its area and transmits them to the malicious node of other area [3]. There are various ways like in-band and out of band ways for the creation of a tunnel. This kind of attack can put a very huge effect on the procedure of routing and localization as there is no need to make any changes in other genuine networks to trigger this attack. Blackhole is again a very dangerous kind of attack as in this attack re-programming in different set of nodes can be done by the attacker. This may lead to the blockage of packets or the attacker can do anything else with the captured packets like generating false messages but does not forward them to the location to gather aggregate information in WSN. Sybil attack is an attack in which a malicious node can reshape itself like other different nodes [4]. Multipath routing distributed systems are very prone to this attack as they have no centralized entity which can be used to verify the identity of each node. With the advent in the

technology, wireless sensor networks emerged as growing technology in many applications such as weather, military aim tracking, and patient monitoring. Hence, protection is necessary for such types of sensor network from prohibited attackers. It is necessary for the sensor networks to have some security measures to mitigate the effects of the attacks [5].

## **II. Literature Review**

**A. Alsirhani, S. Sampalli, et.al (2019)** analyzed DDoS attack by hybrid the classification algorithms. In this paper, dynamic fuzzy approach is used to detect DDoS attack [6]. This system can be effectively used for detect different types of DDoS patterns. It can be profitably used for distributed environment, also impact on delay on fuzzy system. The major cause of this kind of the attacks is causing of large amount of data known as flooding of data.

**Shivam Dhuria and Monika Sachdeva (2018)** proposed two techniques in this paper amongst which the majority of attacks occurring within WSN are prevented through light-weight two-way authentication method. The DDoS attacks are identified and prevented from WSN with the help of another technique which is traffic analysis that is based on data filtering method. Various parameters which include throughput, delay, packet loss, energy consumption and PDR are verified through the Network Simulator 2 (NS2) [7]. Majority of the DDoS attacks are identified and prevented on the basis of authentication and data filtering technique. This evaluation shows that the proposed technique is very simple and at each node it has been deployed. The DDoS attacks cause whole drainage of battery source which can be prevented with the help of small computations of tracking the data rates from fellow nodes.

**Surendra Nagar, Shyam Singh Rajput, et.al (2017)** proposed routing protocol to provide security to wireless sensor network, to prevent the DDoS attack from the network. With the help of this proposed protocol infectious nodes within the network is scanned and scanned node is blocked to prevent further activities in the network. Intrusion prevention scheme has been utilized by the author to protect the network in which the specific node of the network acts as IPS node [10]. Within the region of the network, these nodes operate in the different radio frequencies and regularly scan its neighbors. When a malicious node is identified by the IPS node that involved in passing messages to nodes other than UDP and TCP messages, this malicious node is blocked by the IPS node for further sending empty messages. These empty messages are transferred in order to consume the resources and extract the useful information from the packets hence IPS node sends messages to all the sender nodes to change their routes. NS 2.35 has been utilized in this paper for the simulation process. On the basis of obtained results, it is concluded that proposed method give feasible results to protect the network against DDoS attack as compared to other methods.

**Raksha Upadhyay, Salman Khan, et.al, (2015)**, presented the wireless sensor network which has the capability of sensing and processing obtained information. There are different components in WSN such as battery, microprocessor, storage media and transducer used by sensor nodes. For different applications, it is considered as

the simple and effective method. Due to open nature of the WSN it is effective to minimize various security threats. Due to the presence of the different security threats, they malign the present information or sensor node data. The network is leads to infectious due to the drainage of resource capability which is the main objective of DDOS attack. The network congestion is increased and lifetime of the network and node is degraded due to processing of meaningless messages in huge quantity. The battery life of the battery is directly degraded the life of node as network lifetime is directly dependent on the capacity of battery. In this paper [9] authors proposed that minimizes the effects of the DDOS attack and overcome the issues of battery drainage. Qualnet 5.0 simulator was utilized in this paper in order to determine the performance of the novel technique for AODV and DSR routing protocols in WSN.

**Taranpreet Kaur, Dr. Krishan Kumar Saluji, et.al, (2016)**, have analyze that large number of sensor nodes are present in the wireless sensor networks which has low capabilities of collecting all the required sensitive data. In this network, security is the major concern due to advent in the technology. Various types of attacks are resided in this network such as DDoS attacks [8]. Present malicious node in the network is adopted by many attacks such as flooding attack, black hole attack and wormhole attack so that they can lead disturbance in the functionality of the network. The risk increased more, when it is utilized in the field of military and industrial applications. These are unable to mitigate low energy consumption and false alarm problem.

**William Hurst, Nathan Shone, et.al (2015)** discussed the effects created by the DDoS attack that weakens the server, network or service by flooding data traffic externally by sending communication request. Major impacts are created by the DDoS attack in the network such as infrastructure outage and various impacts on the infrastructure of the network that is yet too identified. The main objective of this paper is to determine the effects of above mentioned attack and proposed approach that determine cyber-attack impacts within the network [11]. Data is represented for run-time and scenario based on attack due to the simulation of a critical infrastructure network. It also demonstrated a technique that accesses the disruptions on integrated critical infrastructure network with the help of obtained dataset. In increasing cyber threat issues can be minimized for which it is required to determine the occurrence of failures in an interconnected network. when the cascading failure occurs in the network it is required to have appropriate recovery plan in order to increase the level of flexibility that plays as essential role.

### **III. Methodology**

The network is initialized in which certain numbers of sensor nodes are deployed. The sensor network is deployed in an environment randomly and sensor network can sense the environmental conditions. There is no need to configure those nodes they can configure themselves according to their environmental conditions. Those sensor nodes can sense the data and collects that data and then send that data to the base station where further processing is done. The whole network is divided into four zones or clusters. Grid topology is used for simulate this. The sensors can send either data packets or control packets which can be checked by the watch dog technique. Those nodes which are

sending the data packets called slaves and those are the legitimate nodes. The sensor nodes which are sending the control packets in the network are detected as malicious nodes from the network. The timer is set which can check the data rate which is defined with the variable name “data” that how much data is transmitted in given amount of time. The total byte of data is defined by the function called size. The node number and their IP address are defined which we prevent from the spoofing. The timer is returned which defines that this number of data is transmitted by particular node in the given amount of time. This technique is applied under the simulated environment to detect malicious nodes from the network which are responsible to trigger DDoS attack.

### **Algorithm to prevent DDoS attack in the network**

We implement an algorithm that detects and prevents the DDoS attack in the network by choosing a node called the key server node which randomly checks the data rate of each node if the node sends the data above the threshold that node will be detected as the malicious node and the legitimate sender alter its path to send the data that it can reach to the destination.

Input: Sensor nodes

Output: Detected malicious nodes

data = represents data rate that how much data is transmitted in given amount of time.

size = represents total byte of data

1. Deploy wireless sensor network with finite number of sensor nodes
2. Define key server in the network and each node register with the key server with their data rate
3. If (Throughput reduces to threshold value)  
Check node which is sending data above threshold value  
If (Node send data with high data rate == true)  
Check traffic type of node  
if (traffic == data traffic)  
Define node = slave node  
Apply monitor mode technique and check with node is sending control packets  
Node which is sending control packets to slave node is detected as malicious nodes
4. Else
5. Communication continue in the network
6. End

This algorithm is used to detect as well as prevent the DDoS attack in the network. This algorithm detects all the unkind nodes from the flat cluster grid network which is creating the DDoS attack in the network.

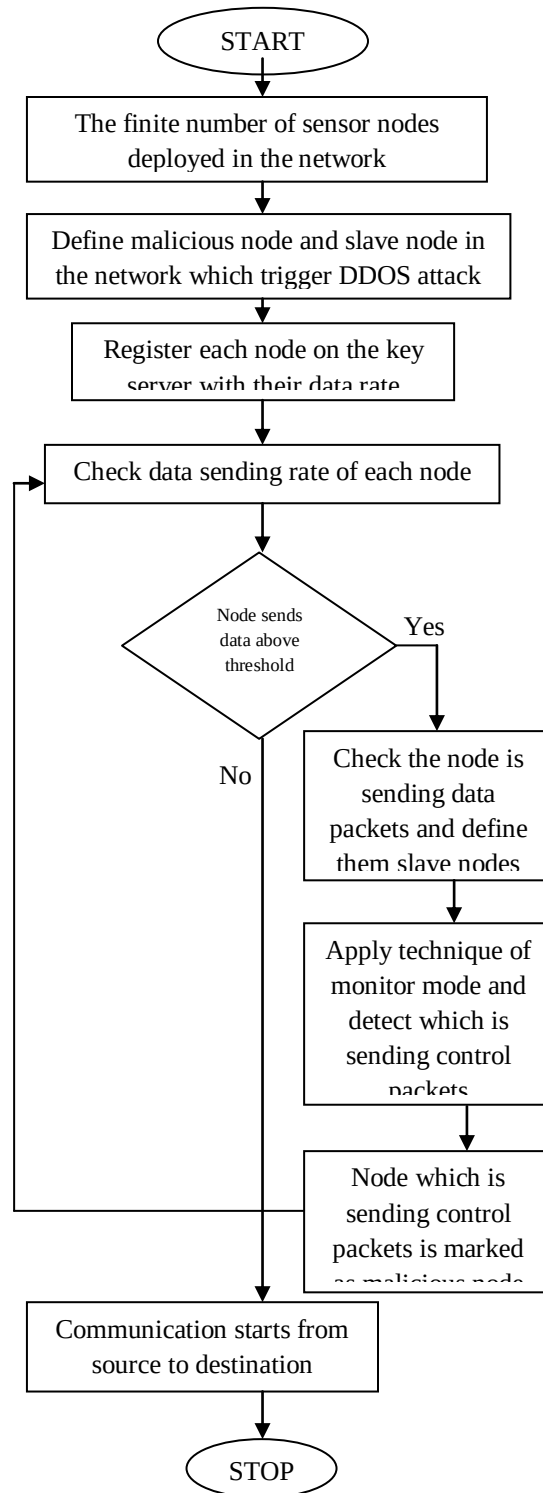


Fig 2: Proposed Flowchart

#### IV. Simulation and Result Analysis

We have implemented AODV protocol with detection and prevention of DDOS attack using the simulator ns 2.35

|                          |             |
|--------------------------|-------------|
| Simulation Tool          | NS 2.35     |
| Time for simulation      | 100s        |
| Data communication Range | 100 m       |
| nodes in the Network     | 10 to 100   |
| Size of Area             | 1500 x 1150 |
| Protocol                 | AODV        |
| Application Traffic      | CBR         |
| Size of packet           | 512 bytes   |

Here we used many performance parameters like packet drop, throughput, and energy consumption to estimate the performance of the Novel algorithm with the standard routing AODV protocol.

First, we deployed the 100 sensor nodes to simulate the behavior of the sensor nodes on different parameters as said. Then we launch the DDoS attack on the same network to check the performance of the network, the performance parameters of the system degraded due to the cruel nodes present into the network. The communication starts in the network and nodes which are least reliable is not selected for the communication. Those nodes which are detected as the malicious nodes are the least reliable nodes and are not used for the communication. At the time of network deployment the key server is chosen which registers all the nodes and when the attack occurs the key server sends the message to the target location which is used to gather the information and from that location, it sends to all the nodes with the key of those nodes which are not reliable for the communication.

In our proposed model a technique has been based on the threshold. In this key server node is chosen that registers each node of the network and checks the data rate of each node. When it detects the malicious node in the network it blocked the malicious nodes in the network and sends the message to all the legitimate nodes which was requesting the target node for routing their data.

The proposed approach is implemented in NS2 and the results are analyzed by making comparisons amongst proposed and existing approaches in terms of packet loss, throughput and energy consumption in the networks.

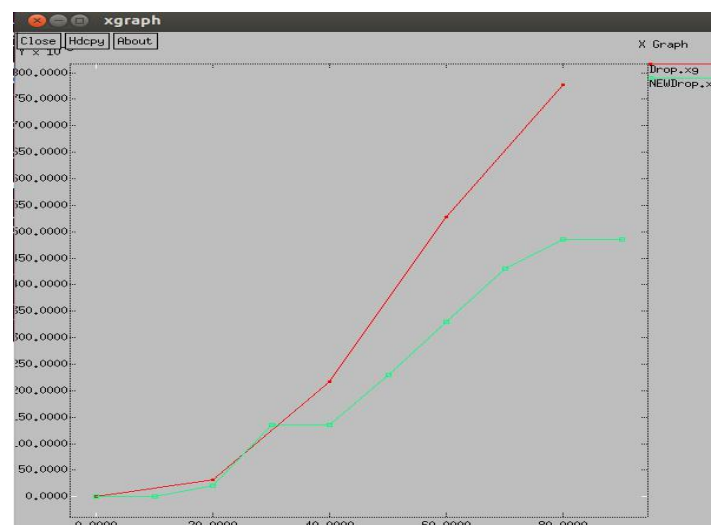
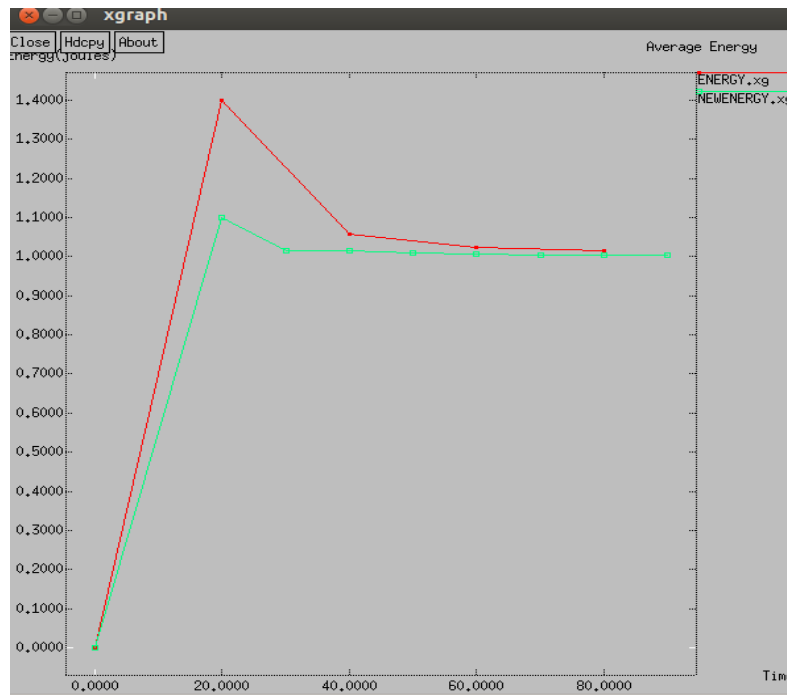


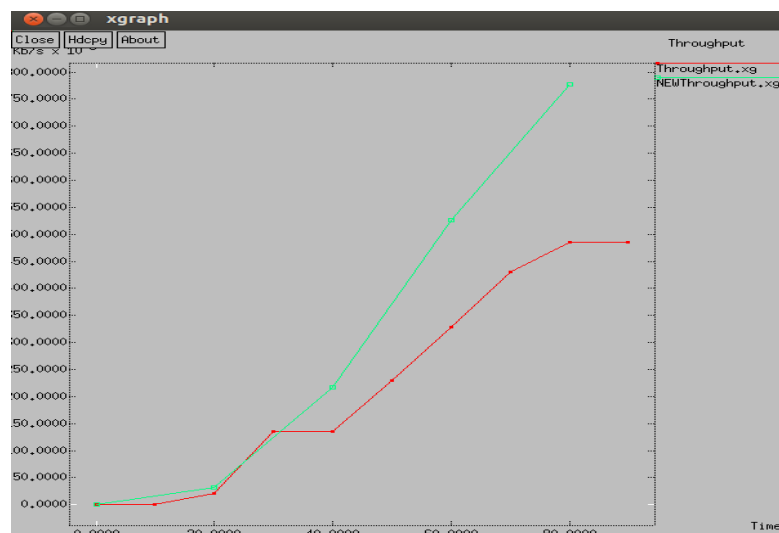
Fig 3: Packet loss Graph

As shown in Fig 3, the technique of neural networks is applied in this research work. The proposed improvement leads detection of malicious nodes due to which packet loss get reduced in the network.



**Fig 4: comparison of Energy Consumption in existing and proposed Novel technique**

As shown in Fig4, the size of sensor nodes is very tiny and adjusts in the network as per access points. Less energy consumption will increase the existence of the network. As per Fig, energy consumption in proposed system is less than the existing system, which increases the life time of the network.

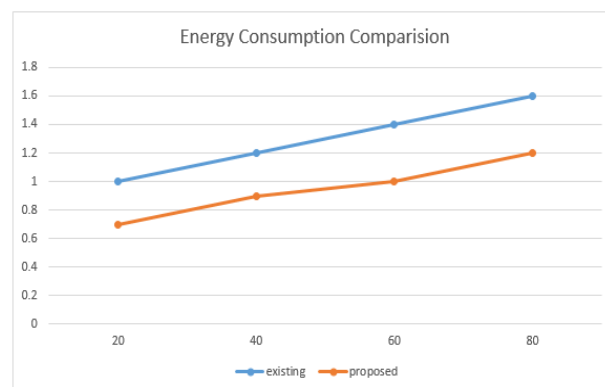


**Fig 5: Throughput Comparison**

As shown in fig 5, the proposed improvement leads detection of malicious nodes due to which packet loss get reduced in the network. Figure shows the condition of the network at the time of the attack and when the attack is prevented. The red line shows the packet loss at the time of attack and the other one show the packet loss at the time when the attack is being prevented. It is observed that when attack is not happen in the network, then throughput is improved at stable rate.

### Comparison Graph

The proposed technique when compared with the existing technique proves to be much reliable and efficient. We compared existing and proposed technique with different parameters like throughput, energy and packet drop.



**Fig 6: Energy Consumption Comparison**

As shown in Fig 6, the energy utilization of proposed and existing technique is compared at different intervals. It is being analysed that energy utilization of proposed system is reduced then the existing technique at those intervals.

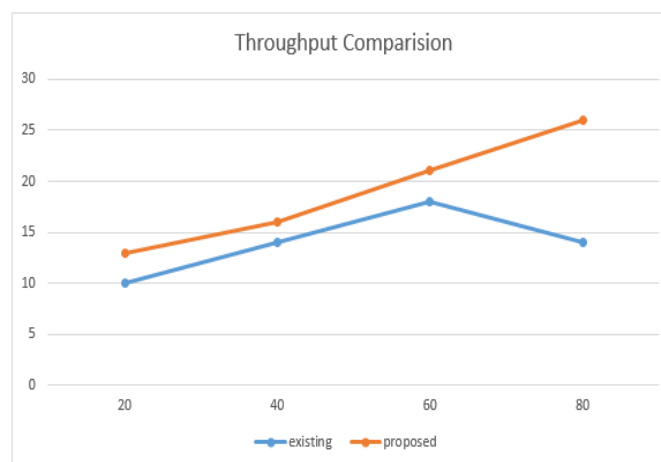


Fig. 7: Comparison of Throughput for existing and proposed system

As shown in Fig. 7, the throughput increases as compared to existing technique at different intervals of time. It is analysed that throughput in novel technique is more than existing technique at those intervals.

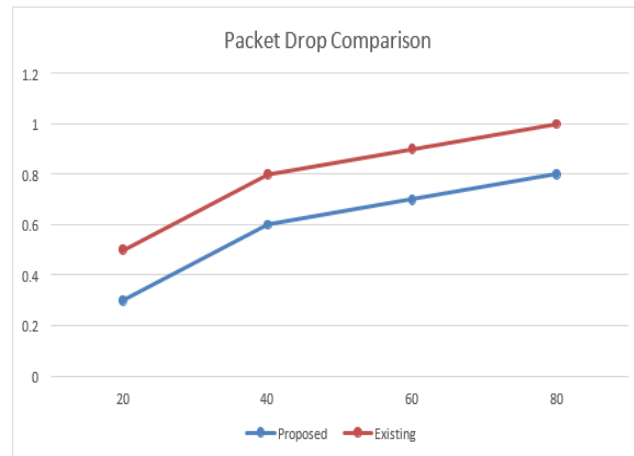


Fig. 8: Packet Drop Comparison

As shown in Fig. 8, the packet drop of proposed and existing technique is compared at different times. In the proposed technique, the packet drop is less due to isolation of DDoS attack in the network

## Conclusion

DDoS attack can disturb communications connection at national level as well as can cause infrastructure issue at country level. Identifying such problems by the attacks is considered as the major concern. This proposed algorithm obtained the useful results and give better results in terms of its scalability to large networks and numbers of attacking nodes. Present adversaries sometimes compromise with the sensors and using redundant messages or fake messages it launch the DoS attack within the network. To detect the malicious nodes from the network, threshold value is. The novel technique enhance the life time, throughput and minimize the network delay. The proposed technique can be further compared with the other technique like slant, TTL etc. to detect the malicious nodes and increase the reliability of the network.

## References

- [1] M.H. Anisi, A.H. Abdullah, S.A. Razak, "Energy-Efficient Data Collection in Wireless Sensor Networks", *Wireless Sensor Networks*, vol. 3, pp. 329-333, 2011.
- [2] P. Mohanty, S. Panigrahi, N. Sarma, and S.S. Satapathy, "Security Issues In Wireless Sensor Network Data Gathering Protocols: A Survey", *Journal of Theoretical and Applied Information Technology*, vol. 13, pp. 14-27, 2010.

- [3] M.K. Jain, "Wireless Sensor Networks: Security Issues and Challenges", International Journal of Computer and Information Technology, vol. 2, pp. 62-67, 2011.
- [4] A.K. Pathan, "Security in Wireless Sensor Networks: Issues and Challenges", Proc. 8th International Conf. Advanced Communication Technology, vol. 2, pp. 1043-1048, 2006.
- [5] Patel MM, Aggarwal A, "Two phase wormhole detection approach for dynamic wireless sensor networks in Wireless Communications Signal Processing and Networking (WiSPNET)", 2016 International Conference on IEEE, vol. 5, pp. 2109-2112, 2016.
- [6] A. Alsirhani, S. Sampalli and P. Bodorik, "DDoS Detection System: Using a Set of Classification Algorithms Controlled by Fuzzy Logic System in Apache Spark," in IEEE Transactions on Network and Service Management, vol. 16, no. 3, pp. 936-949, Sept. 2019.
- [7] ShivamDhuria and Monika Sachdeva, "Detection and Prevention of DDoS Attacks in Wireless Sensor Networks" Springer Nature Singapore Pte Ltd. 2018.
- [8] Taranpreet Kaur, Dr. Krishan Kumar Saluja, DrAnuj Kumar Sharma, "DDOS Attack in WSN: A Survey", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2016), vol. 4, pp. 131-140, 2016.
- [9] RakshaUpadhyay, Salman Khan, HarendraTripathi, Uma Rathore Bhatt, "Detection and Prevention of DDOS Attack in WSN for AODV and DSR using Battery Drain", 2015 Intl. Conference on Computing and Network Communications (CoCoNet'15), vol. 3, pp. 446-451, 2015.
- [10] Surendra Nagar, Shyam Singh Rajput ,Avadesh Kumar Gupta, Munesh Chandra Trivedi, "Secure Routing Against DDoS Attack in Wireless Sensor Network", 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT 2017).
- [11] William Hurst, Nathan Shone, Quentin Monnet, "Predicting the Effects of DDoS Attacks on a Network of Critical Infrastructures", 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications.
- [12] InzimamUl Hassan and A. Kaur, "Prevention and detection of DDoS attack on WSN," pp. 245–249, 2018.
- [13] InzimamUl Hassan and A. Kaur, "Literature Review on Prevention and Detection of DDoS Attack," pp. 353-359, 2018.
- [14] InzimamUl Hassan and A.Kaur, "Literature Review of Prevention and Detection of DDoS Attack on WSN," Volume XII, Issue IV, April 18, pp. 260-266, 2018.