An Enhanced Decision System for Sybil Attack Detection in WSN

Pardeep Kaur,
M.tech (ECE), Student
Punjabi University, Patiala
Punjab, India.
pairikaur@gmail.com

Dr. Harjinder Singh
M.tech (ECE), Assistant Professor,
Punjabi University, Patiala
Punjab, India.
hrjindr@gmail.com

***Abstract*— the wireless sensor network (WSN) is worldwide accepted technology to perform sensor based wireless communication. Thus, there is a wide range of applications that implements the WSN for transmitting the data to the BS. The sensor nodes are vulnerable to the malicious attacks. Thus, this study provides a novel approach to detect the malicious nodes in the network against Sybil attack. The approach implements the trust model to evaluate if the node is attacker or not. The trust model works on the basis of response time of a node, distance of node with adjacent nodes and packet drop rate of the nodes.**

The performance of the proposed security mechanism is analyzed on different levels i.e. at the level of cluster members (CM), at the level of cluster head (CH), and at the level of base station (BS). The simulation outcomes represents that the proposed work outperform the traditional ETS, LDT and GTMS in terms of detection accuracy, energy consumption by the nodes and communication overhead.

Keywords—Wireless Sensor Network, network security, Sybil attack, trust evaluation, fuzzy inference system, detection accuracy, overhead.

I. INTRODUCTION

Wireless Sensor Network (WSN) is utilized to physically monitor the surroundings and to access remote places. WSN is highly recommended in military activities such as reconnaissance and target acquisition [1]. It is also responsible for preventing forest fire and other geophysical activities like volcano activity. Also, it is useful in health data monitoring and civil engineering [2]. There are zero limitations of WSN and its users, are continually increasing day by day. The image in figure 1 represents the topology or architecture of WSN. Following are some major components as per the architecture of the WSN [3].

Sensor Nodes/Field Devices: the sensor node is further comprised of several parts i.e. radio transceiver, transceiver with either inner or outer antenna, a microcontroller to control the overall processing [4], an electronic circuit for supporting the interface among sensor and energy sources, gateway or access points to establish the communication between host and sensor nodes in the network, network manager for configuring the network, communication scheduling, managing the routing tables etc and security manager generating, storing and managing the security keys [5].

The BS plays the major role in the network. The sensor node which plays as the base station is occupied with high processing energy and communication resources [6]. The BS is a kind of gateway between sensor nodes and end user. Along with the BS, the routers are also vital part of the network and routers are specifically designed to evaluate and distribute the routing information [7].

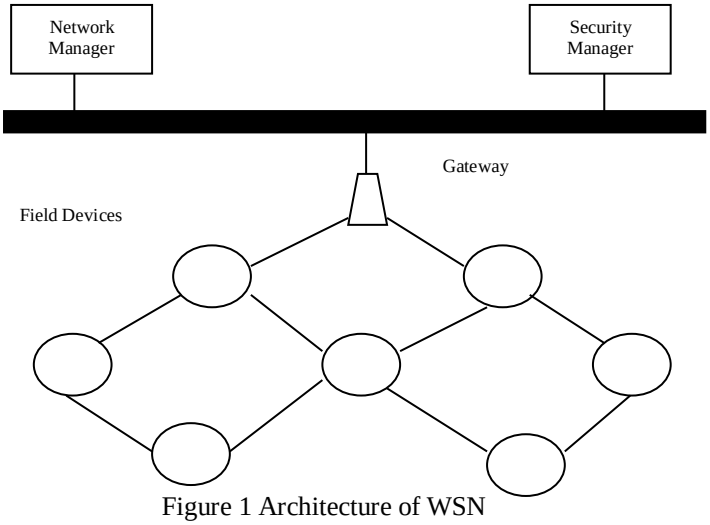

Figure 1 Architecture of WSN

In WSN, the data/information is transferred or broadcasted in an fallacious manner. This process makes it complicated to secure the network and information travelled on it [8-9]. Therefore, it is necessary that good security policies are used and implemented in protecting wireless sensor networks. Cryptography and encryption are some of the prominent methods that can be used for securing the information and network from malicious attacks [10]. However, basic network security measures should not be overlooked and up to date measures should be implemented to better the security posture of wireless sensor networks [11].

The threats that wireless sensor networks face is similar to that of wired networks, but sometimes due to the fact the wireless networks broadcast and can be accessed from a slightly distant place as well makes them more vulnerable. Hence, robust security measures must be implemented on them [12].

The wireless networks are more prone to link attacks such as passive link attacks like eavesdropping and active link attacks like active interfering [13]. Whereas in case of wired networks, the network is prevented from attacks by using firewalls and gateways but in case of wireless network the attacks can enter to the network from all directions and can aim at any node. These attacks can reveal of confidential information [14]. This can violates the rules of security hence it is mandatory that each and every node of the network should be capable to beat these kind of adversaries whether directly or indirectly [15]. The sensor nodes in the network that are autonomous in nature are more prone to the attacks and unintended user's access. Therefore, the hacker or intruder can attack the nodes either from inside or from outside of the network [16]. Since it is quite easy for the intruders to target such nodes and it is also hard to locate such attacks in the network. Any kind of security approach with the placement of the nodes is not approved to be sufficient enough in order to prevent the network from any kind of malicious activity [17]. If the user of the network wants the high availability of the network, a dispersed network without central entity must be employed. The central server in the network sometimes can become a strong reason behind the attacks in the network.

II. PROBLEM STATEMENT

The wireless ad hoc sensor networks are highly prone to the attacks. The mobility of the nodes and dynamic architecture of the network makes it highly susceptible to the attacks such as attacks to data plane and other security issues. A large number of research has been conducted in this filed till now in order to detect the malicious nodes from the network. Similarly, in traditional work [1], the author focused on detecting the nodes affected with Sybil attacks. The attack detection was done on the basis of the energy of the nodes. The traditional technique was a multi level approach to detect the Sybil attack from clustered network. In multilevel approach, in first level, the CM (Clustered Members) transmits the data to the CH (Cluster Head). Along with this data, the CM also sends its ID and amount of residual energy. On other side, the CH maintains a table that comprises of the information related to the CM. On the basis of the facts of this table, the amount of residual energy is compared to a threshold value. After comparing the energy the node is declared as a malicious node if the residual energy is found to be lower than the threshold. On second level, the malicious node was detected from CH to sink. Thus, after concluding the work of traditional energy trust system, it is observed that the only energy is not a major factor that can play a major role to detect the malicious node from the network. As the energy of the node can be degraded due to various other factors such as heavy data load, large distance to cover for transmitting the data packets.

III. PROPOSED WORK

After having a review to the traditional work, it is evaluated that the author considered the energy as the major factor for evaluating the malicious nodes from the network. As it was not the sufficient enough factor. Along with this the work was done in two different levels that makes it little complex. Thus to improve and overcome the issues of traditional work, this study enhances the list of factors for detecting the malicious nodes in the network. The novel list of factors of proposed work is as follows:

1. Energy
2. Packet Delivery Ratio
3. Delay

Other than this, the proposed work introduces the enhanced CH selection approach to eliminate the complexity of traditional work that was happened due to the multi level security detection approach i.e. from CM to CH and then from CH to Sink node. In order to remove this backlog, the proposed work developed an advanced CH selection approach at initial stage of CH selection process in the network. As per the advancements of the proposed work, the initial CH selection is done on by using the Fuzzy Inference System. The input factors for FIS are the parameters that pretend the performance of a node. The considered factors for CH selection or input to the proposed FIS in proposed work are as follows:

1. Distance
2. Response Time
3. Packet Drop Rate

Following is the methodology of the proposed work.

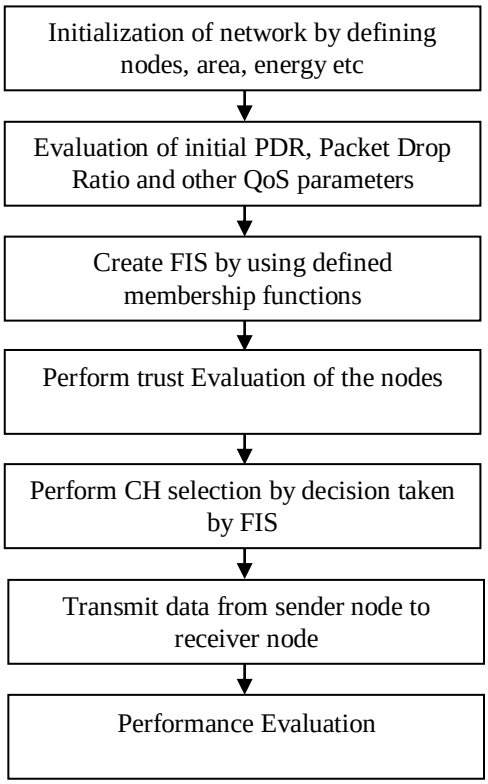

Figure 2 Framework of proposed protocol.

Step 1. The first step is to initialize the network by defining the relevant initial parameters such as area covered

by the network, number of nodes in the network, initial energy of the nodes, etc.

Step 2. After defining the initial parameters, the next step is to set up the network as per the defined parameters.

Step 3. In this step, the evaluation of PDR, Packet Drop Ratio and other QoS parameter is done.

Step 4. In this step, the fuzzy inference system is initialized on the basis of the input membership functions i.e. distance, response time and packet drop rate.

Step 5. After initializing the fuzzy, the evaluation is done on the basis of the defined rule sets and it is observed that whether the node is attacker node or non-attacker node. If the node is an attacker node then it is eliminated from the communication process. This phase is known as trust evaluation of the nodes in the network.

Step 6. Then on the basis of the evaluated trust, the node with the highest trust value is considered as the candidate for the CH. If the count of trusted nodes is higher, the CH selection is done randomly.

Step 7. The CH selection is the major step before initiating the communication in the network. As the cluster member node can only communicate to the BS with the help of CH. Now, in this step the network communication is established.

Step 8. At last, the data packets are received at the base station and the performance of the network is evaluated.

IV. Simulation Results

In this study a novel approach is developed to detect the malicious nodes in the sensor network. The malicious nodes are detected and eliminated from the process of data transmission in order to prevent the network from unintended and unauthorized activities. The network setup of proposed work is as follows:

Table 1: Network Setup Parameters

Parameters	Values
Simulation Time	1200s
Area of Network	500m*500m
Sink Location	250m*250m
Career Frequency	2.4 GHz
T_x (Maximum Transmission Power)	1.1 mW

In proposed work, work is done for detecting the Sybil attack in the network. The malicious nodes are detected on the basis of various parameters such as distance, response time and packet drop rate. The distance refers to the difference from specific node to adjacent nodes within a cluster, the response time refers to the time taken by the node to generate the feedback or response to an event in the network and the packet drop rate defines the rate corresponding to the missed packets or dropped packets during the data transmission by a node in the network. Thus the node with the least distance, least PDR and least response time will have the highest trust value. For evaluating the trust value of the nodes, the fuzzy inference system is applied in proposed work. The following the proposed model of fuzzy inference system (FIS). In this figure, it has been represented that three of the input membership functions are passed to the FIS system and then 27 rules are applied to the input membership function and "mamdani" FIS is used for evaluation. On the basis of defined rule set and evaluation, the trust of the nodes is measured and represented as an output.

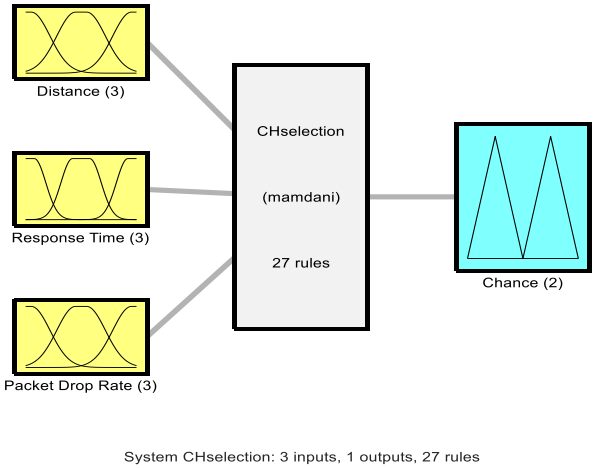

Figure 3 Proposed FIS for node trust evaluation

The performance of the proposed work is evaluated in the terms of the detection accuracy, energy consumption and communication overhead. The detection accuracy defines the accuracy rate of the proposed work for detecting the malicious or attacker nodes in the network, the energy consumption is used to evaluate the amount of energy consumed by the nodes and the overhead is used to define the performance of the proposed work in terms of count of the data packets that are transmitted by the nodes in the network. This section of the study discusses the performance analysis of the proposed work in terms of defined parameters.

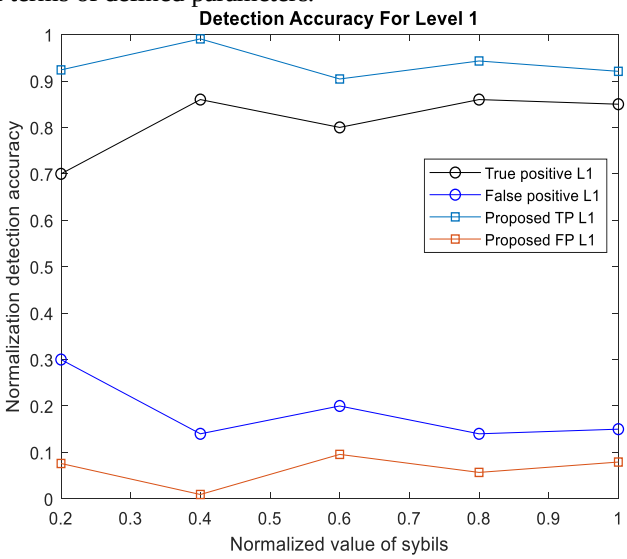

Figure 4 Comparison Analysis of detection accuracy for "Level 1"

The graph in figure 4 represents the comparison of detection accuracy of the proposed work and traditional work. The evaluation of detection accuracy is done in terms of false positive and true positive. The false positive refers to the incorrect detection and true positive refers to the correct detection. The detection accuracy is evaluated on the basis of the levels. The simulation is done on the basis on two different levels i.e. L1 and L2. The L1 defines the communication from cluster members to cluster heads and L2 defines the data transmission from cluster heads to sink location. The detection accuracy is measured on the basis of the normalized value of Sybil attacks and it ranges within 0.2 and 1 with the interval of 0.1. The graph explains that the proposed work has the higher correct detection rate i.e. more than 0.9 whereas the incorrect detection rate of proposed work is quite lower i.e. below 0.1. The respective observed values are shown in table 2.

Table 2 Analysis of Detection Accuracy for Level 1

True Positive L1	False Positive L1	Proposed TP L1	Proposed FP L1
0.7000	0.3000	0.9239	0.0761
0.8600	0.1400	0.9907	0.0093
0.8000	0.2000	0.9043	0.0957
0.8600	0.1400	0.9431	0.0569
0.8500	0.1500	0.9208	0.0792

Likewise, the graph in figure 5 explains the comparison of detection accuracy with level 2. The comparison is performed for the data transmission from CH to sink node

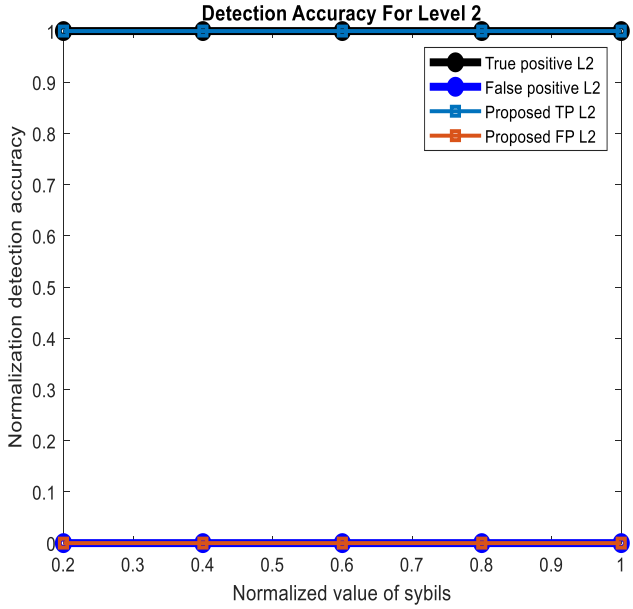

Figure 5 Comparison Analysis of detection accuracy for "Level 2"

The graph also proves that the correct detection by the proposed work is 1 exactly and the incorrect detections is 0. Now on the basis of the facts shown by figure 4 and 5, it is concluded that the proposed work is having the highest correct detection for level 1 and level 2 as well in comparison to the traditional work. The table 3shows the detection accuracy for level 1 and level 2 for true positive and false positive.

Table 3 Analysis of Detection Accuracy for Level 2

True Positive L2	False Positive L2	Proposed TP L2	Proposed FP L2
1	0	1	0
1	0	1	0
1	0	1	0
1	0	1	0
1	0	1	0

The graph in figure 6 defines the comparison analysis of true positive for level 1, level 2 and proposed work for level 1, level 2. The comparison analysis shows that the true positive of proposed work for level 1 and level 2 is higher than the true positive level 1 and true positive level 2. The graph elucidates that the proposed work has the constant value of true positive for L1 and L2 during the variation in the normalized Sybil attack. The increment in proposed work for correct detection is achieved due to the prior evaluation of trust value of the nodes. Hence the pre evaluation of trust value results to the reduction in the existence of malicious nodes in the process of communication.

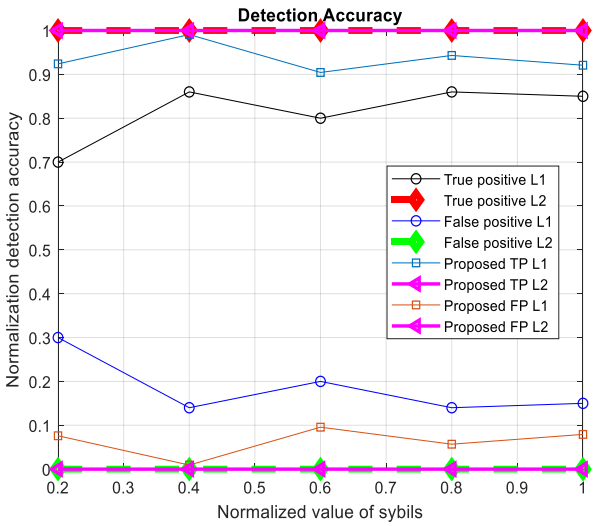

Figure 6 Comparison Analysis of detection accuracy for "Level 1" and "Level 2"

The energy consumption is the major constraint in every kind of sensor network. The graph in figure defines the comparison of traditional work and proposed work with respect to the energy consumption. The energy consumption is evaluated for

the different levels in the network. As the energy consumed in proposed work at the level of Cluster Member (P-CM), at level of Cluster Heads (P-CH) and at the level of Base Station (P-BS). The energy consumption is measured on the basis of the time interval i.e. from 2 minutes to 20 minutes. The graph explains that the energy consumption of the proposed work is lower than the energy consumed by the traditional work with respect to all levels i.e. CM, CH and BS. The amount of energy consumption is increases as the time interval is increasing in the network for processing. The initial energy consumption by the proposed work is 4 joule approximately and the highest energy consumed by the proposed work is 40 joule at the interval of 20 minutes. Whereas the initial energy consumption of the traditional work is 9 joule approximately and the highest amount of energy consumed by the traditional work is 71 joule at the time interval of 20 minutes. Thus it is concluded that the energy consumption of the proposed work is much better and efficient than the energy consumed by the traditional work. Similarly, the facts shown in table 4 are observed from graph below.

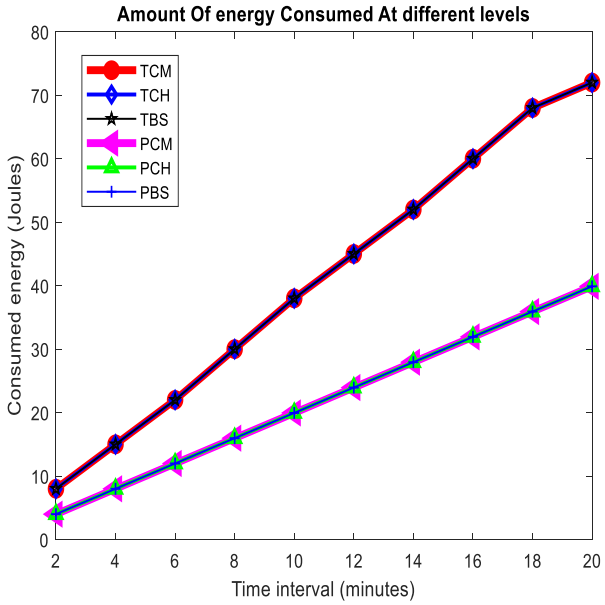

Figure 7 Comparison analysis of Energy consumption at level of Cm, CH and BS respectively

Table 4 Analysis of Energy Consumption by CM, CH and BS for traditional and proposed work

TCM (Traditional-Cluster Members)	TCH (Traditional-Cluster Heads)	TBS (Traditional-Base Station)	PCM(Proposed-CM)	PCH (Proposed-CH)	PBS (Proposed-BS)
8.0000	8.0000	8.0000	4.7978	4.7978	4.7978
15.0000	15.0000	15.0000	9.5921	9.5921	9.5921
22.0000	22.0000	22.0000	14.3814	14.381	14.3814
30.0000	30.0000	30.0000	19.1635	19.163	19.163
38.0000	38.0000	38.0000	23.9372	23.937	23.937
45.0000	45.0000	45.0000	28.7351	28.735	28.735
52.0000	52.0000	52.0000	38.3186	38.3186	38.3186
68.0000	68.0000	68.0000	43.1008	43.1008	43.1008
72.0000	72.0000	72.0000	47.8745	47.8745	47.8745

The communication overhead of proposed and traditional work is analyzed in graph given in figure 8. The communication overhead is evaluated by using the following formulation:

$$C_{max} = m * (n-1) \ldots\ldots (1)$$

For evaluating the communication overhead, the network is assumed to have "m" number cluster heads and "n" number of nodes as shown in above equation.

The graph shows that the communication overhead of GTMS [16] is higher initially but it falls suddenly when the number of clusters increases. Similarly, the communication overhead of LDT [17], ETS [1] and proposed work is lower and remains constant even with the increment in number of clusters in the network. The network with the lowest communication overhead is considered as an idle network. The obtained observations from graph below are represented in table 5.

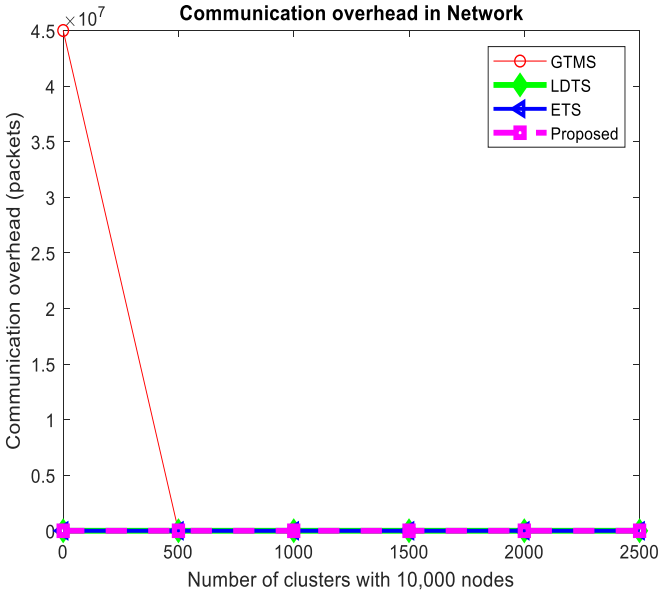

Figure 8 Comparison analysis of Communication Overhead

Table 5 Analysis of Communication Overhead

GTMS	LDTS	ETS	Proposed
45000000	0.3	0	0
0.45	0.2	0	0
0.45	0.3	0	0
0.5	0.5	0	0
0.7	0.6	0	0
1.25	1.2	0	0

V. CONCLUSION AND FUTURE SCOPE

The study implements the novel approach for detecting the malicious nodes in the network in order to prevent the network from Sybil attack. For this purpose, the trust evaluation is done by applying the FIS on the basis of the distance between node to node within the respective cluster, response time of the nodes and packet drop rate of the nodes. These factors are considered as the major ones because these factors play a vital role to detect whether the node is trustworthy or not. After detecting the trust, the CH is selected randomly from the nodes that fall under the category of non-attacker nodes. And in this way, the communication is performed by using the selected CH. The simulation outcomes prove that proposed work outperforms the traditional work in terms of detection accuracy, energy consumption and communication overhead.

The results prove that proposed model is quite efficient to detect the attacker nodes in the network, but still more amendments can be done in this work to enhance the detection accuracy. Along with this, in future the idea of data re-routing can also be considered to handle the scenarios if the attacker node enters to the communication process. Thus in this way the packet drop rate of the network will decreases and directly enhances the overall performance of the sensor network.

REFERENCES

[1]. Noor Alsaedia, Fazirulhisyam Hashima, A. Salia, Fakhrul Z. Rokhani, "Detecting Sybil Attacks in Clustered Wireless Sensor Networks Based on Energy Trust System (ETS)", Elsevier, vol 110, pp 75-825, 2015

[2]. Amol Vasudevaa, Manu Soodb, "Survey on sybil attack defense mechanisms in wireless ad hoc networks", Elsevier, vol 120, pp 78-118, 2018

[3]. Mian Ahmad Janab, Priyadarsi Nandaa, Xiang jian, Hea Ren PingLiu, "A Sybil attack detection scheme for a forest wildfire monitoring application", Elsevier, vol 80, pp 613-626, 2018

[4]. Noor Al saedi, Fazir ul hisyam, Hashim A. Sali, Fakhrul Z. Rokhani, "Detecting sybil attacks in clustered wireless sensor networks based on energy trust system (ETS)", Elsevier, vol 110, pp 75-82, 2017

[5]. Panagiotis Sarigiannidisa, Eirini Karapistolib, Anastasios A. Economides, "Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information", Elsevier, vol 42, issue 21, pp 7560-7572, 2015

[6]. Mojtaba Jamshidia, Ehsan Zangenehb, Mehdi Esnaasharic, Mohammad Reza Meybodid, "A lightweight algorithm for detecting mobile Sybil nodes in mobile wireless sensor networks", Elsevier, vol 64, pp 220-232, 2017

[7]. Meenakshi Tripathi, M.S. Gaur V. Laxmi, "Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN", Elsevier, vol 19, pp 1101-1107, 2013.

[8]. Parmar Amisha, V. B. Vaghela, "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV Protocol", Elsevier, vol 79, pp 700-707, 2016

[9]. David Airehroura Jairo, A. Gutierrez, Sayan Kumar Rayc, "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things", Elsevier, 2018

[10]. Samir Athmani, Azeddine Bilami, Djallel Eddine Boubiche, "EDAK: An Efficient Dynamic Authentication and Key Management Mechanism for heterogeneous WSNs", Elsevier, 2017

[11]. Shehnaz T. Patel ; Nital H. Mistry, "A review: Sybil attack detection techniques in WSN", IEEE, 4th International Conference on Electronics and Communication Systems (ICECS), 2017.

[12]. Noor Alsaedi ; Fazirulhisyam Hashim ; A. Sali, "Energy trust system for detecting sybil attack in clustered wireless sensor networks", IEEE, IEEE 12th Malaysia International Conference on Communications (MICC), 2015.

[13]. T. G. Dhanalakshmi ; N. Bharathi ; M. Monisha,"Safety concerns of Sybil attack in WSN" ,IEEE, International Conference on Science Engineering and Management Research (ICSEMR)2014.

[14]. Shanshan Chen ; Geng Yang ; Shengshou Chen, "A Security Routing Mechanism Against Sybil Attack for Wireless Sensor Networks", IEEE, International Conference on Communications and Mobile Computing, 2010.

[15]. Shahrzad Golestani Najafabadi ; Hamid Reza Naji ; Ali Mahani, "Sybil attack Detection: Improving security of WSNs for smart power grid application", IEEE, Smart Grid Conference (SGC), 2013.

[16]. R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, Y.-J. Song, "Group-based trust management scheme for clustered wireless sensor networks", IEEE Transactions on Parallel and Distributed Systems, vol 20, issue 11, pp 1698–1712, 2009.

[17]. X Li, F.Zhou, J. Du, Ldts "A lightweight and dependable trust system 466 for clustered wireless sensor networks", IEEE Transactions on Information Forensics and Security, vol 8, issue 6, pp 924–935, 2013.